

BASES ESTÁNDAR DE CONCURSO PÚBLICO PARA LA CONTRATACIÓN DE SERVICIOS EN GENERAL

Aprobado mediante Directiva N° 001-2019-OSCE/CD



SUB DIRECCIÓN DE NORMATIVIDAD – DIRECCIÓN TÉCNICO NORMATIVA
ORGANISMO SUPERVISOR DE LAS CONTRATACIONES DEL ESTADO - OSCE




Elaboradas en enero de 2019
Modificadas en junio 2019, diciembre de 2019, julio 2020, julio y diciembre 2021, junio y octubre de 2022

**BASES ESTÁNDAR DE CONCURSO PÚBLICO PARA LA
CONTRATACIÓN DE SERVICIOS EN GENERAL**

CONCURSO PÚBLICO N° 02-2025-DIRECFIN-PNP

PRIMERA CONVOCATORIA

**CONTRATACIÓN DEL: SERVICIO DE TRANSMISIÓN PARA
LA RED PRIVADA DE LA PNP, EN LAS UNIDADES
POLICIALES A NIVEL NACIONAL; SERVICIO DE
SEGURIDAD GESTIONADA Y ACCESO A INTERNET**

DEBER DE COLABORACIÓN

La Entidad y todo proveedor que se someta a las presentes Bases, sea como participante, postor y/o contratista, deben conducir su actuación conforme a los principios previstos en la Ley de Contrataciones del Estado.

En este contexto, se encuentran obligados a prestar su colaboración al OSCE y a la Secretaría Técnica de la Comisión de Defensa de la Libre Competencia del INDECOP, en todo momento según corresponda a sus competencias, a fin de comunicar presuntos casos de fraude, colusión y corrupción por parte de los funcionarios y servidores de la Entidad, así como los proveedores y demás actores que participan en el proceso de contratación.

De igual forma, deben poner en conocimiento del OSCE y a la Secretaría Técnica de la Comisión de Defensa de la Libre Competencia del INDECOP los indicios de conductas anticompetitivas que se presenten durante el proceso de contratación, en los términos del Decreto Legislativo N° 1034, "Ley de Represión de Conductas Anticompetitivas", o norma que la sustituya, así como las demás normas de la materia.

La Entidad y todo proveedor que se someta a las presentes Bases, sea como participante, postor y/o contratista del proceso de contratación deben permitir al OSCE o a la Secretaría Técnica de la Comisión de Defensa de la Libre Competencia del INDECOP el acceso a la información referida a las contrataciones del Estado que sea requerida, prestar testimonio o absolución de posiciones que se requieran, entre otras formas de colaboración.



SECCIÓN GENERAL

DISPOSICIONES COMUNES DEL PROCEDIMIENTO DE SELECCIÓN

(ESTA SECCIÓN NO DEBE SER MODIFICADA EN NINGÚN EXTREMO, BAJO SANCIÓN DE NULIDAD)





CAPÍTULO I ETAPAS DEL PROCEDIMIENTO DE SELECCIÓN

1.1. REFERENCIAS

Cuando en el presente documento se mencione la palabra Ley, se entiende que se está haciendo referencia a la Ley N° 30225, Ley de Contrataciones del Estado, y cuando se mencione la palabra Reglamento, se entiende que se está haciendo referencia al Reglamento de la Ley de Contrataciones del Estado aprobado por Decreto Supremo N° 344-2018-EF.

Las referidas normas incluyen sus respectivas modificaciones, de ser el caso.

1.2. CONVOCATORIA

Se realiza a través de su publicación en el SEACE de conformidad con lo señalado en el artículo 54 del Reglamento, en la fecha señalada en el calendario del procedimiento de selección, debiendo adjuntar las bases y resumen ejecutivo.

1.3. REGISTRO DE PARTICIPANTES

El registro de participantes se realiza conforme al artículo 55 del Reglamento. En el caso de un consorcio, basta que se registre uno (1) de sus integrantes.

Importante

- *Para registrarse como participante en un procedimiento de selección convocado por las Entidades del Estado Peruano, es necesario que los proveedores cuenten con inscripción vigente y estar habilitados ante el Registro Nacional de Proveedores (RNP) que administra el Organismo Supervisor de las Contrataciones del Estado (OSCE). Para obtener mayor información, se puede ingresar a la siguiente dirección electrónica: www.rnp.gob.pe.*
- *Los proveedores que deseen registrar su participación deben ingresar al SEACE utilizando su Certificado SEACE (usuario y contraseña). Asimismo, deben observar las instrucciones señaladas en el documento de orientación "Guía para el registro de participantes electrónico" publicado en <https://www2.seace.gob.pe/>.*
- *En caso los proveedores no cuenten con inscripción vigente en el RNP y/o se encuentren inhabilitados o suspendidos para ser participantes, postores y/o contratistas, el SEACE restringirá su registro, quedando a potestad de estos intentar nuevamente registrar su participación en el procedimiento de selección en cualquier otro momento, dentro del plazo establecido para dicha etapa, siempre que haya obtenido la vigencia de su inscripción o quedado sin efecto la sanción que le impuso el Tribunal de Contrataciones del Estado.*

1.4. FORMULACIÓN DE CONSULTAS Y OBSERVACIONES A LAS BASES

La formulación de consultas y observaciones a las bases se efectúa de conformidad con lo establecido en los numerales 72.1 y 72.2 del artículo 72 del Reglamento.

Importante

No pueden formularse consultas ni observaciones respecto del contenido de una ficha de homologación aprobada, aun cuando el requerimiento haya sido homologado parcialmente respecto a las características técnicas y/o requisitos de calificación y/o condiciones de ejecución. Las consultas y observaciones que se formulen sobre el particular, se tienen como no presentadas.

1.5. ABSOLUCIÓN DE CONSULTAS, OBSERVACIONES E INTEGRACIÓN DE BASES

La absolución de consultas, observaciones e integración de las bases se realizan conforme a las disposiciones previstas en los numerales 72.4 y 72.5 del artículo 72 del Reglamento.

Importante

- No se absolverán consultas y observaciones a las bases que se presenten en forma física.
- Cuando exista divergencia entre lo indicado en el pliego de absolución de consultas y observaciones y la integración de bases, prevalece lo absuelto en el referido pliego; sin perjuicio, del deslinde de responsabilidades correspondiente

1.6. ELEVACIÓN AL OSCE DEL PLIEGO DE ABSOLUCIÓN DE CONSULTAS Y OBSERVACIONES E INTEGRACIÓN DE BASES

Los cuestionamientos al pliego de absolución de consultas y observaciones así como a las bases integradas por supuestas vulneraciones a la normativa de contrataciones, a los principios que rigen la contratación pública u otra normativa que tenga relación con el objeto de la contratación, pueden ser elevados al OSCE de acuerdo a lo indicado en los numerales del 72.8 al 72.11 del artículo 72 del Reglamento.

La solicitud de elevación para emisión de Pronunciamiento se presenta ante la Entidad, la cual debe remitir al OSCE el expediente completo, de acuerdo a lo señalado en el artículo 124 del TUO de la Ley 27444, aprobado por Decreto Supremo N° 004-2019-JUS, al día hábil siguiente de recibida dicha solicitud.

Advertencia

La solicitud de elevación al OSCE de los cuestionamientos al pliego de absolución de consultas y observaciones, así como a las Bases integradas, se realiza de manera electrónica a través del SEACE, a partir de la oportunidad en que establezca el OSCE mediante comunicado.

Importante

Constituye infracción pasible de sanción según lo previsto en el literal n) del numeral 50.1 del artículo 50 de la Ley, presentar cuestionamientos maliciosos o manifiestamente infundados al pliego de absolución de consultas y/u observaciones.

1.7. FORMA DE PRESENTACIÓN DE OFERTAS

Las ofertas se presentan conforme lo establecido en el artículo 59 del Reglamento.

Las declaraciones juradas, formatos o formularios previstos en las bases que conforman la oferta deben estar debidamente firmados por el postor (firma manuscrita o digital, según la Ley N° 27269, Ley de Firmas y Certificados Digitales¹). Los demás documentos deben ser visados por el postor. En el caso de persona jurídica, por su representante legal, apoderado o mandatario designado para dicho fin y, en el caso de persona natural, por este o su apoderado. No se acepta el pegado de la imagen de una firma o visto. Las ofertas se presentan foliadas.

Importante

- Los formularios electrónicos que se encuentran en el SEACE y que los proveedores deben llenar para presentar sus ofertas, tienen carácter de declaración jurada.
- En caso la información contenida en los documentos escaneados que conforman la oferta no coincida con lo declarado a través del SEACE, prevalece la información declarada en los documentos escaneados.
- No se tomarán en cuenta las ofertas que se presenten en físico a la Entidad.

1.8. PRESENTACIÓN Y APERTURA DE OFERTAS

¹ Para mayor información sobre la normativa de firmas y certificados digitales ingresar a: <https://www.indecopi.gob.pe/web/firmas-digitales/firmar-y-certificados-digitales>

El participante presentará su oferta de manera electrónica a través del SEACE, desde las 00:01 horas hasta las 23:59 horas del día establecido para el efecto en el cronograma del procedimiento; adjuntando el archivo digitalizado que contenga los documentos que conforman la oferta de acuerdo a lo requerido en las bases.

El participante debe verificar antes de su envío, bajo su responsabilidad, que el archivo pueda ser descargado y su contenido sea legible.

Importante

Los integrantes de un consorcio no pueden presentar ofertas individuales ni conformar más de un consorcio en un procedimiento de selección, o en un determinado ítem cuando se trate de procedimientos de selección según relación de ítems.

En la apertura electrónica de la oferta, el comité de selección, verifica la presentación de lo exigido en la sección específica de las bases, de conformidad con el numeral 73.2 del artículo 73 del Reglamento y determina si las ofertas responden a las características y/o requisitos y condiciones de los Términos de Referencia, detallados en la sección específica de las bases. De no cumplir con lo requerido, la oferta se considera no admitida.

1.9. EVALUACIÓN DE LAS OFERTAS

La evaluación de las ofertas se realiza conforme a lo establecido en el artículo 74 del Reglamento.

El desempate mediante sorteo se realiza de manera electrónica a través del SEACE.

1.10. CALIFICACIÓN DE OFERTAS

La calificación de las ofertas se realiza conforme a lo establecido en los numerales 75.1 y 75.2 del artículo 75 del Reglamento.

1.11. SUBSANACIÓN DE LAS OFERTAS

La subsanación de las ofertas se sujeta a lo establecido en el artículo 60 del Reglamento. El plazo que se otorgue para la subsanación no puede ser inferior a un (1) día hábil.

La solicitud de subsanación se realiza de manera electrónica a través del SEACE y será remitida al correo electrónico consignado por el postor al momento de realizar su inscripción en el RNP, siendo su responsabilidad el permanente seguimiento de las notificaciones a dicho correo. La notificación de la solicitud se entiende efectuada el día de su envío al correo electrónico.

La presentación de las subsanaciones se realiza a través del SEACE. No se tomará en cuenta la subsanación que se presente en físico a la Entidad.

1.12. RECHAZO DE LAS OFERTAS

Previo al otorgamiento de la buena pro, el comité de selección revisa las ofertas económicas que cumplen los requisitos de calificación, de conformidad con lo establecido para el rechazo de ofertas, previsto en el artículo 68 del Reglamento, de ser el caso.

De rechazarse alguna de las ofertas calificadas, el comité de selección revisa el cumplimiento de los requisitos de calificación de los postores que siguen en el orden de prelación, en caso las hubiere.

1.13. OTORGAMIENTO DE LA BUENA PRO

Definida la oferta ganadora, el comité de selección otorga la buena pro, mediante su publicación en el SEACE, incluyendo el cuadro comparativo y las actas debidamente motivadas de los resultados de la admisión, no admisión, evaluación, calificación, descalificación, rechazo y el otorgamiento de la buena pro.

1.14. CONSENTIMIENTO DE LA BUENA PRO

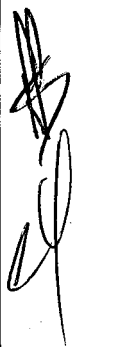

Cuando se hayan presentado dos (2) o más ofertas, el consentimiento de la buena pro se produce a los ocho (8) días hábiles siguientes de la notificación de su otorgamiento, sin que los postores hayan ejercido el derecho de interponer el recurso de apelación.

En caso que se haya presentado una sola oferta, el consentimiento de la buena pro se produce el mismo día de la notificación de su otorgamiento.

El consentimiento del otorgamiento de la buena pro se publica en el SEACE al día hábil siguiente de producido.

Importante

Una vez consentido el otorgamiento de la buena pro, el órgano encargado de las contrataciones o el órgano de la Entidad al que se haya asignado tal función realiza la verificación de la oferta presentada por el postor ganador de la buena pro conforme lo establecido en el numeral 64.6 del artículo 64 del Reglamento.

CAPÍTULO II

SOLUCIÓN DE CONTROVERSIAS DURANTE EL PROCEDIMIENTO DE SELECCIÓN

2.1. RECURSO DE APELACIÓN

A través del recurso de apelación se pueden impugnar los actos dictados durante el desarrollo del procedimiento de selección hasta antes del perfeccionamiento del contrato.

El recurso de apelación se presenta ante y es resuelto por el Tribunal de Contrataciones del Estado.

Los actos que declaren la nulidad de oficio, la cancelación del procedimiento de selección y otros actos emitidos por el Titular de la Entidad que afecten la continuidad de este, se impugnan ante el Tribunal de Contrataciones del Estado.

Importante

- *Una vez otorgada la buena pro, el comité de selección, está en la obligación de permitir el acceso de los participantes y postores al expediente de contratación, salvo la información calificada como secreta, confidencial o reservada por la normativa de la materia, a más tardar dentro del día siguiente de haberse solicitado por escrito.*
Luego de otorgada la buena pro no se da a conocer las ofertas cuyos requisitos de calificación no fueron analizados y revisados por el comité de selección.
- *A efectos de recoger la información de su interés, los postores pueden valerse de distintos medios, tales como: (i) la lectura y/o toma de apuntes, (ii) la captura y almacenamiento de imágenes, e incluso (iii) pueden solicitar copia de la documentación obrante en el expediente, siendo que, en este último caso, la Entidad deberá entregar dicha documentación en el menor tiempo posible, previo pago por tal concepto.*
- *El recurso de apelación se presenta ante la Mesa de Partes del Tribunal o ante las oficinas desconcentradas del OSCE.*

2.2. PLAZOS DE INTERPOSICIÓN DEL RECURSO DE APELACIÓN

La apelación contra el otorgamiento de la buena pro o contra los actos dictados con anterioridad a ella se interpone dentro de los ocho (8) días hábiles siguientes de haberse notificado el otorgamiento de la buena pro.

La apelación contra los actos dictados con posterioridad al otorgamiento de la buena pro, contra la declaración de nulidad, cancelación y declaratoria de desierto del procedimiento, se interpone dentro de los ocho (8) días hábiles siguientes de haberse tomado conocimiento del acto que se desea impugnar.

CAPÍTULO III DEL CONTRATO

3.1. PERFECCIONAMIENTO DEL CONTRATO

Los plazos y el procedimiento para perfeccionar el contrato se realiza conforme a lo indicado en el artículo 141 del Reglamento.

Para perfeccionar el contrato, el postor ganador de la buena pro debe presentar los documentos señalados en el artículo 139 del Reglamento y los previstos en la sección específica de las bases.

3.2. GARANTÍAS

Las garantías que deben otorgar los postores y/o contratistas, según corresponda, son las de fiel cumplimiento del contrato y por los adelantos.

3.2.1. GARANTÍA DE FIEL CUMPLIMIENTO

Como requisito indispensable para perfeccionar el contrato, el postor ganador debe entregar a la Entidad la garantía de fiel cumplimiento del mismo por una suma equivalente al diez por ciento (10%) del monto del contrato original. Esta se mantiene vigente hasta la conformidad de la recepción de la prestación a cargo del contratista.

3.2.2. GARANTÍA DE FIEL CUMPLIMIENTO POR PRESTACIONES ACCESORIAS

En las contrataciones que conllevan la ejecución de prestaciones accesorias, tales como mantenimiento, reparación o actividades afines, se otorga una garantía adicional por una suma equivalente al diez por ciento (10%) del monto del contrato de la prestación accesorio, la misma que debe ser renovada periódicamente hasta el cumplimiento total de las obligaciones garantizadas.

Importante

- En los contratos derivados de procedimientos de selección por relación de ítems, cuando el monto del ítem adjudicado o la sumatoria de los montos de los ítems adjudicados sea igual o menor a doscientos mil Soles (S/ 200,000.00), no corresponde presentar garantía de fiel cumplimiento de contrato ni garantía de fiel cumplimiento por prestaciones accesorias, conforme a lo dispuesto en el literal a) del artículo 152 del Reglamento.
- En los contratos periódicos de prestación de servicios en general que celebren las Entidades con las micro y pequeñas empresas, estas últimas pueden otorgar como garantía de fiel cumplimiento el diez por ciento (10%) del monto del contrato, porcentaje que es retenido por la Entidad durante la primera mitad del número total de pagos a realizarse, de forma prorrateada en cada pago, con cargo a ser devuelto a la finalización del mismo, conforme lo establecen los numerales 149.4 y 149.5 del artículo 149 del Reglamento y numeral 151.2 del artículo 151 del Reglamento.

3.2.3. GARANTÍA POR ADELANTO

En caso se haya previsto en la sección específica de las bases la entrega de adelantos, el contratista debe presentar una garantía emitida por idéntico monto conforme a lo estipulado en el artículo 153 del Reglamento.

3.3. REQUISITOS DE LAS GARANTÍAS

Las garantías que se presenten deben ser incondicionales, solidarias, irrevocables y de realización automática en el país, al solo requerimiento de la Entidad. Asimismo, deben ser emitidas por empresas que se encuentren bajo la supervisión directa de la Superintendencia de Banca, Seguros y Administradoras Privadas de Fondos de Pensiones y que cuenten con clasificación de riesgo B o superior. Asimismo, deben estar autorizadas para emitir garantías; o estar consideradas en la última lista de bancos extranjeros de primera categoría que

periódicamente publica el Banco Central de Reserva del Perú.

Importante

Corresponde a la Entidad verificar que las garantías presentadas por el postor ganador de la buena pro y/o contratista cumplan con los requisitos y condiciones necesarios para su aceptación y eventual ejecución, sin perjuicio de la determinación de las responsabilidades funcionales que correspondan.

Advertencia

Los funcionarios de las Entidades no deben aceptar garantías emitidas bajo condiciones distintas a las establecidas en el presente numeral, debiendo tener en cuenta lo siguiente:

- 1. La clasificadora de riesgo que asigna la clasificación a la empresa que emite la garantía debe encontrarse listada en el portal web de la SBS (<http://www.sbs.gob.pe/sistema-financiero/clasificadoras-de-riesgo>).*
- 2. Se debe identificar en la página web de la clasificadora de riesgo respectiva, cuál es la clasificación vigente de la empresa que emite la garantía, considerando la vigencia a la fecha de emisión de la garantía.*
- 3. Para fines de lo establecido en el artículo 148 del Reglamento, la clasificación de riesgo B, incluye las clasificaciones B+ y B.*
- 4. Si la empresa que otorga la garantía cuenta con más de una clasificación de riesgo emitida por distintas empresas listadas en el portal web de la SBS, bastará que en una de ellas cumpla con la clasificación mínima establecida en el Reglamento.*

En caso exista alguna duda sobre la clasificación de riesgo asignada a la empresa emisora de la garantía, se deberá consultar a la clasificadora de riesgos respectiva.

De otro lado, además de cumplir con el requisito referido a la clasificación de riesgo, a efectos de verificar si la empresa emisora se encuentra autorizada por la SBS para emitir garantías, debe revisarse el portal web de dicha Entidad (<http://www.sbs.gob.pe/sistema-financiero/relacion-de-empresas-que-se-encuentran-autorizadas-a-emitir-cartas-fianza>).

Los funcionarios competentes deben verificar la autenticidad de la garantía a través de los mecanismos establecidos (consulta web, teléfono u otros) por la empresa emisora.

3.4. EJECUCIÓN DE GARANTÍAS

La Entidad puede solicitar la ejecución de las garantías conforme a los supuestos contemplados en el artículo 155 del Reglamento.

3.5. ADELANTOS

La Entidad puede entregar adelantos directos al contratista, los que en ningún caso exceden en conjunto del treinta por ciento (30%) del monto del contrato original, siempre que ello haya sido previsto en la sección específica de las bases.

3.6. PENALIDADES

3.6.1. PENALIDAD POR MORA EN LA EJECUCIÓN DE LA PRESTACIÓN

En caso de retraso injustificado del contratista en la ejecución de las prestaciones objeto del contrato, la Entidad le aplica automáticamente una penalidad por mora por cada día de atraso, de conformidad con el artículo 162 del Reglamento.

3.6.2. OTRAS PENALIDADES

La Entidad puede establecer penalidades distintas a la mencionada en el numeral precedente, según lo previsto en el artículo 163 del Reglamento y lo indicado en la sección

específica de las bases.

Estos dos tipos de penalidades se calculan en forma independiente y pueden alcanzar cada una un monto máximo equivalente al diez por ciento (10%) del monto del contrato vigente, o de ser el caso, del ítem que debió ejecutarse.

3.7. INCUMPLIMIENTO DEL CONTRATO

Las causales para la resolución del contrato, serán aplicadas de conformidad con el artículo 36 de la Ley y 164 del Reglamento.

3.8. PAGOS

El pago se realiza después de ejecutada la respectiva prestación, pudiendo contemplarse pagos a cuenta, según la forma establecida en la sección específica de las bases o en el contrato.

La Entidad paga las contraprestaciones pactadas a favor del contratista dentro de los diez (10) días calendario siguientes de otorgada la conformidad de los servicios, siempre que se verifiquen las condiciones establecidas en el contrato para ello, bajo responsabilidad del funcionario competente.

La conformidad se emite en un plazo máximo de siete (7) días de producida la recepción, salvo que se requiera efectuar pruebas que permitan verificar el cumplimiento de la obligación, en cuyo caso la conformidad se emite en un plazo máximo de quince (15) días, bajo responsabilidad del funcionario que debe emitir la conformidad.

En el caso que se haya suscrito contrato con un consorcio, el pago se realizará de acuerdo a lo que se indique en el contrato de consorcio.

Advertencia

En caso de retraso en los pagos a cuenta o pago final por parte de la Entidad, salvo que se deba a caso fortuito o fuerza mayor, esta reconoce al contratista los intereses legales correspondientes, de conformidad con el artículo 39 de la Ley y 171 del Reglamento, debiendo repetir contra los responsables de la demora injustificada.




3.9. DISPOSICIONES FINALES

Todos los demás aspectos del presente procedimiento no contemplados en las bases se regirán supletoriamente por la Ley y su Reglamento, así como por las disposiciones legales vigentes.

SECCIÓN ESPECÍFICA

CONDICIONES ESPECIALES DEL PROCEDIMIENTO DE SELECCIÓN

(EN ESTA SECCIÓN LA ENTIDAD DEBERÁ COMPLETAR LA INFORMACIÓN EXIGIDA, DE ACUERDO A LAS INSTRUCCIONES INDICADAS)

CAPÍTULO I GENERALIDADES

1.1. ENTIDAD CONVOCANTE

Nombre : DIRECCIÓN DE ECONOMÍA Y FINANZAS PNP-DIRECFIN PNP
RUC N° : 20165465009
Domicilio legal : Calle San German N° 200 - RIMAC
Teléfono: : 01 3811017
Correo electrónico: : depaba.secon@policia.gob.pe

1.2. OBJETO DE LA CONVOCATORIA

El presente procedimiento de selección tiene por objeto la contratación del **SERVICIO DE TRANSMISIÓN PARA LA RED PRIVADA DE LA PNP, EN LAS UNIDADES POLICIALES A NIVEL NACIONAL; SERVICIO DE SEGURIDAD GESTIONADA Y ACCESO A INTERNET.**

ITEM	COMPONENTE	SERVICIO
I	1	Servicio de acceso de internet para la sede principal y secundario (sitio principal y secundario).
	2	Servicio de fibra oscura entre el Datacenter principal y secundario de la PNP
	3	Plataforma digital de servicios para transmisión de voz, video y datos para las sedes desconcentradas PNP, a nivel nacional
	4	Servicio de seguridad de la información, seguridad informática gestionada, adecuación de datacenter
	5	Servicio de Gestión de Identidades
	6	Servicio de housing para el Datacenter secundario PNP
	7	Servicio de Inducción

1.3. EXPEDIENTE DE CONTRATACIÓN

El expediente de contratación fue aprobado mediante FORMATO N° 02-CP-02-2025-DIRECFIN PNP, el 14 de abril de 2025.

1.4. FUENTE DE FINANCIAMIENTO

Recursos Ordinarios (RO).

Importante

La fuente de financiamiento debe corresponder a aquella prevista en la Ley de Equilibrio Financiero del Presupuesto del Sector Público del año fiscal en el cual se convoca el procedimiento de selección.

1.5. SISTEMA DE CONTRATACIÓN

El presente procedimiento se rige por el sistema de suma alzada, de acuerdo con lo establecido en el expediente de contratación respectivo.

1.6. DISTRIBUCIÓN DE LA BUENA PRO

El presente procedimiento se rige por el sistema de suma alzada, de acuerdo con lo establecido en el expediente de contratación respectivo.

1.7. ALCANCES DEL REQUERIMIENTO

El alcance de la prestación está definido en el Capítulo III de la presente sección de las bases.

1.8. PLAZO DE PRESTACIÓN DEL SERVICIO

Los servicios materia de la presente convocatoria se prestarán de acuerdo con el siguiente detalle y en concordancia con lo establecido en el expediente de contratación.

PLAZO DE EJECUCION DE LA PRESTACION

Plazo de implementación. - Inicia a partir del día del siguiente de suscrito el contrato, dándose inicio a la implementación y puesta en funcionamiento del servicio en un plazo máximo de SEIS (06) MESES.

Plazo para suscribir la Conformidad. - Culminada la etapa de implementación y puesta en funcionamiento, el Jefe del DEPGCD-DIVINF-DIRTIC PNP emitirá el Acta de Conformidad de la implementación realizada, previo informe del personal técnico responsable de las Secciones de Operaciones, Redes y Seguridad Informática, en un plazo máximo de SIETE (7) días calendarios.

Inicio del Servicio. - Inicia a partir del día siguiente de suscrita el Acta de conformidad de implementación del servicio, dándose inicio a la ejecución contractual para la prestación del "SERVICIO DE TRANSMISION PARA LA RED PRIVADA DE LA PNP, EN LAS UNIDADES POLICIALES A NIVEL NACIONAL; SERVICIO DE SEGURIDAD GESTIONADA Y ACCESO A INTERNET", por el período de treinta y seis (36) meses contados a partir del día siguiente de suscrito el Acta de Conformidad de la implementación y puesta en funcionamiento.

Se ha considerado los siguientes plazos:

Prestación de servicio

- 1) La implementación y puesta en funcionamiento se realizará en un plazo no mayor a SEIS (06) MESES, contados a partir del día siguiente de la suscripción del contrato.
- 2) El plazo de ejecución del servicio de transmisión para la red privada de la PNP, internet y fibra oscura para la data center principal y secundario PNP, es treinta y seis (36) meses, contabilizados desde el día siguiente de firmada el Acta de conformidad por parte del Jefe del DEPGCD-DIVINF-DIRTIC PNP, previo informe del personal técnico responsable según corresponda.
- 3) La implementación y prestación del servicio se ejecutará según los siguientes plazos y condiciones:
 - **Plazo para reunión de coordinación para el inicio del proyecto:** El Contratista dentro de OCHO (08) días calendarios posteriores a la suscripción del contrato, coordinará con las personas encargadas de DIRTIC-PNP la reunión de coordinación para el inicio del proyecto.
 - **Plazo para presentación del Plan de trabajo:** El Contratista dentro de SEIS (06) días calendarios posteriores a la suscripción del contrato, presentará en la mesa de partes de la DIRTIC-PNP, con copia en la mesa de martes de DIVLOG-PNP, el plan de trabajo para su evaluación y aprobación a cargo del Jefe del DEPGCD - DIVINF-PNP. También se podrá realizar de manera digital a las siguientes direcciones virtuales: depaba.secejecon@policia.gob.pe; y dir tic.ayu@policia.gob.pe.
 - **Plazo para la Evaluación y Aprobación del Plan de Trabajo:** en un plazo máximo de DOS (02) días calendario de entregado el plan de trabajo, el Jefe del DEPGCD DIVINF-PNP, aprobará el referido plan. De existir observaciones la entidad comunicará al contratista el sentido de las mismas mediante correo electrónico, teniendo este último DOS (02) días calendario para la subsanación de las mismas, para cuyo efecto deberá realizar la presentación del plan de trabajo en las respectivas mesas de parte. También se podrá realizar de manera digital a las siguientes direcciones virtuales: depaba.secejecon@policia.gob.pe; y dir tic.ayu@policia.gob.pe.

- **Plazo para la presentación del Diseño de la Topología del Servicio de Conectividad y Protocolo de pruebas:** en un plazo máximo de SEIS (06) días calendarios posteriores al día siguiente de la suscripción del contrato, el contratista presentará en la mesa de partes de la DIRTIC-PNP, con copia en la mesa de partes de DIVLOG-PNP, el Diseño y protocolo de pruebas para su evaluación y aprobación a cargo del Jefe del DEPGCD DIVINF-PNP.
 - **Plazo para la aprobación del Diseño de la Topología del Servicio de Conectividad y Protocolo de pruebas:** la entidad tendrá un plazo de aprobación hasta DOS (02) días calendario, contados a partir del día siguiente de presentado el Diseño y Protocolo de Pruebas. De existir observaciones el contratista tendrá DOS (02) días calendarios para levantar las observaciones presentadas, una vez subsanadas todas las observaciones que se hubiesen presentado, se suscribirá en Acta de conformidad del Diseño de la Topología del Servicio de Conectividad y Protocolo de pruebas, por parte del Jefe del DEPGCD-DIVINF-DIRTIC-PNP.
 - **Plazo para la entrega de los manuales técnicos de los equipos:** hasta SEIS (06) MESES posteriores a la suscripción del contrato:
 - 1) Manual Técnico de equipos de conectividad (Router y switch)
 - 2) Manuales Técnicos de equipos de balanceo de enlaces y de sitios.
 - 3) Manuales Técnicos de equipos de traffic shapping.
 - 4) Manuales Técnicos del servicio de gestión de identidades.
 - 5) Documentos de garantías del equipamiento suministrado.Los manuales podrán ser entregados en el idioma original del fabricante.
- 4) El plazo de implementación es de SEIS (06) MESES contados a partir del día siguiente de la suscripción del contrato. Se suscribirá el Acta de conformidad de Implementación, previa entrega de los entregables descritos en el numeral 5.10.1 y el informe final por parte del Contratista, con esto se dará inicio al Servicio. El plazo máximo para la suscripción de la referida Acta de Implementación y puesta en funcionamiento es de SIETE (07) días calendario, posteriores a la verificación y recepción de la documentación correspondiente.
- 5) La Entidad brindara las facilidades de accesos y/o facilidades requeridas en la etapa de implementación, en el caso de imprevistos por parte de la Entidad, los plazos internos (antes mencionados) podrán ser cambiados en coordinación con el contratista, sin que ello genere la aplicación de ninguna penalidad en contra del contratista.
- 6) El contratista por fuerza mayor podrá solicitar variar los referidos plazos internos antes indicados, en coordinación con el área usuaria, pero sin extender los SEIS (06) MESES, del periodo de implementación, los cambios solicitados requerirán aprobación de LA ENTIDAD.
- 7) Para la inducción se considerará los siguientes plazos y condiciones:
- **Plazo para coordinar cronograma de inducción:** Dentro de los quince (15) días calendarios posteriores a la suscripción del contrato, el contratista y un representante del área del DEPGCD DIVINF DIRTIC PNP, deberán realizar una reunión de coordinación a fin de establecer el cronograma para el desarrollo de la inducción, suscribiendo el acta correspondiente.
 - Las inducciones, se brindarán en las condiciones establecidas según el numeral 5.2.1.5.7 de los presentes términos de referencia.
 - Las inducciones se iniciarán 30 días posteriores a la suscripción del acta de conformidad por la implementación y puesta en marcha del servicio, teniendo como plazo máximo de inicio 24 meses posteriores a la firma del del acta de conformidad por la implementación y puesta en marcha del servicio.

CRONOGRAMA DE ACTIVIDADES ACTIVIDADES	CRONOGRAMA DE ACTIVIDADES POR DÍA					
	Del 1 al 6	Del 7 al 8	Del 9 al 180	Del 181 al 187	Del 188 al 907	Del 907 al 1267
Reunión de coordinación para el inicio del proyecto, a partir del día siguiente de la suscripción del contrato.						
Presentación del Plan de Trabajo						
Evaluación y Aprobación del Plan de Trabajo						
Presentación del Diseño de la Topología del Servicio de Conectividad y Protocolo de pruebas						
Aprobación del Diseño de la Topología del Servicio de Conectividad y Protocolo de pruebas						
Entrega de Manuales Técnicos de los equipos						
Implementación del servicio total (considera todos los componentes)						
Acta de Conformidad de la Implementación del Servicio						
Inicio del servicio						
Inducción						

La ENTIDAD indicará el horario de trabajo para la provisión de los equipos, configuración y pruebas del servicio, garantizando por lo menos ocho (08) horas diarias de lunes a viernes en días laborables, en horarios diurnos o nocturnos para la realización de las actividades; asimismo, se podrá programar actividades de la implementación los sábados, domingos o feriados en coordinación con el responsable técnico de la Entidad.

Las actividades o reuniones de coordinación no se encuentran supeditadas al cumplimiento de la presentación del plan de trabajo dentro del plazo establecido. Dicha documentación se entregará según cronograma del cuadro antes indicado.

1.9. COSTO DE REPRODUCCIÓN Y ENTREGA DE BASES

Los participantes registrados tienen el derecho de recabar un ejemplar de las bases, para cuyo efecto deben cancelar en Agencias del Banco de la Nación con código N° 08494 (Costo por folio fotocopiado según TUPA del Ministerio del Interior es de S/ 0.10); y se recabarán las bases impresas en la Sección de Contrataciones de la DEPABA, sito en Calle San German N° 200 - Rímac - Lima - Lima.

Importante

El costo de entrega de un ejemplar de las bases no puede exceder el costo de su reproducción.

1.10. BASE LEGAL

- Ley N° 32185 Ley del Presupuesto del Sector Público para el Año Fiscal 2025.
- Ley N° 32186 Ley del Equilibrio Financiero del Presupuesto del Sector Público para el Año Fiscal 2025.
- Ley N° 32187 Ley de Endeudamiento del Sector Público para el Año Fiscal 2025.
- Decreto Supremo N°082-2019-EF – Texto Único Ordenado de la Ley N° 30225 - Ley de Contrataciones del Estado, en adelante "la Ley".
- Decreto Supremo N° 344-2018-EF que aprueba el Reglamento de la Ley de Contrataciones del Estado; en adelante "El Reglamento". Modificado por Decreto Supremo N° 377-2019-EF, Decreto Supremo N° 168-2020-EF, Decreto Supremo N° 250-2020-EF, Decreto Supremo N° 162-2021-EF, Decreto Supremo N° 234-2022-EF y Decreto Supremo N° 308-2022-EF.
- Ley N° 27806 - Ley de Transparencia y Acceso a la Información Pública.
- Decreto Supremo N° 004-2019-JUS, Texto Único Ordenado de la Ley N° 27444, Ley de Procedimiento Administrativo General.
- Código Civil
- Directivas y Opiniones del OSCE.
- Cualquier otra disposición legal vigente que permita desarrollar el objeto de la convocatoria, que no contravenga lo regulado por la Ley de Contrataciones del Estado

- Tierras y aterramientos para los sistemas de telecomunicaciones de edificios comerciales
- Reglamento Nacional de Edificaciones del Perú.
- Código Nacional de Electricidad del Perú.
- Resolución Ministerial N° 175-2008-MEM/DM del 11ABR2008.
- Decreto Supremo N°020-2007-MTC; Texto Único Ordenado del Reglamento General de la Ley de Telecomunicaciones
- Reglamento Específico de Homologación de Aparatos y Equipos de Telecomunicaciones
- Norma G.050 seguridad durante la construcción
- Ley 29733 Ley de Protección de datos personales.
- Decreto Supremo 081-2017-PCM "Decreto que aprueba la formulación de un plan de transición al protocolo IPV6 en las entidades de la Administración Pública", de fecha 08 de agosto del 2017.
- Resolución Ministerial 004-2016-PCM Aprobación del uso obligatorio de la Norma técnica peruana "NTP ISO/IEC 27001:2014 Tecnología de la Información Técnicas de Seguridad Sistemas de Gestión de Seguridad de la Información Requisitos 2da Edición.

Las referidas normas incluyen sus respectivas modificaciones, de ser el caso.



CAPÍTULO II DEL PROCEDIMIENTO DE SELECCIÓN

2.1. CALENDARIO DEL PROCEDIMIENTO DE SELECCIÓN

Según el cronograma de la ficha de selección de la convocatoria publicada en el SEACE.

Importante

De conformidad con la vigesimosegunda Disposición Complementaria Final del Reglamento, en caso la Entidad (Ministerios y sus organismos públicos, programas o proyectos adscritos) haya difundido el requerimiento a través del SEACE siguiendo el procedimiento establecido en dicha disposición, no procede formular consultas u observaciones al requerimiento.

2.2. CONTENIDO DE LAS OFERTAS

La oferta contendrá, además de un índice de documentos², la siguiente documentación:

2.2.1. Documentación de presentación obligatoria

2.2.1.1. Documentos para la admisión de la oferta

- a) Declaración jurada de datos del postor. (**Anexo N° 1**)
- b) Documento que acredite la representación de quien suscribe la oferta.

En caso de persona jurídica, copia del certificado de vigencia de poder del representante legal, apoderado o mandatario designado para tal efecto.

En caso de persona natural, copia del documento nacional de identidad o documento análogo, o del certificado de vigencia de poder otorgado por persona natural, del apoderado o mandatario, según corresponda.

En el caso de consorcios, este documento debe ser presentado por cada uno de los integrantes del consorcio que suscriba la promesa de consorcio, según corresponda.

Advertencia

De acuerdo con el artículo 4 del Decreto Legislativo N° 1246, las Entidades están prohibidas de exigir a los administrados o usuarios la información que puedan obtener directamente mediante la interoperabilidad a que se refieren los artículos 2 y 3 de dicho Decreto Legislativo. En esa medida, si la Entidad es usuaria de la Plataforma de Interoperabilidad del Estado – PIDE³ y siempre que el servicio web se encuentre activo en el Catálogo de Servicios de dicha plataforma, no corresponderá exigir el certificado de vigencia de poder y/o documento nacional de identidad.

- c) Declaración jurada de acuerdo con el literal b) del artículo 52 del Reglamento. (**Anexo N° 2**)
- d) Declaración jurada de cumplimiento de los Términos de Referencia contenidos en el numeral 3.1 del Capítulo III de la presente sección. (**Anexo N° 3**)

² La omisión del índice no determina la no admisión de la oferta.

³ Para mayor información de las Entidades usuarias y del Catálogo de Servicios de la Plataforma de Interoperabilidad del Estado – PIDE ingresar al siguiente enlace <https://www.gobiernodigital.gob.pe/interoperabilidad/>

e)

Se requerirá que, para la presentación de la oferta, el postor debe acreditar que los bienes ofertados no se deberán encontrar en fin de soporte o End Of Support (EOS), periodo en el que el producto ya no tiene soporte, lo que se debe evidenciar el postor mediante carta del fabricante, a fin de garantizar lo ofertado, los cuales se podrán presentar en español o en su idioma original. Se aclara que los bienes ofertados hacen referencia a todo el equipamiento físico requerido y a ser instalado por el contratista tanto en el Datacenter Principal, Datacenter Secundario y cada dependencia policial en los Componentes N°1,2,3 y 4 (no aplica los bienes a instalar en la adecuación del Datacenter numeral 5.2.1.5.4.1.23). Esta exigencia, es a fin de garantizar que el equipamiento propuesto tenga vigencia durante la prestación del servicio contratado.

f)

El Postor deberá presentar en su oferta una carta del fabricante, en idioma español o en su idioma original, de la solución indicando el cumplimiento de todas las características técnicas descritas para el **optimizador de tráfico y traffic shapping** según el numeral 5.2.1.5.1.6 de los presentes términos de referencia (documentación de carácter obligatorio en la etapa de presentación de oferta).

g)

Para garantizar que los **routers y switches** sean de marcas líderes a nivel global en el mercado, las marcas propuestas de routers y switches deberán estar como líderes en el cuadrante de gartner (copia de la publicación oficial de Gartner y la "url" (link) del enlace web respectivo) **"Wired and wireless LAN access infrastructure"** en los últimos 04 años. Dicha información **deberá ser presentada al momento de la presentación de la oferta mediante carta simple emitida por el postor.**

h)

El postor tiene la libertad de incorporar en su oferta técnica una plataforma tercera que realice descifrado del tráfico y cumpla todas las especificaciones indicadas, en caso el NGFW propuesto no pueda realizarlo o no esté diseñado para ello. En caso de optar por esta alternativa, se deberá incluir una plataforma por cada una de las 14 sedes.

Para este caso, el postor **deberá presentar como documentación sustentatoria para su oferta,** una Carta del Fabricante, ya sea en idioma español o en su idioma original, de la plataforma tercera, en la cual se evidencie técnicamente el cumplimiento de la sección DESCIFRADO DE TRÁFICO SSL/TLS según los numerales 5.2.1.5.3.3.10, 5.2.1.5.3.3.11 y 5.2.1.5.4.1.13.

i)

Para las Sedes tipo 2, (firewall de próxima generación) en caso la solución propuesta no tenga este módulo de aprendizaje, el postor deberá incluir en su oferta técnica el **servicio de configuración/migración** de todas las políticas de seguridad basadas en puertos, a políticas basadas en aplicaciones, este servicio deberá ser realizado por el área de **servicios profesionales del propio fabricante**. Considerar un estimado de 1,400 políticas de seguridad entre todos los dispositivos de este tipo de sede. Para este caso, el postor deberá presentar como documentación sustentatoria en su oferta, una Carta del Fabricante, en idioma español o en su idioma original, de los equipos de Firewall de próxima generación, en la cual se evidencie que será el fabricante el que realizará la configuración/migración según corresponda considerando lo descrito en el párrafo anterior.

j)

Para la solución de firewall de nueva generación, para red externa y red interna, en caso la solución propuesta no tenga este módulo de aprendizaje, el postor deberá incluir en su oferta técnica el servicio de configuración/migración de todas las políticas de seguridad basadas en puertos, a políticas basadas en aplicaciones, este servicio deberá ser realizado por el área de servicios profesionales del propio fabricante. Considerar un estimado de 1,400 políticas de seguridad entre todos los dispositivos de este tipo de sede. Para este caso, el postor deberá presentar como documentación sustentatoria en su oferta, una Carta del Fabricante, en idioma español o en su idioma original, de los equipos de Firewall de próxima generación, en la cual se evidencie que será el fabricante el que realizará la configuración/migración según corresponda.

k)

Para los Firewall de próxima generación para sedes policiales (1001) y Firewall de próxima generación (Complejos 01) (14 sedes en HA), en caso el postor haya integrado tecnologías de terceros externas al NGFW, también se deberá considerar dentro de la propuesta técnica la consola de gestión para dicha tecnología. Para este caso, el postor deberá presentar como documentación sustentatoria en su oferta, una Carta del Fabricante, en idioma español o en su idioma original, de la tecnología de terceros externas al NGFW que el postor halla integrado, en la cual se evidencie técnicamente el cumplimiento de la sección ADMINISTRACIÓN según los numerales 5.2.1.5.3.3.10 y 5.2.1.5.3.3.11

l)

El Postor debe presentar el modelo de la solución propuesta que debe contar con la certificación o reconocimiento como líder en firewall de base de datos, en reportes de analistas como Gartner y/o forrester, documentación que se debe presentar en el momento de la presentación de la oferta.

m) Declaración jurada de plazo de prestación del servicio. (Anexo N° 4)⁴

n) Promesa de consorcio con firmas legalizadas, de ser el caso, en la que se consigne los integrantes, el representante común, el domicilio común y las obligaciones a las que se compromete cada uno de los integrantes del consorcio así como el porcentaje equivalente a dichas obligaciones. (Anexo N° 5)

o) El precio de la oferta en soles. Adjuntar obligatoriamente el Anexo N° 6.

El precio total de la oferta y los subtotales que lo componen son expresados con dos (2) decimales. Los precios unitarios pueden ser expresados con más de dos (2) decimales.

Importante

- El comité de selección verifica la presentación de los documentos requeridos. De no cumplir con lo requerido, la oferta se considera no admitida.
- En caso de requerir estructura de costos o análisis de precios, esta se presenta para el perfeccionamiento del contrato.

2.2.1.2. Documentos para acreditar los requisitos de calificación

Incorporar en la oferta los documentos que acreditan los “Requisitos de Calificación” que se detallan en el numeral 3.2 del Capítulo III de la presente sección de las bases.

⁴ En caso de considerar como factor de evaluación la mejora del plazo de prestación del servicio, el plazo ofertado en dicho anexo servirá también para acreditar este factor.

2.2.2. Documentación de presentación facultativa:

Advertencia

El comité de selección no podrá exigir al postor la presentación de documentos que no hayan sido indicados en los acápite "Documentos para la admisión de la oferta", "Requisitos de calificación" y "Factores de evaluación".

2.3. REQUISITOS PARA PERFECCIONAR EL CONTRATO

El postor ganador de la buena pro debe presentar los siguientes documentos para perfeccionar el contrato:

- a) Garantía de fiel cumplimiento del contrato.
- b) Garantía de fiel cumplimiento por prestaciones accesorias, de ser el caso.
- c) Contrato de consorcio con firmas legalizadas ante Notario de cada uno de los integrantes de ser el caso.
- d) Código de cuenta interbancaria (CCI) o, en el caso de proveedores no domiciliados, el número de su cuenta bancaria y la entidad bancaria en el exterior.
- e) Copia de la vigencia del poder del representante legal de la empresa que acredite que cuenta con facultades para perfeccionar el contrato, cuando corresponda.
- f) Copia de DNI del postor en caso de persona natural, o de su representante legal en caso de persona jurídica.

Advertencia

De acuerdo con el artículo 4 del Decreto Legislativo N° 1246, las Entidades están prohibidas de exigir a los administrados o usuarios la información que puedan obtener directamente mediante la interoperabilidad a que se refieren los artículos 2 y 3 de dicho Decreto Legislativo. En esa medida, si la Entidad es usuaria de la Plataforma de Interoperabilidad del Estado – PIDE⁵ y siempre que el servicio web se encuentre activo en el Catálogo de Servicios de dicha plataforma, no corresponderá exigir los documentos previstos en los literales e) y f).

- g) Domicilio para efectos de la notificación durante la ejecución del contrato.
- h) Autorización de notificación de la decisión de la Entidad sobre la solicitud de ampliación de plazo mediante medios electrónicos de comunicación ⁶ (**Anexo N° 12**).
- i) Detalle de los precios unitarios del precio ofertado⁷.
- j) Estructura de costos⁸.
- k) Detalle del precio de la oferta de cada uno de los servicios que conforman el paquete⁹.
- l)

Para la solución de firewall de base de datos (numeral 5.2.1.5.4.1.15), el Postor adjudicatario de la buena pro debe asegurar que la solución cuente con un servicio de investigación sobre vulnerabilidades y amenazas informáticas, para lo cual presenta la documentación respectiva (en idioma español o en su idioma original) en el descubrimiento de éstas. El presente requerimiento se validará mediante la presentación de una Declaración Jurada que establezca lo solicitado en los Términos de Referencia.

⁵ Para mayor información de las Entidades usuarias de la Plataforma de Interoperabilidad del Estado – PIDE ingresar al siguiente enlace <https://www.gobiernodigital.gob.pe/interoperabilidad/>

⁶ En tanto se implemente la funcionalidad en el SEACE, de conformidad con la Primera Disposición Complementaria Transitoria del Decreto Supremo N° 234-2022-EF.

⁷ Incluir solo en caso de la contratación bajo el sistema a suma alzada.

⁸ Incluir solo cuando resulte necesario para la ejecución contractual, identificar los costos de cada uno de los rubros que comprenden la oferta.

⁹ Incluir solo en caso de contrataciones por paquete.

m)

Para el perfeccionamiento del Contrato el postor ganador debe incluir los datasheets en idioma original de los dispositivos y/o equipamiento propuesto con su número de parte (part number) correspondiente, licenciamiento, accesorios y componentes necesarios para asegurar el nivel de servicio; el Diagrama técnico detallará la arquitectura y topología de la solución tecnológica propuesta, esto aplica para todos los componentes del ítem 1; asimismo, el contratista no podrá colocar equipos distintos a los indicados en su propuesta técnica durante la etapa de implementación y/o durante la prestación del servicio, a menos que sea por mejora tecnológica, previa aprobación por parte del área usuaria.

n)

El postor ganador debe estar autorizado por el MTC para proveer servicios transmisión de datos y/o de internet y/o servicios de valor añadido y, debe ser parte del NAP (Network Access Point) Perú, proveyendo un enlace dedicado con conexión directa y overbooking 1:1 al NAP Perú; en consecuencia, deberá presentar para el perfeccionamiento del contrato, la documentación necesaria que acredite ser como miembro activo del NAP Perú.

o)

Para la solución de firewall de aplicaciones, debe tener la capacidad de efectuar el parchado virtual de las aplicaciones web, para remediar las vulnerabilidades detectadas y debe permitir tener integración con software de detección de vulnerabilidades (la solución debe permitir integrarse como mínimo con dos vendedores de scanner de vulnerabilidades que debe ser indicado mediante una carta del fabricante, en idioma español o en su idioma original, que acredite dicha integración, la misma que se debe presentar para el perfeccionamiento del contrato).

p)

Para la solución de Firewall de próxima generación (Complejos 01) (14 sedes en HA) (numeral 5.2.1.5.3.3.10), se deberá enviar una carta emitido por el contratista con el link con documentación pública del fabricante que respalde la comprobación del requerimiento de throughput.

q)

Para la solución de Firewall de próxima generación para sedes policiales (1001) distribuidos para sedes del tipo 1 (numeral 5.2.1.5.3.3.11), se deberá enviar una carta emitido por el contratista con el link con documentación pública del fabricante que respalde la comprobación del requerimiento de throughput.

r)

Para la solución de FIREWALL DE NUEVA GENERACIÓN, PARA RED EXTERNA Y RED INTERNA (numeral 5.2.1.5.4.1.13), se deberá enviar una carta emitido por el contratista con el link con documentación pública del fabricante que respalde la comprobación del requerimiento de throughput.

s)

Para la solución de PROTECCIÓN DE PORTALES WEB Y BASE DE DATOS (numeral 5.2.1.5.4.1.15), se deberá enviar una carta con autorización del fabricante o su representante para comercializar la marca y brindar los servicios solicitados.

t)

El personal que realizará la implementación debe estar certificado por el fabricante de los materiales y/o equipamiento a utilizar. Se deberá enviar una declaración jurada demostrando dicho cumplimiento.

Importante

- En caso que el postor ganador de la buena pro sea un consorcio, las garantías que presente este para el perfeccionamiento del contrato, así como durante la ejecución contractual, de ser el caso, además de cumplir con las condiciones establecidas en el artículo 33 de la Ley y el artículo 148 del Reglamento, deben consignar expresamente el nombre completo o la denominación o razón social de los integrantes del consorcio, en calidad de garantizados, de

lo contrario no podrán ser aceptadas por las Entidades. No se cumple el requisito antes indicado si se consigna únicamente la denominación del consorcio, conforme lo dispuesto en la Directiva "Participación de Proveedores en Consorcio en las Contrataciones del Estado".

- En los contratos periódicos de prestación de servicios en general que celebren las Entidades con las micro y pequeñas empresas, estas últimas pueden otorgar como garantía de fiel cumplimiento el diez por ciento (10%) del monto del contrato, porcentaje que es retenido por la Entidad durante la primera mitad del número total de pagos a realizarse, de forma prorrateada en cada pago, con cargo a ser devuelto a la finalización del mismo, conforme lo establece el numeral 149.4 del artículo 149 del Reglamento y numeral 151.2 del artículo 151 del Reglamento. Para dicho efecto los postores deben encontrarse registrados en el REMYPE, consignando en la Declaración Jurada de Datos del Postor (Anexo N° 1) o en la solicitud de retención de la garantía durante el perfeccionamiento del contrato, que tienen la condición de MYPE, lo cual será verificado por la Entidad en el link <http://www2.trabajo.gob.pe/servicios-en-linea-2-2> opción consulta de empresas acreditadas en el REMYPE.
- En los contratos derivados de procedimientos de selección por relación de ítems, cuando el monto del ítem adjudicado o la sumatoria de los montos de los ítems adjudicados sea igual o menor a doscientos mil Soles (S/ 200,000.00), no corresponde presentar garantía de fiel cumplimiento de contrato ni garantía de fiel cumplimiento por prestaciones accesorias, conforme a lo dispuesto en el literal a) del artículo 152 del Reglamento.

Importante

- Corresponde a la Entidad verificar que las garantías presentadas por el postor ganador de la buena pro cumplan con los requisitos y condiciones necesarios para su aceptación y eventual ejecución, sin perjuicio de la determinación de las responsabilidades funcionales que correspondan.
- De conformidad con el Reglamento Consular del Perú aprobado mediante Decreto Supremo N° 076-2005-RE para que los documentos públicos y privados extendidos en el exterior tengan validez en el Perú, deben estar legalizados por los funcionarios consulares peruanos y refrendados por el Ministerio de Relaciones Exteriores del Perú, salvo que se trate de documentos públicos emitidos en países que formen parte del Convenio de la Apostilla, en cuyo caso bastará con que estos cuenten con la Apostilla de la Haya¹⁰.
- La Entidad no puede exigir documentación o información adicional a la consignada en el presente numeral para el perfeccionamiento del contrato.

2.4. PERFECCIONAMIENTO DEL CONTRATO

El contrato se perfecciona con la suscripción del documento que lo contiene. Para dicho efecto el postor ganador de la buena pro, dentro del plazo previsto en el artículo 141 del Reglamento, debe presentar la documentación requerida en Mesa de Partes de la Sección de Ejecución Contractual de la Dirección de Economía y Finanzas - Policía Nacional del Perú, sito en la Calle San German N° 200 (Tercer piso), en el horario de 08:30 a.m. a 17:00 p.m, de lunes a viernes y en días hábiles.

Importante

En el caso de procedimientos de selección por relación de ítems, se puede perfeccionar el contrato con la suscripción del documento o con la recepción de una orden de servicios, cuando el monto del valor estimado del ítem no supere los doscientos mil Soles (S/ 200,000.00).

2.5. FORMA DE PAGO

La Entidad realizará el pago de la contraprestación pactada a favor del contratista en pagos mensuales.

¹⁰ Según lo previsto en la Opinión N° 009-2016/DTN.

El pago de la prestación del servicio se realizará en TREINTA Y SEIS (36) pagos periódicos mensuales, al final de cada ciclo de facturación, dentro de los diez (10) días calendarios siguiente de otorgada la conformidad de los servicios. Para efectos del pago de las contraprestaciones ejecutadas por el contratista, la Entidad debe contar con la siguiente documentación:

- Comprobante de pago
- Acta de conformidad firmada por el Jefe del DEPGCD-DIVINF-DIRTIC PNP, previo informe de las áreas competentes según sus funciones (DEPGCD-DIVINF-DIRTIC PNP de la DIRTIC-PNP)

Para el caso del primer pago se solicitará de manera adicional, el acta de conformidad de implementación y puesta en marcha del servicio, y en el caso del veinticuatroavo pago, se solicitará adicionalmente la constancia y/o certificado de Inducción según lo indicado en el numeral 5.2.1.5.7 de los presentes términos de referencia.

Dicha documentación se debe presentar en la Mesa de Partes de la Sección de Ejecución Contractual del Departamento de Abastecimiento de la DIVLOG PNP, sito en Calle San Germán N° 200- Rímac, de lunes a viernes de 8:00 a 16:00 horas.



CAPÍTULO III REQUERIMIENTO

Importante

De conformidad con el numeral 29.8 del artículo 29 del Reglamento, el área usuaria es responsable de la adecuada formulación del requerimiento, debiendo asegurar la calidad técnica y reducir la necesidad de su reformulación por errores o deficiencias técnicas que repercutan en el proceso de contratación.

3.1. TERMINOS DE REFERENCIA

TÉRMINOS DE REFERENCIA

1 DENOMINACIÓN DE LA CONTRATACIÓN:

“SERVICIO DE TRANSMISION PARA LA RED PRIVADA DE LA PNP, EN LAS UNIDADES POLICIALES A NIVEL NACIONAL; SERVICIO DE SEGURIDAD GESTIONADA Y ACCESO A INTERNET”

2 FINALIDAD PÚBLICA

Garantizar la continuidad del servicio de los Datacenter de la DIRTIC PNP (**Activo Crítico Nacional**) para que estos cuenten con una infraestructura de comunicación de datos en banda ancha hacia Internet y fibra oscura entre el sitio principal y Secundario, servicio de housing para el Datacenter secundario PNP y servicio de seguridad de la información, que permita la publicación de las aplicaciones policiales en alta disponibilidad hacia la ciudadanía, así como la interoperabilidad con otras entidades públicas, que redundará en el mejoramiento del servicio de seguridad ciudadana.

3 ANTECEDENTES

La Dirección de Tecnología de Información y Comunicaciones de la Policía Nacional del Perú (DIRTIC-PNP), es la unidad responsable de la administración y monitoreo del Datacenter de la PNP, y de la tecnología que ésta contiene.

De conformidad con lo establecido en el Art. 2ª de la Ley de Contrataciones del Estado, Principios que rigen las contrataciones, es de primordial relevancia mantener la Vigencia Tecnológica de los servicios a contratar bajo estándares de calidad y modernidad tecnológicas necesarias para cumplir con la finalidad pública, bajo este contexto, la División de Informática de la DIRTIC-PNP, ha realizado el levantamiento de información y la actualización correspondiente, a fin de que las soluciones tecnológicas y los servicios de telecomunicaciones cuenten con la infraestructura necesaria para la continuidad del servicio a nivel nacional.

Cabe señalar, que LA ENTIDAD cuenta con sistemas informáticos destinados al soporte tecnológico de los procesos de investigación criminal, de prevención de delitos y faltas; y de atención al ciudadano, en las unidades policiales a nivel nacional, así como la interconexión con otras entidades del estado.

Con Resolución de la Dirección Nacional de Inteligencia Nro. 148.-2022-DINI-01 del 07NOV22, mediante el cual se valida como **Activo Crítico Nacional a la Plataforma Digital de Información Operativa de la Policía Nacional del Perú** (Datacenter de la PNP), uno de cuyos componentes es la Plataforma de Comunicaciones de Datos que se requiere contratar en el presente requerimiento, significando que es una parte muy importante del ACN, en ese sentido, sería un riesgo no contratar el presente servicio el cual pondría en peligro la infraestructura y sistemas que son esenciales e imprescindibles para mantener el desarrollo de capacidades nacionales.

ACTIVIDAD POI

La presente contratación del servicio encuentra enmarcada dentro del POI multianual 2023-2025 de la Policía Nacional del Perú, Objetivo Estratégico Sectorial N° 4: Incrementar la calidad de los servicios en beneficio de los ciudadanos en el ámbito nacional: Objetivos Estratégicos Institucional N°8 Fortalecer la gestión institucional en le Ministerio del Interior: Acciones Estratégicas Institucionales N°8.2 Plan Marioano Santos MS30 implemenetado en la PNP del MININTER.

4 OBJETIVOS DE LA CONTRATACIÓN

4.1 Objetivo General

Contratar a una empresa o empresas que brinden los servicios de transmisión para la Red Privada de la PNP (INTRANET PNP), a nivel nacional, con acceso a internet, interconexión entre el datacenter principal y secundario PNP, servicio de seguridad de la información y servicio de facilities para el Datacenter Principal de la DIRTIC PNP; y, servicio de housing para el Datacenter secundario.

- **Objetivos específicos contar con los servicios de conectividad redundante a Internet, en el Datacenter Principal y de secundario de la PNP.**
- tener alta disponibilidad entre los enlaces de INTERNET en el Datacenter Principal y Secundario PNP.
- tener Optimizado el tráfico de datos hacia internet desde el Datacenter principal y secundario.
- Contar con el servicio de balanceo de enlaces y de sitio.
- tener alta disponibilidad de los switch core de los Datacenter principal y secundario.
- Contar con el servicio de comunicación redundante a través de fibra oscura entre el Datacenter Principal y Secundario de la PNP.
- Contar con una plataforma digital de servicios para transmisión de voz, video y datos, así como plataformas de backbone de fibra y gabinetes para las sedes desconcentradas pnp, a nivel nacional.
- Contar con los servicios de conectividad a Intranet (RED PRIVADA), en las Unidades policiales a nivel nacional.
- Contar con alta disponibilidad entre los enlaces de INTRANET (RED PRIVADA) en el Datacenter Principal PNP y de Secundario.
- Tener el servicio de seguridad de la información y seguridad informática gestionada
- Contar con el Servicio de Gestión de identidades
- Contar con el servicio de housing para el datacenter secundario PNP.
- Contar con el Servicio de Inducción.

5 CARACTERÍSTICAS Y CONDICIONES DEL SERVICIO A CONTRATAR

El presente requerimiento comprende un ítem de 07 componentes, según el siguiente detalle:

SERVICIO DE TRANSMISION PARA LA RED PRIVADA DE LA PNP, EN LAS UNIDADES POLICIALES A NIVEL NACIONAL; SERVICIO DE SEGURIDAD GESTIONADA Y ACCESO A INTERNET



COMPONENTE	SERVICIO
1	Servicio de acceso de internet para la sede principal y secundario (sitio principal y secundario).
2	Servicio de fibra oscura entre el Datacenter principal y secundario de la PNP
3	Plataforma digital de servicios para transmisión de voz, video y datos para las sedes desconcentradas PNP, a nivel nacional
4	Servicio de seguridad de la información, seguridad informática gestionada, adecuación de datacenter
5	Servicio de Gestión de Identidades
6	Servicio de housing para el Datacenter secundario PNP
7	Servicio de Inducción

a. Documentación para acreditar el cumplimiento al momento de la presentación de la oferta:

1. **Se requerirá que, para la presentación de la oferta,** el postor debe acreditar que los bienes ofertados no se deberán encontrar en fin de soporte o End Of Support (EOS), período en el que el producto ya no tiene soporte, lo que se debe evidenciar el postor mediante carta del fabricante, a fin de garantizar lo ofertado, los cuales se podrán presentar en español o en su idioma original. Se aclara que los bienes ofertados hacen referencia a todo el equipamiento físico requerido y a ser instalado por el contratista tanto en el Datacenter Principal, Datacenter Secundario y cada dependencia policial en los Componentes N°1,2,3 y 4 (no aplica los bienes a instalar en la adecuación del Datacenter numeral 5.2.1.5.4.1.23). Esta

exigencia, es a fin de garantizar que el equipamiento propuesto tenga vigencia durante la prestación del servicio contratado.

2. **El Postor deberá presentar en su oferta** una carta del fabricante, en idioma español o en su idioma original, de la solución indicando el cumplimiento de todas las características técnicas descritas para el **optimizador de tráfico y traffic shapping** según el numeral 5.2.1.5.1.6 de los presentes términos de referencia (documentación de carácter obligatorio en la etapa de presentación de oferta).
3. Para garantizar que los **routers y switches** sean de marcas líderes a nivel global en el mercado, las marcas propuestas de routers y switches deberán estar como líderes en el cuadrante de gartner (copia de la publicación oficial de Gartner y la "url" (link) del enlace web respectivo) "Wired and wireless LAN access infrastructure" en los últimos 04 años. Dicha información **deberá ser presentada al momento de la presentación de la oferta mediante carta simple emitida por el postor.**
4. El postor tiene la libertad de incorporar en su oferta técnica una plataforma tercera que realice descifrado del tráfico y cumpla todas las especificaciones indicadas, en caso el NGFW propuesto no pueda realizarlo o no esté diseñado para ello. En caso de optar por esta alternativa, se deberá incluir una plataforma por cada una de las 14 sedes.
Para este caso, el postor **deberá presentar como documentación sustentatoria para su oferta**, una Carta del Fabricante, ya sea en idioma español o en su idioma original, de la plataforma tercera, en la cual se evidencie técnicamente el cumplimiento de la sección DESCIFRADO DE TRÁFICO SSL/TLS según los numerales 5.2.1.5.3.3.10, 5.2.1.5.3.3.11 y 5.2.1.5.4.1.13.
5. Para las Sedes tipo 2, (firewall de próxima generación) en caso la solución propuesta no tenga este módulo de aprendizaje, el postor deberá incluir en su oferta técnica el **servicio de configuración/migración** de todas las políticas de seguridad basadas en puertos, a políticas basadas en aplicaciones, este servicio deberá ser realizado por el área de **servicios profesionales del propio fabricante**. Considerar un estimado de 1,400 políticas de seguridad entre todos los dispositivos de este tipo de sede. Para este caso, el postor deberá presentar como documentación sustentatoria en su oferta, una Carta del Fabricante, en idioma español o en su idioma original, de los equipos de Firewall de próxima generación, en la cual se evidencie que será el fabricante el que realizará la configuración/migración según corresponda considerando lo descrito en el párrafo anterior.
6. Para la solución de firewall de nueva generación, para red externa y red interna, en caso la solución propuesta no tenga este módulo de aprendizaje, el postor deberá incluir en su oferta técnica el **servicio de configuración/migración** de todas las políticas de seguridad basadas en puertos, a políticas basadas en aplicaciones, este servicio deberá ser realizado por el área de **servicios profesionales del propio fabricante**. Considerar un estimado de 1,400 políticas de seguridad entre todos los dispositivos de este tipo de sede. Para este caso, el postor deberá presentar como documentación sustentatoria en su oferta, una Carta del Fabricante, en idioma español o en su idioma original, de los equipos de Firewall de próxima generación, en la cual se evidencie que será el fabricante el que realizará la configuración/migración según corresponda.
7. Para los Firewall de próxima generación para sedes policiales (1001) y Firewall de próxima generación (Complejos 01) (14 sedes en HA), en caso el postor haya integrado tecnologías de terceros externas al NGFW, también se deberá considerar dentro de la propuesta técnica la consola de gestión para dicha tecnología. Para este caso, el postor deberá presentar como documentación sustentatoria en su oferta, una Carta del Fabricante, en idioma español o en



su idioma original, de la tecnología de terceros externas al NGFW que el postor halla integrado, en la cual se evidencie técnicamente el cumplimiento de la sección ADMINISTRACIÓN según los numerales 5.2.1.5.3.3.10 y 5.2.1.5.3.3.11

8. El Postor debe presentar el modelo de la solución propuesta que debe contar con la certificación o reconocimiento como líder en firewall de base de datos, en reportes de analistas como Gartner y/o forrester, **documentación que se debe presentar en el momento de la presentación de la oferta.**

b. Documentación para el perfeccionamiento del contrato

1. Para la solución de firewall de base de datos (numeral 5.2.1.5.4.1.15), el Postor adjudicatario de la buena pro debe asegurar que la solución cuente con un servicio de investigación sobre vulnerabilidades y amenazas informáticas, para lo cual presenta la documentación respectiva (en idioma español o en su idioma original) en el descubrimiento de éstas. El presente requerimiento se validará mediante la presentación de una Declaración Jurada que establezca lo solicitado en los Términos de Referencia.
2. **Para el perfeccionamiento del Contrato** el postor ganador debe incluir los datasheets en idioma original de los dispositivos y/o equipamiento propuesto con su número de parte (part number) correspondiente, licenciamiento, accesorios y componentes necesarios para asegurar el nivel de servicio; el Diagrama técnico detallará la arquitectura y topología de la solución tecnológica propuesta, esto aplica para todos los componentes del ítem 1; asimismo, el contratista no podrá colocar equipos distintos a los indicados en su propuesta técnica durante la etapa de implementación y/o durante la prestación del servicio, a menos que sea por mejora tecnológica, previa aprobación por parte del área usuaria.
3. El postor ganador debe estar autorizado por el MTC para proveer servicios transmisión de datos y/o de internet y/o servicios de valor añadido y, debe ser parte del NAP (Network Access Point) Perú, proveyendo un enlace dedicado con conexión directa y overbooking 1:1 al NAP Perú; en consecuencia, **deberá presentar para el perfeccionamiento del contrato, la documentación necesaria que acredite ser como miembro activo del NAP Perú.**
4. Para la solución de firewall de aplicaciones, debe tener la capacidad de efectuar el parchado virtual de las aplicaciones web, para remediar las vulnerabilidades detectadas y debe permitir tener integración con software de detección de vulnerabilidades **(la solución debe permitir integrarse como mínimo con dos vendedores de scanner de vulnerabilidades que debe ser indicado mediante una carta del fabricante, en idioma español o en su idioma original, que acredite dicha integración, la misma que se debe presentar para el perfeccionamiento del contrato).**
5. Para la solución de Firewall de próxima generación (Complejos 01) (14 sedes en HA) (numeral 5.2.1.5.3.3.10), se deberá enviar una carta emitido por el contratista con el link con documentación pública del fabricante que respalde la comprobación del requerimiento de throughput.
6. Para la solución de Firewall de próxima generación para sedes policiales (1001) distribuidos para sedes del tipo 1 (numeral 5.2.1.5.3.3.11), se deberá enviar una carta emitido por el contratista con el link con documentación pública del fabricante que respalde la comprobación del requerimiento de throughput.
7. Para la solución de FIREWALL DE NUEVA GENERACIÓN, PARA RED EXTERNA Y RED INTERNA (numeral 5.2.1.5.4.1.13), se deberá enviar una carta emitido por el contratista con el link con documentación pública del fabricante que respalde la comprobación del requerimiento de throughput.



8. Para la solución de PROTECCIÓN DE PORTALES WEB Y BASE DE DATOS (numeral 5.2.1.5.4.1.15), se deberá enviar una carta con autorización del fabricante o su representante para comercializar la marca y brindar los servicios solicitados.
9. El personal que realizará la implementación debe estar certificado por el fabricante de los materiales y/o equipamiento a utilizar. Se deberá enviar una declaración jurada demostrando dicho cumplimiento.

5.2 DESCRIPCIÓN Y CANTIDAD DEL SERVICIO A CONTRATAR

5.2.1 "SERVICIO DE TRANSMISION PARA LA RED PRIVADA DE LA PNP, EN LAS UNIDADES POLICIALES A NIVEL NACIONAL; SERVICIO DE SEGURIDAD GESTIONADA Y ACCESO A INTERNET"

5.2.1.1 Descripción y cantidad del servicio a contratar

Para la contratación del servicio de transmisión para la red privada de la PNP, en las unidades policiales a nivel nacional; servicio de seguridad gestionada y acceso a internet, el contratista suministrará los servicios requeridos como prestación del mismo a través de los siguientes componentes:

COMPONENTE	SERVICIO
1	Servicio de acceso de internet para la sede principal y secundario (sitio principal y secundario).
2	Servicio de fibra oscura entre el Datacenter principal y secundario de la PNP
3	Plataforma digital de servicios para transmisión de voz, video y datos para las sedes desconcentradas PNP, a nivel nacional
4	Servicio de seguridad de la información, seguridad informática gestionada, adecuación de datacenter
5	Gestión de Identidades
6	Servicio de housing para el Datacenter secundario PNP
7	Servicio de Inducción.

Todo el equipamiento o soluciones implementados para la prestación de los servicios estarán en situación de administración compartida con el Departamento de Gestión de Centro de Datos de la División de Informática de la PNP a excepción del equipamiento propio del Contratista que no tenga relación con activos de la Entidad.

- **El componente 1, Servicio de acceso de internet para la sede principal y secundario (sitio principal y secundario).** comprende:
 - Servicios de acceso a Internet a través de líneas de datos redundante de banda ancha en el Datacenter principal y secundario, optimización de tráfico – traffic shapping, balanceador de enlaces y balanceador de sitios, así como el equipamiento necesario para su operatividad.
- **El componente 2, Servicio de fibra oscura entre el Datacenter principal y secundario de la PNP** comprende:
 - Servicio de fibra oscura entre el Datacenter principal y secundario de la PNP, estos deben ser redundantes y deben permitir el multiplexado de canales de comunicación entre sitios.

• **El componente 3, Plataforma digital de servicios para transmisión de voz, video y datos para las sedes desconcentradas PNP, a nivel nacional comprende:**

- Servicio de acceso a través de líneas de datos IP VPN de una plataforma digital red tipo MPLS y/o MetroEthernet, para mil dieciocho (1018) sedes de la Policía Nacional del Perú a nivel nacional, según relación detallada en el Anexo A del presente, conformando la red privada de datos de La Entidad denominada Intranet PNP. Cabe señalar que para la ejecución de la prestación existen dos tipos de sedes policiales las mismas que se encuentran detalladas en los anexos Anexo 2-A, Anexo 2-B.
- Servicio de plataforma de backbone de fibra y gabinetes por sede
- Servicio de conexión de enlace MPLS y/o MetroEthernet, para los nodos principal y secundario de la Policía Nacional.
- Servicio de solución firewall para sedes policiales a nivel nacional, así como el equipamiento necesario para su operatividad y funcionamiento en la red de privada de datos de la Entidad.

• **El componente 4, Servicio de seguridad de la información y seguridad informática gestionada comprende:**

El Servicio de seguridad de la información y seguridad informática gestionada, considerando los siguientes componentes:

- Firewall de nueva generación, para red externa y red interna.
- Solución de detección y control de malware avanzado.
- Solución de protección de portales web y base de datos
- Servicio de antispam Firewall y protección ante phishing dirigido
- Servicio de Protección contra ataques de denegación de servicios distribuido
- Servicio de análisis de vulnerabilidades y ciberseguridad de red
- Servicio de Herramienta informática que permitan la prevención de pérdida de información.
- Servicio de antivirus para servidores y usuarios finales de la DIRITC PNP.
- Servicio de SOC Gestionado, Herramienta de Análisis de incidentes y Correlación de logs de seguridad
- Servicio de seguridad de la información.
- Adecuación del Datacenter Principal de la PNP para el equipamiento a proveer requerido en el presente servicio

• **El componente 5, Servicio de Gestión de Identidades comprende:**

- Servicio de envío de mensajes cortos de texto (SMS), considerando una bolsa ilimitada de mensajes SMS durante el periodo de vigencia del contrato. El contratista es libre de brindar servicios como mejora a fin de cumplir con todas las especificaciones solicitadas en el presente componente. Dicha mejora antes de ser aceptada como tal, deberá pasar una prueba de concepto para comprobar que cumple con las necesidades y objetivos de la entidad.

• **El componente 6, Servicio de housing para el Datacenter secundario PNP comprende:**
Servicio de housing del equipamiento de cómputo, seguridad informática y comunicaciones comprendidos en el Datacenter secundario PNP, el contratista debe garantizar la alta disponibilidad en alimentación eléctrica estabilizada, climatización y seguridad física en los ambientes donde residirán los equipos antes indicados. Asimismo, en el presente servicio se considerará lo siguiente:



- Servicio de alojamiento de gabinetes, equipos de comunicación, seguridad y computo.

- **El componente 7, Servicio de inducción comprende:**

Servicio de inducción, el desarrollo continuo de habilidades técnicas y competencias en tecnologías es imperioso, en ese sentido, las inducciones se realizarán en relación a las soluciones y especializaciones afines requeridas para favorecer el mejor desempeño en la utilización de las soluciones propuestas y la administración de recursos adquiridos por la Entidad. Las inducciones iniciaran posteriores a la firma del acta de conformidad de implementación. Todos los servicios de inducción solicitados en los términos de referencia podrán ser brindados de manera presencial o virtual a facultad del contratista, siempre y cuando cumpla con todos los requerimientos solicitados. La coordinación para el inicio de las mismas deberá ser realizada entre el contratista y la PNP, y aprobada por la entidad.

El equipamiento a ser implementado por el contratista deberá operar con la última versión de software y firmware disponible en el mercado, al día de la implementación o con la versión de software y firmware recomendada por el fabricante

El equipamiento tecnológico (Comunicaciones o computacional), empleado como parte del servicio del contratista, a la finalización del contrato, podrá ser replegado o retirado por éste, dentro del plazo de noventa (90) días posteriores a la culminación del contrato. Pasado el plazo de 180 días posteriores a la finalización del servicio, si el contratista no logra replegar o retirar todo el equipamiento tecnológico, la entidad no será responsable de los bienes dejados por el contratista ante un posible desperfecto o pérdida de los mismos.

El equipamiento exclusivamente dedicado a la comunicación local (RED LAN) de cada Unidad Policial, podrá ser replegado o retirado por el contratista, siempre y cuando retire todos los accesorios empleados o utilizados en dicho entorno, así como el resane o reparación correspondiente por la afectación a la infraestructura, de las Unidades Policiales PNP (repintado, porcelanatos, mayólicas, y otros, de los ambientes que fueron utilizados para brindar el servicio).

5.2.1.2 El contratista debe seguir lo siguiente:

- **Coordinación**

El contratista debe trabajar de manera conjunta con el personal técnico del Departamento de Gestión de Centro de Datos – DEPGCD y el Departamento de Gestión de Proyectos, Mantenimiento y Desarrollo de Sistemas Informáticos - DGPMDSI de la División de Informática de la DIRTIC-PNP, supervisando la implementación y ejecución de los servicios correspondientes. La Jefatura de la DIVINF-DIRTIC-PNP, nombrará responsables Técnicos del proyecto, según componente, en un plazo de tres (03) días calendarios posteriores a la suscripción del contrato, comunicándolo vía correo electrónico al contratista, los mismos que serán los encargados de las coordinaciones con el Jefe de Proyecto del contratista, de modo que la implementación se ejecute en forma coordinada.

Por "trabajar de manera conjunta", se entienden que las partes realizaran las coordinaciones y comunicaciones necesarias durante la vigencia del contrato para llevar a cabo de forma eficiente y oportuna, la ejecución del servicio, a través del Jefe de Proyectos por parte del contratista y de los responsables técnicos del Proyecto de la Entidad el cual será nombrado por el Jefe de la DIVINF-DIRTIC-PNP.

- **Backbone**

El backbone de la red del contratista en Lima Metropolitana debe ser redundante y estar basado en una plataforma 100% en fibra óptica, con protocolo de enrutamiento MPLS o el correspondiente para MetroEthernet. El backbone de la red fuera de Lima Metropolitana debe estar basado en infraestructura de fibra óptica; esta debe contar con 3 anillos redundantes interdepartamentales ubicados en el norte, centro y sur del Perú para asegurar la redundancia en el transporte. (Incluir un diagrama de la distribución de los mismos sobre el territorio nacional en el Plan de trabajo).

- **Disponibilidad**

El contratista es responsable de la operatividad de los componentes contenidos en el presente ítem, necesarios para la prestación del servicio, los cuales deben estar disponibles y operativos las veinticuatro (24) horas del día, los siete (07) días a la semana y trescientos sesenta y cinco (365) días del año. El nivel de disponibilidad de servicio debe ser como mínimo del 99.7% para los servicios del componente 1, 2, 4, 5 y 6, medidos mes a mes; y del 99.5% para el componente 3.

Para el **componente 1 y 3**, se define su disponibilidad como la continuidad del servicio requerido en capacidad de transporte y en la capacidad de las funcionalidades requeridas de optimización de tráfico - traffic shapping, balanceador de enlaces, balanceador de sitios, firewall de sedes remotas, switches de comunicación. Asimismo, para el **Componente 2**, se define su disponibilidad como la continuidad del servicio requerido en capacidad de transporte (entre el Datacenter principal y Datacenter secundario) a través de los canales de multiplexación requeridos por la DEPGCD-DIVINF-DIRTIC-PNP.

Para el **componente 4**, su disponibilidad es la continuidad del servicio de monitoreo, automatización, administración y evaluación constante del funcionamiento de los sistemas y equipos de seguridad de los data center principal y secundario, así como los swtches lan y equipos de seguridad de las sedes remotas a nivel nacional, proveyendo soluciones proactivas ante posibles incidentes de seguridad de la información; asimismo, su disponibilidad es garantizar el cumplimiento de los tres principios fundamentales de la seguridad informática, es decir, confidencialidad, integridad y disponibilidad de la información.

- **Gestión del servicio**

El término "avería" se refiere a la pérdida parcial, total o decremento de las soluciones suministradas por el contratista. En ese sentido, el contratista debe proveer un sistema web, correo electrónico y centro de atención telefónico (helpdesk), disponible las veinticuatro (24) horas al día, los trescientos sesenta y cinco (365) días del año, para atención de reportes de incidencias del servicio de acuerdo al SLA contratado.

El Contratista debe proveer al DEPGCD-DIVINF-DIRTIC-PNP el acceso al Centro de atención web a través de un usuario y contraseña que les permita lo siguiente:

- Generar los tickets de averías y monitorear la atención de los mismos, reportados por la Entidad; asimismo, debe permitir la búsqueda del historial de las averías.
- La verificación del consumo de ancho de banda de los circuitos de datos a nivel nacional.
- Visualizar las estadísticas gráficas del tráfico entrante y saliente de cada enlace.
- Visualizar a través de una bandeja de datos los registros de pérdidas de conexión de manera diaria, semanal, mensual y anual, que especifique la hora de inicio y término de la avería.
- Monitorear la velocidad de transmisión de datos en línea.

- Almacenar como mínimo 12 meses de logs/histórico de los circuitos de datos a nivel nacional.

En el caso que ocurra una avería en los servicios contratados, serán reportados al Centro de averías del contratista vía la aplicación online del Centro de atención de averías con interfaz web, correo electrónico o centro de atención telefónico (helpdesk); éste tendrá un plazo máximo de acuerdo al SLA contratado, para la solución del mismo computados desde la comunicación, aun así, éste incluya un RMA.

El plazo para la solución de las averías se contabilizará desde la generación de un ticket por parte de la Entidad. Para ello la entidad antes de generar un ticket de avería previamente se realizará procedimientos básicos de revisión (verificación de fluido eléctrico, verificación del cableado estructurado, conexiones de equipamiento de comunicaciones y seguridad, y otros que pudieran ser necesarios para el diagnóstico del incidente), con el fin de describir correctamente la avería. En aquellos casos que se presenten demoras por parte de la entidad, el contratista debe coordinar con la Unidad Usuaria para que dicha demora sea considerada como parada de reloj y dicho tiempo será descontado del tiempo de atención de la avería. La parada del reloj entre el contratista y la unidad usuaria será necesario realizarla mediante el envío al correo electrónico institucional. Adicionalmente, se podrá adjuntar la evidencia mediante fotografía y/o videos para justificar las demoras por parte de la entidad; no serán exigidas constancias adicionales ni tramite burocráticos y/o legales.

El Contratista está obligado a mantener respaldado la información del histórico del estado de las soluciones propuestas durante la ejecución del Contrato, con la finalidad de emitir reportes a requerimiento de la Entidad o el DEPGCD.

En el caso de presentarse averías, el contratista deberá informarlo a través de correo electrónico al DEPGCD-DIVINF-DIRTIC-PNP, asimismo, notificará su resolución por el mismo medio, bajo la observancia de las penalidades existentes.



5.2.1.3 LA VIGENCIA DEL CONTRATO

5.2.1.3.1 Plazo de implementación. - Inicia a partir del día del siguiente de suscrito el contrato, dándose inicio a la implementación y puesta en funcionamiento del servicio en un plazo máximo de SEIS (06) MESES.

5.2.1.3.2 Plazo para suscripción de la Conformidad. - Culminada la etapa de implementación y puesta en funcionamiento, el Jefe del DEPGCD-DIVINF-DIRTIC PNP suscribirá el Acta de Conformidad de la implementación realizada, previo informe del personal técnico responsable de las Secciones de Operaciones, Redes y Seguridad Informática, e infraestructura de Servidores, en un plazo máximo de SIETE (07) días calendarios.

5.2.1.3.3 Inicio del Servicio. - inicia a partir del día siguiente de suscrita el Acta de conformidad de implementación del servicio, dándose inicio a la ejecución contractual para la prestación del **"SERVICIO DE TRANSMISION PARA LA RED PRIVADA DE LA PNP, EN LAS UNIDADES POLICIALES A NIVEL NACIONAL; SERVICIO DE SEGURIDAD GESTIONADA Y ACCESO A INTERNET"**, por el periodo de treinta y seis (36) meses, la misma que está constituida por los siguientes componentes:

5.2.1.3.3.1 1.- Servicio de acceso de internet para la sede principal y secundario (sitio principal y secundario).

5.2.1.3.3.2 2.- Servicio de fibra oscura entre el Datacenter principal y secundario de la PNP

El consolidado de la cantidad de líneas de datos a internet, equipos de comunicaciones, equipos de seguridad, fibra oscura para los datacenter principal y secundario (**Componente 1 y 2**), son los siguientes:

Nº	DATACENTER	PRINCIPAL	SECUNDARIO	TOTAL
1	LÍNEA DE FIBRA ÓPTICA A INTERNET DE 2Gbps	2	2	4
2	ROUTER DE INTERNET	2	2	4
3	SWITCHES PARA COMUNICACIÓN LAN/WAN	11	5	16
4	BALANCEADORES DE ENLACES	1	1	2
5	OPTIMIZADOR DE TRAFICO Y TRAFFIC SHAPPING	1	1	2
6	BALANCEADOR DE SITIOS	1	1	2
7	LÍNEA DE FIBRA OSCURA DE 40 Gbps	1	1	2
8	MUX DE FIBRA ÓPTICA	1	1	2
9	SWITCH CORE LAN	1	1	2

5.2.1.3.3.3

3.- Plataforma digital de servicios para transmisión de voz, video y datos para las sedes desconcentradas PNP, a nivel nacional

El consolidado de la cantidad de líneas de datos a internet, equipos de comunicación, equipos de seguridad (**Componente 3**), es el siguiente:

Nº	SERVICIO Y/O EQUIPAMIENTO	CANTIDAD
1	LINEAS DE FIBRA OPTICA CON CONEXIÓN A INTRANET E INTERNET DE 100 Mbps	927
2	LINEAS DE FIBRA OPTICA CON CONEXIÓN A INTRANET E INTERNET DE 150 Mbps	32
3	LINEAS DE FIBRA OPTICA CON CONEXIÓN A INTRANET E INTERNET DE 200 Mbps	41
4	LINEAS DE FIBRA OPTICA CON CONEXIÓN A INTRANET E INTERNET DE 300 Mbps	2
5	LINEAS DE FIBRA OPTICA CON CONEXIÓN A INTRANET E INTERNET DE 400 Mbps	16
6	LINEAS DE FIBRA OPTICA CON CONEXIÓN A LA INTRANET PNP (CABECERA VPN) DE 05 Gbps	4
7	FIREWALL DE PRÓXIMA GENERACIÓN (COMPLEJOS 01)	28
8	FIREWALL DE PRÓXIMA GENERACIÓN PARA SEDES POLICIALES	1002
9	SWITCH CORE L3 LAN PARA SEDES TIPO 2	13
10	SWITCH LAN DE DISTRIBUCIÓN SEDES TIPO 2	30
11	SWITCH LAN PARA SEDES TIPO 1 - A	137
12	SWITCH LAN PARA SEDES TIPO 1 - B	891

Se debe considerar el 5% de equipamiento tipo spare o de respaldo para las siguientes soluciones o equipos requeridos; (excepto para el equipamiento con una cantidad menor a VEINTE (20), se considerará como mínimo UN (01) equipo tipo spare o de respaldo):

- Firewall de próxima generación (Complejos 01)
- Firewall de próxima generación para sedes policiales
- Switch core L3 LAN para sedes tipo 2
- Switch LAN de distribución sedes tipo 2
- Switch LAN para sedes tipo 1 – A
- Switch LAN para sedes tipo 1 – B
- Líneas de Fibra Óptica con conexión a intranet e internet (ROUTER)

Los equipos tipo spare deberán ser almacenados por el contratista y los números de serie del dicho equipamiento debe ser parte del informe final de implementación.

5.2.1.3.3.4

4.- Servicio de seguridad de la información y seguridad informática gestionada.

El consolidado de la cantidad de equipos de seguridad y monitoreo que se utilizaran para brindar el presente servicio, es el siguiente:

Componente 4

Nº	SERVICIO Y/O EQUIPAMIENTO	CANTIDAD
1	FIREWALL DE NUEVA GENERACIÓN, PARA RED EXTERNA Y RED INTERNA	4
2	EQUIPO DE DETECCIÓN Y CONTROL DE MALWARE AVANZADO	2
3	EQUIPO DE PROTECCIÓN DE PORTALES WEB	2
4	EQUIPO DE PROTECCIÓN DE BASE DE DATOS	2
5	EQUIPO SPAM FIREWALL Y PROTECCIÓN ANTE PHISHING DIRIGIDO	2
6	EQUIPO DE PROTECCIÓN CONTRA ATAQUES DE DENEGACIÓN DE SERVICIO DISTRIBUIDOS	2
7	ANÁLISIS DE VULNERABILIDADES Y CIBERSEGURIDAD DE RED	1
8	HERRAMIENTA INFORMÁTICA PARA PREVENCIÓN DE PERDIDA DE INFORMACIÓN EN LA RED	2
9	SOLUCIÓN DE ANTIVIRUS PARA SERVIDORES Y ENDPOINT DEL DATACENTER PRINCIPAL	1000
10	SERVICIO DE SOC GESTIONADO, HERRAMIENTA DE ANÁLISIS DE INCIDENTES Y CORRELACIÓN DE LOGS DE SEGURIDAD	1
11	SERVICIO DE SEGURIDAD DE LA INFORMACIÓN	1

Servicio de adecuación del Datacenter de la PNP:

5.2.1.3.3.5

5. Gestión de Identidades: Proveerá el servicio gestión de Identidades que contempla la habilitación del servicio de envío de mensajes cortos de texto (SMS), considerando una bolsa ilimitada de mensajes SMS durante el periodo de vigencia del contrato.

5.2.1.3.3.6

6.- Proveerá el Servicio de housing para el Datacenter secundario PNP:

Implementación y habilitación de los servicios del data center secundario, Servicio de alojamiento de Gabinetes y equipos.

5.2.1.3.4 **Respecto a las visitas técnicas:**

La empresa participante presentará su Carta de representación en la cual consignará el nombre y apellido y DNI de los visitantes que realizarán la visita técnica, así como la ficha de registro de estar inscritos en el SEACE como participantes al procedimiento de selección; Información que deberá ser presentada en Mesa de Partes del Departamento de Abastecimiento de la DIVLOG PNP, sito en Calle San Germán N° 200 – Rímac (3er piso), de lunes a viernes en el horario de 08:00 a 16:00 horas

La visita técnica en caso de que el participante considere necesario, se realizará, previa coordinación con la División de Informática de la Dirección de Tecnología de la Información y Comunicaciones PNP (DIRTIC PNP) Teléfono: 943694761 Ceopol DIRTIC PNP, desde la fecha de la convocatoria hasta un día antes de la fecha de presentación de su oferta, días laborables de lunes a viernes, en el horario de 10:00 a 16:00 horas. La PNP brindará una respuesta de confirmación al día de visita, dentro del plazo máximo de tres (03) días calendarios, desde presentada la solicitud.

5.2.1.3.5 **Garantía del servicio:**

El CONTRATISTA debe brindar la garantía de los bienes para mantener los niveles de servicio en base a los SLA descritos en el presente termino de referencia con garantía "on site" (en el sitio) disponible durante la vigencia del contrato (36 MESES), contados a partir del día siguiente de la emisión del Acta de Conformidad de la implementación.

Se precisa que el termino garantía "on site" se refiere a la garantía del fabricante, que debe estar vigente durante la ejecución del plazo contractual y en el sitio donde se brinde los servicios.

Para los bienes que sea aplicable, el contratista deberá permitir a los usuarios que designe el DEPGCD-DIVINF-DIRTIC-PNP, el acceso a través de una interfaz web al Centro de Atención Técnica del Fabricante, en caso lo requiera, así como permitirle acceder a descargar actualizaciones de software de la página web del fabricante, para ello debe entregarse usuario y contraseña o desde otro medio el cual será informado por el fabricante a la Entidad, sin costo adicional para la Entidad y tendrá vigencia dentro del alcance de la garantía. Asimismo, para los equipos de conectividad/seguridad y switches el área usuaria podrá solicitar al contratista que realice la actualización del software.

5.2.1.4 **Actualización tecnológica:**

En relación a los equipos de conectividad, en caso de ocurrir el lanzamiento al mercado, por el fabricante, de una nueva versión para la misma marca y producto, que a la vez no garantice a futuro el soporte post venta del(os) producto(s) y/o componente(s) y/o servicio(s) inicialmente propuesto, es decir el(los) producto(s) y/o componente(s) y/o servicio (s) inicialmente propuesto pierden vigencia tecnológica, entonces, estamos ante un caso de "Actualización Tecnológica", el cual se fija en un plazo máximo hasta de treinta (30) días calendarios luego de firmado el contrato con la Entidad.

Si alguna de las partes advierte la existencia de actualización tecnológica, dentro del plazo previsto, se obligan a realizar la comunicación correspondiente a fin de que el contratista cumpla con lo establecido en el párrafo anterior.

En caso de presentarse una "Actualización Tecnológica" en el(los) producto(s) y/o componente(s) y/o servicio(s) propuestos, el Contratista debe proporcionar el(los) nuevo(s) producto(s) y/o componente(s) y/o servicio(s), siempre y cuando cuente con la aprobación de LA ENTIDAD, ello

no debe alterar los plazos de entrega inicialmente propuesto y no representar cargo adicional alguno para LA ENTIDAD.

DOCUMENTACIÓN QUE SERVIRÁ PARA ACREDITAR EL CUMPLIMIENTO DE LOS COMPONENTES DEL TÉRMINO DE REFERENCIA.

Se requerirá que, para la presentación de la oferta, el postor debe acreditar que los bienes ofertados no se deberán encontrar en fin de soporte o End Of Support (EOS), período en el que el producto ya no tiene soporte, lo que se debe evidenciar el postor mediante carta del fabricante, a fin de garantizar lo ofertado, los cuales se podrán presentar en español o en su idioma original. Se aclara que los bienes ofertados hacen referencia a todo el equipamiento físico requerido y a ser instalado por el contratista tanto en el Datacenter Principal, Datacenter Secundario y cada dependencia policial en los Componentes N°1,2,3 y 4 (no aplica los bienes a instalar en la adecuación del Datacenter numeral 5.2.1.5.4.1.23). Esta exigencia, es para que se garantice que el equipamiento propuesto tenga el soporte necesario durante la vigencia del contrato.

5.2.1.5 Requerimientos técnicos mínimos

5.2.1.5.1 COMPONENTE 1: SERVICIO DE ACCESO DE INTERNET PARA EL NODO CENTRAL Y SECUNDARIO (SITIO PRINCIPAL Y SECUNDARIO)

La activación de estos circuitos está sujeto a la implementación del servicio, previa suscripción del acta correspondiente.

El inicio de la contraprestación mensual se encuentra sujeto al inicio del servicio, previa suscripción del Acta de conformidad correspondiente.

El Diagrama sugerido por La Entidad para la implementación de este Componente es el siguiente:

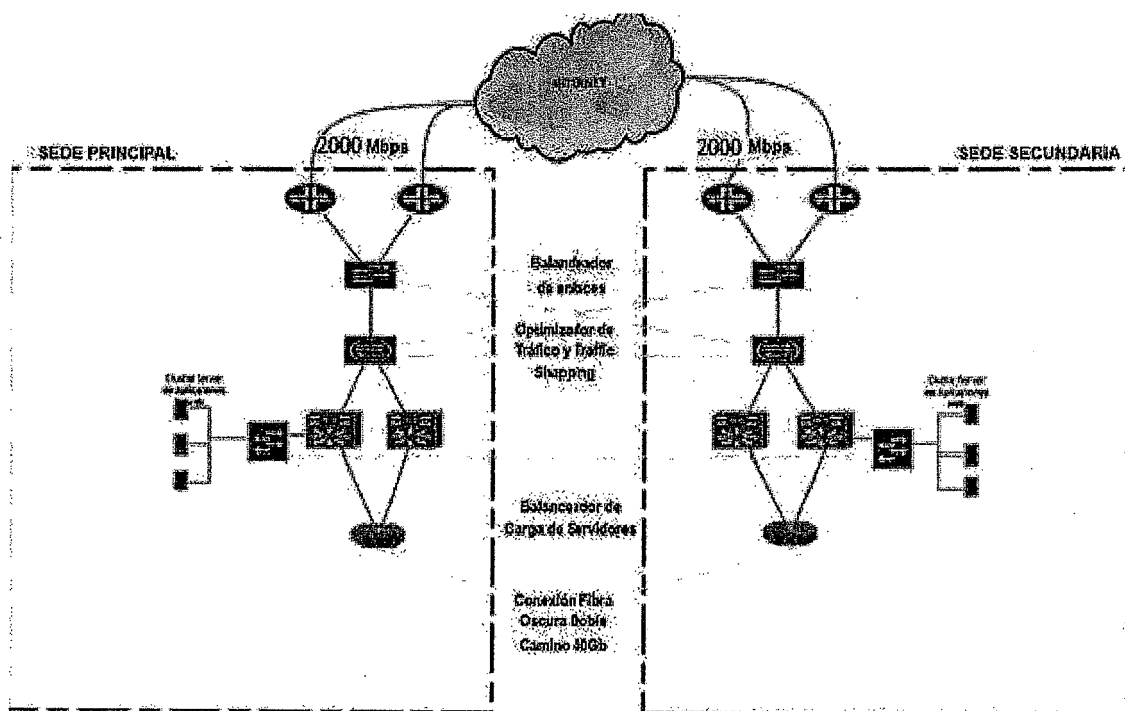


Diagrama N° 01 Diseño sugerido del Servicio de Acceso a Internet para el nodo central y secundario (Sitio principal y secundario)

5.2.1.5.1.1 Datacenter Principal (Sitio Principal)

- Dos (02) circuitos de acceso a Internet, una como línea dedicada principal y otra como contingencia, de tipo simétrica, de 2000 Mbps de ancho de banda cada una, con tasa de acceso garantizada al 100% (overbooking 1:1) empleando como medio físico fibra óptica. El contratista debe garantizar que el ancho de banda proporcionado sea el mismo desde la puerta de enlace hasta la salida internacional, asimismo este enlace debe contar con un mínimo de 256 direcciones IPv4 públicas en prefijo /24, válidos para ser utilizadas por la Entidad en la publicación de sus aplicaciones y/o servicios.
- Todos los equipos routers y switches requeridos en el Componente N°01 para el Datacenter Principal deberán contar con vigencia tecnológica o en su defecto proveer equipamiento nuevo, que garanticen los niveles de SLA exigidos.
- La marca de los equipos routers y switches serán de la misma marca, para optimizar un mejor rendimiento del sistema, al ser un servicio de nivel crítico, no pudiendo la entidad aceptar ningún fallo a nivel de interoperabilidad de marcas. Asimismo, para garantizar que el postor proponga marcas líderes a nivel global en el mercado, las marcas propuestas de routers y switches deberán estar como líderes en el cuadrante de gartner "Wired and wireless LAN access infrastructure" en los últimos 04 años.
- El postor ganador debe estar autorizado por el MTC para proveer servicios transmisión de datos y/o de internet y/o servicios de valor añadido y, debe ser parte del NAP (Network Access Point) Perú, proveyendo un enlace dedicado con conexión directa y overbooking 1:1 al NAP Perú; en consecuencia, deberá presentar para el perfeccionamiento del contrato, la documentación necesaria que acredite ser como miembro activo del NAP Perú.
- El contratista como parte del proceso de implementación del servicio debe implementar y/o subcontratar dos (02) salidas internacionales con distintos proveedores TIER-1 que se encuentren configurados en alta disponibilidad, y ambos accesos con redundancia. Las capacidades de estos enlaces deben asegurar un overbooking 1:1 para la salida a Internet en el tramo local y en la salida internacional, debiéndose asegurar que estas interconexiones tienen independencia de operación y conexión hacia la red de su proveedor TIER 1.
- El contratista será responsable de efectuar e instalar las herramientas y actividades necesarias para la correcta implementación del servicio (el contratista debe adjuntar a su plan de trabajo el diagrama final de su diseño dentro del plazo establecido según cronograma de actividades por día consignada en el numeral 5.9.2 con la finalidad que sea aprobado por el Jefe del DEPGCD-DIVINF-DIRTIC-PNP.
- La línea de Internet estará en la capacidad de operar en modo activo/activo, con la línea de Internet del sitio secundario (como un clúster), o activo/pasivo siempre que el área usuaria lo solicite; el plazo para la reconfiguración de los enlaces, una vez que sea notificado, formalmente el cambio, será de 7 días. esta actividad estará sujeta al cronograma de implementación establecido en las bases o durante la ejecución del servicio según requerimiento de la Entidad. En tal sentido, la Entidad será responsable de la configuración de redundancia del equipamiento informático a nivel de infraestructura de servidores, storage y base de datos. El contratista debe considerar la implementación del equipamiento de comunicaciones y conmutación para tal fin.

5.2.1.5.1.2 Datacenter Secundario (Sitio secundario)

- Dos (02) circuitos de acceso a Internet, una como línea dedicada principal y otra como contingencia, de tipo simétrica, de 2000 Mbps de ancho de banda, con tasa de acceso garantizada al 100% (overbooking 1:1) empleando como medio físico fibra óptica, que debe llegar por una ruta y a un nodo diferente de la línea

dedicada a internet del Nodo Central (Datacenter Principal). El contratista debe garantizar que el ancho de banda proporcionado sea el mismo desde la puerta de enlace hasta la salida internacional, asimismo este enlace debe contar con un mínimo de 256 direcciones IPv4 públicas en prefijo /24, válidos para ser utilizadas por la Entidad en la publicación de sus aplicaciones.

- Todos los equipos routers y switches requeridos en el Componente N°01 para el Datacenter Secundario deberán contar con vigencia tecnológica o en su defecto proveer equipamiento nuevo, que garanticen los niveles de SLA exigidos.
- La marca de los equipos routers y switches serán de la misma marca, para optimizar un mejor rendimiento del sistema, al ser un servicio de nivel crítico, no pudiendo la entidad aceptar ningún fallo a nivel de interoperabilidad de marcas. Asimismo, para garantizar que el postor proponga marcas líderes a nivel global en el mercado, las marcas propuestas de routers y switches deberán estar como líderes en el cuadrante de gartner "Wired and wireless LAN access infrastructure" en los últimos 04 años.
- El postor debe estar autorizado por el MTC para proveer servicios transmisión de datos y/o de internet y/o de servicios de valor añadido y, debe ser parte del NAP (Network Access Point) Perú, proveyendo un enlace dedicado con conexión directa y overbooking 1:1 al NAP Perú. En caso que, el postor confirme ser parte del NAP (Network Access Point) Perú, deberá presentar para el perfeccionamiento del contrato, la documentación necesaria que acredite ser miembro activo del NAP Perú
- El contratista como parte del proceso de implementación del servicio debe implementar y/o subcontratar dos (02) salidas internacionales con distintos proveedores TIER-1 que se encuentren configurados en alta disponibilidad, y ambos accesos con redundancia. Las capacidades de estos enlaces deben asegurar un overbooking 1:1 para la salida a Internet en el tramo local y en la salida internacional, debiéndose asegurar que estas interconexiones tienen independencia de operación y conexión hacia la red de su proveedor TIER 1.
- El contratista será responsable de efectuar e instalar las herramientas y actividades necesarias para la correcta implementación del servicio (el contratista debe adjuntar a su plan de trabajo el diagrama inicial de su diseño dentro del plazo establecido según cronograma de actividades por día consignada en el numeral 5.9.2, con la finalidad que sea aprobado por el Jefe del DEPGCD-DIVINF-DIRTIC-PNP); y a la culminación de la implementación del servicio, se presentará un Diagrama Final de Diseño, adjunto al Informe final de implementación, el mismo que estará sujeto a validación similar que el inicial.
- La línea de Internet del sitio secundario estará en la capacidad de operar en modo activo/activo, con la línea de Internet del sitio principal (como un clúster), o activo/pasivo siempre que el área usuaria lo solicite; el plazo para la reconfiguración de los enlaces, una vez que sea notificado, formalmente el cambio, será de 7 días. esta actividad estará sujeta al cronograma de implementación establecido en las bases o durante la ejecución del servicio según requerimiento de la Entidad. En tal sentido, la Entidad será responsable de la configuración de redundancia del equipamiento informático a nivel de infraestructura de servidores, storage y base de datos. El contratista debe considerar la implementación del equipamiento de comunicaciones y conmutación para tal fin.



5.2.1.5.1.3 Equipamiento

5.2.1.5.1.4 EQUIPO ROUTER

Se requiere cuatro (04) equipos router dos para cada sitio, como mínimo con las siguientes características técnicas:

- Deberá disponer de al menos 06 interfaces 1GE RJ45.
- Deberá disponer de al menos 04 interfaces 10 GE SFP+.
- Deberá soportar throughput de 3Gbps full dúplex (o 6Gbps agregado), con crecimiento de hasta el 50% del ancho de banda contratado.
- Deberá contar con 01 puerto de consola RJ45 y 01 puerto USB.
- Deberá contar con memoria RAM de 4 GB de capacidad.
- Fuente de poder interna y/o externa redundante AC.
- Deberá contar con un procesador multi-core.
- Deberá soportar DHCP server/client/relay, PPPoE server/client, NAT, y gestión de sub-interfaces.
- Deberá soportar los estándares IEEE 802.1p, IEEE 802.1q, IEEE 802.3, gestión de VLAN, VLAN aggregation (opcional), gestión de MAC, protocolos STP/RSTP.
- Soporte de políticas de enrutamiento IPv4 e IPv6, rutas estáticas IPv4 e IPv6, protocolos RIP, RIPng, OSPF y OSPFv3, IS-IS, IS-IS para IPv6, BGP y BGP4+.
- Soporte, de manera opcional, de protocolos de tunelización en IPv6, tales como generación de túneles, túneles automáticos, túneles GRE, túneles IPv6 over IPv4, túneles 6 to 4 e ISATAP
- Para el caso haya dos o más usuarios administradores realizando configuraciones de manera simultánea, los cambios realizados serán independientes entre ellos. Por lo tanto, cuando un usuario administrador autorice el cambio, el sistema no considerará la información ingresada por los otros administradores.
- En caso el usuario administrador autoriza ejecutar al sistema, la configuración realizada por este, el sistema deberá validarla. En caso de encontrar algún error sobre la configuración, ésta no será ejecutada y el sistema adicionalmente deberá indicar claramente cuál es el error o errores encontrados para su posterior corrección.
- El usuario administrador del equipo debe decidir cuándo aplicar los cambios en la configuración. Los comandos ingresados no se ejecutarán de forma inmediata, sino únicamente cuando el administrador lo autorice, garantizando un mejor control y gestión de la configuración.
- Si hay múltiples administradores configurando simultáneamente, los cambios deben ser independientes, y el sistema no debe considerar la información ingresada por otros al aplicar una modificación, con el fin de garantizar un mejor control en la gestión de la configuración.
- Cuando el usuario administrador autorice la ejecución de la configuración, el sistema debe validarla. Si se detecta un error, la configuración no debe ejecutarse y el sistema debe indicar claramente los errores encontrados para su corrección, con el fin de garantizar un mejor control en la gestión de la configuración.



5.2.1.5.1.5 EQUIPOS SWITCH CORE LAN CAPA 3

El contratista debe brindar dos (02) equipos SWITCH CORE L3, uno (01) en cada sitio, principal (01) y secundario (01)", haciendo un total de dos (02) con las siguientes características técnicas mínimas.

EQUIPO DE SWITCH CORE SEDE PRINCIPAL Y SEDE SECUNDARIA CANTIDAD: DOS (02)	
DESCRIPCIÓN	DETALLES TÉCNICOS
Hardware	<ul style="list-style-type: none"> • Switches Core de tipo Chasis. • Mínimo capacidad de conmutación: 5.2 Tbps • Número de slots: 08 • Número de slots para tarjetas: 04 • Número de slots de supervisión: 02 • Redundancia de supervisión: Si • Número de bahías para energía: 04 • Número de bahías para ventiladores: 02 • Unidades de rack: máximo 8 RU por cada Switch. • Mínimo 144 puertos SFP+ (1/10G) • Mínimo 16 puertos 40/100G QSFP28 • Deberá tener un puerto de administración fuera de banda, tipo RJ-45 • Deberá tener un puerto serial tipo RS-232 o RJ45 o micro USB • Deberá tener un puerto tipo USB • Todos los puertos deberán soportar tasas completas (full rate) independiente al tamaño de paquetes transmitidos • Deberá tener instalado un sistema de alimentación de energía redundante con capacidad de ser retirado en caliente (Hot Swap) • Las fuentes de energía deberán soportar 200-240 VAC a 60 Hz. • Se deberán incluir los cables de energía eléctrica con terminación tipo C13 (tomas de energía utilizadas dentro del Centro de Datos) • Soporte de fabricante, el cual garantice una atención con el centro de soporte de fabricante 24x7 y reemplazo de partes, con tiempo de respuesta menor a 4 horas. EL CONTRATISTA ganador deberá gestionar la atención al centro de Soporte del fabricante. • Todos los puertos de los Switch solicitados deberán encontrarse activos, sin que se inhabilite unos a otros
Funcionalidades	<ul style="list-style-type: none"> • Toda funcionalidad de software, establecida para el funcionamiento del switch de red y que cumpla con las características técnicas descritas a continuación, deberá contar con el respectivo licenciamiento y la capacidad de actualizarse sin incurrir en costos adicionales para la entidad, durante el plazo de responsabilidad del CONTRATISTA.



EQUIPO DE SWITCH CORE SEDE PRINCIPAL Y SEDE SECUNDARIA
CANTIDAD: DOS (02)

DESCRIPCIÓN	DETALLES TÉCNICOS
	<ul style="list-style-type: none"> • Contar con la última versión estable del sistema operativo recomendado por el fabricante, la cual se deberá actualizar durante el plazo máximo de responsabilidad del CONTRATISTA, sin que ello incurra en costos adicionales para la entidad. • Contar con un sistema operativo modular, que permita la separación del plano de control y del plano de datos. • Permitir exportar copias de seguridad de configuración mediante FTP o SFTP, TFTP y/o USB y/o SCP. • Soporte de interfaces de programación de aplicación abiertas (APIs) y scripting. • Deberá tener licenciamiento habilitado para las tecnologías de enrutamiento y switching tales como BGP, GRE o IS-IS, MSDP, OSPF, PBR, PIM SSM o PIM SM, VRF, VXLAN, EVPN o SRv6. • Capacidad instalada de Balanceo de carga persuasivo y Ruteo Tenant multicast o ECMP • Deberá tener la capacidad de operar en diversos modos, tales como: Core, Agregación y Gateway. • Deberá soportar la carga del firmware y/o parches de seguridad en caliente, es decir, sin que sea necesario desconectar el switch de la red, detener servicios para el usuario final o apagar el equipo, siempre que se defina una alta disponibilidad. • Operatividad en capa 2 y capa 3. • Soporte para enrutamiento basado en políticas (PBR). • Soporte para listas de Control de Acceso en Capa 2 (ingress) y 3 (ingress y egress): 700 entradas de ingreso y 1000 entradas de egreso. • Rutas IPv4 multicast: 4,094 • Entradas de MAC: mínimo 64,000 • Número de Port Channels o enlaces agregados: 32 • Número de VLAN: 4000 • Número de instancias VRF: 256 • Enrutamiento unicast, multicast basado en hardware, es decir, que utilice recursos de hardware destinados para tal finalidad, sea mediante ASIC o mecanismos de reservación de recursos de hardware del sistema.
Cumplimiento de normas, Estándares	<ul style="list-style-type: none"> • RFC-791 IPv4 • RFC-792 ICMP • RFC-793 TCP • RFC-826 ARP • RFC-8200 o IPv6 • RFC-1901 o SNMPv2c • RFC-3414 SNMPv3 • RFC-2328 OSPFv2 • RFC-5340 OSPFv3 • RFC-2453 RIPv2 • RFC-1105 BGP o BGP4 • RFC-4271 BGP-4 RFC-5798 VRRP



EQUIPO DE SWITCH CORE SEDE PRINCIPAL Y SEDE SECUNDARIA CANTIDAD: DOS (02)	
DESCRIPCIÓN	DETALLES TÉCNICOS
	<ul style="list-style-type: none"> • RFC-7348 VXLAN • RFC-7432 BGP MPLS-Based Ethernet VPN (EVPN) o EVPN • RFC-2236 IGMP v2 • RFC-3376 IGMP v3 • RFC-7761 PIM-SM • RFC-1256 IPv4 ICMP Router Discovery • RFC-2138 o RFC-2865 o RADIUS Authentication • RFC-2139 o RFC-2866 o RADIUS Accounting • IEEE 802.3ab 1000BASE-T, Gigabit sobre cobre. • IEEE 802.3z 1000BASE-X, Gigabit sobre fibra. • IEEE 802.3ae 10 Gigabit Ethernet • IEEE 802.3ba 40/100 Gigabit Ethernet • IEEE 802.1d, STP • IEEE 802.1q, trunking • IEEE 802.1s, MSTP • IEEE 802.1w, RSTP • IEEE 802.1ab LLDP • IEEE 802.3ad, LACP • IEEE 802.3x, Control de flujo. • IEEE 802.1p o PCP, Calidad de Servicio y DSCP
Gestión y Monitoreo	<ul style="list-style-type: none"> • Administración remota mediante SSH versión 2, HTTPS • Administración local mediante conexión serial. • Permitir múltiples sesiones simultáneas de conexión remota. • Permitir múltiples niveles de privilegios de acceso. • Registro de eventos vía Syslog y Syslog Remoto. • Soporte de protocolos de transferencia de archivos TFTP y/o SFTP. • Soporte para permitir procesos de debug para el análisis detallado de fallas y tráfico de datos. • Soporte para contar con herramientas que permitan recolectar datos para el análisis de tráfico en tiempo real: Debug de paquetes, Consulta a Tabla ARP, etc. Dichas herramientas podrán ser internas (mediante el switch de red) y/o externas (mediante una consola de gestión). • Análisis de tráfico usando protocolos tipo Netflow y/o sFlow en todos los puertos de los switches, sin que ello impacte en el procesamiento del equipo. • Brindar la funcionalidad de "puerto espejo" por puerto físico o grupo de puertos. • Soporte de diagnóstico mediante línea de comandos, que permita verificar el hardware usando diferentes pruebas predefinidas en demanda o calendarizadas.
Accesorios que deben incluirse (por cada switch)	Debe incluir por equipos: <ul style="list-style-type: none"> • Kit de Montaje • Un (01) cable de Consola.



EQUIPO DE SWITCH CORE SEDE PRINCIPAL Y SEDE SECUNDARIA CANTIDAD: DOS (02)	
DESCRIPCIÓN	DETALLES TÉCNICOS
core)	<ul style="list-style-type: none"> • Todas las características solicitadas deben estar habilitadas • Incluir 144 transceivers de SFP+/LC 10Gbps. • Incluir 16 transceivers QSFP+ y/o QSFP28 de 40/100 Gbps.
Condiciones mínimas de la provisión	<ul style="list-style-type: none"> • Se deberá trasladar la configuración de los switches Core a satisfacción de la entidad. • Los switches de red deberán ser configurados con los parámetros de enrutamiento que la entidad defina, debiendo restablecer la conectividad hacia la red de servidores, red de distribución, la Internet y redes remotas de usuarios. • Los switches de red deberán ser configurados con los parámetros SNMPv2c y SNMPv3 que la entidad disponga. • Los switches de red deberán ser configurados con los parámetros de ruteo hacia los switches de distribución que la entidad disponga. • Al finalizar el contrato, estos equipos Switch Core pasarán a ser propiedad de la entidad sin costo adicional, debiendo coordinar con la entidad el procedimiento para la transferencia de la propiedad.

5.2.1.5.1.6 EQUIPO OPTIMIZADOR DE TRÁFICO Y TRAFFIC SHAPPING

Se requiere una solución de optimizadores de tráfico y traffic shapping de propósito específico (No aceptan soluciones embebidas sobre enrutadores, firewalls, NGFW, UTM, entre otras) para optimizar el tráfico de la WAN (Publicaciones) y LAN (Usuarios internos) por cada datacenter (Sitio principal y sitio secundario) como mínimo 02 appliance. Cada optimizador debe cumplir con las siguientes características:

- Deberá contar con al menos 3,000 aplicaciones identificadas.
- Características del equipo:
 - Dos (02) bridges bypass interno de 10G, es decir, 4 puertos 10GE fibra multimodo,
 - Licenciado a 8 Gbps de throughput simétrico inicialmente con capacidad de poder incrementar (con licenciamiento adicional) a 15Gbps como mínimo.
 - Soporte de 5 millones de flujos concurrentes.
 - Soporte de 3 millones de paquetes por segundo.
 - El equipo deberá contar con fuente redundantes
- La solución deberá brindar Calidad de Servicio (QoS) para proteger el ancho de banda de aplicaciones críticas y contener el tráfico no deseado tanto en IPv4 e IPv6.



- Permitir la generación de políticas de control de ancho de banda para el tráfico entrante y saliente de manera independiente para las aplicaciones y usuarios, deben permitir: priorización de tráfico (al menos 10 niveles de prioridades), definir un mínimo ancho de banda garantizado y un máximo ancho de banda permitido
- Deberá soportar la creación de políticas de control basadas en tiempo.
- Deberá soportar la creación de políticas de control basadas en usuarios.
- La solución deberá integrarse con los Directorios Activos (AD) de la Entidad con la finalidad de manejar políticas basadas en usuarios.
- Permitir la creación de aplicaciones personalizadas de la propia Entidad para su visibilidad y control.
- La solución deberá tener capacidad de identificar y mostrar los sistemas operativos de los dispositivos que están que cursan tráfico a través del equipo
- Deberá agrupar aplicaciones en categorías existentes como: Redes Sociales, P2P, Actualizaciones de Software, Video y Música, entre otros. Así como también se debe poder crear grupos de aplicaciones personalizadas.
- Deberá permitir la creación de los siguientes reportes históricos basados en gráficos para un periodo de tiempo configurable:
 - o Tráfico de descarga y de subida
 - o Top 10 de Host con mayor consumo
 - o Top 10 de Usuarios con mayor consumo (cuando se haya integrado con el Directorio Activo).
 - o Top 10 de Aplicaciones con mayor consumo
 - o Top 10 de Aplicaciones más populares (muestra qué aplicaciones que tienen mayor número de usuarios sin importar su consumo de ancho de banda)
- Deberá contar con el análisis histórico de distintas métricas del desempeño a nivel de un usuario utilizando una aplicación específica, mínimamente:
 - o Troughput (In / Out)
 - o Bytes transmitidos (In / Out)
 - o Número de Sesiones activas y nuevas sesiones por segundo
 - o Número de Paquetes descartados y paquetes descartados por segundo
 - o Desempeño de la calidad de la aplicación
- Monitoreo en tiempo real con actualizaciones cada segundo a través de gráficos que permitan visualizar su variación a través del tiempo y realizar un análisis de tráfico en profundidad hasta la búsqueda de una estación de trabajo y un servicio específico, para el diagnóstico de problemas y cuellos de botella en la red.
- El análisis estadístico del consumo de ancho de banda y del desempeño de las aplicaciones debe considerar, entre otras, las siguientes métricas:

o Utilización de ancho de banda (throughput) por cada clase de tráfico (bytes, paquetes, kbps en utilización pico y promedio)

o Bytes transmitidos

o Paquetes Retransmitidos (Retransmitted Packets)

o Round trip time (RTT)

o RTT Client

o RTT Server

o Análisis de hosts más activos (top talkers / top listeners)

o Desempeño de la calidad de la aplicación

o Goodput

o Paquetes Descartados

o Tasa de Paquetes Descartados

o Eventos de Retransmisión

o Tasa de Eventos de Retransmisión

o Timeouts

o Tasa de Timeouts

o Número de flujos

o Tasa de número de flujos

• Monitoreo en tiempo real con actualizaciones de los siguientes indicadores a nivel de un usuario utilizando una aplicación específica:

o Throughput (In / Out)

o Bytes transmitidos (In / Out)

o Número de Sesiones activas y nuevas sesiones por segundo

o Número de Paquetes descartados y paquetes descartados por segundo

o Desempeño de la calidad de la aplicación

• El equipo a instalarse deberá enviar alarmas por medio de email y por traps (snmp) y correr scripts.

• El equipo deberá poder conectarse con el servidor de actualizaciones del fabricante para que pueda descargar e instalar las actualizaciones automáticamente. De esta forma se garantizará que el equipo siempre se encuentre actualizado con la última versión publicada por el fabricante.

• El equipo debe garantizar el almacenamiento de datos en su disco duro interno de por lo menos los últimos 24 meses, independientemente de la presencia de un sistema de colección externa, para la posterior generación de reportes y estadísticas.

• Deberá considerar una consola de administración web en el mismo equipo que permita, de forma gráfica, administrar, configurar y generar reportes del equipo Administrador de Ancho de Banda. Se deberá poder mostrar información de reportes al menos de los últimos 24 meses.

• El software para el manejo de reportes y acceso a la consola de gestión del equipo debe ser provisto en el mismo appliance sin utilizar hardware (servidor) ni software adicional, ni virtualizando el



equipo. Por políticas de seguridad de la Entidad, no se permitirá una consola de administración externa o en la nube del fabricante.

- La Entidad deberá contar con acceso de lectura al equipo para la obtención de reportes en cualquier momento. Estos usuarios serán distintos a los que tendrá el proveedor del servicio.

- El equipo debe ser nuevo, de primer uso y que no se encuentre en End of Support por su fabricante.

- Garantía del fabricante por el HW a través de RMA (Return Merchandise Authorization, Autorización de Devolución de Mercadería) por el tiempo que dure el contrato.

- El equipo deberá detectar y mostrar anomalías en la red correspondientes a diversos tipos de ataques (DoS, SYN ATTACKS, Spoofing), enviando alertas y permitiendo la ejecución de acciones automáticas que minimicen su impacto.

- El Postor deberá presentar en su oferta una carta del fabricante de la solución indicando el cumplimiento de todas las características técnicas descritas para el optimizador de tráfico y traffic shapping (documentación de carácter obligatorio en la etapa de presentación de oferta).

- El reemplazo por RMA (Return Merchandise Authorization/ Autorización de Devolución de Material) de partes o hardware cubre únicamente en caso de fallas del equipo. No cuando se deba a fallas eléctricas, ni uso impropio, accidentes, abuso, fuego o desastres naturales. El proveedor se encargará del proceso del RMA en caso fuese necesario.

- El Contratista deberá reemplazar el equipo en caso de falla dentro de las 4 horas por un equipo similar o superior mientras se realiza el proceso del RMA con el fabricante.

- Debe incluir una inducción a nivel de usuario sobre el uso del equipo propuesto para 4 personas por no menos de 10 horas

- Deberá permitir la creación de políticas de control de ancho de banda avanzadas considerando el comportamiento de los flujos o sesiones. Es decir, políticas basadas en la duración de los flujos, la cantidad de paquetes, la velocidad de transferencia y por el total de transferencia.

- El equipo deberá ser capaz de mostrar la geografía del tráfico, es decir contra que países se está realizando el intercambio de datos. Así como soportar la creación de políticas que permitan limitar y bloquear el tráfico desde o hacia uno o varios países.

- La solución debe permitir acceso a estadísticas almacenadas y modificar la configuración vía API, con la opción ampliar la capacidad de monitoreo y analítica con herramientas de terceros. Se debe poder configurar la dirección IP de la herramienta para permita únicamente el acceso a estas consultas a fin de evitar accesos indeseados, como también la configuración de unas credenciales personalizadas para esta comunicación.

- Deberá contar con capacidad de monitoreo de la utilización de ancho de banda y de la cantidad de conexiones activas totales y por equipo (host IP). Siendo capaz de limitar el número de conexiones activas para cada equipo (host IP).



- Para garantizar una profunda visibilidad en tiempo real con actualizaciones cada segundo, se deberá monitorear y mostrar a través gráficos y tablas al menos 20 métricas de cada flujo que pase por el equipo
- La solución debe presentar reportes de gráficos lineales (históricos y de tiempo real con actualizaciones cada segundo) de las políticas de optimización, de al menos las siguientes métricas:
 - o Número de flujos activos
 - o Bytes transmitidos de descarga y subida
 - o Utilización de ancho de banda (throughput) de descarga y subida
 - o Paquetes descartados de descarga y subida
 - o Congestión de la política de descarga y subida

5.2.1.5.1.7 SWITCHES PARA COMUNICACIÓN LAN/WAN

Se requiere dieciséis (16) equipos Switches para comunicación LAN/WAN para la sede principal y secundaria respectivamente bajo la siguiente cantidad de equipos:

- Switches WAN: 04 (los 4 de iguales características).
- Switches de distribución: 06 (los 6 de iguales características).
- Switches de Gestión: 04 (los 4 de iguales características).
- Switches Extranet: 02 (los 2 de iguales características).

Se requiere que, por cada Switch, se considere el valor del throughput de switching y la siguiente cantidad de puertos/interfaces (incluyendo transceivers para todos los puertos) para el procesamiento de datos:

- Switches WAN: 480 Gbps de throughput y como mínimo 24 puertos 1/10G SFP+, 4x 40 QSFP y/o 4x 25 SFP28, 01 puerto de consola y 01 gestión RJ45 dedicado para administración local.
- Switches de distribución (sede Mininter):
 - o 05 switches con 128 Gbps de throughput y como mínimo 48 puertos 10/100/1000Base-T y 8x 10G SFP+. Adicionalmente 01 puerto de consola y 01 gestión RJ45 dedicado para administración local.
 - o 01 switches con 1.5 Tbps de throughput y como mínimo 48 puertos 1/10G SFP+. y 4 puertos de 40G/100G QSFP+/ QSFP28. Adicionalmente 01 puerto de consola y 01 gestión RJ45 dedicado para administración local. (para convergir los sw de distribución, estará ubicado en el centro de datos principal)
- Switches de Gestión: 128 Gbps de throughput y como Mínimo 48 puertos 10/100/1000Base-T y 4x 10G SFP+. Adicionalmente 01 puerto de consola y 01 gestión RJ45 dedicado para administración local (02 en el sitio principal y dos en el sitio secundario)
- Switches Extranet: 128 Gbps de throughput y como Mínimo 48 puertos 10/100/1000Base-T y 4x 10G SFP+.



Adicionalmente 01 puerto de consola y 01 gestión RJ45 dedicado para administración local.

Los equipos antes mencionados además deben tener las siguientes características mínimas:

- Cada equipo debe poder trabajar con alimentación 220V AC 60Hz y bajo consumo de energía.
- Cada equipo debe poder operar a una temperatura de funcionamiento entre 0 °C y 40 °C.
- El switch debe soportar 4K VLANs.
- El switch debe soportar VLAN de voz y VLAN de invitados.
- El switch debe soportar Private VLAN o similares.
- El switch debe soportar los siguientes protocolos de enrutamiento de capa 3: enrutamiento estático, RIPv1/v2, RIPng, OSPF, OSPFv3, VRRP, y VRRP para IPv6.
- Debe soportar la capacidad mínima de entradas de MAC address de 64K.
- La plataforma debe soportar un número total de 32K rutas en IPv4 y de 16K rutas en IPv6.
- La plataforma debe soportar escenarios de red con transporte de tráfico multicast, y soportar, como mínimo, los siguientes protocolos: PIM-DM, PIM-SM, IGMP v1/v2/v3 e IGMP snooping.
- Debe soportar manejo de políticas de tráfico.
- Debe manejar ocho colas en cada puerto.
- El switch debe soportar algoritmos de programación de colas: Priority Queuing (PQ), Weighted Deficit Round Robin (WDRR), PQ+WDRR, Weighted Round Robin (WRR), PQ+WRR o similares.
- Debe soportar remarcado de la prioridad 802.1p.
- Debe soportar el filtrado de paquetes desde la capa 2 hasta la capa 4.
- Debe traffic shaping en los puertos.
- Debe soportar la defensa contra ataques DoS, ataques ARP (como ARP spoofing), ataques ICMP, así como DHCP Snooping.
- Debe soportar autenticación vía IEEE 802.1x, RADIUS y TACACS o similares.
- Debe soportar aprendizaje automático de MAC address y envejecimiento de MAC address.
- Debe soportar entradas de MAC address estática, dinámica y blackhole.
- Debe soportar limitación de aprendizaje de MAC address por interfaz, así como sticky MAC.
- El switch debe soportar protocolos de tipo IP flow como sFlow, Netflow o similares.
- Debe proveer, de manera opcional, mecanismos de eficiencia energética (Energy Efficient Ethernet) mediante el estándar 802.3az.
- Debe soportar los protocolos IEEE 802.1d STP, IEEE 802.1w RSTP y IEEE 802.1s MSTP.



- Debe soportar la funcionalidad para protección BPDU en puertos de acceso.
- Debe soportar la funcionalidad para protección root y loop.
- Debe soportar la protección (conmutación) en milisegundos en topologías de anillo.
- Debe soportar protocolos de gestión SNMP v1/v2c/v3.
- Debe soportar gestión basada en web.
- Debe soportar gestión y configuración remota a través de Telnet.
- Debe soportar protocolo SSHv2 para administración remota.
- Debe soportar RMON.
- Opcionalmente soportar los protocolos Y.1731, G.8032, OAM: EFM OAM (IEEE 802.3ah), CFM OAM (IEEE 802.1ag) y pruebas de performance del protocolo Y.1731.

5.2.1.5.1.8

EQUIPO BALANCEADOR DE ENLACES

Se requiere dos (02) equipos en Alta Disponibilidad (HA) uno para el site principal y el secundario respectivamente, garantizando la alta disponibilidad de los enlaces de Internet instalados en los sitio principal y secundario.

El contratista debe realizar la configuración de los equipos antes indicados durante el periodo de implementación, con la finalidad de:

- Debe comprobar el rendimiento de los enlaces a Internet de los Datacenter Principal y secundario dirige a los usuarios a la mejor conexión posible. Este seguimiento activo se ajusta a variables como la capacidad de procesamiento, el flujo de tráfico y la disponibilidad de Proveedor de Internet, lo que debe mejorar el rendimiento de las aplicaciones policiales y la redistribución del tráfico para reducir la saturación de los enlaces.
- Los equipos deben monitorear el estado y la disponibilidad de los enlaces de Internet del Datacenter Principal y secundario, si detectan un problema en uno de los enlaces debe redirigir el tráfico de datos hacia el otro enlace disponible, garantizando la conectividad de usuario policial sin incurrir en los costos del tiempo de inactividad.

Características de Redundancia y Funciones Generales

- Debe soportar la instalación en ambiente de alta disponibilidad
 - Activo / Activo (soportando el 100% de los enlaces de internet de cada nodo)
- El equipo debe ser nuevo, de primer uso y que no se encuentre en End of Support por su fabricante.
- Un par de equipos, al estar conectados en un ambiente redundante deben soportar sincronización de las sesiones entre ambos. La falla del equipo principal no debe causar la interrupción de las sesiones balanceadas.
- El equipo debe soportar "agregación de puertos" mediante LACP.





- El equipo debe soportar el transporte de múltiples VLANs por un único puerto (o bundle LACP) utilizando el protocolo 802.1q.
- El equipo debe soportar Spanning-Tree Protocol (802.1d), Rapid Spanning-Tree Protocol (802.1w) y Multiple Spanning-Tree Protocol (802.1s)
- El equipo debe soportar enrutamiento dinámico RIP, OSPF y BGP.
- El equipo debe soportar IPv6
- Debe contar con 4 interfaces de 10Gb sfp+ con sus respectivos transceivers.
- La solución debe poder ser controlada mediante Ansible, y deberá contar con módulos que sean soportados y mantenidos en los repositorios oficiales de Ansible (Ansible Galaxy)
- La solución debe incluir una métrica por proximidad que correlacione la latencia y el número de saltos hacia un origen determinado, para el balanceo de salida y desde un origen determinado para el balanceo entrante.
- La solución debe permitir el balanceo de enlaces de acuerdo con el payload del tráfico enviado.
- La solución debe soportar IPv6/IPv4 Gateway para el balanceo entrante y el balanceo saliente.
- La solución debe permitir el balanceo de enlaces utilizando el SNI para la toma de decisiones, sin necesidad de desencriptar el tráfico
- Cada equipo debe disponer de una cierta cantidad de CPUs físicos dedicados completamente para la administración de la capa del OS y no utilizar los recursos asignados a las instancias virtuales para el procesamiento del tráfico. El equipo debe tener una completa separación entre los recursos asignados a la propia OS y las instancias virtuales que procesara el tráfico de las aplicaciones.
- El sistema operativo del equipo tiene que ser desarrollado por el mismo fabricante y tiene que estar basado en Kubernetes, permitiendo por sobre este, llevar a cabo hasta 08 particiones o tenants virtuales completamente aisladas. A cada tenant o partición virtual se le deberá poder asignar recursos de vCPU y memoria dedicados, y se deberán poder asignar VLANs específicas para la conectividad de la red.

Características de Capa 7

- El equipo debe soportar como mínimo:
 - 50 Gbps en capa 4
 - 40 Gbps en capa 7
 - Más de 1 Millón de requests ps en capa 7
 - 37 millones de conexiones concurrentes en L4.
- Las funciones básicas de switching de capa 7 deben incluir:
 - Server Load-Balancing
 - Firewall Load-Balancing
 - Proxy Load-Balancing



- Debe ser capaz de balancear servidores de cualquier tipo de hardware, sistema operativo y tipo de aplicación
- Debe ser capaz de abrir un número reducido de conexiones TCP hacia el servidor e insertar los requests HTTP generados por los clientes en estas conexiones ya abiertas, reduciendo la necesidad de establecimiento de nuevas conexiones con los servidores.
- Debe soportar los siguientes métodos de balanceo:
 - Round Robin
 - Least Connections
 - Weighted Percentage (por peso)
 - Servidor con respuesta más rápida basada en tráfico real
 - Weighted Percentage dinámico (basado en el número de conexiones)
 - Considerando de manera opcional el método de balanceo dinámico, basado en parámetros del servidor coletados vía SNMP o WMI
- Debe ser capaz de balancear conexiones nuevas mientras se preservan las sesiones ya establecidas en los servidores seleccionados. La implementación de la persistencia debe incluir:
 - por cookie – inserción de una nueva cookie
 - por cookie – utilización de un valor de cookie existente
 - dirección IP de destino
 - dirección IP de origen
 - sesión SSL
 - a través del análisis de la URL accedida
 - a través del análisis de cualquier parámetro de la cabecera HTTP
 - a través del análisis de cualquier parámetro de la porción de datos de la aplicación.
- Debe soportar los siguientes métodos de monitoreo de los servidores:
 - Capa 3 (ICMP)
 - Conexiones TCP o UDP al puerto del servicio
 - Capa 7 (HTTP, HTTPS, FTP, SASP, RADIUS, SMTP, MSSQL, ORACLE, RPC, LDAP, IMAP, NNTP, POP3, SIP, Real Server, SOAP, SNMP y WMI).
- Debe ser capaz de limitar las conexiones establecidas con cada servidor real
- Debe ser capaz de limitar las conexiones establecidas con cada servidor virtual
- Debe soportar las siguientes funciones de seguridad:
 - Network Address Translación (NAT)
 - Protección contra Denial of Service (DoS)
 - SYN-Guard
 - SYN-Defense
 - Listas de Control de Acceso (ACL)
 - Limpieza de la cabecera HTTP

- El equipo debe permitir la manipulación del contenido de la aplicación para remover o alterar la información enviada al servidor o al cliente
- La configuración del equipo debe ser basada en perfiles.
 - Los perfiles deben ser jerarquizados, permitiendo mayor facilidad en la administración de políticas
- Debe permitir la creación de servidores virtuales creado con dirección IPv4 mientras que los servidores reales utilicen IPv6
- Debe ser capaz de realizar la compresión del contenido HTTP para reducir la cantidad de información enviada al cliente
- Debe poseer 30 Gbps de throughput para compresión
- Debe ser posible implementar la compresión en hardware
- Debe ser posible definir qué tipo de compresión se habilitará (gzip1, gzip9, deflate)
- Debe ser posible definir la compresión para ciertos tipos de objetos
- Debe ser capaz de realizar aceleración de SSL, donde los certificados digitales son instalados en el equipo y los pedidos HTTP son enviadas a los servidores reales con o sin criptografía (según se requiera).
- En aceleración SSL, tanto el intercambio de llaves, como la encriptación deben ser realizadas por hardware.
- Debe soportar como mínimo 30.000 TPS SSL con llaves de 2K RSA
- Debe soportar cache del contenido para HTTP, permitiendo que los objetos sean almacenados en RAM y los pedidos HTTP sean respondidos directamente por el equipo.
- Debe permitir definir qué objetos se almacenarán en cache.
- Debe permitir definir qué cantidad de memoria se destinará a cache.
- Debe soportar Calidad de Servicio con reserva de ancho de banda (Rate Shapping)
- Debe ser posible aplicar políticas diferentes a cada servidor virtual, permitiendo priorización y reserva de recursos en capa 7.

Administración

- Acceso vía SSH.
- Interfaz de línea de comandos CLI.
- Tres niveles de usuario CLI (Super-user, usuario con permisos reducidos, solo lectura).
- Interfaz Web Grafica.
- Administración vía SNMP.
- Soporte para SNMPv1, SNMPv2 y SNMPv3.
- Soporte para RMON, con mínimo de 4 grupos soportados (Statistics (1), History (2), Alarms (3) y Events (4)).
- Los logs del sistema deben tener la opción de ser almacenados internamente en el sistema o en un servidor externo.



- Debe permitir el aprovisionamiento y configuración remota a través de una API para desarrollo

5.2.1.5.1.9 BALANCEADOR DE SITIOS

Se requiere dos (02) equipos configurados en Alta Disponibilidad (HA) para el balanceo de carga dirigida hacia los servidores de la entidad, distribuidos uno en el Datacenter principal y secundario.

Características de Redundancia y Funciones Generales

REQUERIMIENTOS GENERALES

- El equipo debe soportar como mínimo:
 - 50 Gbps en capa 4
 - 40 Gbps en capa 7
 - Más de 1 Millón de requests ps en capa 7
 - 37 millones de conexiones concurrentes en L4.
- Debe contar con 4 interfaces de 10Gb sfp+ con sus respectivos transceivers.
- El equipo debe ser nuevo, de primer uso y que no se encuentre en End of Support por su fabricante.
- Debe contar con un modo de test de monitores, que permita validar si los monitoreos configurados están bien configurados.
- La solución debe de proveer un soporte nativo para Aplicaciones como Microsoft Exchange, Teams, SharePoint, remoto Desktop.
- La solución debe poder ser controlada mediante Ansible, y deberá contar con módulos que sean soportados y mantenidos en los repositorios oficiales de Ansible (Ansible Galaxy)
- La solución debe incluir una métrica por proximidad que correlacione la latencia y el número de saltos hacia un origen determinado, para el balanceo de salida y desde un origen determinado para el balanceo entrante.
- La solución debe permitir el balanceo de enlaces de acuerdo con el payload del tráfico enviado.
- La solución debe soportar IPv6/IPv4 Gateway para el balanceo entrante y el balanceo saliente.
- La solución debe permitir el balanceo de enlaces utilizando el SNI para la toma de decisiones, sin necesidad de desencriptar el tráfico.
- Cada equipo debe disponer de una cierta cantidad de CPUs físicos dedicados completamente para la administración de la capa del OS y no utilizar los recursos asignados a las instancias virtuales para el procesamiento del tráfico. El equipo debe tener una completa separación entre los recursos asignados a la propio OS y las instancias virtuales que procesara el tráfico de las aplicaciones.
- El sistema operativo del equipo tiene que ser desarrollado por el mismo fabricante y tiene que estar basado en Kubernetes, permitiendo por sobre este, llevar a cabo hasta



08 particiones o tenants virtuales completamente aisladas. A cada tenant o partición virtual se le deberá poder asignar recursos de vCPU y memoria dedicados, y se deberán poder asignar VLANs específicas para la conectividad de la red.

ENTREGA DE APLICACIONES

- Balanceo de carga para protocolos TCP/UDP.
- Descarga de TLS (SSL Offload).
- Caché transparente para HTTP/HTTPS.
- Compresión de contenido dinámico y estático HTTP/HTTPS.
- Soporte para HTTP/2.
- Reenvío de paquetes basado en NAT.
- Soporte para DSR (Retorno directo de servidor).
- Soporte para S-NAT.
- La solución debe tener arquitectura Full-Proxy o reverse-proxy, control de entrada y salida de conexiones distinguiendo conexiones del lado del cliente y del lado del servidor o los recursos.

COMPROBACIÓN DE SALUD

- El sistema debe ser capaz de identificar fallos en servicios para redundancia de las aplicaciones.
- Comprobación de salud ICMP.
- Comprobación HTTP/HTTPS.
- Comprobación sobre capa 4.
- Comprobación sobre capa 7.
- Comprobaciones de salud agregadas.

PERSISTENCIA DE SESIONES

- La solución debe incluir características de persistencia de sesiones compatibles con tecnologías como IIS, Apache, SharePoint, Moodle y Remote Desktop Services, entre otros.

MÉTODOS DE BALANCEO DE CARGA

- Round Robin.
- Round Robin Ponderado.
- Menor conexión.
- Respuesta más rápida.

CARACTERÍSTICAS SSL/TLS

- Soporte para validación extendida de certificados.
- Validación de certificados OCSP.
- Compatibilidad con certificados wildcard (ejemplo: *.dominio.gob.pe).
- Soporte para mínimo 256 certificados TLS (SSL).
- Compatibilidad con protocolos de correo (POP, SMTP, IMAP) STARTTLS.
- Soporte para Identificación de Nombre de Dominio (SNI).

ADMINISTRACIÓN

- Auditoría sobre cambios.
- Interfaz de usuario web (WUI).
- Consola SSH
- Monitoreo en tiempo real de rendimiento y disponibilidad.



- Plantillas de aplicaciones.
- Automatización de tareas de backup.
- Restauración selectiva de la configuración.
- Herramientas para la generación de reportes.
- Soporte de SNMP.

SEGURIDAD

- Listas de control de acceso.
- Filtrado por reputación de IP con actualizaciones automáticas.
- Soporte para autenticación en múltiples dominios y SSO.
- Formularios de login personalizados.
- Integración con Directorio Activo, RADIUS, LDAP y SAML.
- Compatibilidad con autenticación de doble factor.

5.2.1.5.2 COMPONENTE 2: SERVICIO DE FIBRA OSCURA ENTRE EL DATACENTER PRINCIPAL Y SECUNDARIO DE LA PNP

5.2.1.5.2.1 Descripción del servicio

Un (01) enlace terrestre principal de comunicación punto a punto y un (01) enlace terrestre redundante de comunicación punto a punto para conectar dos entidades bajo un mismo protocolo, con capacidad mínima de 40 Gbps de ancho de banda, divididos en 04 canales de 10Gbps cada uno, con capacidad no menor a 40 Gbps, Full Dúplex, que incluya todo el equipo necesario para la ejecución de la comunicación entre el DATACENTER principal de la PNP ubicado en la Plaza 30 de Agosto s/n Urb. Corpac, San Isidro y el local secundario que considere el Contratista.

5.2.1.5.2.2 Referencias técnicas

Enlace punto a punto de fibra óptica oscura con equipos terminales o convertidores de fibra a cobre compatibles a velocidades de 40 Gbps Ethernet. Dicho enlace deberá ser canalizado subterráneo (no se aceptará microcanalizado) en todo su recorrido entre el DATACENTER principal de la PNP ubicado en la Plaza 30 de Agosto s/n Urb. Corpac, San Isidro y el local secundario que considere el Contratista.

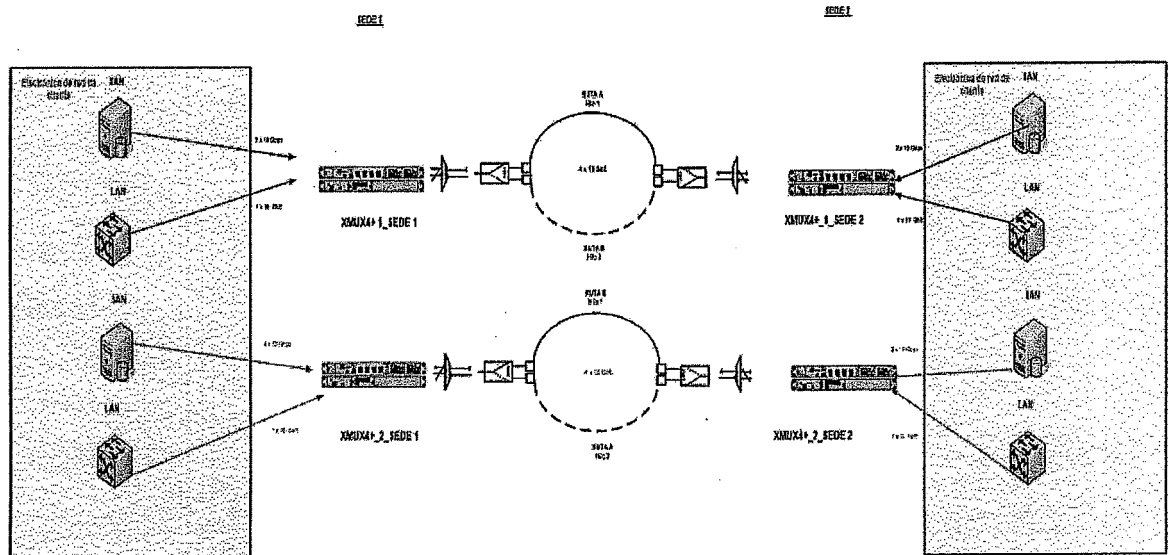
Los equipos terminales deben permitir la conexión transparente y sin limitaciones de clientes ya sea por Mac Address o por direccionamiento IP, debe soportar tráfico de los protocolos necesarios para el funcionamiento de los sistemas de la PNP tales como comunicación de bases de datos, protocolos de enrutamiento, y otros que deben tener compatibilidad universal con los diferentes equipos activos a 40 Gbps Ethernet que la Policía Nacional del Perú pueda interconectar para lograr una comunicación eficiente entre los sitios.

Se debe disponer de un doble enlace punto a punto mediante infraestructura DWDM para el transporte de un (01) servicio principal y un (01) servicio de respaldo entre el DATACENTER principal de la PNP y su sitio secundario:

- Cuatro (04) canales de 10 Gbps por cada enlace.



Los multiplexores ópticos por división de longitud de onda (DWDM) deben soportar una variedad de configuraciones en cuanto a topología y densidad de canales. El siguiente esquema será implementado:



El equipamiento debe contar con las siguientes características generales:

- Tecnología de transmisión DWDM, ajustándose a la rejilla y parámetros ópticos recomendados en la norma ITU-T G.694.1.
- Los sistemas deben ser gestionados vía interfaz de comandos (ssh), acceso gráfico vía web (https) y permitir el acceso vía SNMP y Syslog.
- Los sistemas deben permitir un alcance de hasta 40 km sin regeneración y/o amplificación.
- Para la interconexión los sistemas deben contar con las siguientes características:
 - a) Se requiere que los sistemas trabajen sobre un único pelo de fibra óptica bidireccionalmente.
 - b) Sistemas escalables con una capacidad de crecimiento hasta de 40 canales bidireccionales (80 lambdas).
 - c) Los sistemas deben tener la capacidad de incorporar módulos de monitorización de la calidad y detección de intrusión/manipulación en la fibra.
 - d) Los servicios se deben ofrecer sobre canales ópticos nativos, no mediante canales TDM (aunque los sistemas deben ser compatibles con multiplexación temporal).
 - e) Los sistemas ofrecidos no deben introducir ninguna latencia. Únicamente se permitirá introducir la latencia intrínseca del medio de transmisión (latencia de 5 μ s/km es el valor).

- f) Los sistemas deben ofrecer mecanismos de protección: redundancia de alimentación, redundancia de canales, redundancia de equipamiento y redundancia de ruta óptica (doble enlace punto a punto y doble infraestructura DWDM).
- g) La solución debe tener la capacidad para incluir un sistema de conmutación óptico en cada una de las dos infraestructuras.



El sistema de conmutación óptica que pueda ser incorporado en el enlace debe ser compatible para funcionamiento sobre red DWDM sin intrusión en el tráfico de cliente y no debe tener ningún punto activo de fallo. El tiempo de conmutación del conmutador óptico debe ser inferior a 50 ms en cualquiera de los casos y debe permitir la monitorización en tiempo real de la disponibilidad tanto de la ruta principal como de la ruta de backup.

Al momento de la provisión, se deben emplear todos los hilos que contenga la media instalada para proporcionar las redundancias adecuadas, incluye que se conecten solamente 2 hilos y se dejen terminados e instalados conectores en ambos extremos de todos los hilos, con un mínimo de 6 (2 a emplear y 4 en reserva). De ser configurables los equipos terminales, un técnico designado por el Departamento de Gestión de Centros de Datos de la División de Informática PNP DIRTIC PNP debe tener acceso a las configuraciones del equipo proporcionado para el incremento de rutas y/o cambios de cualquier configuración que a la ENTIDAD le pueda ser de utilidad.

Descripción técnica del servicio, materiales y provisión:

- a) Ductería galvanizada y/o PVC según sea determinado, indicadas dentro de las normas del ANSI/EIA/TIA.
- b) Cajas de registro adecuadas para la fibra óptica
- c) Bandeja o cajas de distribución de fibra para rack o gabinete
- d) Fusión de dos (02) pares de fibra óptica ST/SC o SC/SC (o del par mínimo necesario)
- e) Patch cord de Fibra Óptica monomodo ST/SC o SC/SC (para los pares instalados).
- f) Patch cord de fibra óptica y/o tranceiver requeridos para la comunicación de los multiplexores con los Switch Core de Datacenter del Nodo Central y del Sitio secundario.
- g) Los siguientes requisitos deben ser presentados en forma impresa para que se pueda dar por aceptada la provisión del servicio:



- 
- 
- (1) Reporte de medición de las fibras con OTDR.
 - (2) Gráfica de la medición de la distancia de la fibra óptica.
 - (3) Reporte del estado de pérdida de decibelios en fusiones, en el camino y los extremos.
 - (4) Diagrama geográfico y topología para identificación del tendido, que incluya un informe de identificación de nodos o mufas en el trayecto (si existieran).
 - (5) Certificación de ancho de banda real mediante cualquier software.

El medio para el enlace físico obligatorio es fibra óptica, directamente desde los extremos en ambos sitios.

El enlace debe ser punto a punto, sin conexión alguna al anillo de fibra óptica de la empresa contratista y/o de ninguna otra.

La media de comunicación empleada debe soportar crecimientos en el ancho de banda sin necesidad de cambios amplios o que determinen cualquier tipo de suspensión temporal del servicio.






El contratista está obligado a considerar todos los componentes, dispositivos y materiales que requiera para la integración de la solución adquirida con la red de la Entidad, así como para el cumplimiento de la finalidad del servicio requerido.

Restricciones:

Con relación a la línea redundante del enlace principal, al momento de la provisión está debe realizarse sin compartir los mismos medios de planta externa y debe utilizar una ruta geográfica completamente diferente a la de la línea principal.

Soporte:

El tiempo de atención en caso de caída de señal, no debe exceder los SLA, el contratista es responsable de la operatividad de la solución integral del presente componente a fin de brindar prestación del servicio, los cuales deben estar disponibles y operativos las veinticuatro (24) horas del día, los siete (07) días a la semana y trescientos sesenta y cinco (365) días del año, deberá contemplar la forma de cobertura de comunicación para contingencias no determinadas, número de caídas programadas en el año (efectos geo estacionales, mantenimientos y cambios de tecnología)



Toda desconexión del servicio programada debe ser notificada con 24 horas de anticipación y debe proporcionarse el canal supletorio de la comunicación.

5.2.1.5.3 COMPONENTE 3: PLATAFORMA DIGITAL DE SERVICIOS PARA TRANSMISION DE VOZ, VIDEO Y DATOS PARA LAS SEDES DESCONCENTRADAS PNP, A NIVEL NACIONAL

La Plataforma digital de servicios debe considerar los siguientes subcomponentes:

SUB COMPONENTE	SERVICIO
A	Servicio de conexión de enlace a Intranet (RED PRIVADA), a través de una red tipo MPLS o MetroEthernet, para mil dieciocho (1018) sedes para la Policía Nacional del Perú a nivel nacional.
B	Servicio de conexión de enlace MPLS y/o MetroEthernet, para los nodos principal y secundario de la Policía Nacional.
C	Implementación de solución firewall para sedes policiales a nivel nacional.

5.2.1.5.3.1 Sub-componente A:

Servicio de conexión de enlace a Intranet (RED PRIVADA), a través de una red tipo MPLS o Metroethernet, para mil dieciocho (1018) sedes para la Policía Nacional del Perú a nivel nacional.

Las velocidades de transmisión y ubicación geográfica de las sedes policiales mencionadas en el punto anterior se detallan en el Anexo N° A del presente.

Las sedes policiales para el presente proceso se han categorizado en Sedes Tipo 1 y Sedes Tipo 2, según el siguiente detalle:

Sede Tipo 1: Corresponden a aquellas sedes policiales desconcentradas con enlaces entre 100 y 400 Mbps que presentan volumen intermedio o bajo de usuarios y/o el área de las sedes son de dimensión mediana; éstas son novecientos setenta y cinco (975), que se obtiene de excluir las cuarenta y tres (43) sedes señaladas en el Anexo B2 de la relación suministrada en el Anexo A.

Sede Tipo 2: Corresponden a aquellos complejos policiales a nivel nacional con enlaces de 200 y 400 Mbps, que presentan un alto volumen de usuarios o el área de las sedes son de grandes dimensiones, se han identificado cuarenta y tres (43) de este Tipo cuya información se detalla en el Anexo N° B2 del presente.

Para este subcomponente no deben considerarse la sede principal y secundario.

5.2.1.5.3.1.1 Condiciones generales para Sedes Tipo 1 y Tipo 2:

- Toda la conexión (medio de acceso) debe ser usando el medio fibra óptica.
- El contratista, para todas las sedes del Tipo 1 y Tipo 2, debe desplegar un enlace el cual en la última milla cuente con un nodo de comunicaciones principal. Se aclara que se denomina nodo de comunicaciones del contratista a aquella ubicación geográfica que cuente con la infraestructura mínima para ser considerado como tal;



se denomina nodo de comunicaciones a: aquella ubicación geográfica que cuente con la infraestructura mínima para ser considerado como tal, debiendo contar con un sistema de autonomía de energía mínima, ruteador de comunicaciones y gabinete de transmisiones como mínimo.

- Todos los equipos routers y switches a proveer por el contratista requeridos para el Componente 3 deben contar con vigencia tecnológica o en su defecto proveer equipamiento nuevo, que garanticen los niveles de SLA exigidos.
- Los routers y switches deben ser de la misma marca, para optimizar un mejor rendimiento del sistema, al ser un servicio de nivel crítico, no pudiendo la entidad aceptar ningún fallo a nivel de interoperabilidad de marcas. Asimismo, para garantizar que el postor proponga marcas líderes a nivel global en el mercado, las marcas propuestas de routers y switches deberán estar como líderes en el cuadrante de gartner (copia de la publicación oficial de Gartner y la "url" del enlace web respectivo) "Wired and wireless LAN access infrastructure" en los últimos 04 años. Dicha información deberá ser presentada al momento de la presentación de la oferta.
- La interconexión entre los routers de las sedes del tipo 1 y 2 con los equipos Firewall de Next generation firewalls podrá ser por medio de fibra o por cobre.
- Todos los enlaces de fibra óptica, deben ser simétricos con el ancho de banda contratado garantizado al 100%
- La comunicación entre las Unidades debe realizarse bajo el esquema de un grupo cerrado de usuarios, para tal efecto debe asignarse direcciones IP privadas para cada acceso simétrico, el rango de subredes IP serán suministrados por el DEPGCD-DIVINF-DIRTIC-PNP, debiendo ser de las versiones 4 y 6 del protocolo TCP/IP.
- El servicio debe estar preparado para migrar a mayores velocidades, (interfaces wan) al menos, al 50% más de lo contratado, sin cambiar de equipamiento, que soporte lo requerido por la entidad.
- El contratista será responsable de proveer las herramientas y efectuar las actividades necesarias para la puesta en marcha del servicio.
- El contratista debe establecer enlaces privados de datos entre las redes LAN Ethernet de todas las sedes solicitadas por PNP, incluyendo los nodos principal y secundario.
- Sobre la misma línea de transmisión de datos requerida, vía fibra óptica, debe tener la capacidad de transmitir señal hacia la red privada de datos Intranet PNP y hacia la red pública Internet directamente a través de la red MPLS o MetroEthernet de la contratista.
- La transmisión de datos hacia la Intranet PNP, a través de las líneas contratadas debe tener una prioridad de 70/30 sobre el tráfico simultaneo hacia internet, esto implica que cuando el tráfico hacia ambas redes sea simultaneo, para intranet se tendrá disponible el 70% de la velocidad de transmisión contratada y el tráfico hacia internet solo el 30%, en la situación que solo haya tráfico hacia internet o intranet, se usará el 100% de la velocidad a contratar en cada caso; los caudales de video y voz a configurar por sede, se brindará en la fase de implementación.
- El servicio debe proponer versatilidad para la conformación de Intranets y Extranet, aprovechando los propios servicios de la red.
- La infraestructura debe permitir contar con un alto grado de robustez y seguridad, que permitirá disponibilidades de 99.5% como mínimo para todas las sedes.
- La solución a plantear debe Permitir conectividad total todos-contra-todos entre todas las sedes solicitadas por la PNP garantizando una latencia estable (ping constante con 15% de variabilidad). Toda la conexión (medio de acceso) debe ser usando el medio fibra óptica. Se aceptará que en un máximo de 5% del total de



sedes se pueda realizar el despliegue de última milla mediante radioenlaces (no satelital), siempre y cuando se respeten las siguientes condiciones técnicas:

- Ancho de Banda dedicado, 100% garantizado
 - Overbooking 1:1
 - Latencia: 60ms
 - Perdida de Paquetes máximo: 1%
- Se define latencia al retardo máximo de un paquete de datos, desde el equipo de borde de la sede remota hacia el equipo de borde de uno o ambos Datacenters de la PNP. Esta latencia toma en cuenta el retardo por propagación y por procesamiento de paquetes, así como el tiempo de espera en colas en los nodos de la Red.
 - Se aceptará que la latencia entre sedes será en promedio de 20ms en ambos sentidos (Ida y vuelta) para Lima Metropolitana y 40 ms en ambos sentidos (Ida y vuelta) para provincias a nivel nacional.
 - Para los puntos de Fibra Óptica esta será Canalizada y/o aérea desde el nodo del Operador hasta las diversas sedes de la PNP. Esta red deberá ser propia del operador.
 - La solución debe proporcionar gestión de incidencias y reportes permanente desde un Centro de Gestión, NOC, el cual estará en capacidad de realizar detección proactiva de alarmas tempranas, acciones de control preventivo, correctivo y pruebas técnicas.
 - El contratista debe suministrar una aplicación propia Web con credenciales de acceso para el personal responsable de la Entidad, a través del cual podrá generar tickets de atención de reportes de averías, asimismo se debe tener la posibilidad de monitorear el seguimiento de la atención de la avería reportada.
 - Complementariamente el contratista debe contar con un centro de llamadas para el reporte de fallas, atención de cambios en la configuración del sistema o el tratamiento de reclamos.
 - La configuración de equipos para contingencia debería de funcionar de manera automática y transparente.
 - El contratista debe garantizar trabajos simultáneos en las diferentes sedes a fin de garantizar la continuidad del servicio.
 - La red del operador de telecomunicaciones debe estar configurada en Full-mesh, para la conexión de todas las sedes policiales.
 - El Operador de Telecomunicaciones debe tener disponibilidad de protocolo de ruteo IPV4/IPV6, según decreto supremo 081-2017-PCM.
 - El contratista del servicio realizará la interconexión de los locales que incluye la provisión y configuración de todos los equipos de comunicación necesarios para su funcionamiento; así como, para la integración de las redes de datos con las que cuenta la entidad.
 - Las suscripciones y licencias que son parte del servicio deben estar a nombre de la entidad y se debe entregar con el informe final de implementación.
 - La administración de los equipos quedará a cargo del contratista del servicio de comunicaciones, permitiendo que personal técnico dispuesto por la Entidad tenga acceso de lectura/escritura a la gestión de los servicios y equipamiento propuesto y estos niveles de acceso y/o roles de gestión serán coordinados durante la etapa de implementación.
 - El contratista debe proporcionar un acceso web y una comunidad SNMP que permita el monitoreo del consumo de ancho de banda y disponibilidad de los enlaces. Asimismo, este medio será una de las herramientas de validación de los



enlaces durante el proceso de implementación, debiendo ser considerado como elemento probatorio para la conformidad de la implementación.

- El protocolo IP a configurar en la Plataforma será híbrida, se utilizarán a la vez las versiones 4 y 6, EL CONTRATISTA proveerá asesoramiento a la Entidad en el diseño de red (WAN y las soluciones implementadas que son parte del presente servicio) utilizando el protocolo IP v6.
- La configuración IP de toda la plataforma será proporcionada a la Entidad; será realizada por el contratista, con los rangos IP internos (privados IP v4 y v6) que proporcionará la entidad al momento de la implementación. Esto quiere decir que, la configuración IP que el contratista realizará en toda la solución será proporcionada a la Entidad.
- El acceso a través de los canales de datos debe ofrecer un esquema de direccionamiento IP permanente.
- Todos los enlaces de comunicación deben garantizar el correcto funcionamiento de las siguientes aplicaciones y protocolos:
 - Voz sobre IP.
 - Terminal Server.
 - Citrix (Protocolo ICA)
 - HTTP, HTTPS, FTP, SFTP, SMB, TELNET, SNMP.
 - Otros protocolos que el Contratista debe garantizar para el cumplimiento de los requerimientos mínimos del servicio contratado.
- Se debe garantizar la disponibilidad de poder aplicar prioridad de protocolos y aplicaciones de acuerdo al tráfico crítico QoS, entiéndase que prioridad se refiere a que la red debe operar bajo estándares de calidad de servicio; el sistema debe permitir como mínimo colas de prioridad y estos deben ser administrados por la Entidad y el equipo "in-house". (equipamiento router y/o firewall que está instalado dentro de las sedes de la Entidad).
- La configuración debe ser realizada mediante el equipamiento router y/o firewall respectivo.
- La administración y gestión del servicio que incluye prioridad de protocolos y aplicaciones de acuerdo con el tráfico crítico y otros, serán responsabilidad de la Entidad.
- Se debe considerar la disponibilidad de cambio de equipos (hardware instalado) ante cualquier falla de este, de manera inmediata. (SLA solicitado en las bases).
- La conexión de las sedes de la Entidad a una red VPN, permitirá la integración posterior de múltiples servicios a nivel de WAN: Voz, video, videoconferencias, intercambio seguro de datos estructurados y/o no estructurados; así como el aprovechamiento y/o mejora de medios de comunicación, tales como cableado interno y/o redes inalámbricas seguras.
- La disponibilidad de cambio de equipos se realizará según tiempo de atención. El contratista debe considerar en un 5% adicional de todos los componentes, para tareas de respaldo y soporte durante todo el período de duración del contrato.
- El contratista será responsable de las siguientes actividades requeridas para el suministro del servicio:
 - Estudio de factibilidades técnicas y de campo, diseño de la red de conectividad de las Instituciones.
 - Suministro (incluido transporte) de los equipos que correspondan en alquiler para la provisión del servicio de conectividad en cada Institución.
 - Obras civiles en el exterior del local (cuando se trate de fibra óptica u otra obra relacionada a la provisión del servicio por parte del contratista).
 - Gestión de los permisos municipales necesarios para la ejecución de obras civiles en caso sean necesarios.



- Transporte y viáticos de su personal.
- Montaje de los equipos (incluye dotación de bandejas en caso no puedan ser colocados adecuadamente en los gabinetes). Asimismo, se debe proporcionar cables de poder y material de ferretería necesarios para su provisión.
- Provisión y configuración de los routers y otros equipos que se requieran para la operatividad del servicio.
- Provisión de estructuras para la solución de conectividad.
- Pruebas de funcionamiento y validación.
- Operación y mantenimiento del sistema.
- Supervisión de los SLA (Acuerdo de Nivel de Servicio).
- Todos los gastos derivados de la implementación del servicio serán asumidos por el contratista.
- La Entidad se compromete a brindar:
 - Permiso de acceso al personal del contratista para los trabajos correspondientes.
 - La ubicación y el respectivo espacio donde se proveerá el gabinete dentro de la Institución.
 - Suministro eléctrico 220V. en el tablero eléctrico respectivo.
 - Designación del personal para las coordinaciones del Proyecto y para las instalaciones en cada sede.
- Las labores de montaje y provisión en cada local deben ser comunicadas con la debida anticipación a los responsables de la gestión del proyecto que la Entidad designe.
- Para la provisión del servicio de conectividad en cada local policial el contratista debe coordinar con el personal que la Entidad designe.
- El contratista debe realizar la supervisión permanente de los enlaces instalados en cada local policial a través de su centro de gestión y monitoreo a fin de que se cumplan los SLA solicitados.
- El contratista debe brindar adecuada protección eléctrica a los equipos que instale en cada Sede mediante:
 - La provisión de un pozo a tierra, el cual debe estar acorde a las normas nacionales vigentes (Código Nacional de Electricidad – "Utilización" 2006/Sección 060)
- El contratista es responsable por la protección eléctrica de los equipos instalados.
- El contratista debe incluir todo lo necesario para el funcionamiento
- El contratista se hace responsable por los equipos que proporcione y de evidenciarse que no satisfacen lo requerido o no permiten una adecuada performance de la red debe asumir el total de los gastos que correspondan para cambiar por otros el total de estos en las sedes policiales.
- Durante la ejecución del servicio el contratista es responsable por mantener su equipamiento en correcto funcionamiento.
- La Entidad anotará el día y la hora en la cual realiza la llamada reportando la falla y/o avería en el servicio. Recuerde que ante cada falla en el servicio el contratista debe generar un ticket por el incidente reportado y solucionarlo en cuatro (04) horas si la sede policial queda en zona urbana, y doce (12) horas si queda en zona rural (según INEI) considerando que el horario de atención de las Sedes policiales para labores administrativas se ha definido entre las 8:00 y las 18:00 horas de lunes a viernes y entre las 9:00 am hasta las 13:00 sábados (según disponibilidad del personal de las sedes policiales). En caso la avería se produzca fuera del horario laboral establecido en los Términos de Referencia y requiera de una visita del equipo del contratista a la sede policial para su respectiva solución, el periodo de





- solución quedará en stand by hasta que se reinicie el horario laboral de las sedes policiales, no siendo computado dentro del tiempo de resolución de la avería.
- Para presentar una queja y/o reclamo en la prestación del servicio o la atención de los incidentes enviar un correo a: centrodeatención@operador.ganador (correo referencial).
 - Los daños irreparables en los equipos, se evaluará previamente si esta deberá recaer sobre el contratista o sobre la Entidad; en tal sentido, imputables a la Entidad será cuando: existe pérdida del equipo y deterioro por agentes externos generados por la Entidad (derrame de líquidos sobre el equipo y caídas), en el caso que el uso negligente sea comprobado e imputable a la Entidad, será ésta quien asuma los costos, dichos costos serán facturados por separado; para los casos de mal funcionamiento o deterioro de fábrica de los equipos, dentro del periodo de servicio, así como el daño por agentes externos no atribuible a la Entidad, esto será asumido por el contratista.
 - El contratista se compromete a no reasignar ni remover al Jefe del Proyecto. Excepto si por razones de fuerza mayor debe ser reemplazado el reemplazante debe ser aprobado por la Entidad y debe reunir al menos la misma competencia y la experiencia que el reemplazado.
 - LA PNP podrá solicitar al contratista que cualquier miembro de su personal o subcontratista o cualquier personal de este sea retirado y reemplazado en el momento que lo requiera a través de correo electrónico institucional por parte del Jefe del Departamento de Gestión de Centro de Datos de la DIVINFOR-DIRTIC. La PNP hará el requerimiento de manera sustentada y de manera formal mediante el envío de una carta al contratista. Dicho requerimiento deberá atenderse en un plazo máximo de siete (07) días calendario.
 - Para los enlaces se requiere que sea simétrico y 100% garantizado. Overbooking 1:1.
 - Debido a que durante la vigencia el contrato del presente servicio, algunas sedes policiales podrían trasladarse, El contratista, debe considerar una bolsa de traslado a otras locaciones para la Entidad, de acuerdo al siguiente detalle:
 - **Sede tipo 1:** 70 traslados del servicio a otro local policial nivel nacional y 70 cambios de reubicación interna en la misma sede.
 - El traslado de servicio a otro local estará sujeto a un previo estudio de factibilidad técnica por parte del Contratista; esta factibilidad será sustentada con documentación y deberá ser presentada en un plazo máximo de CINCO (05) días calendarios. Asimismo, en el tercer año de ejecución del contrato, la cantidad de traslados que no se hayan realizado para las sedes tipo 2 podrán ser considerados en las sedes tipo 1.
 - Los traslados se realizarán con todo el equipamiento implementado por el contratista o según requerimiento de la Entidad.
 - **Sede tipo 2:** 20 traslados del servicio a otro local policial y 20 cambios de reubicación interna en la misma sede. El traslado de servicio a otro local estará sujeto a un previo estudio de factibilidad técnica por parte del Contratista; esta factibilidad será sustentada con documentación y deberá ser presentada en un plazo máximo de CINCO (05) días calendarios. Asimismo, en el tercer año de ejecución del contrato, la cantidad de traslados que no se hayan realizado para las sedes tipo 2 podrán ser considerados en las sedes tipo 1.
 - El traslado se realizará con todo el equipamiento del servicio (todos los equipos de comunicación, firewall y todos los componentes que comprende el presente servicio) o parte del equipamiento del servicio según coordinación con la Entidad.

- El plazo de ejecución de traslado una vez de recibido el requerimiento de LA ENTIDAD por parte del Contratista, será dentro de los cuarenta y cinco (45) días calendario. Durante el tiempo que se realice el traslado, el Contratista deberá suspender el servicio juntamente con la facturación correspondiente al período que demore el traslado. Si el traslado no se realice dentro del periodo establecido, se considerará la suspensión del servicio como también la facturación del circuito en proceso de traslado.
- Ante la "desactivación" de alguna sede por razones internas de la Entidad, el contratista debe considerar estas opciones:
 - Trasladar el enlace de la unidad "desactivada" hacia otra sede a nivel nacional, dispuesta por la Entidad o
 - Anular el enlace e incrementar el ancho de banda hacia alguna sede dispuesta por la Entidad.
- El contratista está obligado a considerar todos los componentes, dispositivos y materiales que requiera para la integración de la solución adquirida con la red de la Entidad, así como para el cumplimiento de la finalidad del servicio requerido.
- El contratista deberá proveer la conexión de al menos una computadora de la Entidad conectada al switch, a fin de validar el servicio por parte del usuario, a través de una conexión (canaletas, conectores, cables, accesorios, entre otros), considerando el cableado estructurado por cada sede policial.

5.2.1.5.3.1.2 EQUIPAMIENTO DE SEDES

El contratista debe considerar como mínimo los siguientes componentes y/o equipamientos según corresponda, adjuntando la documentación que así lo acredite como parte del expediente para la aprobación del Plan de Trabajo, con el fin de asegurar el óptimo performance de los enlaces requeridos, así como la seguridad digital gestionada y garantizar el cumplimiento del Acuerdo del Nivel de Servicio (SLA) contratado.

Los daños irreparables en los equipos, se evaluará previamente si esta deberá recaer sobre el contratista o sobre la Entidad; en tal sentido, imputables a la Entidad será cuando: existe pérdida del equipo y deterioro por agentes externos generados por la Entidad (derrame de líquidos sobre el equipo y caídas), en el caso que el uso negligente sea comprobado e imputable a la Entidad, será ésta quien asuma los costos; para los casos de mal funcionamiento o deterioro de fábrica de los equipos, dentro del periodo de servicio, así como el daño por agentes externos no atribuible a la Entidad, esto será asumido por el contratista.

Sedes tipo 1

- La relación está considerada en el Anexo A, excluyendo a las sedes señaladas como sedes tipo 2, se obtiene un total de novecientos ochenta y cinco (985) sedes policiales que contarán con switches. Se considera bajo la siguiente cantidad de equipos:
 - **SEDES TIPO 1 - A: 96 (los 96 de iguales características y marca).**
 - **SEDES TIPO 1 - B: 889 (los 889 de iguales características y marca).**
- Se requiere que, por cada Switch, se considere el valor del throughput de switching y la siguiente cantidad de puertos/interfaces.
- **SEDES TIPO 1 - A: como mínimo 128 Gbps throughput, como mínimo 24 puertos 10/100/1000Base-T y 4-port SFP+. Adicionalmente 01 puerto de consola para administración local.**



- 5.2.1.5.3.1.3 **SEDES TIPO 1 - B: como mínimo 128 Gbps de throughput, como Mínimo 48 puertos 10/100/1000Base-T y 4x 10G SFP+. Adicionalmente 01 puerto de consola y 01 puerto de gestión RJ45 dedicado para administración local**
- CARACTERÍSTICAS DEL SWITCH LAN SEDES TIPO 1 – A (96) y TIPO 1 – B (889):**

El modelo de switch debe contar con vigencia tecnológica y como mínimo contar con las siguientes características técnicas:

- El switch de 24 puertos debe contar con una capacidad de reenvío no menor a 95 Mpps.
- El switch de 48 puertos debe contar con una capacidad de reenvío no menor a 130 Mpps.
- Cada equipo debe poder trabajar con alimentación 220V AC 60Hz y bajo consumo de energía.
- Cada equipo debe poder operar a una temperatura de funcionamiento entre 0 °C y 40 °C.
- El switch debe soportar 4K VLANs.
- El switch debe soportar VLAN de voz y VLAN de invitados.
- El switch debe soportar Private VLAN o similares.
- El switch debe soportar los siguientes protocolos de enrutamiento de capa 3: enrutamiento estático, RIPv1/v2, RIPv6, OSPF, OSPFv3, VRRP, y VRRP6.
- Debe soportar la capacidad mínima de entradas de MAC address de 16K.
- La plataforma debe soportar un número total de 4000 rutas en IPv4 y de 1000 rutas en IPv6.
- La plataforma debe soportar escenarios de red con transporte de tráfico multicast, y soportar, como mínimo, los siguientes protocolos: PIM-DM, PIM-SM, IGMP v1/v2/v3 e IGMP snooping.
- Debe soportar manejo de políticas de tráfico.
- Debe manejar ocho colas en cada puerto.
- El switch debe soportar algoritmos de programación de colas: Priority Queuing (PQ o SP) y Deficit Round Robin (DRR) o similares.
- Debe soportar remarcado de la prioridad 802.1p.
- Debe soportar el filtrado de paquetes desde la capa 2 hasta la capa 4.
- Debe traffic shaping en los puertos.
- Debe soportar la defensa contra ataques DoS, ataques ARP (como ARP spoofing), ataques ICMP, así como DHCP Snooping.
- Debe soportar autenticación vía IEEE 802.1x, RADIUS y TACACS o similares.
- Debe soportar aprendizaje automático de MAC address y envejecimiento de MAC address.
- Debe soportar entradas de MAC address estática, dinámica y blackhole.
- Debe soportar limitación de aprendizaje de MAC address por interfaz, así como sticky MAC.
- El switch debe soportar protocolos de tipo IP flow como sFlow, Netflow o similares.
- Debe proveer mecanismos de eficiencia energética (Energy Efficient Ethernet) mediante el estándar 802.3az.
- Debe soportar los protocolos IEEE 802.1d STP, IEEE 802.1w RSTP y IEEE 802.1s MSTP.



- Debe soportar la funcionalidad para protección BPDU en puertos de acceso.
- Debe soportar la funcionalidad para protección root y loop.
- Debe soportar protocolos de gestión SNMP v1/v2c/v3.
- Debe soportar gestión basada en web.
- Debe soportar gestión y configuración remota a través de Telnet.
- Debe soportar protocolo SSHv2 para administración remota.
- Debe soportar RMON.
- Opcionalmente podrá soportar los protocolos Y.1731 y G.8032,
- Debe contar con un dispositivo modular SFP que permita la verificación de la conexión de área local, a través del cual se pueda diagnosticar de forma automática la falta de servicio, advertir en que parte/zona de la red se encuentra el problema de conectividad y generar un reporte de forma automática y pueda visualizarse a partir de una interfaz web de administración, a fin de que el usuario de la entidad pueda contar con esta evidencia y pueda generar los ticket de avería para la atención por el proveedor; asimismo, este dispositivo, para el lado del proveedor generará la evidencia de la falla presentada de forma automatizada, y cuando el problema se encuentre en la red local será de exclusiva responsabilidad de la entidad. Dicho dispositivo está orientado a la resolución de problemas en operación a nivel de usuario final (Aplicaciones)

Sedes tipo 2.

- Relación de sedes tipo 2, según el anexo N° A.
- Para las sedes tipo 2, se considerará la provisión de Switch Core LAN capa 3 o principal, Switch LAN de distribución, según indicación en el Anexo N° A del presente, como mínimo deben cumplir con las siguientes características técnicas:

5.2.1.5.3.1.4 Switch Core LAN (cantidad 14):

El modelo de switch debe contar con vigencia tecnológica y como mínimo contar con las siguientes características técnicas:

- El switch propuesto debe proveer como mínimo 48 puertos RJ45 de 10/100/1000 Base T.
- Debe proveer 04 puertos 1/10 Gbps SFP+ todos los transceivers requeridos en la presente solución.
- El switch debe contar con una capacidad de conmutación no menor a 480 Gbps.
- El switch debe contar con una capacidad de reenvío no menor a 369 Mpps como mínimo.
- El switch debe incluir 01 cable de stacking para apilamiento.
- Cada equipo debe poder trabajar con alimentación 220V AC 60Hz y bajo consumo de energía.
- Cada equipo debe poder operar a una temperatura de funcionamiento entre 0 °C y 40 °C.
- El switch debe soportar 4K VLANs.
- El switch debe soportar VLAN de voz y VLAN de invitados.
- El switch debe soportar Private VLAN o similares.
- El switch debe soportar los siguientes protocolos de enrutamiento de capa 3: enrutamiento estático, RIPv1/v2, RIPv3, OSPF, OSPFv3, VRRP, y VRRP para IPv6.





- Debe soportar la capacidad mínima de entradas de MAC address de 16K.
 - La plataforma debe soportar un número total de 16K rutas en IPv4 y de 8K rutas en IPv6.
 - La plataforma debe soportar escenarios de red con transporte de tráfico multicast, y soportar, como mínimo, los siguientes protocolos: PIM-DM, PIM-SM, IGMP v1/v2/v3 e IGMP snooping.
 - Debe soportar manejo de políticas de tráfico.
 - Debe manejar ocho colas en cada puerto.
 - El switch debe soportar algoritmos de programación de colas: Priority Queuing (PQ), Weighted Deficit Round Robin (WDRR), PQ+WDRR, Weighted Round Robin (WRR), PQ+WRR o similares.
 - Debe soportar remarcado de la prioridad 802.1p.
 - Debe soportar el filtrado de paquetes desde la capa 2 hasta la capa 4.
 - Debe traffic shaping en los puertos.
 - Debe soportar la defensa contra ataques DoS, ataques ARP (como ARP spoofing), ataques ICMP, así como DHCP Snooping.
 - Debe soportar autenticación vía IEEE 802.1x, RADIUS y TACACS o similares.
 - Debe soportar aprendizaje automático de MAC address y envejecimiento de MAC address.
 - Debe soportar entradas de MAC address estática, dinámica y blackhole.
 - Debe soportar limitación de aprendizaje de MAC address por interfaz, así como sticky MAC.
 - El switch debe soportar protocolos de tipo IP flow como sFlow, Netflow o similares.
 - Debe proveer mecanismos de eficiencia energética (Energy Efficient Ethernet) mediante el estándar 802.3az.
 - Debe soportar los protocolos IEEE 802.1d STP, IEEE 802.1w RSTP y IEEE 802.1s MSTP.
 - Debe soportar la funcionalidad para protección BPDU en puertos de acceso.
 - Debe soportar la funcionalidad para protección root y loop.
 - Debe soportar la protección (conmutación) en milisegundos en topologías de anillo.
 - Debe soportar protocolos de gestión SNMP v1/v2c/v3.
 - Debe soportar gestión basada en web.
 - Debe soportar gestión y configuración remota a través de Telnet.
 - Debe soportar protocolo SSHv2 para administración remota.
 - Debe soportar RMON.
 - Opcionalmente podrá soportar los protocolos Y.1731, G.8032, OAM: EFM OAM (IEEE 802.3ah), CFM OAM (IEEE 802.1ag) y pruebas de performance del protocolo Y.1731.
- Debe contar con un dispositivo modular SFP que permita la verificación de la conexión de área local, a través del cual se pueda diagnosticar de forma automática la falta de servicio, advertir en que parte/zona de la red se encuentra el problema de conectividad y generar un reporte de forma automática y pueda visualizarse a partir de una interfaz web de administración, a fin de que el usuario de la entidad pueda contar con esta evidencia

y pueda generar los ticket de avería para la atención por el proveedor; asimismo, este dispositivo, para el lado del proveedor generará la evidencia de la falla presentada de forma automatizada, y cuando el problema se encuentre en la red local será de exclusiva responsabilidad de la entidad. Dicho dispositivo está orientado a la resolución de problemas en operación a nivel de usuario final (Aplicaciones)

5.2.1.5.3.1.5

SWITCH LAN DE DISTRIBUCIÓN PARA SEDES TIPO 2 (Cantidad 162):

Características técnicas mínimas.

- El switch propuesto debe proveer como mínimo 48 puertos RJ45 de 10/100/1000 Base T.
- Cada switch debe incluir los transceivers y cables para apilamiento de ser requeridos en la presente solución.
- Debe proveer puertos de uplink con capacidad de 10Gbps SFP+, con un mínimo de 4 puertos 10 Gbps SFP+, con todos los transceivers requeridos en la presente solución.
- El switch deber contar con una capacidad de conmutación no menor a 200 Gbps.
- El switch debe contar con una capacidad de reenvío no menor a 150 Mpps.
- El switch debe incluir 01 cable de stacking para apilamiento si es requerido en la presente solución.
- Cada equipo debe poder trabajar con alimentación 220V AC 60Hz y bajo consumo de energía.
- Cada equipo debe poder operar a una temperatura de funcionamiento entre 0 °C y 40 °C.
- El switch debe soportar 4K VLANs.
- El switch debe soportar VLAN de voz y VLAN de invitados.
- El switch debe soportar Private VLAN o similares.
- El switch debe soportar los siguientes protocolos de enrutamiento de capa 3: enrutamiento estático, RIPv1/v2, RIPng, OSPF, OSPFv3, VRRP, y VRRP para IPv6.
- Debe soportar la capacidad mínima de entradas de MAC address de 16K.
- La plataforma debe soportar un número total de 16K rutas en IPv4 y de 8K rutas en IPv6.
- La plataforma debe soportar escenarios de red con transporte de tráfico multicast, y soportar, como mínimo, los siguientes protocolos: PIM-DM, PIM-SM, IGMP v1/v2/v3 e IGMP snooping.
- Debe soportar manejo de políticas de tráfico.
- Debe manejar ocho colas en cada puerto.
- El switch debe soportar algoritmos de programación de colas: Priority Quering (PQ), Weighted Deficit Round Robin (WDRR), PQ+WDRR, Weighted Round Robin (WRR), PQ+WRR o similares.
- Debe soportar remarcado de la prioridad 802.1p.
- Debe soportar el filtrado de paquetes desde la capa 2 hasta la capa 4.
- Debe traffic shaping en los puertos.





- Debe soportar la defensa contra ataques DoS, ataques ARP (como ARP spoofing), ataques ICMP, así como DHCP Snooping.
- Debe soportar autenticación vía IEEE 802.1x, RADIUS y TACACS o similares.
- Debe soportar aprendizaje automático de MAC address y envejecimiento de MAC address.
- Debe soportar entradas de MAC address estática, dinámica y blackhole.
- Debe soportar limitación de aprendizaje de MAC address por interfaz, así como sticky MAC.
- El switch debe soportar protocolos de tipo IP flow como sFlow, Netflow o similares.
- Debe proveer mecanismos de eficiencia energética (Energy Efficient Ethernet) mediante el estándar 802.3az.
- Debe soportar los protocolos IEEE 802.1d STP, IEEE 802.1w RSTP y IEEE 802.1s MSTP.
- Debe soportar la funcionalidad para protección BPDU en puertos de acceso.
- Debe soportar la funcionalidad para protección root y loop.
- Debe soportar la protección (conmutación) en milisegundos en topologías de anillo.
- Debe soportar protocolos de gestión SNMP v1/v2c/v3.
- Debe soportar gestión basada en web.
- Debe soportar gestión y configuración remota a través de Telnet.
- Debe soportar protocolo SSHv2 para administración remota.
- Debe soportar RMON.
- Opcionalmente podrá soportar los protocolos Y.1731, G.8032, OAM: EFM OAM (IEEE 802.3ah), CFM OAM (IEEE 802.1ag) y pruebas de performance del protocolo Y.1731.
- Debe contar con un dispositivo modular SFP que permita la verificación de la conexión de área local, a través del cual se pueda diagnosticar de forma automática la falta de servicio, advertir en que parte/zona de la red se encuentra el problema de conectividad y generar un reporte de forma automática y pueda visualizarse a partir de una interfaz web de administración, a fin de que el usuario de la entidad pueda contar con esta evidencia y pueda generar los ticket de avería para la atención por el proveedor; asimismo, este dispositivo, para el lado del proveedor generará la evidencia de la falla presentada de forma automatizada, y cuando el problema se encuentre en la red local será de exclusiva responsabilidad de la entidad. Dicho dispositivo está orientado a la resolución de problemas en operación a nivel de usuario final (Aplicaciones)

- Los Switch de distribución debe ser de la misma marca de los Switch Core o principal propuestos por el contratista. La cantidad y distribución se señalan en el Anexo N° A del presente.
- El Contratista debe tomar las debidas precauciones para evitar dañar las instalaciones y en caso esto suceda ejecutar inmediatamente su respectiva restauración. También mantendrá los lugares de trabajo libre de cualquier desecho, producto de la utilización de los materiales propios del trabajo a realizar.

- La administración de todas las soluciones y equipamiento solicitado por la Entidad, serán de administración compartida, en ese sentido, el contratista entregará credenciales de usuarios a nivel de read/write a usuarios designados por la Entidad.
- Se debe tomar las previsiones del caso para que los trabajos que se desarrollan no interfieran con el normal cumplimiento de las funciones propias de la oficina. En coordinación con el personal de la DIRTIC-PNP, se establecerán los horarios normales y especiales (de ser necesario) para realizar los trabajos.
- El contratista realizará todos los trabajos necesarios en la configuración de switches, routers, firewall y otros equipos, a fin de brindar el servicio requerido por la Entidad.
- Todos los diagramas, topologías red lógicas físicas y configuraciones realizadas por el Contratistas serán entregados en informe impreso y digital para administración de la Entidad, los entregables tendrán por lo menos el siguiente alcance:
 - Memoria descriptiva.
 - Descripción de datos. (topología de red, vlan, segmento de red, IPs, usuarios de administración, configuración de switches, distribución de patch panel, diccionario de datos, etiquetado y tabla de asignación de: puntos de red, patch panel y puertos de switch utilizados, direcciones IP de todos los router, switches y firewall; topología lógica y física de todas las unidades considerando puertos de red utilizados, ip utilizadas, segmentos de red, conexiones físicas con indicación de origen y destino, ancho de banda, medio físico entre otros)

Debe efectuarse un mantenimiento preventivo cada doce (12) meses (03 veces durante la ejecución del servicio, previa coordinación entre la entidad y el contratista.). El mantenimiento preventivo deberá asegurar una correcta prestación del servicio. Podrá ser físico o lógico dependiendo de la situación de cada equipamiento.

- El contratista está obligado a considerar todos los componentes, dispositivos y materiales que requiera para la integración de la solución adquirida con la red de la Entidad, así como para el cumplimiento de la finalidad del servicio requerido.

5.2.1.5.3.1.6 Provisión de equipamiento "Access Point"

- El contratista suministrara la cantidad de mil quinientos 1500 dispositivos Wireless (Access Point), los mismos que serán instalados y conectorizados a los switches de acceso de cada unidad según distribución establecida por el área usuaria.
- El contratista suministrara el Access point con las siguientes características mínimas:
 - ✓ Recolectar información dinámicamente de todos los equipos finales y correlacionar para una rápida respuesta.
 - ✓ Soportar mas de 150 cambios de estado y capturar para cada equipo cliente y Access point por cada 10 segundos

- ✓ Programable, usando APIs de código abierto, para tener una completa automatización y poder integrar con otras soluciones.
 - ✓ Información específica del tráfico y clientes.
 - ✓ Información general sobre el rendimiento, incluida la experiencia del nivel de servicio a nivel de sitio, el número de clientes y las tendencias de tráfico.
 - ✓ Análisis de fallas del cliente.
 - ✓ El agente de software puede ser compatible con dispositivos Android y Windows.
 - ✓ Compatibilidad con integraciones con Zoom y Microsoft Teams Experience Insights.
 - ✓ Compatibilidad con la integración de ChatGPT
 - ✓ 802.11ax (Wi-Fi 6) MU-MIMO. Compatibilidad con versiones anteriores de 802.11a/b/g/n/ac.
- El contratista suministrará el cableado estructurado necesario para la interconexión de los Access point, a fin de garantizar la disponibilidad del servicio para el acceso a los servicios internos de la entidad. El contratista deberá considerar como distancia promedio para el cableado estructurado del Access Point de 50 mts.
 - El contratista deberá proveer un sistema de gestión centralizado para garantizar los servicios brindados a través de los dispositivos Access point.
 - El contratista deberá proveer un mecanismo de validación a través de un portal cautivo.

5.2.1.5.3.1.7 Provisión de plataforma de backbone de fibra y gabinetes por sede

- El servicio de plataforma de backbone y gabinetes por sede será brindado para mil dieciocho (1018) sedes de la Policía Nacional del Perú a nivel nacional y la sede principal del ministerio del interior, las mismas que se detallan en el Anexo "A" del presente.
- Consideraciones generales
- Para la ejecución del servicio, el contratista se obliga a proveerá el equipamiento necesario, a todo costo
- La plataforma de backbone corresponde a proveer fibra óptica entre los gabinetes principales y de distribución en las dependencias policiales y la sede del ministerio del interior, se según se detalla en el Anexo N° A, habilitando la interconexión del switch principal y los de distribución a 10Gbps ubicados en los respectivos gabinetes, proveyendo todo el equipamiento necesario para su operatividad (bandejas de fibra, conectores, patch cord entre otros.)
- La provisión de gabinetes será realizada en cada una de las sedes que se instale los enlaces de comunicación.
- De existir deterioro, manchas, daños y/o alteraciones de la infraestructura existente, por parte del personal del contratista en la ejecución de sus obligaciones, este deberá realizar la reparación o la reposición de lo dañado en forma inmediata, según corresponda, sin que ello genere un gasto al Proyecto.
- El contratista efectuará las conexiones del gabinete principal con los gabinetes de distribución a través de fibra óptica con capacidad de ancho de banda de 10 Gbps.
- El contratista proveerá la plataforma de backbone y gabinetes en el Ministerio del Interior con seis (06) gabinetes de distribución y deberán

estar interconectado con fibra óptica con un ancho de banda de 10 Gbps, la referida interconexión se efectuará entre el switch del gabinete principal y los switches de los gabinetes de distribución, el verificando la interconexión entre switches.

- El contratista será responsable de proveer la plataforma de backbone y gabinetes para el correcto funcionamiento del servicio, lo que debe ser considerado el plan de trabajo.
- Para los puntos de Fibra Óptica esta será Canalizada o aérea desde el nodo del Operador hasta las unidades y/o sedes de la PNP a nivel nacional, siendo responsabilidad del CONTRATISTA el cumplimiento del servicio.
- El contratista será responsable de las siguientes actividades requeridas para el suministro de la plataforma de backbone y gabinetes por sede:
- Estudio de factibilidades técnicas y de campo, diseño de la red de conectividad de las sedes policiales.
- Suministro (incluido transporte) de los equipos que correspondan para la provisión del servicio de conectividad en cada sede policial, a nivel nacional.
- Obras civiles en el exterior del local
- El contratista efectuará los trámites y/o gestión de los permisos municipales necesarios para la ejecución de obras civiles en caso sean necesarios.
- Pruebas de funcionamiento y validación mediante la certificación de puntos de interconexión entre los switches principal y distribución que será adjuntado en el acta de conformidad de la implementación, por cada unidad.
- Todos los gastos derivados de la implementación del servicio serán asumidos por el contratista.

La entidad se compromete a brindar:

- Permiso de acceso al personal del contratista para los trabajos correspondientes en las unidades policiales a nivel nacional.
- La ubicación y el respectivo espacio donde se proveerá el gabinete dentro de la Institución.
- Designación del personal para las coordinaciones del Proyecto y para las instalaciones en cada sede.
- El contratista remitirá por correo electrónico a la dirección datacenterpnp@policia.gob.pe el listado del personal autorizado para efectuar las labores de implementación y/o montaje y/u obras civiles en cada sede policial a nivel nacional, con un mínimo de 72 horas de anticipación, adjuntando nombre y apellidos completos, copia de DNI y certificado de SCTR.
- El punto eléctrico al que se conecte el gabinete, debe estar conectado a un Interruptor termomagnético independiente que el contratista debe interconectar en el tablero eléctrico principal de las unidades policiales donde realice la provisión. Dicho punto debe ser cubierto adecuadamente con canaletas de piso y/o pared.
- El contratista se obliga a efectuar las conexiones necesarias (canaletas, llaves, cableado eléctrico, entre otros materiales para el cumplimiento de la obligación) para cumplir con la interconexión previamente señalada.
- El abastecimiento de la energía eléctrica será provisto por la entidad, y será de exclusiva responsabilidad del contratista estabilizar dicha energía



eléctrica a todo el equipamiento a proveer por el postor y que sea instalado en el gabinete de cada sede.

- Para las zonas donde la energía eléctrica sea fluctuante e inestable, el contratista se obliga a proveer adicionalmente los transformadores de aislamiento, con la finalidad de proteger y garantizar la disponibilidad del servicio y la operatividad del equipamiento (equipos de comunicación), esto implica en la implementación y de ser necesario durante la ejecución del servicio.

- **El contratista debe incluir todo lo necesario para el funcionamiento:**

- El contratista se hace responsable por los materiales que proporcione en la plataforma de backbone y gabinetes por sede y de evidenciarse que no satisfacen lo requerido o no permiten una adecuada performance de la red, se obliga a realizar los cambios requeridos en su totalidad, bajo su responsabilidad y costo.
 - Durante la ejecución del servicio el contratista es responsable por mantener la plataforma de backbone y gabinetes por sede, en buenas condiciones.
 - El contratista debe proporcionar gabinetes de piso para ser utilizados como gabinetes principales y gabinetes de distribución, según Anexo A.
 - El gabinete principal será de 32RU el cual debe tener capacidad para colocar los equipos de comunicación, seguridad, ordenadores de cable y patch panel debidamente rackeados con sus respectivos accesorios.
 - El gabinete de Distribución será de 24RU en el cual debe tener capacidad para colocar los equipos de comunicación, ordenadores de cable y patch panel debidamente rackeados con sus respectivos accesorios.
 - Los gabinetes deben tener puerta y llave, como mínimo dos (02) ventiladores con ruido menores a 60 db y un PDU (Unidad de Distribución de Energía) de al menos 08 tomas eléctricas. asimismo, deberán colocar mallas o algún material en la parte inferior del gabinete, para evitar que ingresen roedores o animales dentro del gabinete.
 - Los gabinetes de piso tendrán una separación de 30 centímetros del nivel de piso (deben tener patas de metal que soporten como mínimo 200 kilos), el mismo que será fijado para que no sea movido de lugar.
 - En caso ya exista un gabinete y/o rack con patch panel y/o punto de llegada de cableado, el contratista deberá acondicionar la interconexión entre los gabinetes antiguo (gabinete preexistente) y el gabinete provisto (gabinete del contratista) considerando canaletas, cable utp y habilitado para su interconexión.
 - Cualquier cambio en la infraestructura, producto de la implementación solicitada debe ser refaccionada y dejarse con las mismas características que las encontró o mejoradas.
- El personal del contratista debe colocar de manera visible en la puerta frontal del gabinete un "aviso informativo del servicio de conectividad" en media cuartilla de tamaño A4 elaborado en lámina de polietileno con señalización en screen o vinilo autoadhesivo impreso en calidad laser o superior (considerar 4 colores) y el cual debe tener la siguiente información (referencial):
- Servicio de cableado estructurado de fibra (como título)
 - Incluido el logo de la PNP.
 - En caso de falla o deterioro de cableado estructurado de fibra (gabinetes, conexiones de fibra) llamar a la línea gratuita <0800 xxxxx> (número gratuito que proporcione el contratista).



- Numero de servicio (Circuito Digital) que el contratista asignara a cada sede policial a nivel nacional.
- Para presentar una queja y/o reclamo en la prestación del servicio o la atención de los incidentes enviar un correo a: centrodeatención@operador (correo referencial). Correo que proporcione el contratista.
- Adicionalmente estará las siguientes líneas:
 - Servicio de enlace de internet /intranet (como título)
 - En caso de falla en servicio enlace de internet /intranet llamar a la línea:
- (gratuita <0800 xxxxx> (número gratuito que proporcione el contratista).
- Numero de servicio (Circuito Digital) que el contratista asignara a cada sede policial a nivel nacional
- Ej.

-----21cm-----

(Logo PNP)
SERVICIO DE RED PRIVADA (INTRANET) PARA LAS UNIDADES POLICIALES A NIVEL NACIONAL, CON ACCESO A INTERNET

En caso de falla en servicio enlace de internet /intranet llamar a la línea gratuita:
 |
 | <0800 xxxxx.....>
 Numero de servicio (Circuito Digital)
 Para presentar una queja y/o reclamo en la prestación del servicio o la atención de los incidentes enviar un correo a: |
 |.....centrodeatención@operador
 15cm



DEL TRASLADO: durante la vigencia contractual el contratista se obliga a efectuar traslados a nivel nacional, a solicitud de la entidad, de la totalidad del servicio, componentes, equipamiento y materiales según el siguiente detalle:

- **Sede tipo 1:** 70 traslados del servicio a otro local policial a nivel nacional y 70 cambios de reubicación interna en la misma sede.
- **Sede tipo 2:** 20 traslados del servicio a otro local policial a nivel nacional y 20 cambios de reubicación interna en la misma sede. Asimismo, a partir del mes 25 de la ejecución del servicio, los traslados que no se hayan ejecutado en las sedes tipo 2 podrán ser efectuados en las sedes tipo 1, a solicitud de la entidad.
- El plazo de ejecución del traslado del servicio y reubicación interna, será hasta cuarenta y cinco (45) días calendario, posteriores a la solicitud por parte de la entidad. Durante el tiempo que se efectúe el traslado y/o reubicación, el Contratista deberá suspender el servicio.
- Para efectuar el traslado y/o reubicación del gabinete, se realizará en coordinación y previa autorización del personal de la entidad.
- Ante la "desactivación" de alguna sede por razones internas de la Entidad, el contratista, a solicitud de la Entidad, realizará el traslado de la plataforma de backbone o gabinetes según corresponda hacia otra sede a nivel nacional, dispuesto por la Entidad; asimismo, se considerará para este caso todas las Unidades PNP que estén o no referenciadas en los Anexos A ,A1,B1 y B2

- La provisión del servicio de la plataforma de backbone y gabinetes, según corresponda en cada sede para las sedes policiales desconcentradas a nivel nacional, será para mil dieciocho (1018) sedes de la policía nacional del Perú a nivel nacional, según relación detallada en el Anexo A del presente.
- Se debe considerar una bolsa de cableado de fibra óptica de 24 kilómetros para interconexión de los equipos de comunicación en las sedes policiales que la Entidad requiera, según Anexo A.

Equipamiento de sedes

Las sedes están detalladas en el Anexo A del presente, obteniendo un total de mil dieciocho (1018) sedes policiales de las cuales en (971) se proveerá un solo gabinete principal, en (47) la plataforma de backbone y por último la sede principal del ministerio del interior.

a. Sedes tipo 1

Provisión de gabinete principal en cada sede (967).

Provisión de la plataforma de backbone para (08) sedes.

La conexión entre el switch principal y los switches de distribución deberá ser por fibra óptica con un ancho de banda de 10 Gbps

b. Sedes tipo 2.

Provisión del gabinete principal en cada sede (4).

Provisión de la plataforma de backbone para (39) sedes.

La conexión entre el switch principal y los switches de distribución deberá ser por fibra óptica con un ancho de banda de 10 Gbps

c. Ministerio del Interior.

Provisión de la plataforma de backbone para la sede central del Ministerio Del Interior.

La conexión entre el switch principal y los switches de distribución deberá ser por fibra óptica con un ancho de banda de 10 Gbps.

El consolidado de la cantidad de cableado de fibra óptica, es el siguiente:

Nº	SERVICIO Y/O EQUIPAMIENTO	CANTIDAD
01	CABLEADO ESTRUCTURADO DE FIBRA OPTICA LAN (EN KM)	24

CARACTERÍSTICAS DE LA PLATAFORMA DE BACKBONE

- La conexión del Backbone será desde el gabinete central de comunicaciones hacia los gabinetes de distribución, de los Switch principal a los Switch de distribución empleando fibra óptica con un ancho de banda de 10 Gbps.
- Las llegadas de los enlaces con cable de fibra óptica para todos los extremos terminaran en una bandeja para fibra óptica al interior de un gabinete.
- La bandeja y la solución de fibra óptica para los gabinetes principales y de distribución deben contener los suficientes acopladores del tipo LC para conectar a todas las fibras ópticas que reciba. Los acopladores deben de ser de material cerámico.
- Los enlaces deben de ser de fibra óptica tipo multimodo de 4 hilos mínimo. Enlace principal debe de estar conectorizado en sus extremos. El Backbone de fibra óptica

deberá permitir transmisiones de hasta 10 Gigabit Ethernet por cada enlace de fibra multimodo de 50/125 μm . hasta una distancia de 300 mt. mínimo. Esta fibra óptica debe ser continua y libre de empalmes intermedios.

- El Jumper de Fibra Óptica es el cable utilizado para conectar los puertos de la Bandeja de Fibra Óptica con el equipo activo en red.
- El Sistema de Canalización del cableado en vertical o backbone es el que protege a la fibra óptica de todo su recorrido. Adicionalmente se debe dejar instalado una ruta libre para futuros servicios. En los tramos a proveer ductos de PVC, estos deben de ser de alta densidad de al menos 3" de diámetro y con accesorios de pase en las curvaturas, considerar además proveer abrazaderas para fijar estos tubos y las cajas de paso a paredes y/o techos. Estos accesorios deben permitir la provisión del cable de fibra óptica.
- Dimensionamiento y provisión de un tablero eléctrico para control de los gabinetes principales y de distribución, el tablero incluirá todas las llaves termomagnéticas para la totalidad de circuitos. Dicho punto debe ser cubierto adecuadamente con canaletas de piso y/o pared.
- Provisión del cableado de energía hacia cada uno de los paneles de energía de los gabinetes principales y de distribución. El dimensionamiento del calibre del cable lo realizara el contratista.
- Dimensionamiento y provisión de un sistema de cableado matriz de tierras para gabinetes de comunicación. Estos cableados de tierra partirán desde el tablero de distribución de tierras hacia el tablero de Gabinetes principales y a los diferentes gabinetes de distribución, el cable de tierra que acometerá será dimensionado por el proveedor y terminará en una barra de tierra propia del interior del tablero y de los gabinetes.
- Pruebas de continuidad y aislamiento del sistema.
- Los componentes de conexión de fibra óptica deben de ser de la misma marca y fabricante. Ellos comprenden a los citados a continuación: Bandeja de Fibra, acopladores y Jumper de Fibra.

Backbone de Fibra Óptica

- El cable de fibra óptica a emplearse debe permitir transmisiones de hasta 10 Gigabit Ethernet en una distancia de 300 metros (según la IEEE802.3e) por cada enlace de fibra multimodo de 50/125 μm . Esta fibra óptica debe ser continua y libre de empalmes intermedios.
- Cada fibra debe de tener un diámetro de core de μm y un diámetro de cladding de 125 μm . Debe cumplir con las especificaciones de dispersión de la IEC 60793 y la EIA/TIA 492 para fibras de 50/125 μm .
- Cada enlace de fibra óptica instalado debe ser compatible con protocolos Ethernet, Fast Ethernet, Gigabit Ethernet y 10 Gigabit Ethernet.
- Cada hilo de extremo debe tener conectores de tipo LC para unirse con los acopladores de la bandeja de fibra óptica. El conector y el acoplador deben ser de material cerámico.
- Los gabinetes de distribución deberán de conectarse por medio de la fibra óptica de 50/125 μm , a su respectivo gabinete principal.

Bandeja de Fibra Óptica

- La bandeja de fibra óptica se ubica en los gabinetes de comunicaciones para recibir a la fibra óptica del Backbone en los acopladores.
- La bandeja para fibra óptica para los gabinetes sede ser de 19" para ser montado sobre los bastidores de los gabinetes. La máscara de la bandeja debe



ser de material metálico, con tapa. Cada bandeja debe contar con un sistema de enrollamiento para la fibra óptica.

- o La bandeja y la solución de fibra óptica para los gabinetes deben contener los suficientes acopladores del tipo LC para conectar a todas las fibras ópticas que reciba. Los acopladores deben ser de material cerámico.

Jumper de Fibra Óptica

- o El Jumper de Fibra Óptica es el cable utilizado para conectar los puertos de la Bandeja de Fibra Óptica con el equipo activo de red y entre estos.
- o Los jumpers de fibra óptica a entregar deben ser dúplex con conectores LC en ambos extremos, garantizando un perfecto recorrido por los ordenadores de cables.
- o El Jumper de Fibra Óptica debe ser del tipo multimodo 50/125 μm , y deben estar certificados por el fabricante para ser compatibles con protocolos Ethernet, Fast Ethernet, Gigabit Ethernet y 10 Gigabit Ethernet.
- o El cable de Jumper de Fibra Óptica debe contar con propiedades de retardo a la propagación de flama.
- o La pérdida de inserción típica del Patch Cord se deberá de acuerdo a ANSI/TIA/EIA 568C.3.

b. GABINETE DE COMUNICACIONES.

EL contratista suministrara los gabinetes que sean necesarios para la instalación del servicio, debiendo considerar las dimensiones, accesorios y partes, que sean necesarios para la implementación y disponibilidad del servicio; En tal sentido, considerará los estándares internacionales para dicha ejecución.

- c. **Estabilizadores de ocho (8) tomas eléctricas**, y para los casos donde la corriente no es estable, el proveedor debe proveer estabilizadores ferroresonantes para mitigar las fallas de energía.

De los materiales

El ingreso de los materiales a las unidades policiales deberá ser reportado al personal policial a cargo, a fin de que este realice la inspección correspondiente.

Limpieza y eliminación de desmonte

El contratista está obligado a mantener una limpieza permanente en todas las áreas de trabajo y eliminar todo el material excedente y/o desmonte producto de los trabajos realizados, a fin de que las áreas queden limpias, libre de escombros, residuos, desmonte, basuras, etc.

Si para el correcto diseño y dimensionamiento se necesita empotrar tubos, este debe ser provista por el contratista, sin perjuicio para el área usuaria.

El Contratista debe tomar las debidas precauciones para evitar dañar las instalaciones y en caso esto suceda ejecutar inmediatamente su respectiva restauración. También mantendrá los lugares de trabajo libre de cualquier desecho, producto de la utilización de los materiales propios del trabajo a realizar.

Se debe tomar las previsiones del caso para que los trabajos que se desarrollan no interfieran con el normal cumplimiento de las funciones propias de la oficina.



En coordinación con el personal de la DIRTIC-PNP, se establecerán los horarios normales y especiales (de ser necesario) para realizar los trabajos.

La provisión de gabinetes y la plataforma de dentro de las unidades policiales Tipo 1 y Tipo 2 y sede ministerio del interior, será coordinada entre el Jefe de Proyecto del CONTRATISTA y el personal encargado de la DEPGCD PNP, este último será quien finalmente aprobará la referida distribución

5.2.1.5.3.2 Sub-componente B:

5.2.1.5.3.2.8 Servicio de conexión de enlace MPLS y/o METROETHERNET, para los nodos principal y secundario de la Policía Nacional.

Corresponde a un servicio de conexión de enlace VPN (Intranet PNP), a través de una red tipo MPLS y/o METROETHERNET, para los nodos principal y secundario de la Policía Nacional del Perú.

Las líneas de transmisión requeridas serán instaladas en las siguientes ubicaciones:

No.	Cantidad de hilos	Ubicaciones
1	2	DATACENTER PNP ubicado en el local del Ministerio del Interior en la Plaza 30 de agosto s/n Urb. CORPAC San Isidro (2do nivel).
2	2	DATACENTER propuesto por el Contratista

Condiciones generales:

- Toda la conexión debe ser usando el medio fibra óptica.
- Todos los enlaces deben ser simétricos, de Cinco (05) Gbps por cada uno (05 Gbps de subida y 05 Gbps de bajada).
- Para la sede principal, deberá contar con dos (02) circuitos de acceso a la VPN, una como línea dedicada principal y otra como contingencia, de tipo simétrica, de 05 Gbps de ancho de banda cada una, con tasa de acceso garantizada al 100% (overbooking 1:1) empleando como medio físico fibra óptica.
- Para la sede secundaria, deberá contar con dos (02) circuitos de acceso a la VPN, una como línea dedicada principal y otra como contingencia, de tipo simétrica, de 05 Gbps de ancho de banda cada una, con tasa de acceso garantizada al 100% (overbooking 1:1) empleando como medio físico fibra óptica.
- Equipo Router con las características técnicas mínimas que garantice el acuerdo de nivel de servicio del 99.5%
- La comunicación entre las Unidades debe realizarse bajo el esquema de un grupo cerrado de usuarios, para tal efecto debe asignarse direcciones IP privadas para cada acceso simétrico.
- A requerimiento de la entidad las líneas de transmisión contratadas deben estar configuradas en una configuración de alta disponibilidad activo/activo, con balance carga, que permita distribuir los enlaces de las sedes policiales en cargas similares distribuidas en las dos líneas de datos conectadas a las sedes Principal y Secundaria, se señala que la Entidad posee un servicio de directorio de Microsoft con un servicio DNS integrado al mismo y que será utilizado para la resolución de nombres de dominio de los recursos de red de la Intranet PNP, dichos servidores estarán distribuidos en Primario en la Sede principal y Secundario.





- El servicio debe estar preparado para migrar a mayores velocidades, al menos, el 20% de lo contratado, sin cambiar de equipamiento.
- La Entidad cuenta con una red híbrida, la misma que está compuesta por una red privada (nube privada) que brinda servicios a su público interno y una red pública (internet) mediante la cual se brinda servicios a la ciudadanía, por tanto, el servicio debe tener la capacidad de dar visibilidad y optimizar aplicaciones (gestión de aplicaciones a través del equipamiento que el postor considere), tanto locales como de nube, según necesidades de la Entidad. Este permitirá un menor consumo de ancho de banda y una mayor flexibilidad. La configuración deberá ser realizada mediante el equipamiento router y/o firewall respectivo.
- El contratista será responsable de efectuar y proveer las herramientas y actividades necesarias para la correcta implementación del servicio.
- La administración de todas las soluciones y equipamiento solicitado por la Entidad, serán de administración compartida, en ese sentido, el contratista entregará credenciales de usuarios a nivel de read/write a usuarios designados por la Entidad.
- La Infraestructura debe ser capaz de soportar múltiples aplicaciones en Red (hosting, voz sobre IP, Comercio en Red, Video broadcasting, etc.)
- El servicio debe proponer versatilidad para la conformación de Intranets y Extranet, aprovechando los propios servicios de la red.
- La infraestructura debe permitir contar con un alto grado de robustez y seguridad, que permitirá disponibilidades de 99.5% como mínimo.
- Se aceptará que la latencia entre sedes con enlaces será en promedio de 20 ms para Lima Metropolitana y 40 ms para provincias a nivel nacional. La latencia promedio solicitada será medida en condiciones, tal que no se supere el 70% del uso del ancho de banda nominal contratado.
- Para los puntos de Fibra Óptica estar será Canalizada y/o aérea desde el nodo del Operador hasta las diversas sedes de la PNP. Esta red debe ser propia del operador.
- La solución debe proporcionar gestión de incidencias y reportes permanente desde un Centro de Gestión, NOC, el cual estará en capacidad de realizar detección proactiva de alarmas tempranas, acciones de control preventivo, correctivo y pruebas técnicas.
- El contratista debe contar con un centro de llamadas para el reporte de fallas, atención de cambios en la configuración del sistema o el tratamiento de reclamos.
- La configuración de equipos para contingencia debe de funcionar de manera automática y transparente.
- El contratista debe garantizar trabajos simultáneos a fin de garantizar la continuidad del servicio.
- La red del contratista debe estar configurada en Full-mesh, para la conexión de todas las oficinas de la entidad.
- El Operador de Telecomunicaciones debe tener disponibilidad de protocolo de ruteo IPV4/IPV6, según Decreto Supremo 081-2017-PCM.
- El medio de última milla debe ser por Fibra óptica.
- El contratista del servicio realizará la interconexión que incluye la provisión y configuración de todos los equipos de comunicación necesarios para su funcionamiento; así como, para la integración de las redes de datos con las que cuenta la entidad.
- La configuración de la red privada virtual debe de contemplar los respectivos parámetros de seguridad informática que permitan entre otras cosas: autenticación y autorización entre los equipos de la red interna, integridad de los

datos enviados mediante algoritmos hash o similares, confidencialidad para que los datos sólo sean interpretados por los destinatarios usando algoritmos de cifrado. Dicha configuración se podrá hacer a través del equipamiento solicitado para los sitios 1 y 2, tales como firewall y/o router para el cumplimiento de las funcionalidades exigidas.

- La administración de los equipos quedará a cargo del contratista del servicio de comunicaciones, permitiendo a la Entidad acceder a los equipos de toda la solución a través de una administración (lectura/escritura) compartida, que personal técnico dispuesto por la Entidad tenga acceso de lectura/escritura a la gestión de los servicios y equipamiento propuesto y estos niveles de acceso y/o roles de gestión serán coordinados durante la etapa de implementación.
- El contratista debe proporcionar un acceso web y una comunidad SNMP que permita el monitoreo del consumo de ancho de banda y disponibilidad de los enlaces.
- La configuración IP de toda la plataforma será proporcionada a la Entidad. Esto quiere decir que, la configuración IP que el contratista realizará en toda la solución será proporcionada a la Entidad.
- El acceso a través de los canales de datos debe ofrecer un esquema de direccionamiento IP permanente.
- Todos los enlaces de comunicación deben garantizar el correcto funcionamiento de las siguientes aplicaciones y protocolos:
 - Voz sobre IP.
 - Terminal Server.
 - Citrix (Protocolo ICA)
 - HTTP, HTTPS, FTP, SFTP, SMB, TELNET, SNMP.
 - Otros protocolos de uso común que requiera la Entidad.
- Se debe garantizar la disponibilidad de poder aplicar prioridad de protocolos y aplicaciones de acuerdo al tráfico crítico, el sistema debe permitir como mínimo colas de prioridad y estos debe ser administrados por la Entidad y el equipo "in-house" (equipamiento que está instalado dentro de las sedes de la Entidad).
- La administración y gestión del servicio que incluye prioridad de protocolos y aplicaciones de acuerdo al tráfico crítico y otros, serán responsabilidad de la Entidad.
- Permite priorización de las comunicaciones según el tipo de tráfico cursado sin costo alguno a requerimiento de la Entidad, sin costo, y con uso ilimitado de cambios. Para ello, el contratista debe considerar un equipo "in-house" a disponibilidad de la Entidad. Este equipo in-house será el mismo para el sub-componente A- podrá hacer uso del equipamiento solicitado para los sitios 1 y 2, tales como firewall y/o router para el cumplimiento de las funcionalidades requeridas. Priorización se refiere a que la red debe operar bajo estándares de calidad de servicio.
- Se debe considerar la disponibilidad de cambio de equipos (hardware instalado) ante cualquier falla del mismo de manera inmediata (SLA solicitado en las bases).
- La disponibilidad de cambio de equipos se realizará según tiempo de atención. El contratista debe considerar equipamiento adicional del tipo redundante (SPARE) de todos los componentes, para tareas de respaldo y soporte durante todo el período de duración del contrato. Asimismo, el equipamiento del tipo redundante estará en custodia del contratista y sólo será utilizado para tareas de respaldo y soporte durante este período.



- El contratista está obligado a considerar todos los componentes, dispositivos y materiales que requiera para la integración de la solución adquirida con la red de la Entidad, así como para el cumplimiento de la finalidad del servicio requerido.

5.2.1.5.3.3 Sub-componente C:

5.2.1.5.3.3.9 Implementación de solución firewall para sedes policiales.

La finalidad del presente servicio consiste en brindar protección informática perimetral a los activos que se encuentran en las diferentes sedes policiales, según las condiciones o situaciones de la sede policial, se realizará la creación e implementación de políticas de protección perimetral, para el cumplimiento del presente servicio el contratista requiere implementar una solución firewall de próxima generación en cada sede policial que se indican en el Anexo 01, las políticas a implementar serán coordinadas con la Entidad, dicho equipamiento estará administrado a través de una consola de administración por el servicio de seguridad gestionado y personal de la Sección de Redes y Seguridad Informática del DEPGCD-DIVINF DIRTIC PNP.

EL contratista realizará las actividades necesarias para la integración de la solución indicada a la red MPLS y/o MetroEthernet a fin de cumplir con la finalidad del presente servicio, la solución de firewall deberá contar con las siguientes capacidades:

- Funcionalidades de router
- Control por políticas o similar,
- Control de aplicaciones o similar,
- Prevención de amenazas o similar,
- Análisis de malware moderno o similar,
- Filtro de contenidos o similar,
- Identificación de usuarios o similar,
- Calidad de servicio o similar,
- Filtro de datos o similar,
- Geolocalización o similar,
- Red privada virtual VPN o similar.

Sedes tipo 1 y 2 = Firewall de próxima generación para sedes policiales (1001)

Sedes tipo 2 = Firewall de próxima generación (Complejos 01) catorce (14 sedes en HA)

De acuerdo a los tipos de sedes que tiene la plataforma digital, el Contratista debe implementar el equipamiento necesario de seguridad para las sedes tipo 1 y 2 de acuerdo al Anexo 1. Los nodos principal y secundario (site 1 y site 2) estarán considerados en el Componente 4 Servicios de seguridad de la información y seguridad informática gestionada, para nodos principal y secundario.

5.2.1.5.3.3.10 Generalidades - Sedes tipo 2 - Firewall de próxima generación (Complejos 01) (14 sedes en HA):

Consideraciones:

- Adquisición de una solución de Next Generation Firewall (NGFW) para la seguridad de PNP.

- El equipo debe ser nuevo, de primer uso y que no se encuentre en End of Support por su fabricante.
- El Postor tiene la libertad de añadir consolas terceras para cumplir con los requerimientos técnicos solicitados, ya sea para capacidades de gestión, reportes y/o seguridad.
- El fabricante debe pertenecer al cuadrante de Líderes de Gartner para "Enterprise Network Firewall" o "Firewalls de Redes Empresariales" en los últimos 10 reportes.
- El fabricante debe estar catalogado como líder en el último informe de Forrester Wave Enterprise Firewalls

Requerimientos de soporte:

- Ninguno de los modelos ofertados podrá estar listados ni anunciado en el sitio web del fabricante como end-of-life, end-of-sale o end-of-support. Se deberá adjuntar el link público del fabricante que verifique que los modelos propuestos no están en ese listado.
- La solución propuesta deberá tener soporte vigente de fabrica durante la fecha de contrato del servicio, el soporte del fabricante deberá incluir atención de incidentes de software o hardware de la plataforma, reposición de partes o equipo de reemplazo en caso de falla de hardware.
- El soporte deberá estar disponible 24x7x365, la apertura de casos deberá poder realizarse vía online o vía telefónica.
- Se deberá proporcionar accesos al portal de soporte del fabricante, donde se tenga la potestad de dar seguimiento a los mismos.



FIREWALL DE PRÓXIMA GENERACIÓN	
CARACTERÍSTICAS	REQUERIMIENTOS MÍNIMOS
CARACTERÍSTICAS PRINCIPALES	<p>Firewall de próxima generación en alta disponibilidad</p> <ul style="list-style-type: none"> • Throughput de Prevención de Amenazas de 1.2 Gbps. Este throughput deberá estar medido con tráfico productivo real (transacciones usando una mixtura de aplicaciones de capa 7, transacciones medidas en condiciones empresariales), con las siguientes funcionalidades habilitadas simultáneamente: Control de aplicaciones, Sistema de Prevención de Intrusos (IPS), Seguridad del tráfico DNS, Antivirus/Antimalware de red, Antispyware/AntiBot, Sandboxing, Filtro de Archivos y Logging activo. Si el fabricante tuviese diferentes niveles o modos de inspección de seguridad, el equipo ofertado deberá soportar el throughput requerido con el modo más alto de inspección de seguridad. Se debe garantizar que el equipo no degrade su performance por debajo de lo requerido al habilitar los módulos de seguridad indicados en el modo más alto de inspección. No se aceptarán mediciones hechas con tráfico UDP o RFCs 3511, 2544, 2647 o 1242. • No se aceptarán cartas de fabricante como fundamento para el cumplimiento de performance, se deberá comprobar el requerimiento de throughput con documentación pública del fabricante adjuntando el link que lo respalde. Se deberá enviar una carta emitido por

	<p>el contratista con el link con documentación pública del fabricante que respalde la comprobación del requerimiento de throughput.</p> <ul style="list-style-type: none"> • La plataforma de hardware debe soportar hasta 190,000 sesiones (o conexiones) concurrentes y/o simultáneas y 30,000 sesiones (o conexiones) por segundo, medidos en capa 7 (con transacciones HTTP). En caso de que la solución propuesta no cuente con este tipo de métricas, el hardware deberá soportar hasta 2,500,000 de sesiones (o conexiones) concurrentes y/o simultáneas y 150,00 sesiones (o conexiones) por segundo, medidos en capa 4 (con transacciones TCP o en condiciones ideales). • Ocho (08) interfaces de red en cobre 10/100/1000, • Una (01) interfaz de fibra SFP 1Gbps (Se deberá incluir los transceivers originales de fábrica) • Un (01) interfaz de gestión fuera de banda RJ45 • Un (01) puerto de consola RJ45 • Dos (02) puertos USB • Deberá contar con fuentes redundantes donde de fallar una unidad, se pueda intercambiar sin interrupción del servicio • Deberá contar con dos (02) sistemas o dominios virtuales
CAPACIDADES DE NETWORKING	<ul style="list-style-type: none"> • El dispositivo de seguridad debe soportar VLAN Tags 802.1q, agregación de links 802.3ad, policy based routing o policy based forwarding, ruteo multicast, jumbo frames, sub-interfaces ethernet lógicas, NAT de origen y destino. • Debe soportar enrutamiento estático y dinámico (RIPv2, BGP y OSPFv2). • Debe ser capaz de operar en los modos Capa 3 (con capacidades completas de Ruteo y NAT), Capa 2, Transparente y Sniffer, de forma simultánea mediante el uso de sus interfaces físicas. • Soportar diferentes características de networking operando en el protocolo IPv6, como mínimo: ruteo estático OSPFv3, MP-BGP, policy based routing o policy based forwarding, ECMP, dual-stack, QoS, DSCP, NPTv6 o NAT66, NAT64, LLDP, BFD, DHCPv6 Relay, SLAAC, SNMP. • Debe soportar Multicast Source Discovery Protocol (MSDP). • La plataforma propuesta por el fabricante debe contar con certificación USGv6-r1 para las pruebas de Firewall, IDS e IPS
ALTA DISPONIBILIDAD	<ul style="list-style-type: none"> • Soporte a configuración de alta disponibilidad Activo/Pasivo y Activo/Activo, con despliegues de los equipos tanto en modo transparente como en modo capa 3 (L3).



	<ul style="list-style-type: none"> • La configuración en alta disponibilidad debe sincronizar: sesiones, certificados de descifrado, configuraciones, incluyendo, más no limitado a políticas de seguridad, NAT, QoS y objetos de red. • Debe ser posible el monitoreo de fallo de enlaces, ya sea ante la caída de al menos una de las interfaces del equipo, una conexión física adyacente o pérdida de conectividad hacia una IP desde una de las interfaces.
FUNCIONALIDADES DE FIREWALL	<ul style="list-style-type: none"> • Control de políticas puertos, direcciones IP, segmentos y/o rangos de red, región geográfica, usuarios y grupos de usuarios, aplicaciones, grupos estáticos de aplicaciones, grupos dinámicos de aplicaciones (basados en sus atributos). • Permitir agrupar las políticas de seguridad utilizando etiquetas u otro método. • Debe mostrar la primera y última vez que se utilizó una regla de seguridad, así como la cantidad de hits. • Debe mostrar la fecha de creación y última fecha de modificación de la regla de seguridad. • Debe permitir tener un registro de auditoría en cada política que permita conocer que cambios se realizó con anterioridad.
DESCIFRADO DE TRÁFICO SSL/TLS	<ul style="list-style-type: none"> • Debe permitir descifrar el tráfico de navegación de todos los usuarios a internet mediante la instalación de un certificado digital en los equipos. • Debe permitir descifrar el tráfico entrante hacia servidores HTTPS publicados en internet importando el certificado del servidor en el NGFW. • Deberá soportar al menos los siguientes algoritmos: RSA, DHE, ECDHE; 3DES, RC4, AES128, AES256, CHACHA20-POLY1305; MD5, SHA1, SHA256, SHA384. • Capacidad de bloquear la conexión hacia sitios web cifrados con protocolos obsoletos y/o no fiables, a pesar de no descifrar el tráfico. • Debe soportar certificados que utilicen Subject Alternative Name (SAN) y Server Name Indication (SNI). • Permitir el descifrado selectivo de categorías de URLs, por ejemplo, debe ser capaz de especificar excluir del descifrado a páginas con contenido sensible y descifrar el resto de las páginas. • Permitir excluir sitios a los cuales no se les aplicará la política de descifrado en base al Common Name del certificado. • Debe contar con un dashboard que muestre gráficamente la proporción del tráfico descifrado, aplicaciones y dominios con descifrado correcto, errores de descifrado, versiones de TLS usadas, entre otros. • Debe contar con un panel de logs dedicados a monitorear el tráfico de descifrado SSL/TLS, estos logs



	<p>deberán permitir una identificación rápida de problemas del descifrado.</p> <ul style="list-style-type: none"> • Desde la consola gráfica deberá mostrar todo el detalle de la sesión SSL/TLS identificada, tales como IP origen y destino, subject common name, issuer common name, server name indication, datos del certificado digital (fecha de expiración, serial number), versión de TLS, algoritmo asimétrico, algoritmo simétrico, hash, estado del descifrado (correcto o con error), motivo del error del descifrado. Este detalle de logs no deberá afectar el performance del equipo. • El postor tiene la libertad de incorporar en su oferta técnica una plataforma tercera que realice descifrado del tráfico y cumpla todas las especificaciones indicadas, en caso el NGFW propuesto no pueda realizarlo o no esté diseñado para ello. En caso de optar por esta alternativa, se deberá incluir una plataforma por cada una de las 14 sedes. Para este caso, el postor deberá presentar como documentación sustentatoria para su oferta, una Carta del Fabricante de los equipos de Firewall de próxima generación, en la cual se evidencie el cumplimiento técnico según corresponda considerando lo descrito en el párrafo anterior.
<p>VISIBILIDAD EN CAPA 7 Y CONTROL DE APLICACIONES</p>	<ul style="list-style-type: none"> • La solución propuesta deberá reconocer por lo menos 20,000 aplicaciones, incluyendo, más no limitando a aplicaciones de tipo peer-to-peer, redes sociales, acceso remoto, update de software, protocolos de red, voip, audio, vídeo, proxy, mensajería instantánea, email. • Las aplicaciones deberán estar clasificadas en al menos 30 tipos, de tal manera que se puedan configurar políticas en base al tipo de aplicación. • Las aplicaciones deberán contar con atributos descriptivos tales como tipo, nivel de riesgo y etiqueta. • Deberás ser capaz de mostrar información contextual por cada aplicación SaaS, mostrando las regulaciones que cumple, controles de seguridad que cumple, entre otros. • Deberá ser posible definir grupos de aplicaciones en base a sus atributos, por ejemplo, un grupo de aplicaciones de riesgo alto que sea dinámicamente alimentado. • Para tráfico cifrado (SSL/TLS), debe permitir el descifrado de paquetes con el fin de permitir la lectura del payload de la aplicación cifrada. • Debe inspeccionar el payload del paquete de datos con el objetivo de detectar las aplicaciones en capa 7, a través de expresiones regulares, firmas u otro mecanismo. Debe ser capaz de determinar si una aplicación está utilizando su puerto default o no, por ejemplo, RDP en el puerto 80 en vez del 3389.





	<ul style="list-style-type: none"> • Las políticas de seguridad deben poder definirse netamente en base a aplicaciones, sin necesidad de especificar puertos. • Las políticas de seguridad deberán poder definirse 100% en base a aplicaciones pudiendo aplicar reglas específicas a cada aplicación. Es decir, si 2 aplicaciones utilizan el mismo puerto y protocolo, se debe poder crear 2 políticas de seguridad en las cuales se apliquen controles diferentes a cada aplicación. • Con el objetivo de controlar aplicaciones propietarias en capa 7, la solución debe permitir la creación de aplicaciones personalizadas desde la interfaz de gestión. • Deberá contar con un módulo de aprendizaje que permita migrar las políticas basadas en puertos específicos y políticas con puertos ALL/ANY, a políticas basadas en aplicaciones. • El módulo de aprendizaje deberá ser específico por cada política de seguridad. • El módulo de aprendizaje deberá mostrar el nombre de la(s) aplicación(es) que han pasado por una política de seguridad, fecha de primera y última ocurrencia y volumen de datos transferido por cada aplicación. • Deberá contar con un wizard que permita convertir una política basada en puertos (capa 4) a una política basada en aplicaciones (capa 7) en base al aprendizaje realizado. • Este módulo de aprendizaje deberá estar operativo de manera nativa, así la política no esté configurada con el módulo de control de aplicaciones. • Para todas las políticas de seguridad, deberá ser posible especificar la aplicación directamente en la misma política, como un criterio más, no como un perfil. • En caso la solución propuesta no tenga este módulo de aprendizaje, el postor deberá incluir en su oferta técnica el servicio de configuración/migración de todas las políticas de seguridad basadas en puertos, a políticas basadas en aplicaciones, este servicio deberá ser realizado por el área de servicios profesionales del propio fabricante. Considerar un estimado de 1,400 políticas de seguridad entre todos los dispositivos de este tipo de sede. Para este caso, el postor deberá presentar como documentación sustentatoria en su oferta, una Carta del Fabricante de los equipos de Firewall de próxima generación, en la cual se evidencie que será el fabricante el que realizará la configuración/migración según corresponda considerando lo descrito en el párrafo anterior.
PREVENCION DE AMENAZAS	<ul style="list-style-type: none"> • La solución propuesta deberá contar con capacidades de IPS (Intrusion Prevention System), Antivirus/Antimalware, Antispyware/Antibot.



- El equipo deberá soportar el throughput solicitado operando en el máximo nivel o modo de seguridad de inspección de IPS, Antivirus y Antispyware/Antibot.
- El módulo de IPS debe ser capaz de bloquear ataques en base a firmas, heurística y anomalías en el protocolo.
- El módulo de IPS debe permitir personalizar firmas directamente desde la consola gráfica.
- Este tipo de análisis deberá realizarse en línea, para bloquear la amenaza antes de que el NGFW deje pasar el tráfico.
- Respecto a ataques de malware, las firmas deberán estar basadas en patrones y no únicamente en hashes, con el objetivo de identificar y bloquear el malware polimórfico que pertenezca a una misma familia.
- Con la finalidad de contar con una protección robusta contra amenazas emergentes a nivel mundial, la solución deberá ser capaz de actualizar su base de datos de firmas de malware en tiempo real sin afectar el rendimiento del equipo.
- Adicionalmente al uso de firmas y heurística para la protección contra el malware, exploits, command & control y otro tipo de amenazas, la solución deberá contar con mecanismos avanzados basados en inteligencia artificial (algoritmos de machine learning y deep learning específicamente entrenados para tal fin) para prevenir la transferencia de dichas amenazas por la red. Estos algoritmos deberán ser capaces de identificar al menos los siguientes tipos de ataques: inyección de comandos, cobalt strike, command & control, malware 0-day camuflado en al menos archivos de tipo Ejecutables, Powershell, Office, ELF, Shell y otros.
- Debe ser capaz de realizar análisis basado en deep learning de manera local en el mismo NGFW, para detectar y bloquear amenazas de día cero.
- El análisis basado en algoritmos de machine learning y deep learning deberá ser realizado en línea y de manera inmediata, el archivo y tráfico analizado deberá ser retenido hasta que finalice el análisis. Con el objetivo de evitar el ingreso por pacientes cero.
- Debe permitir customizar firmas de IPS en capa 7, así también a nivel de capa 3 y capa 4 con los parámetros de la cabecera del paquete de red.
- Debe ser permitir convertir las firmas de IPS basadas en la sintaxis de Snort y Suricata automáticamente a la plataforma.
- Debe ser capaz de detectar y bloquear el virus y malware en general que se propague en, al menos, los siguientes protocolos: HTTP, HTTPS, HTTP/2, FTP, SFTP, SMB, SMTP, IMAP y POP3.
- Deberá incorporar un módulo de automatización, que permita colocar una IP y Usuario dentro de un grupo de

	<p>cuarentena, si el Firewall identifica que dicha IP y/o Usuario están realizando acciones maliciosas o si dicho equipo se encuentra comprometido (por ejemplo, ser parte de una botnet, tener actividad de command & control, estar realizando movimiento lateral, intentar explotar vulnerabilidades dentro de la red interna). Estas acciones, deberán poder ser personalizadas en la consola del equipo.</p> <ul style="list-style-type: none"> • Mientras que la IP y/o Usuario se encuentren dentro del grupo de cuarentena, la solución deberá ser capaz de bloquear todo tipo de comunicación que intente atravesar el Firewall; deberá permitir configurar excepciones para este tipo de restricción.
<p>PREVENCIÓN DE AMENAZAS AVANZADAS CAMUFLADAS EN DNS</p>	<ul style="list-style-type: none"> • Todo el tráfico DNS deberá ser analizado en su totalidad y de manera multicapa. La primera capa de análisis deberá consistir en verificar la reputación del dominio, si éste es malicioso se deberá bloquear el DNS Query; la segunda capa de análisis deberá consistir en el uso de algoritmos de inteligencia artificial en tiempo real, para detectar amenazas sofisticadas (en donde no se tiene conocimiento de la reputación, ni una firma del dominio analizado), tales como ataques de DGA o Tunneling. • La solución deberá identificar las consultas que realizan los hosts infectados hacia dominios maliciosos, de tal forma que se pueda bloquear dichas consultas DNS. • Ser capaz de identificar los equipos potencialmente infectados en base al análisis de su tráfico DNS, inclusive si el tráfico entre la potencial víctima y su servidor DNS utilizado no pasa por el NGFW. • Deberá utilizar el método de DNS Sinkhole para interceptar solicitudes DNS maliciosas. • Deberá ser capaz de identificar amenazas sobre el tráfico DNS encriptado camuflado sobre HTTPS (DNS over HTTPS – DoH), y también DNS sobre TLS. • El análisis del tráfico DNS deberá analizar tanto el Query así como el Response. • El análisis del tráfico DNS se podrá realizar de manera local en el mismo equipo o a través del redireccionamiento del tráfico DNS hacia una plataforma externa (en nube u onpremise) del mismo u otro fabricante. • En caso de que el NGFW propuesto no cuente con estas capacidades, se aceptará que el postor integre en su oferta una solución de otro fabricante que cubra estos requerimientos. • El análisis del tráfico DNS no deberá requerir desplegar infraestructura adicional en la Entidad, ni hacer cambios de configuración en los servidores DNS. El NGFW deberá ser capaz de redireccionar todos los Querys DNS a una nube de procesamiento escalable,



	<p>que utilice inteligencia artificial para el análisis avanzado de este tipo de amenazas.</p> <ul style="list-style-type: none"> • En caso de ser una plataforma en nube deberá estar certificado en SOC2 Tipo II de AICPA. • La nube de procesamiento deberá estar certificada en SOC2 Tipo II de AICPA. • Los algoritmos basados en inteligencia artificial deberán ser capaces de prevenir ataques como DGA (Domain Generation Algorithm) Random y de Diccionario, DNS Tunneling, Fast Flux Domains, NXNS Attack, DNS Rebinding, abuso de wildcards, CNAME cloaking, infiltración de DNS. • Deberá soportar el manejo de excepciones para poder mitigar los falsos positivos. • Deberá contar con dashboards y estadísticas sobre la cantidad, tipo de peticiones DNS, clasificación de la amenaza, veredicto del tráfico DNS (benigno, maligno), generadas por los dispositivos internos de la Institución. • El dashboard deberá permitir identificar potenciales equipos comprometidos dentro de la red interna, a partir del análisis avanzado de su tráfico DNS.
<p>ANÁLISIS DE MALWARE DE DÍA CERO</p>	<ul style="list-style-type: none"> • La plataforma de Sandbox podrá ser ofrecido en Nube (Cloud), On-premise o ambos. • La plataforma de Sandbox podrá ser ofrecido en Nube e integrado nativamente a los NGFW, de tal manera que no requiera dar mantenimiento a infraestructura física adicional. • Con la finalidad de promover la pluralidad de postores, el postor podrá incluir en su oferta técnica soluciones de sandbox del mismo fabricante del NGFW o un tercero capaz de cumplir todos los requerimientos técnicos solicitados. Para este caso, el postor deberá presentar como documentación sustentatoria en su oferta, una Carta del Fabricante de los equipos propuestos, en la cual se evidencie el cumplimiento según corresponda considerando lo descrito en el párrafo anterior. • Deberá ser capaz de emular el potencial malware en entornos Windows, Linux y MacOS. • El análisis dinámico deberá realizarse de forma paralela para todos los archivos enviados y no deberá tomar más de 10 minutos en dar un veredicto. • En caso de tratarse de una plataforma de Sandbox Cloud, deberá cumplir con los siguientes requerimientos: • El NGFW deberá ser capaz de enviar al menos 1000 archivos por hora al sandbox, todos los archivos deberán ser analizados dinámicamente (emulación) de manera paralela y el tiempo de análisis por cada archivo no deberá ser mayor a 10 minutos. • Deberá tener una disponibilidad de al menos 99.9% contabilizados mensualmente.





- Deberá garantizar la privacidad y confidencialidad del contenido de los archivos analizados, para lo cual se requiere que el servicio cuente como mínimo con certificaciones SOC2 Plus de AICPA, ISO 27001, ISO 27017 e ISO 27018.
- En caso de tratarse de una plataforma de Sandbox On-premise, deberá cumplir con los siguientes requerimientos:
 - Deberá soportar un throughput de 1 Gbps
 - Debe tener una capacidad de procesamiento de al menos 1000 archivos por hora realizando análisis dinámico (entiéndase por análisis dinámico aquel que no está basado en firmas, ni prefiltros, sino en emulación completa del potencial malware).
 - Deberá ser desplegado en Alta Disponibilidad (Activo-Pasivo) en cada sede, con el objetivo de mantener los controles de seguridad en caso de contingencia.
 - Deberá estar desplegado en la interfaz LAN del NGFW, de tal forma que por lo menos tenga visibilidad de todos los archivos descargados por los usuarios desde internet.
- Debe proveer información forense sobre las acciones realizadas por el malware, tales como resumen del comportamiento visto, actividad sobre los archivos, peticiones DNS, conexiones de red, actividad de los archivos, procesos y registros. Esta información deberá poder ser extraída en un reporte PDF.
- Deberá ser capaz de analizar archivos sospechosos que se transfieran por los protocolos SMTP, POP3, IMAP, SMB, FTP, HTTP y HTTPS.
- Debe ser capaz de identificar amenazas de tipo Fileless.
- Deberá soportar por lo menos el análisis de los siguientes tipos de archivos: Flash, Batch, DLL, HTML, Java, Javascript, Archivos Office, PDF, Portables/Ejecutables, Powershell, Python, RAR, 7zip, Shell, VBS, MSI, LNK, ELF, PKG, DMG, APK, DEX.
- Luego del análisis realizado por el sandbox, éste deberá generar automáticamente las firmas de malware y bloquear el acceso a las URLs maliciosas utilizadas por el malware. Las firmas deben estar basadas en patrones del malware y no únicamente hashes, de tal forma que sea capaz de bloquear el malware polimórfico con una única firma. Estas firmas deberán ser distribuidas automáticamente al NGFW o en su defecto estar instaladas dentro de la misma plataforma Sandbox (en caso de ofertar una solución on-premise)
- Deberá ser capaz de analizar URLs desconocidas (es decir, no categorizadas en la base de datos del fabricante) con técnicas avanzadas basadas en

	<p>propiedades y el comportamiento del sitio web, con el objetivo de identificar si es un sitio Phishing o no.</p> <ul style="list-style-type: none"> • Debe permitir al administrador la descarga del archivo original analizado por el sandbox. • Debe permitir reportar al fabricante eventos que son falso-positivo y falso-negativo en el análisis de malware de día cero a partir de la propia consola de administración. • Permitir la subida de archivos al sandbox de forma manual y vía API, con el objetivo de automatizar las tareas de análisis dinámico. • Debe detectar técnicas usadas para evadir herramientas de sandboxing como detección de hypervisor (no debe usar hypervisores comerciales), inyección de código a procesos permitidos y deshabilitación de funcionalidades de seguridad del host.
<p>FILTRO DE CONTENIDO WEB</p>	<ul style="list-style-type: none"> • Debe poseer al menos 70 categorías de URLs, incluyendo las de malware, command and control, proxy, phishing, redes sociales, páginas de adultos. • Debe soportar un cache local de URLs en el dispositivo, evitando el delay de comunicación/validación de las URLs • Debido a que diariamente se crean más de 100,000 nuevas páginas web y muchos atacantes usan mecanismos anti-crawling (para evitar ser categorizados por tecnologías de seguridad), la solución deberá ser capaz de analizar en línea y en tiempo real aquellas páginas que no se encuentran categorizadas en la base de datos de reputación del fabricante, con el objetivo de identificar contenido malicioso que intente infectar el equipo del usuario que navega a internet. • El análisis en línea y en tiempo real deberá ejecutarse al momento que un usuario intente acceder a una URL y retener su acceso hasta finalizar el análisis, éste deberá estar basado en algoritmos de machine learning y deep learning, con el objetivo de detectar amenazas camufladas en contenido javascript, websites asociados a command & control, link cloaking, entre otros. • La protección basada en inteligencia artificial también deberá ser capaz de identificar y bloquear el acceso a páginas de phishing de día cero, analizando los diferentes atributos del sitio web que intente robar las credenciales del usuario. Se precisa que este análisis también deberá ejecutarse en línea y en tiempo real, cuando un usuario intente acceder a una página potencialmente phishing que no se encuentra categorizada en la base de datos del fabricante. • Debe contar con medidas de antievasión como Cloaking, Captcha falsos, codificación de caracteres HTML, entre otros.



	<ul style="list-style-type: none"> • Debe permitir la creación de categorías personalizadas. • Debe permitir la personalización de la página de bloqueo. • Debe permitir notificar al usuario, mostrándole solo una página de alerta personalizable, pero permitiéndole continuar la navegación al site. • Debe ser capaz de registrar el User-agent, Referer, XFF de cada sesión hacia internet • Debe ser capaz de forzar la navegación de los usuarios en el modo Safe Search Enforcement. • Debe identificar cuando un usuario envía credenciales corporativas de red a sitios no autorizados y debe poder bloquear dicho envío, previniendo así ataques de robo de credenciales.
<p>IDENTIFICACION DE USUARIOS</p>	<ul style="list-style-type: none"> • Debe permitir la creación de políticas de seguridad basadas en la identidad del usuario y grupo al cual pertenece, a través de la integración de servicios de autenticación como Active Directory, Novell eDirectory, Open LDAP y base de datos local. • Debe contar con varios mecanismos para la identificación del usuario y la dirección IP del equipo en donde se encuentra autenticado. Como mínimo deberá poder integrarse a las siguientes plataformas para cubrir este requerimiento: <ul style="list-style-type: none"> ○ Eventos de login gestionados en Domain Controller. ○ Terminal Server de Microsoft o Citrix ○ Consultando directamente a cada estación de trabajo a través del protocolo WMI ○ Capacidad de leer eventos de login y logout usando el protocolo WinRM. ○ Lectura de la cabecera XFF al integrarse con soluciones terceras de Proxy ○ Capacidad de extraer la información de IP y usuarios a través de la lectura y extracción de datos del tráfico syslog. ○ Integración con soluciones de Wireless LAN Controller basadas en 802.1x y Soluciones NAC, con el objetivo de que el NGFW no dependa del Domain Controller para identificar al usuario. ○ A través de agentes instalados en las estaciones de trabajo, que reporten directamente al NGFW el usuario y dirección IP de cada equipo. • Deberá contar con un componente que permita integrarse a diversas plataformas de identidades tales como Azure LDAP, Google Directory, Okta, Cisco Duo, PingID. • Debe contar con la funcionalidad de Portal Cautivo (Captive Portal), de tal manera que el NGFW muestre un portal al usuario para que se autentique



	<p>manualmente. Las cuentas podrán ser definidas localmente en el NGFW o integradas con plataformas terceras.</p> <ul style="list-style-type: none"> • Debe tener integración con plataformas de MFA (Multi Factor Authentication), de tal forma que cuando un dispositivo requiera acceder a recurso, se le solicite el OTP.
SD-WAN	<ul style="list-style-type: none"> • La solución debe soportar una consola de monitoreo con la capacidad de poder identificar fácilmente las aplicaciones y enlaces sus estados dentro de la red de SD-WAN (aplicaciones con problemas de jitter, latencia, pérdida de paquetes y sus diferentes estados dentro de la red) pudiendo ver el estado de estas en por lo menos en los últimos 5 minutos, última hora, último día o bien haciendo filtros personalizados. • La solución debe soportar la capacidad de poder monitorear la salud de los enlaces en términos de jitter, latencia y pérdida de paquetes, tomando decisiones inteligentes de enrutamiento basado en la condición de los enlaces de manera dinámica. • La solución debe soportar con la posibilidad de hacer reportes del estado de los enlaces y aplicaciones, indicando volúmenes de datos con respecto a las veces que fueron degradados o afectados. • Soportar la opción de cambiar dinámicamente de camino al detectar alguna degradación del enlace sin afectar o cortar la sesión establecida de la aplicación, es decir, que el usuario no perciba corte en la aplicación, ni tener que reiniciar la sesión. • Soportar de algoritmo de corrección de errores (FEC - Forward Error Correction) con el objetivo de poder garantizar una buena experiencia en el uso de aplicaciones de voz y video a través de la red de SD-WAN. • Soportar la transmisión de paquetes duplicados por diferentes enlaces al utilizar la red de SD-WAN con el objetivo de mantener una calidad de experiencia alta al usar aplicaciones de misión crítica y prevenir la pérdida de paquetes, incremento de latencia, jitter, etc. • Soportar la opción de monitorear la salud de los enlaces a través de aplicaciones de SaaS y aplicaciones de Cloud, para poder determinar si esas aplicaciones son enviadas a internet de manera directa o bien a través de algún camino de la red de SD-WAN. • Soportar la capacidad de definir el tiempo de intercambio de heartbeats entre los puntos del túnel SD-WAN. • Deberá soportar la funcionalidad de SD-WAN en interfaces agregadas (IEEE 802.1AX) y en subinterfaces. • Debe soportar configuraciones de SDWAN en IPv6 • Soportar fail over a nivel de sub segundos



	<ul style="list-style-type: none"> • Soportar dashboards de monitoreo basado en el rendimiento de una aplicación y del enlace físico.
ADMINISTRACIÓN	<ul style="list-style-type: none"> • Se deberá entregar una consola de administración centralizada o en su defecto deberán ser administrados por la consola central de administración de los Firewalls de Datacenter. • En caso el postor haya integrado tecnologías de terceros externas al NGFW, también se deberá considerar dentro de la propuesta técnica la consola de gestión para dicha tecnología. Para este caso, el postor deberá presentar como documentación sustentatoria en su oferta, una Carta del Fabricante de los equipos, en la cual se evidencie el cumplimiento técnico, según corresponda, considerando lo descrito en el párrafo anterior. • Debe permitir exportar las reglas de seguridad del NGFW en formato CSV y PDF • Debe contar con un dashboard interactivo y gráfico que permita monitorear el uso de las aplicaciones en capa 7, sitios web visitados, actividad de los usuarios, actividad por IP (origen y destino), países origen y destino del tráfico, uso de las reglas de seguridad, actividad del tráfico malicioso. Esta información podrá ser vista en base a Bytes y Sesiones, y ser filtrado en base a un rango de tiempo, IP, usuario, país y regla de seguridad. • Debe permitir el control de acceso a la gestión del equipo a través de roles personalizables. • Debe permitir la captura de paquetes en formato PCAP para poder ser leídos por una herramienta tercera. La captura de paquetes deberá poder ser filtrada antes del proceso de ejecución en base a la interfaz, IP y Puerto (origen y destino) • Ante escenarios donde existan dos o más administradores en el equipo, logueados y realizando cambios en simultáneo en la consola de gestión, la solución deberá de ser capaz de solo aplicar los cambios realizados por cada administrador individual, sin afectar o sobrescribir los cambios del otro administrador. • Contar con un módulo que permita comparar y que indique específicamente que cambio se hizo a una política de seguridad respecto a una versión anterior de dicha política. • Debe poder realizar una copia de seguridad (backup) automática de las configuraciones y rollback de configuración a la última configuración salvada. • Debe permitir el monitoreo de eventos basados en SNMP, integración con SIEM a través de Syslog, y envío de alertas por correo electrónico (integrándose a un servidor SMTP). • Debe permitir la generación de logs de auditoría detallados, informando de la configuración realizada, el



	<p>administrador que la realizo, su IP y el horario de la alteración.</p> <ul style="list-style-type: none"> • La gestión de NGFW debe permitir la asignación de una cuota de uso de disco para definir una capacidad máxima de almacenamiento de logs de tráfico de datos, amenazas, auditoría de configuraciones, eventos de sistema. • Debe soportar la personalización de reportes, permitiendo mostrar información de eventos de antivirus, antispyware, IPS, navegación a internet, aplicaciones, malware de día cero, debe permitir seleccionar las columnas a mostrar, filtrar la información en base a usuarios, grupos de usuarios, direcciones IP, el rango de fechas de los datos, deben poder ser exportados en PDF y enviados automáticamente vía correo electrónico. • Debe permitir configurar reportes para ver el tiempo de navegación de los usuarios en internet, clasificado por tipo de página web y URL. • Debe contar con reportes predeterminados que muestren información y diversas estadísticas sobre el uso de aplicaciones SaaS. • La gestión de NGFW debe permitir realizar tareas de gestión a través del API basado en XML.
--	---



5.2.1.5.3.3.11

Generalidades – Firewall de próxima generación para sedes policiales (1001) distribuidos para sedes del tipo 1

Consideraciones:

- Adquisición de una solución de Next Generation Firewall (NGFW) para la seguridad de PNP.
- El equipo debe ser nuevo, de primer uso y que no se encuentre en End of Support por su fabricante.
El Contratista tiene la libertad de añadir consolas terceras para cumplir con los requerimientos técnicos solicitados, ya sea para capacidades de gestión, reportes y/o seguridad.
- El fabricante debe pertenecer al cuadrante de Líderes de Gartner para "Enterprise Network Firewall" o "Firewalls de Redes Empresariales" en los últimos 10 reportes.
- El fabricante debe estar catalogado como líder en el último informe de Forrester Wave Enterprise Firewalls

Requerimientos de soporte:

- Ninguno de los modelos ofertados podrá estar listados ni anunciado en el sitio web del fabricante como end-of-life, end-of-sale o end-of-support. Se deberá adjuntar el link público del fabricante que verifique que los modelos propuestos no están en ese listado.
- La solución propuesta deberá tener soporte vigente de fabrica durante la fecha de contrato del servicio, el soporte del

fabricante deberá incluir atención de incidentes de software o hardware de la plataforma, reposición de partes o equipo de reemplazo en caso de falla de hardware.

- El soporte deberá estar disponible 24x7x365, la apertura de casos deberá poder realizarse vía online o vía telefónica.
- Se deberá proporcionar accesos al portal de soporte del fabricante, donde se tenga la potestad de dar seguimiento a los mismos.

FIREWALL DE PROXIMA GENERACIÓN	
CARACTERÍSTICAS	REQUERIMIENTOS MÍNIMOS
CARACTERÍSTICAS PRINCIPALES	<p>Firewall de próxima generación en alta disponibilidad</p> <ul style="list-style-type: none"> • Throughput de Prevención de Amenazas de 700 Mbps. Este throughput deberá estar medido con tráfico productivo real (transacciones usando una mixtura de aplicaciones de capa 7, transacciones medidas en condiciones empresariales), con las siguientes funcionalidades habilitadas simultáneamente: Control de aplicaciones, Sistema de Prevención de Intrusos (IPS), Seguridad del tráfico DNS, Antivirus/Antimalware de red, Antispyware/AntiBot, Sandboxing, Filtro de Archivos y Logging activo. Si el fabricante tuviese diferentes niveles o modos de inspección de seguridad, el equipo ofertado deberá soportar el throughput requerido con el modo más alto de inspección de seguridad. Se debe garantizar que el equipo no degrade su performance por debajo de lo requerido al habilitar los módulos de seguridad indicados en el modo más alto de inspección. No se aceptarán mediciones hechas con tráfico UDP o RFCs 3511, 2544, 2647 o 1242. • No se aceptarán cartas de fabricante como fundamento para el cumplimiento de performance, se deberá comprobar el requerimiento de throughput con documentación pública del fabricante adjuntando el link que lo respalde. Se deberá enviar una carta emitida por el contratista con el link con documentación pública del fabricante que respalde la comprobación del requerimiento de throughput • La plataforma de hardware debe soportar hasta 60,000 sesiones (o conexiones) concurrentes y/o simultáneas y 10,000 sesiones (o conexiones) por segundo, medidos en capa 7 (con transacciones HTTP). En caso de que la solución propuesta no cuente con este tipo de métricas, el hardware deberá soportar hasta 800,000 de sesiones (o conexiones) concurrentes y/o simultáneas y 50,00 sesiones (o conexiones) por segundo, medidos en capa 4 (con transacciones TCP o en condiciones ideales). • Ocho (08) interfaces de red en cobre 10/100/1000



	<ul style="list-style-type: none"> • Una (01) interfaz de fibra SFP 1Gbps (Se deberá incluir los transceivers originales de fábrica) • Un (01) interfaz de gestión fuera de banda RJ45 • Un (01) puerto de consola RJ45 • Dos (02) puertos USB • Deberá contar con fuentes redundantes donde de fallar una unidad, se pueda intercambiar sin interrupción del servicio
CAPACIDADES DE NETWORKING	<ul style="list-style-type: none"> • El dispositivo de seguridad debe soportar VLAN Tags 802.1q, agregación de links 802.3ad, policy based routing o policy based forwarding, ruteo multicast, jumbo frames, sub-interfaces ethernet lógicas, NAT de origen y destino. • Debe soportar enrutamiento estático y dinámico (RIPv2, BGP y OSPFv2). • Debe ser capaz de operar en los modos Capa 3 (con capacidades completas de Ruteo y NAT), Capa 2, Transparente y Sniffer, de forma simultánea mediante el uso de sus interfaces físicas. • Soportar diferentes características de networking operando en el protocolo IPv6, como mínimo: ruteo estático OSPFv3, MP-BGP, policy based routing o policy based forwarding, ECMP, dual-stack, QoS, DSCP, NPTv6 o NAT66, NAT64, LLDP, BFD, DHCPv6 Relay, SLAAC, SNMP. • La plataforma propuesta por el fabricante debe contar con certificación USGv6-r1 para las pruebas de Firewall, IDS e IPS
FUNCIONALIDADES DE FIREWALL	<ul style="list-style-type: none"> • Control de políticas puertos, direcciones IP, segmentos y/o rangos de red, región geográfica, usuarios y grupos de usuarios, aplicaciones, grupos estáticos de aplicaciones, grupos dinámicos de aplicaciones (basados en sus atributos). • Permitir agrupar las políticas de seguridad utilizando etiquetas u otro método. • Debe mostrar la primera y última vez que se utilizó una regla de seguridad, así como la cantidad de hits. • Debe mostrar la fecha de creación y última fecha de modificación de la regla de seguridad. • Debe permitir tener un registro de auditoría en cada política que permita conocer que cambios se realizó con anterioridad.
DESCIFRADO DE TRÁFICO SSL/TLS	<ul style="list-style-type: none"> • Debe permitir descifrar el tráfico de navegación de todos los usuarios a internet mediante la instalación de un certificado digital en los equipos. • Debe permitir descifrar el tráfico entrante hacia servidores HTTPS publicados en internet importando el certificado del servidor en el NGFW. • Deberá soportar al menos los siguientes algoritmos: RSA, DHE, ECDHE; 3DES, RC4, AES128, AES256,



	<p>CHACHA20-POLY1305; MD5, SHA1, SHA256, SHA384.</p> <ul style="list-style-type: none"> • Capacidad de bloquear la conexión hacia sitios web cifrados con protocolos obsoletos y/o no fiables, a pesar de no descifrar el tráfico. • Debe soportar certificados que utilicen Subject Alternative Name (SAN) y Server Name Indication (SNI). • Permitir el descifrado selectivo de categorías de URLs, por ejemplo, debe ser capaz de especificar excluir del descifrado a páginas con contenido sensible y descifrar el resto de las páginas. • Permitir excluir sitios a los cuales no se les aplicará la política de descifrado en base al Common Name del certificado. • Debe contar con un dashboard que muestre gráficamente la proporción del tráfico descifrado, aplicaciones y dominios con descifrado correcto, errores de descifrado, versiones de TLS usadas, entre otros. • Debe contar con un panel de logs dedicados a monitorear el tráfico de descifrado SSL/TLS, estos logs deberán permitir una identificación rápida de problemas del descifrado. • Desde la consola gráfica deberá mostrar todo el detalle de la sesión SSL/TLS identificada, tales como IP origen y destino, subject common name, issuer common name, server name indication, datos del certificado digital (fecha de expiración, serial number), versión de TLS, algoritmo asimétrico, algoritmo simétrico, hash, estado del descifrado (correcto o con error), motivo del error del descifrado. Este detalle de logs no deberá afectar el performance del equipo. • El postor tiene la libertad de incorporar en su oferta técnica una plataforma tercera que realice descifrado del tráfico y cumpla todas las especificaciones indicadas, en caso el NGFW propuesto no pueda realizarlo o no esté diseñado para ello. En caso de optar por esta alternativa, se deberá incluir una plataforma por cada una de las 1001 sedes.
<p>VISIBILIDAD EN CAPA 7 Y CONTROL DE APLICACIONES</p>	<ul style="list-style-type: none"> • La solución propuesta deberá reconocer por lo menos 20,000 aplicaciones, incluyendo, más no limitando a aplicaciones de tipo peer-to-peer, redes sociales, acceso remoto, update de software, protocolos de red, voip, audio, vídeo, proxy, mensajería instantánea, email. • Las aplicaciones deberán estar clasificadas en al menos 30 tipos, de tal manera que se puedan configurar políticas en base al tipo de aplicación. • Las aplicaciones deberán contar con atributos descriptivos tales como tipo, nivel de riesgo y etiqueta. • Deberás ser capaz de mostrar información contextual por cada aplicación SaaS, mostrando las regulaciones



que cumple, controles de seguridad que cumple, entre otros.

- Deberá ser posible definir grupos de aplicaciones en base a sus atributos, por ejemplo, un grupo de aplicaciones de riesgo alto que sea dinámicamente alimentado.
- Para tráfico cifrado (SSL/TLS), debe permitir el descifrado de paquetes con el fin de permitir la lectura del payload de la aplicación cifrada.
- Debe inspeccionar el payload del paquete de datos con el objetivo de detectar las aplicaciones en capa 7, a través de expresiones regulares, firmas u otro mecanismo. Debe ser capaz de determinar si una aplicación está utilizando su puerto default o no, por ejemplo, RDP en el puerto 80 en vez del 3389.
- Las políticas de seguridad deben poder definirse netamente en base a aplicaciones, sin necesidad de especificar puertos.
- Las políticas de seguridad deberán poder definirse 100% en base a aplicaciones pudiendo aplicar reglas específicas a cada aplicación. Es decir, si 2 aplicaciones utilizan el mismo puerto y protocolo, se debe poder crear 2 políticas de seguridad en las cuales se apliquen controles diferentes a cada aplicación.
- Con el objetivo de controlar aplicaciones propietarias en capa 7, la solución debe permitir la creación de aplicaciones personalizadas desde la interfaz de gestión.
- Deberá contar con un módulo de aprendizaje que permita migrar las políticas basadas en puertos específicos y políticas con puertos ALL/ANY, a políticas basadas en aplicaciones.
- El módulo de aprendizaje deberá ser específico por cada política de seguridad.
- El módulo de aprendizaje deberá mostrar el nombre de la(s) aplicación(es) que han pasado por una política de seguridad, fecha de primera y última ocurrencia y volumen de datos transferido por cada aplicación.
- Deberá contar con un wizard que permita convertir una política basada en puertos (capa 4) a una política basada en aplicaciones (capa 7) en base al aprendizaje realizado.
- Este módulo de aprendizaje deberá estar operativo de manera nativa, así la política no esté configurada con el módulo de control de aplicaciones.
- Para todas las políticas de seguridad, deberá ser posible especificar la aplicación directamente en la misma política, como un criterio más, no como un perfil.
- En caso la solución propuesta no tenga este módulo de aprendizaje, el postor, podrá presentar como alternativa técnica el servicio de configuración/migración de todas las políticas de seguridad basadas en puertos a políticas

	<p>basadas en aplicaciones en los Firewalls de Próxima Generación (Sedes tipo 1), este servicio deberá ser realizado por el área de servicios profesionales del propio fabricante, para cuyo efecto, deberá garantizar que será el mismo fabricante de la solución propuesta el que realizará dicho servicio. Mediante Carta del fabricante se debe evidenciar que dicho servicio se ejecutará por él mismo, (dicha documentación será presentada para la presentación de la oferta). Considerar un estimado de 1,400 políticas de seguridad como mínimo, entre todos los dispositivos de este tipo de sede.</p>
PREVENCION DE AMENAZAS	<ul style="list-style-type: none"> • La solución propuesta deberá contar con capacidades de IPS (Intrusion Prevention System), Antivirus/Antimalware, Antispyware/Antibot. • El equipo deberá soportar el throughput solicitado operando en el máximo nivel o modo de seguridad de inspección de IPS, Antivirus y Antispyware/Antibot. • El módulo de IPS debe ser capaz de bloquear ataques en base a firmas, heurística y anomalías en el protocolo. • El módulo de IPS debe permitir personalizar firmas directamente desde la consola gráfica. • Este tipo de análisis deberá realizarse en línea, para bloquear la amenaza antes de que el NGFW deje pasar el tráfico. • Respecto a ataques de malware, las firmas deberán estar basadas en patrones y no únicamente en hashes, con el objetivo de identificar y bloquear el malware polimórfico que pertenezca a una misma familia. • Con la finalidad de contar con una protección robusta contra amenazas emergentes a nivel mundial, la solución deberá ser capaz de actualizar su base de datos de firmas de malware en tiempo real sin afectar el rendimiento del equipo. • Adicionalmente al uso de firmas y heurística para la protección contra el malware, exploits, command & control y otro tipo de amenazas, la solución deberá contar con mecanismos avanzados basados en inteligencia artificial (algoritmos de machine learning y deep learning específicamente entrenados para tal fin) para prevenir la transferencia de dichas amenazas por la red. Estos algoritmos deberán ser capaces de identificar al menos los siguientes tipos de ataques: inyección de comandos, cobalt strike, command & control, malware 0-day camuflado en al menos archivos de tipo Ejecutables, Powershell, Office, ELF, Shell y otros. • Debe ser capaz de realizar análisis basado en deep learning de manera local en el mismo NGFW, para detectar y bloquear amenazas de día cero. • El análisis basado en algoritmos de machine learning y deep learning deberá ser realizado en línea y de manera inmediata, el archivo y tráfico analizado deberá





	<p>ser retenido hasta que finalice el análisis. Con el objetivo de evitar el ingreso por pacientes cero.</p> <ul style="list-style-type: none"> • Debe permitir customizar firmas de IPS en capa 7, así también a nivel de capa 3 y capa 4 con los parámetros de la cabecera del paquete de red. • Debe ser permitir convertir las firmas de IPS basadas en la sintaxis de Snort y Suricata automáticamente a la plataforma. • Debe ser capaz de detectar y bloquear el virus y malware en general que se propague en, al menos, los siguientes protocolos: HTTP, HTTPS, HTTP/2, FTP, SFTP, SMB, SMTP, IMAP y POP3. • Deberá incorporar un módulo de automatización, que permita colocar una IP y Usuario dentro de un grupo de cuarentena, si el Firewall identifica que dicha IP y/o Usuario están realizando acciones maliciosas o si dicho equipo se encuentra comprometido (por ejemplo, ser parte de una botnet, tener actividad de command & control, estar realizando movimiento lateral, intentar explotar vulnerabilidades dentro de la red interna). Estas acciones, deberán poder ser personalizadas en la consola del equipo. • Mientras que la IP y/o Usuario se encuentren dentro del grupo de cuarentena, la solución deberá ser capaz de bloquear todo tipo de comunicación que intente atravesar el Firewall; deberá permitir configurar excepciones para este tipo de restricción.
<p>PREVENCIÓN DE AMENAZAS AVANZADAS CAMUFLADAS EN DNS</p>	<ul style="list-style-type: none"> • Todo el tráfico DNS deberá ser analizado en su totalidad y de manera multicapa. La primera capa de análisis deberá consistir en verificar la reputación del dominio, si éste es malicioso se deberá bloquear el DNS Query; la segunda capa de análisis deberá consistir en el uso de algoritmos de inteligencia artificial en tiempo real, para detectar amenazas sofisticadas (en donde no se tiene conocimiento de la reputación, ni una firma del dominio analizado), tales como ataques de DGA o Tunneling. • La solución deberá identificar las consultas que realizan los hosts infectados hacia dominios maliciosos, de tal forma que se pueda bloquear dichas consultas DNS. • Deberá contar con un mecanismo que permita identificar los equipos potencialmente infectados en base al análisis de su tráfico DNS, inclusive si el tráfico entre la potencial víctima y su servidor DNS utilizado no pasa por el NGFW. • Deberá utilizar el método de DNS Sinkhole para interceptar solicitudes DNS maliciosas. • Deberá ser capaz de identificar amenazas sobre el tráfico DNS encriptado camuflado sobre HTTPS (DNS over HTTPS – DoH), y también DNS sobre TLS.



	<ul style="list-style-type: none"> • El análisis del tráfico DNS deberá analizar tanto el Query así como el Response. • El análisis del tráfico DNS se podrá realizar de manera local en el mismo equipo o a través del redireccionamiento del tráfico DNS hacia una plataforma externa (en nube u onpremise) del mismo u otro fabricante. • En caso de que el NGFW propuesto no cuente con estas capacidades, se aceptará que el postor integre en su oferta una solución de otro fabricante que cubra estos requerimientos. • El análisis del tráfico DNS no deberá requerir desplegar infraestructura adicional en la Entidad, ni hacer cambios de configuración en los servidores DNS. El NGFW deberá ser capaz de redireccionar todos los Querys DNS a una nube de procesamiento escalable, que utilice inteligencia artificial para el análisis avanzado de este tipo de amenazas. • En caso de ser una plataforma en nube deberá estar certificado en SOC2 Tipo II de AICPA. • La nube de procesamiento deberá estar certificada en SOC2 Tipo II de AICPA. • Los algoritmos basados en inteligencia artificial deberán ser capaces de prevenir ataques como DGA (Domain Generation Algoritmo) Random y de Diccionario, DNS Tunneling, Fast Flux Domains, NXNS Attack, DNS Rebinding, abuso de wildcards, CNAME cloaking, infiltración de DNS. • Deberá soportar el manejo de excepciones para poder mitigar los falsos positivos. • Deberá contar con dashboards y estadísticas sobre la cantidad, tipo de peticiones DNS, clasificación de la amenaza, veredicto del tráfico DNS (benigno, maligno), generadas por los dispositivos internos de la Institución. • El dashboard deberá permitir identificar potenciales equipos comprometidos dentro de la red interna, a partir del análisis avanzado de su tráfico DNS.
ANÁLISIS DE MALWARE DE DÍA CERO	<ul style="list-style-type: none"> • La plataforma de Sandbox podrá ser ofrecido en Nube (Cloud), On-premise o ambos. • La plataforma de Sandbox podrá ser ofrecido en Nube e integrado nativamente a los NGFW, de tal manera que no requiera dar mantenimiento a infraestructura física adicional. • Con la finalidad de promover la pluralidad de postores, el postor podrá incluir en su oferta técnica soluciones de sandbox del mismo fabricante del NGFW o un tercero capaz de cumplir todos los requerimientos técnicos solicitados. • Deberá ser capaz de emular el potencial malware en entornos Windows, Linux y MacOS.



- El análisis dinámico deberá realizarse de forma paralela para todos los archivos enviados y no deberá tomar más de 10 minutos en dar un veredicto.
- En caso de tratarse de una plataforma de Sandbox Cloud, deberá cumplir con los siguientes requerimientos:
 - El NGFW deberá ser capaz de enviar al menos 1000 archivos por hora al sandbox, todos los archivos deberán ser analizados dinámicamente (emulación) de manera paralela y el tiempo de análisis por cada archivo no deberá ser mayor a 10 minutos.
 - Deberá tener una disponibilidad de al menos 99.9% contabilizados mensualmente.
 - Deberá garantizar la privacidad y confidencialidad del contenido de los archivos analizados, para lo cual se requiere que el servicio cuente como mínimo con certificaciones SOC2 Plus de AICPA, ISO 27001, ISO 27017 e ISO 27018.
- En caso de tratarse de una plataforma de Sandbox On-premise, deberá cumplir con los siguientes requerimientos:
 - Deberá soportar un throughput de 1 Gbps
 - Debe tener una capacidad de procesamiento de al menos 1000 archivos por hora realizando análisis dinámico (entiéndase por análisis dinámico aquel que no está basado en firmas, ni prefiltros, sino en emulación completa del potencial malware).
 - Deberá ser desplegado en Alta Disponibilidad (Activo-Pasivo) en cada sede, con el objetivo de mantener los controles de seguridad en caso de contingencia.
 - Deberá estar desplegado en la interfaz LAN del NGFW, de tal forma que por lo menos tenga visibilidad de todos los archivos descargados por los usuarios desde internet.
- Debe proveer información forense sobre las acciones realizadas por el malware, tales como resumen del comportamiento visto, actividad sobre los archivos, peticiones DNS, conexiones de red, actividad de los archivos, procesos y registros. Esta información deberá poder ser extraída en un reporte PDF.
- Deberá ser capaz de analizar archivos sospechosos que se transfieran por los protocolos SMTP, POP3, IMAP, SMB, FTP, HTTP y HTTPS.
- Debe ser capaz de identificar amenazas de tipo Fileless.
- Deberá soportar por lo menos el análisis de los siguientes tipos de archivos: Flash, Batch, DLL, HTML, Java, Javascript, Archivos Office, PDF,



	<p>Portables/Ejecutables, Powershell, Python, RAR, 7zip, Shell, VBS, MSI, LNK, ELF, PKG, DMG, APK, DEX.</p> <ul style="list-style-type: none"> • Luego del análisis realizado por el sandbox, éste deberá generar automáticamente las firmas de malware y bloquear el acceso a las URLs maliciosas utilizadas por el malware. Las firmas deben estar basadas en patrones del malware y no únicamente hashes, de tal forma que sea capaz de bloquear el malware polimórfico con una única firma. Estas firmas deberán ser distribuidas automáticamente al NGFW o en su defecto estar instaladas dentro de la misma plataforma Sandbox (en caso de ofertar una solución on-premise) • Deberá ser capaz de analizar URLs desconocidas (es decir, no categorizadas en la base de datos del fabricante) con técnicas avanzadas basadas en propiedades y el comportamiento del sitio web, con el objetivo de identificar si es un sitio Phishing o no. • Debe permitir al administrador la descarga del archivo original analizado por el sandbox. • Debe permitir reportar al fabricante eventos que son falso-positivo y falso-negativo en el análisis de malware de día cero a partir de la propia consola de administración. • Permitir la subida de archivos al sandbox de forma manual y vía API, con el objetivo de automatizar las tareas de análisis dinámico. • Debe detectar técnicas usadas para evadir herramientas de sandboxing como detección de hypervisor (no debe usar hypervisores comerciales), inyección de código a procesos permitidos y deshabilitación de funcionalidades de seguridad del host.
FILTRO DE CONTENIDO WEB	<ul style="list-style-type: none"> • Debe poseer al menos 70 categorías de URLs, incluyendo las de malware, command and control, proxy, phishing, redes sociales, páginas de adultos. • Debe soportar un cache local de URLs en el dispositivo, evitando el delay de comunicación/validación de las URLs • Debido a que diariamente se crean más de 100,000 nuevas páginas web y muchos atacantes usan mecanismos anti-crawling (para evitar ser categorizados por tecnologías de seguridad), la solución deberá ser capaz de analizar en línea y en tiempo real aquellas páginas que no se encuentran categorizadas en la base de datos de reputación del fabricante, con el objetivo de identificar contenido malicioso que intente infectar el equipo del usuario que navega a internet. • El análisis en línea y en tiempo real deberá ejecutarse al momento que un usuario intente acceder a una URL y retener su acceso hasta finalizar el análisis, éste deberá estar basado en algoritmos de machine



	<p>learning y deep learning, con el objetivo de detectar amenazas camufladas en contenido javascript, websites asociados a command & control, link cloaking, entre otros.</p> <ul style="list-style-type: none"> • La protección basada en inteligencia artificial también deberá ser capaz de identificar y bloquear el acceso a páginas de phishing de día cero, analizando los diferentes atributos del sitio web que intente robar las credenciales del usuario. Se precisa que este análisis también deberá ejecutarse en línea y en tiempo real, cuando un usuario intente acceder a una página potencialmente phishing que no se encuentra categorizada en la base de datos del fabricante. • Debe contar con medidas de antievasión como Cloaking, Captcha falsos, codificación de caracteres HTML, entre otros. • Debe permitir la creación de categorías personalizadas. • Debe permitir la personalización de la página de bloqueo. • Debe permitir notificar al usuario, mostrándole solo una página de alerta personalizable, pero permitiéndole continuar la navegación al site. • Debe ser capaz de registrar el User-agent, Referer, XFF de cada sesión hacia internet • Debe ser capaz de forzar la navegación de los usuarios en el modo Safe Search Enforcement. • Debe identificar cuando un usuario envía credenciales corporativas de red a sitios no autorizados y debe poder bloquear dicho envío, previniendo así ataques de robo de credenciales.
IDENTIFICACION DE USUARIOS	<ul style="list-style-type: none"> • Debe permitir la creación de políticas de seguridad basadas en la identidad del usuario y grupo al cual pertenece, a través de la integración de servicios de autenticación como Active Directory, Novell eDirectory, Open LDAP y base de datos local. • Debe contar con varios mecanismos para la identificación del usuario y la dirección IP del equipo en donde se encuentra autenticado. Como mínimo deberá poder integrarse a las siguientes plataformas para cubrir este requerimiento: <ul style="list-style-type: none"> ○ Eventos de login gestionados en Domain Controller. ○ Terminal Server de Microsoft o Citrix ○ Consultando directamente a cada estación de trabajo a través del protocolo WMI ○ Capacidad de leer eventos de login y logout usando el protocolo WinRM. ○ Lectura de la cabecera XFF al integrarse con soluciones terceras de Proxy ○ Capacidad de extraer la información de IP y usuarios a través de la lectura y extracción de datos del tráfico syslog.

	<ul style="list-style-type: none"> ○ Integración con soluciones de Wireless LAN Controller basadas en 802.1x y Soluciones NAC, con el objetivo de que el NGFW no dependa del Domain Controller para identificar al usuario. ○ A través de agentes instalados en las estaciones de trabajo, que reporten directamente al NGFW el usuario y dirección IP de cada equipo. ● Deberá contar con un componente que permita integrarse a diversas plataformas de identidades tales como Azure LDAP, Google Directory, Okta, Cisco Duo, PingID. ● Debe contar con la funcionalidad de Portal Cautivo (Captive Portal), de tal manera que el NGFW muestre un portal al usuario para que se autentique manualmente. Las cuentas podrán ser definidas localmente en el NGFW o integradas con plataformas terceras. ● Debe tener integración con plataformas de MFA (Multi Factor Authentication), de tal forma que cuando un dispositivo requiera acceder a recurso, se le solicite el OTP.
SD-WAN	<ul style="list-style-type: none"> ● La solución debe soportar una consola de monitoreo con la capacidad de poder identificar fácilmente las aplicaciones y enlaces sus estados dentro de la red de SD-WAN (aplicaciones con problemas de jitter, latencia, pérdida de paquetes y sus diferentes estados dentro de la red) pudiendo ver el estado de estas en por lo menos en los últimos 5 minutos, última hora, último día o bien haciendo filtros personalizados. ● La solución debe soportar la capacidad de poder monitorear la salud de los enlaces en términos de jitter, latencia y pérdida de paquetes, tomando decisiones inteligentes de enrutamiento basado en la condición de los enlaces de manera dinámica. ● La solución debe soportar con la posibilidad de hacer reportes del estado de los enlaces y aplicaciones, indicando volúmenes de datos con respecto a las veces que fueron degradados o afectados. ● Soportar la opción de cambiar dinámicamente de camino al detectar alguna degradación del enlace sin afectar o cortar la sesión establecida de la aplicación, es decir, que el usuario no perciba corte en la aplicación, ni tener que reiniciar la sesión. ● Soportar de algoritmo de corrección de errores (FEC - Forward Error Correction) con el objetivo de poder garantizar una buena experiencia en el uso de aplicaciones de voz y video a través de la red de SD-WAN. ● Soportar la transmisión de paquetes duplicados por diferentes enlaces al utilizar la red de SD-WAN con el objetivo de mantener una calidad de experiencia alta al





	<p>usar aplicaciones de misión crítica y prevenir la pérdida de paquetes, incremento de latencia, jitter, etc.</p> <ul style="list-style-type: none"> • Soportar la opción de monitorear la salud de los enlaces a través de aplicaciones de SaaS y aplicaciones de Cloud, para poder determinar si esas aplicaciones son enviadas a internet de manera directa o bien a través de algún camino de la red de SD-WAN. • Soportar la capacidad de definir el tiempo de intercambio de heartbeats entre los puntos del túnel SD-WAN. • Deberá soportar la funcionalidad de SD-WAN en interfaces agregadas (IEEE 802.1AX) y en subinterfaces. • Debe soportar configuraciones de SDWAN en IPv6 • Soportar fail over a nivel de sub segundos • Soportar dashboards de monitoreo basado en el rendimiento de una aplicación y del enlace físico.
ADMINISTRACIÓN	<ul style="list-style-type: none"> • Se deberá entregar una consola de administración centralizada o en su defecto deberán ser administrados por la consola central de administración de los Firewalls de Datacenter. • En caso el postor haya integrado tecnologías de terceros externas al NGFW, también se deberá considerar dentro de la propuesta técnica la consola de gestión para dicha tecnología. • Debe permitir exportar las reglas de seguridad del NGFW en formato CSV y PDF • Debe contar con un dashboard interactivo y gráfico que permita monitorear el uso de las aplicaciones en capa 7, sitios web visitados, actividad de los usuarios, actividad por IP (origen y destino), países origen y destino del tráfico, uso de las reglas de seguridad, actividad del tráfico malicioso. Esta información podrá ser vista en base a Bytes y Sesiones, y ser filtrado en base a un rango de tiempo, IP, usuario, país y regla de seguridad. • Debe permitir el control de acceso a la gestión del equipo a través de roles personalizables. • Debe permitir la captura de paquetes en formato PCAP para poder ser leídos por una herramienta tercera. La captura de paquetes deberá poder ser filtrada antes del proceso de ejecución en base a la interfaz, IP y Puerto (origen y destino) • Ante escenarios donde existan dos o más administradores en el equipo, logueados y realizando cambios en simultáneo en la consola de gestión, la solución deberá de ser capaz de solo aplicar los cambios realizados por cada administrador individual, sin afectar o sobrescribir los cambios del otro administrador. • Contar con un módulo que permita comparar y que indique específicamente que cambio se hizo a una

	<p>política de seguridad respecto a una versión anterior de dicha política.</p> <ul style="list-style-type: none"> • Debe poder realizar una copia de seguridad (backup) automática de las configuraciones y rollback de configuración a la última configuración salvada. • Debe permitir el monitoreo de eventos basados en SNMP, integración con SIEM a través de Syslog, y envío de alertas por correo electrónico (integrándose a un servidor SMTP). • Debe permitir la generación de logs de auditoría detallados, informando de la configuración realizada, el administrador que la realizó, su IP y el horario de la alteración. • La gestión de NGFW debe permitir la asignación de una cuota de uso de disco para definir una capacidad máxima de almacenamiento de logs de tráfico de datos, amenazas, auditoría de configuraciones, eventos de sistema. • Debe soportar la personalización de reportes, permitiendo mostrar información de eventos de antivirus, antispymware, IPS, navegación a internet, aplicaciones, malware de día cero, debe permitir seleccionar las columnas a mostrar, filtrar la información en base a usuarios, grupos de usuarios, direcciones IP, el rango de fechas de los datos, deben poder ser exportados en PDF y enviados automáticamente vía correo electrónico. • Debe permitir configurar reportes para ver el tiempo de navegación de los usuarios en internet, clasificado por tipo de página web y URL. • Debe contar con reportes predeterminados que muestren información y diversas estadísticas sobre el uso de aplicaciones SaaS. • La gestión de NGFW debe permitir realizar tareas de gestión a través del API basado en XML.
--	--

La administración de todas las soluciones y equipamiento solicitado por la Entidad, serán de administración compartida, en ese sentido, el contratista entregará credenciales de usuarios a nivel de read/write a usuarios designados por la Entidad. El contratista está obligado a considerar todos los componentes, dispositivos y materiales que requiera para la integración de la solución adquirida con la red de la Entidad, así como para el cumplimiento de la finalidad del servicio requerido.

5.2.1.5.4 COMPONENTE 4: SERVICIO DE SEGURIDAD DE LA INFORMACIÓN Y SEGURIDAD INFORMÁTICA GESTIONADA.

Se desea contratar los servicios gestionados de:

- Firewall de nueva generación, para red externa y red interna.
- Detección y control de malware avanzado.
- Protección de portales web y base de datos
- Spam Firewall y protección ante phishing dirigido
- Protección contra ataques de denegación de servicios distribuido

- f) Análisis de vulnerabilidades de red
- g) Herramienta informática para prevención de pérdida de información, auditoría y anticorrupción.
- h) Solución de antivirus para servidores y endpoint de la DIRITC PNP.
- i) Servicio de SOC Gestionado, Herramienta de Análisis de incidentes y Correlación de logs de seguridad.
- j) Servicios de seguridad de la información.

Nota:

- a. Estos servicios se deben implementar en los sites principal y secundario de la Entidad.
- b. Para el perfeccionamiento del Contrato se adjuntará datasheets, whitepapers u otra documentación técnica en el idioma original del fabricante.
- c. La arquitectura sugerida se indica en el DIAGRAMA DE ENLACES DE DATOS DEL ANEXO C.

5.2.1.5.4.1.12 Descripción de los servicios:

5.2.1.5.4.1.13 FIREWALL DE NUEVA GENERACIÓN, PARA RED EXTERNA Y RED INTERNA.

Se implementarán dos (02) equipos para el perímetro externo, y dos (02) equipos para el perímetro interno, los que operarán en HA utilizando la fibra oscura que interconecta el site principal y secundario.

Consideraciones:

- Adquisición de una solución de Next Generation Firewall (NGFW) para la seguridad de PNP.
- El equipo debe ser nuevo, de primer uso y que no se encuentre en End of Support por su fabricante.
- El Postor tiene la libertad de añadir consolas terceras para cumplir con los requerimientos técnicos solicitados, ya sea para capacidades de gestión, reportes y/o seguridad.
- El fabricante debe pertenecer al cuadrante de Líderes de Gartner para "Enterprise Network Firewall" o "Firewalls de Redes Empresariales" en los últimos 10 reportes.
- El fabricante debe estar catalogado como líder en el último informe de Forrester Wave Enterprise Firewalls

Requerimientos de soporte:

- Ninguno de los modelos ofertados podrá estar listados ni anunciado en el sitio web del fabricante como end-of-life, end-of-sale o end-of-support. Se deberá adjuntar el link público del fabricante que verifique que los modelos propuestos no están en ese listado.
- La solución propuesta deberá tener soporte vigente de fabrica durante la fecha de contrato del servicio, el soporte del fabricante deberá incluir atención de incidentes de software o hardware de la plataforma, reposición de partes o equipo de reemplazo en caso de falla de hardware.
- El soporte deberá estar disponible 24x7x365, la apertura de casos deberá poder realizarse vía online o vía telefónica.
- Se deberá proporcionar accesos al portal de soporte del fabricante, donde se tenga la potestad de dar seguimiento a los mismos.

FIREWALL DE PRÓXIMA GENERACIÓN	
CARACTERÍSTICAS	REQUERIMIENTOS MÍNIMOS

CARACTERISTICAS
PRINCIPALES

Firewall de próxima generación en alta disponibilidad

- Throughput de Prevención de Amenazas de 19 Gbps. Este throughput deberá estar medido con tráfico productivo real (transacciones usando una mezcla de aplicaciones de capa 7, transacciones medidas en condiciones empresariales), con las siguientes funcionalidades habilitadas simultáneamente: Control de aplicaciones, Sistema de Prevención de Intrusos (IPS), Seguridad del tráfico DNS, Antivirus/Antimalware de red, Antispyware/AntiBot, Sandboxing y Logging activo. Si el fabricante tuviese diferentes niveles o modos de inspección de seguridad, el equipo ofertado deberá soportar el throughput requerido con el modo más alto de inspección de seguridad. Se debe garantizar que el equipo no degrade su performance por debajo de lo requerido al habilitar los módulos de seguridad indicados en el modo más alto de inspección. No se aceptarán mediciones hechas con tráfico UDP o RFCs 3511, 2544, 2647 o 1242.
- No se aceptarán cartas de fabricante como fundamento para el cumplimiento de performance, se deberá comprobar el requerimiento de throughput con documentación pública del fabricante adjuntando el link que lo respalde. Se deberá enviar una carta emitida por el contratista con el link con documentación pública del fabricante que respalde la comprobación del requerimiento de throughput
- La plataforma de hardware debe soportar hasta 2,900,000 sesiones (o conexiones) concurrentes y/o simultáneas y 260,000 sesiones (o conexiones) por segundo, medidos en capa 7 (con transacciones HTTP). En caso de que la solución propuesta no cuente con este tipo de métricas, el hardware deberá soportar hasta 37,500,000 de sesiones (o conexiones) concurrentes y/o simultáneas y 1,300,00 sesiones (o conexiones) por segundo, medidos en capa 4 (con transacciones TCP o en condiciones ideales). Se precisa que estas mediciones deberán estar basadas con el NGFW configurado en modo estándar, donde tenga disponible habilitar sus módulos de seguridad; no se aceptarán mediciones en donde el NGFW no permita habilitar todos sus módulos de seguridad (mediciones hiperscalable, multiconvergente o similares).
- Doce (12) interfaces de red en cobre 10/100/1000
- Diez (10) interfaces de red en fibra 10G, SFP+ (Se deberá incluir los transceivers originales de fábrica)
- Cuatro (04) interfaces de fibra de 25G SFP28
- Dos (02) interfaces de fibra 40/100G QSFP/QSFP28
- Dos (02) puertos alta disponibilidad dedicados, se podrán utilizar interfaces de red adicionales a las solicitadas para la configuración del HA
- Un (01) interfaz de gestión fuera de banda RJ45



	<ul style="list-style-type: none"> • Un (01) puerto de consola RJ45 • Un (01) puerto USB • Deberá contar con fuentes redundantes donde de fallar una unidad, se pueda intercambiar sin interrupción del servicio • Deberá contar con al menos diez (10) sistemas o dominios virtuales
CAPACIDADES DE NETWORKING	<ul style="list-style-type: none"> • El dispositivo de seguridad debe soportar VLAN Tags 802.1q, agregación de links 802.3ad, policy based routing o policy based forwarding, ruteo multicast, jumbo frames, sub-interfaces ethernet lógicas, NAT de origen y destino. • Debe soportar enrutamiento estático y dinámico (RIPv2, BGP y OSPFv2). • Debe ser capaz de operar en los modos Capa 3 (con capacidades completas de Ruteo y NAT), Capa 2, Transparente y Sniffer, de forma simultánea mediante el uso de sus interfaces físicas. • Soportar diferentes características de networking operando en el protocolo IPv6, como mínimo: ruteo estático OSPFv3, MP-BGP, policy based routing o policy based forwarding, ECMP, dual-stack, QoS, DSCP, NPTv6 o NAT66, NAT64, LLDP, BFD, DHCPv6 Relay, SLAAC, SNMP. • La plataforma propuesta por el fabricante debe contar con certificación USGv6-r1 para las pruebas de Firewall.
ALTA DISPONIBILIDAD	<ul style="list-style-type: none"> • Soporte a configuración de alta disponibilidad Activo/Pasivo y Activo/Activo, con despliegues de los equipos tanto en modo transparente como en modo capa 3 (L3). • La configuración en alta disponibilidad debe sincronizar: sesiones, certificados de descifrado, configuraciones, incluyendo, más no limitado a políticas de seguridad, NAT, QoS y objetos de red. • Debe ser posible el monitoreo de fallo de enlaces, ya sea ante la caída de al menos una de las interfaces del equipo, una conexión física adyacente o pérdida de conectividad hacia una IP desde una de las interfaces.
FUNCIONALIDADES DE FIREWALL	<ul style="list-style-type: none"> • Control de políticas puertos, direcciones IP, segmentos y/o rangos de red, región geográfica, usuarios y grupos de usuarios, aplicaciones, grupos estáticos de aplicaciones, grupos dinámicos de aplicaciones (basados en sus atributos). • Permitir agrupar las políticas de seguridad utilizando etiquetas u otro método. • Debe mostrar la primera y última vez que se utilizó una regla de seguridad, así como la cantidad de hits. • Debe mostrar la fecha de creación y última fecha de modificación de la regla de seguridad.



	<ul style="list-style-type: none"> • Debe permitir tener un registro de auditoría en cada política que permita conocer que cambios se realizó con anterioridad.
DESCIFRADO DE TRÁFICO SSL/TLS	<ul style="list-style-type: none"> • Debe permitir descifrar el tráfico de navegación de todos los usuarios a internet mediante la instalación de un certificado digital en los equipos. • Debe permitir descifrar el tráfico entrante hacia servidores HTTPS publicados en internet importando el certificado del servidor en el NGFW. • Deberá soportar al menos los siguientes algoritmos: RSA, DHE, ECDHE; 3DES, RC4, AES128, AES256, CHACHA20-POLY1305; MD5, SHA1, SHA256, SHA384. • Capacidad de bloquear la conexión hacia sitios web cifrados con protocolos obsoletos y/o no fiables, a pesar de no descifrar el tráfico. • Debe soportar certificados que utilicen Subject Alternative Name (SAN) y Server Name Indication (SNI). • Permitir el descifrado selectivo de categorías de URLs, por ejemplo, debe ser capaz de especificar excluir del descifrado a páginas con contenido sensible y descifrar el resto de las páginas. • Permitir excluir sitios a los cuales no se les aplicará la política de descifrado en base al Common Name del certificado. • Debe contar con un dashboard que muestre gráficamente la proporción del tráfico descifrado, aplicaciones y dominios con descifrado correcto, errores de descifrado, versiones de TLS usadas, entre otros. • Debe contar con un panel de logs dedicados a monitorear el tráfico de descifrado SSL/TLS, estos logs deberán permitir una identificación rápida de problemas del descifrado. • Desde la consola gráfica deberá mostrar todo el detalle de la sesión SSL/TLS identificada, tales como IP origen y destino, subject common name, issuer common name, server name indication, datos del certificado digital (fecha de expiración, serial number), versión de TLS, algoritmo asimétrico, algoritmo simétrico, hash, estado del descifrado (correcto o con error), motivo del error del descifrado. Este detalle de logs no deberá afectar el performance del equipo. • El postor tiene la libertad de incorporar en su oferta técnica una plataforma tercera que realice descifrado del tráfico y cumpla todas las especificaciones indicadas, en caso el NGFW propuesto no pueda realizarlo o no esté diseñado para ello. En caso de optar por esta alternativa, se deberá incluir al menos una plataforma para esta sede.



VISIBILIDAD EN CAPA 7
Y CONTROL DE
APLICACIONES

- La solución propuesta deberá reconocer por lo menos 20,000 aplicaciones, incluyendo, más no limitando a aplicaciones de tipo peer-to-peer, redes sociales, acceso remoto, update de software, protocolos de red, voip, audio, vídeo, proxy, mensajería instantánea, email.
- Las aplicaciones deberán estar clasificadas en al menos 30 tipos, de tal manera que se puedan configurar políticas en base al tipo de aplicación.
- Las aplicaciones deberán contar con atributos descriptivos tales como tipo, nivel de riesgo y etiqueta.
- Deberá ser capaz de mostrar información contextual por cada aplicación SaaS, mostrando las regulaciones que cumple, controles de seguridad que cumple, entre otros.
- Debe contar con algoritmos basados en machine learning para automatizar el descubrimiento y generar firmas de nuevas aplicaciones SaaS
- Debe monitorear la actividad de usuarios y la exposición de datos a través de aplicaciones SaaS
- Deberá ser posible definir grupos de aplicaciones en base a sus atributos, por ejemplo, un grupo de aplicaciones de riesgo alto que sea dinámicamente alimentado.
- Para tráfico cifrado (SSL/TLS), debe permitir el descifrado de paquetes con el fin de permitir la lectura del payload de la aplicación cifrada.
- Debe inspeccionar el payload del paquete de datos con el objetivo de detectar las aplicaciones en capa 7, a través de expresiones regulares, firmas u otro mecanismo. Debe ser capaz de determinar si una aplicación está utilizando su puerto default o no, por ejemplo, RDP en el puerto 80 en vez del 3389.
- Las políticas de seguridad deben poder definirse netamente en base a aplicaciones, sin necesidad de especificar puertos.
- Las políticas de seguridad deberán poder definirse 100% en base a aplicaciones pudiendo aplicar reglas específicas a cada aplicación. Es decir, si 2 aplicaciones utilizan el mismo puerto y protocolo, se debe poder crear 2 políticas de seguridad en las cuales se apliquen controles diferentes a cada aplicación.
- Con el objetivo de controlar aplicaciones propietarias en capa 7, la solución debe permitir la creación de aplicaciones personalizadas desde la interfaz de gestión.
- Deberá contar con un módulo de aprendizaje que permita migrar las políticas basadas en puertos específicos y políticas con puertos ALL/ANY, a políticas basadas en aplicaciones.
- El módulo de aprendizaje deberá ser específico por cada política de seguridad.

	<ul style="list-style-type: none">• El módulo de aprendizaje deberá mostrar el nombre de la(s) aplicación(es) que han pasado por una política de seguridad, fecha de primera y última ocurrencia y volumen de datos transferido por cada aplicación.• Deberá contar con un wizard que permita convertir una política basada en puertos (capa 4) a una política basada en aplicaciones (capa 7) en base al aprendizaje realizado.• En caso la solución propuesta no tenga este módulo de aprendizaje el postor deberá incluir en su oferta técnica el servicio de configuración migración de todas las políticas de seguridad basadas en puertos a políticas basadas en aplicaciones, este servicio deberá ser realizado por el área de servicios profesionales del propio fabricante. Considerar un estimado de 3,000 políticas de seguridad entre ambos cluster de NGFW.
PREVENCION DE AMENAZAS	<ul style="list-style-type: none">• La solución propuesta deberá contar con capacidades de IPS (Intrusion Prevention System), Antivirus/Antimalware, Antispyware/Antibot.• El equipo deberá soportar el throughput solicitado operando en el máximo nivel o modo de seguridad de inspección de IPS, Antivirus y Antispyware/Antibot.• El módulo de IPS debe ser capaz de bloquear ataques en base a firmas, heurística y anomalías en el protocolo.• El módulo de IPS debe permitir personalizar firmas directamente desde la consola gráfica.• Este tipo de análisis deberá realizarse en línea, para bloquear la amenaza antes de que el NGFW deje pasar el tráfico.• Respecto a ataques de malware, las firmas deberán estar basadas en patrones y no únicamente en hashes, con el objetivo de identificar y bloquear el malware polimórfico que pertenezca a una misma familia.• Con la finalidad de contar con una protección robusta contra amenazas emergentes a nivel mundial, la solución deberá ser capaz de actualizar su base de datos de firmas de malware en tiempo real sin afectar el rendimiento del equipo.• Adicionalmente al uso de firmas y heurística para la protección contra el malware, exploits, command & control y otro tipo de amenazas, la solución deberá contar con mecanismos avanzados basados en inteligencia artificial (algoritmos de machine learning y deep learning específicamente entrenados para tal fin) para prevenir la transferencia de dichas amenazas por la red. Estos algoritmos deberán ser capaces de identificar al menos los siguientes tipos de ataques: inyección de comandos, cobalt strike, command & control, malware 0-day camuflado en al menos archivos de tipo Ejecutables, Powershell, Office, ELF, Shell y otros.



	<ul style="list-style-type: none"> • El análisis basado en algoritmos de machine learning y deep learning deberá ser realizado en línea y de manera inmediata, el archivo y tráfico analizado deberá ser retenido hasta que finalice el análisis. Con el objetivo de evitar el ingreso por pacientes cero. • Debe ser capaz de detectar y bloquear el virus y malware en general que se propague en, al menos, los siguientes protocolos: HTTP, HTTPS, HTTP/2, FTP, SFTP, SMB, SMTP, IMAP y POP3. • Deberá incorporar un módulo de automatización, que permita colocar una IP y Usuario dentro de un grupo de cuarentena, si el Firewall identifica que dicha IP y/o Usuario están realizando acciones maliciosas o si dicho equipo se encuentra comprometido (por ejemplo, ser parte de una botnet, tener actividad de command & control, estar realizando movimiento lateral, intentar explotar vulnerabilidades dentro de la red interna). Estas acciones, deberán poder ser personalizadas en la consola del equipo. • Mientras que la IP y/o Usuario se encuentren dentro del grupo de cuarentena, la solución deberá ser capaz de bloquear todo tipo de comunicación que intente atravesar el Firewall; deberá permitir configurar excepciones para este tipo de restricción.
<p>PREVENCIÓN DE AMENAZAS AVANZADAS CAMUFLADAS EN DNS</p>	<ul style="list-style-type: none"> • Todo el tráfico DNS deberá ser analizado en su totalidad y de manera multicapa. La primera capa de análisis deberá consistir en verificar la reputación del dominio, si éste es malicioso se deberá bloquear el DNS Query; la segunda capa de análisis deberá consistir en el uso de algoritmos de inteligencia artificial en tiempo real, para detectar amenazas sofisticadas (en donde no se tiene conocimiento de la reputación, ni una firma del dominio analizado), tales como ataques de DGA o Tunneling. • La solución deberá identificar las consultas que realizan los hosts infectados hacia dominios maliciosos, de tal forma que se pueda bloquear dichas consultas DNS. • Deberá contar con un mecanismo que permita identificar los equipos potencialmente infectados en base al análisis de su tráfico DNS, inclusive si el tráfico entre la potencial víctima y su servidor DNS utilizado no pasa por el NGFW. • Deberá ser capaz de identificar amenazas sobre el tráfico DNS encriptado camuflado sobre HTTPS (DNS over HTTPS – DoH), y también DNS sobre TLS. • El análisis del tráfico DNS deberá analizar tanto el Query así como el Response. • El análisis del tráfico DNS se podrá realizar de manera local en el mismo equipo o a través del redireccionamiento del tráfico DNS hacia una



	<p>plataforma externa (en nube u onpremise) del mismo u otro fabricante.</p> <ul style="list-style-type: none"> • En caso de que el NGFW propuesto no cuente con estas capacidades, se aceptará que el postor integre en su oferta una solución de otro fabricante que cubra estos requerimientos. • En caso de ser una plataforma en nube deberá estar certificado en SOC2 Tipo II de AICPA. • Los algoritmos basados en inteligencia artificial deberán ser capaces de prevenir ataques como DGA (Domain Generation Algorithm) Random y de Diccionario, DNS Tunneling, Fast Flux Domains, NXNS Attack, DNS Rebinding, abuso de wildcards, CNAME cloaking, infiltración de DNS. • Deberá soportar el manejo de excepciones para poder mitigar los falsos positivos. • Deberá contar con dashboards y estadísticas sobre la cantidad, tipo de peticiones DNS, clasificación de la amenaza, veredicto del tráfico DNS (benigno, maligno), generadas por los dispositivos internos de la Institución. • El dashboard deberá permitir identificar potenciales equipos comprometidos dentro de la red interna, a partir del análisis avanzado de su tráfico DNS.
<p>ANÁLISIS DE MALWARE DE DÍA CERO</p>	<ul style="list-style-type: none"> • La plataforma de Sandbox podrá ser ofrecido en Nube (Cloud), On-premise o ambos. • Con la finalidad de promover la pluralidad de postores, el postor podrá incluir en su oferta técnica soluciones de sandbox del mismo fabricante del NGFW o un tercero capaz de cumplir todos los requerimientos técnicos solicitados. • Deberá ser capaz de emular el potencial malware en entornos Windows, Linux y MacOS. • El análisis dinámico deberá realizarse de forma paralela para todos los archivos enviados y no deberá tomar más de 10 minutos en dar un veredicto. • En caso de tratarse de una plataforma de Sandbox Cloud, deberá cumplir con los siguientes requerimientos: <ul style="list-style-type: none"> ○ El NGFW deberá ser capaz de enviar al menos 5000 archivos por hora al sandbox, todos los archivos deberán ser analizados dinámicamente (emulación) de manera paralela y el tiempo de análisis por cada archivo no deberá ser mayor a 10 minutos. ○ Deberá tener una disponibilidad de al menos 99.9% contabilizados mensualmente. ○ Deberá garantizar la privacidad y confidencialidad del contenido de los archivos analizados, para lo cual se requiere que el servicio cuente como mínimo con certificaciones SOC2 Plus de AICPA, ISO 27001, ISO 27017 e ISO 27018.





- En caso de tratarse de una plataforma de Sandbox On-premise, deberá cumplir con los siguientes requerimientos:
 - Deberá soportar un throughput de 15 Gbps
 - Debe tener una capacidad de procesamiento de al menos 5000 archivos por hora realizando análisis dinámico (entiéndase por análisis dinámico aquel que no está basado en firmas, ni prefiltros, sino en emulación completa del potencial malware).
 - Deberá ser desplegado en Alta Disponibilidad (Activo-Pasivo) en cada sede, con el objetivo de mantener los controles de seguridad en caso de contingencia.
 - Deberá estar desplegado en la interfaz LAN del NGFW, de tal forma que por lo menos tenga visibilidad de todos los archivos descargados por los usuarios desde internet.
- Debe proveer información forense sobre las acciones realizadas por el malware, tales como resumen del comportamiento visto, actividad sobre los archivos, peticiones DNS, conexiones de red, actividad de los archivos, procesos y registros. Esta información deberá poder ser extraída en un reporte PDF.
- Deberá ser capaz de analizar archivos sospechosos que se transfieran por los protocolos SMTP, POP3, IMAP, SMB, FTP, HTTP y HTTPS.
- Debe ser capaz de identificar amenazas de tipo Fileless.
- Deberá soportar por lo menos el análisis de los siguientes tipos de archivos: Flash, Batch, DLL, HTML, Java, Javascript, Archivos Office, PDF, Portables/Ejecutables, Powershell, Python, RAR, 7zip, Shell, VBS, MSI, LNK, ELF, PKG, DMG, APK, DEX.
- Luego del análisis realizado por el sandbox, éste deberá generar automáticamente las firmas de malware y bloquear el acceso a las URLs maliciosas utilizadas por el malware. Las firmas deben estar basadas en patrones del malware y no únicamente hashes, de tal forma que sea capaz de bloquear el malware polimórfico con una única firma. Estas firmas deberán ser distribuidas automáticamente al NGFW o en su defecto estar instaladas dentro de la misma plataforma Sandbox (en caso de ofertar una solución on-premise)
- Deberá ser capaz de analizar URLs desconocidas (es decir, no categorizadas en la base de datos del fabricante) con técnicas avanzadas basadas en propiedades y el comportamiento del sitio web, con el objetivo de identificar si es un sitio Phishing o no.
- Debe permitir al administrador la descarga del archivo original analizado por el sandbox.

	<ul style="list-style-type: none">• Debe permitir reportar al fabricante eventos que son falso-positivo y falso-negativo en el análisis de malware de día cero a partir de la propia consola de administración.• Permitir la subida de archivos al sandbox de forma manual y vía API, con el objetivo de automatizar las tareas de análisis dinámico.• Debe detectar técnicas usadas para evadir herramientas de sandboxing como detección de hypervisor (no debe usar hypervisores comerciales), inyección de código a procesos permitidos y deshabilitación de funcionalidades de seguridad del host.
FILTRO DE CONTENIDO WEB	<ul style="list-style-type: none">• Debe poseer al menos 70 categorías de URLs, incluyendo las de malware, command and control, proxy, phishing, redes sociales, páginas de adultos.• Debe soportar un cache local de URLs en el dispositivo, evitando el delay de comunicación/validación de las URLs• Debido a que diariamente se crean más de 100,000 nuevas páginas web y muchos atacantes usan mecanismos anti-crawling (para evitar ser categorizados por tecnologías de seguridad), la solución deberá ser capaz de analizar en línea y en tiempo real aquellas páginas que no se encuentran categorizadas en la base de datos de reputación del fabricante, con el objetivo de identificar contenido malicioso que intente infectar el equipo del usuario que navega a internet.• El análisis en línea y en tiempo real deberá ejecutarse al momento que un usuario intente acceder a una URL y retener su acceso hasta finalizar el análisis, éste deberá estar basado en algoritmos de machine learning y deep learning, con el objetivo de detectar amenazas camufladas en contenido javascript, websites asociados a command & control, link cloaking, entre otros.• La protección basada en inteligencia artificial también deberá ser capaz de identificar y bloquear el acceso a páginas de phishing de día cero, analizando los diferentes atributos del sitio web que intente robar las credenciales del usuario. Se precisa que este análisis también deberá ejecutarse en línea y en tiempo real, cuando un usuario intente acceder a una página potencialmente phishing que no se encuentra categorizada en la base de datos del fabricante.• Debe permitir la creación de categorías personalizadas.• Debe permitir la personalización de la página de bloqueo.• Debe permitir notificar al usuario, mostrándole solo una página de alerta personalizable, pero permitiéndole continuar la navegación al site.

	<ul style="list-style-type: none">• Debe ser capaz de registrar el User-agent, Referer, XFF de cada sesión hacia internet• Debe ser capaz de forzar la navegación de los usuarios en el modo Safe Search Enforcement.
DETECCIÓN DE DISPOSITIVOS IOT	<ul style="list-style-type: none">• La solución deberá contar con un módulo de monitoreo, descubrimiento, identificación y clasificación de dispositivos IoT (Internet de las Cosas) como por ejemplo teléfonos IP, cámaras de vigilancia, consolas de videojuegos, impresoras, dispositivos médicos, equipos industriales, entre otros.• Por cada dispositivo identificado deberá mostrar la marca del fabricante, tipo de dispositivo, serial number, sistema operativo, dirección IP, dirección MAC, tipo de conexión (cableada o wireless), nombre del SSID o Puerto del switch al cual está conectado, según corresponda.• Debe descubrir y mantener un inventario de dispositivos de forma automática, y estar basado en mecanismos de descubrimiento basado en Firmas, Patrones de comportamiento asociado al tráfico y Machine Learning. No deberá depender únicamente de la dirección MAC para identificar el dispositivo, pues solo ese dato no garantiza la correcta identificación.• Debe identificar dispositivos que posean software o hardware desactualizado y vulnerable, junto con su respectivo identificador CVE.• Deberá contar con un módulo que permita identificar comportamientos anómalos en los dispositivos IoT.• Mostrar el nivel de riesgo de cada dispositivo IoT clasificando su severidad por nivel Bajo, Medio, Alto y Crítico o una clasificación equivalente.• Mostrar los ataques e intentos de ataques hacia los dispositivos IoT.• Mostrar la actividad en la red de los dispositivos IoT, a nivel de tráfico entrante y saliente. Adicionalmente deberá mostrar la aplicación, protocolo y puerto utilizado para dicha actividad de red.• Si se detecta que un dispositivo IOT está generando ataques, la plataforma deberá permitir rápidamente aislar dicho equipo, ya sea colocándolo a un grupo de cuarentena o restringido dentro del NGFW o integrándose a una plataforma NAC.• Deberá contar con un mapa geográfico que facilite el monitoreo de la actividad de red del dispositivo IoT.• Deberá contar con un panel de recomendaciones de subsanación ante las alertas de seguridad identificadas.• Deberá estar integrado a la plataforma NGFW, con el objetivo de que la política de seguridad se pueda realizar directamente en base al Dispositivo IoT, en lugar de usar Direcciones IP.• Los logs del NGFW deberán ser enriquecidos a través de esta integración, mostrando adicionalmente a la

	<p>dirección IP origen y/o destino, el tipo de dispositivo, marca, familia y sistema operativo, del dispositivo IoT.</p> <ul style="list-style-type: none"> • Esta funcionalidad podrá estar embebida dentro del mismo NGFW o ser una plataforma externa del mismo u otro fabricante.
IDENTIFICACION DE USUARIOS	<ul style="list-style-type: none"> • Debe permitir la creación de políticas de seguridad basadas en la identidad del usuario y grupo al cual pertenece, a través de la integración de servicios de autenticación como Active Directory, Novell eDirectory, Open LDAP y base de datos local. • Debe contar con varios mecanismos para la identificación del usuario y la dirección IP del equipo en donde se encuentra autenticado. Como mínimo deberá poder integrarse a las siguientes plataformas para cubrir este requerimiento: <ul style="list-style-type: none"> ○ Eventos de login gestionados en Domain Controller. ○ Terminal Server de Microsoft o Citrix ○ Consultando directamente a cada estación de trabajo a través del protocolo WMI ○ Lectura de la cabecera XFF al integrarse con soluciones terceras de Proxy ○ Capacidad de extraer la información de IP y usuarios a través de la lectura y extracción de datos del tráfico syslog. ○ Integración con soluciones de Wireless LAN Controller basadas en 802.1x y Soluciones NAC, con el objetivo de que el NGFW no dependa del Domain Controller para identificar al usuario. ○ A través de agentes instalados en las estaciones de trabajo, que reporten directamente al NGFW el usuario y dirección IP de cada equipo. • Deberá contar con un componente que permita integrarse a diversas plataformas de identidades tales como Azure LDAP, Google Directory, Okta, Cisco Duo, PingID. • Debe contar con la funcionalidad de Portal Cautivo (Captive Portal), de tal manera que el NGFW muestre un portal al usuario para que se autentique manualmente. Las cuentas podrán ser definidas localmente en el NGFW o integradas con plataformas terceras. • Debe tener integración con plataformas de MFA (Multi Factor Authentication), de tal forma que cuando un dispositivo requiera acceder a recurso, se le solicite el OTP.
POSTURA DE SEGURIDAD DEL ENDPOINT	<ul style="list-style-type: none"> • El NGFW deberá ser capaz de controlar el acceso a la red en base a una validación de la postura de seguridad del endpoint dentro de la red interna y sin necesidad de configurar túneles VPN.





	<ul style="list-style-type: none"> • A través de políticas de seguridad, el NGFW deberá ser capaz de validar si el equipo que intenta acceder a algún recurso de red (IP o IPs destino) cuenta con una postura de seguridad adecuada. • La restricción al recurso de red debe ser personalizable, es decir, el NGFW deberá permitir acceder de manera total o parcial al recurso de red destino en base al nivel de cumplimiento de la postura de seguridad del equipo. Por ejemplo, si cumple parcialmente con la postura de seguridad únicamente se le dará acceso para hacer PING a un servidor, si cumple completamente podrá acceder vía RDP. • La validación de la postura de seguridad del endpoint deberá ser continua; el NGFW automáticamente deberá restringir el acceso si es que luego de la conexión establecida el equipo modifica su postura de seguridad. • Como mínimo la postura de seguridad del deberá validar lo siguiente: <ul style="list-style-type: none"> ○ Sistema operativo del equipo ○ Serial number del equipo ○ Pertenencia al dominio de red de la Entidad. ○ Software antivirus instalado y/o habilitado en tiempo real ○ Software antivirus con la base de datos de firmas actualizada ○ Marca del software antivirus ○ Parche de seguridad instalado, según su nivel de criticidad ○ Firewall de host habilitado ○ Permitir crear validaciones personalizadas • Las políticas de validación de postura del endpoint deberán poder ser aplicadas a un grupo de usuarios o direcciones IP. • Deberá permitir configurar un mensaje personalizado, el cual permita notificar al usuario que controles no está cumpliendo. • Esta verificación se podrá realizar a través de un agente instalado en los endpoints. Debe tener soporte como mínimo para Windows y MacOS. • El postor tiene la libertad de integrar en su propuesta técnica una solución de un fabricante tercero al NGFW para cumplir este requerimiento.
VPN	<ul style="list-style-type: none"> • Soportar VPN Site-to-Site en protocolo IPSec • La VPN site to site debe soportar como mínimo: <ul style="list-style-type: none"> ○ AES 128, AES 256 (Advanced Encryption Standard) ○ Autenticación MD5, SHA-1, SHA-2; ○ Diffie-Hellman Group 1, Group 2, Group 5 y Group 14; ○ Algoritmo Internet Key Exchange (IKEv1 & IKEv2);



- Permitir la aplicación de políticas de seguridad y visibilidad para las aplicaciones que circulan dentro de los túneles VPN.
- Permitir aplicar QoS dentro de los túneles VPN.
- Soportar VPN client-to-site pudiendo operar usando el protocolo IPSec o SSL.
- Permitir la conexión por medio de agente instalado en el sistema operativo.
- Soportar autenticación vía AD/LDAP, Kerberos, TACACS+, SAML, Certificados Digitales y RADIUS.
- Capacidad de integrarse con plataformas de Doble Factor de Autenticación (2FA).
- Debe permitir definir segmentos de red para ser agregadas de forma automática en la tabla de rutas de la interfaz túnel del equipo que tenga instalado el agente de VPN.
- Debe soportar Split Tunnel para elegir los segmentos de red que serán enrutados por la VPN, incluyendo el soporte de Split DNS.
- El Split Tunnel debe permitir elegir el tipo tráfico que se enrutará por el túnel VPN, basado en el nombre de la Aplicación y el Dominio.
- Debe permitir los siguientes tipos de conexión del cliente al túnel VPN:
 - Antes del usuario se autentique en la estación.
 - Después de la autenticación del usuario en la estación usando Single Sign On (SSO).
 - A demanda, de forma manual por parte del usuario.
- El agente de VPN client-to-site debe ser compatible al menos con Windows 10, MacOS, Linux, Android y iPhone.
- La plataforma debe ser capaz de colocar en cuarentena equipos con actividad maliciosa identificada, de manera manual y automática. Los equipos en cuarentena no deberán tener conexión con ningún recurso de red protegido por la solución.
- Deberá permitir la configuración de controles de acceso basados en una arquitectura de ZTNA (Zero Trust Network Access), validando al menos los siguientes elementos:
 - Acceso basado en la identidad del usuario, con integración a plataformas MFA.
 - Validación continua de la postura de seguridad del host, no solo para denegar o permitir el acceso VPN, sino para controlar granularmente el acceso a los recursos. Por ejemplo, deberá ser posible dar acceso a los recursos de manera limitada, si el equipo es parcialmente compliance con la postura de seguridad requerida; estas configuraciones de control de acceso deberán poder ser personalizadas directamente en la consola de la solución.

	<ul style="list-style-type: none"> ○ Si el equipo cumple los requisitos de postura y logra establecer una conexión VPN, pero posterior a ello el equipo sufre alguna alteración que cause un incumplimiento de dichos requisitos, la solución deberá restringir el acceso de manera automática, hasta que su equipo vuelva a ser compliance. ○ El acceso otorgado a la red interna deberá cumplir el principio de mínimo privilegio, es decir, no deberá tener acceso total a la red interna, sino únicamente a los recursos que se requieran de manera granular para cada usuario, con controles de tráfico basado en capa 7 (aplicaciones), no solo capa 4 (puertos). ○ La solución deberá ser capaz de inspeccionar el tráfico entrante y saliente del túnel VPN por cada usuario, esto implica ser capaz de analizar a nivel de Control de aplicaciones, Antispyware, Antivirus de Red, Sandboxing. ● Respecto a los parámetros para validar la postura de seguridad del host, por lo menos se deberá poder validar los siguientes parámetros (permitiendo no solo una validación individual, sino también una combinación de ellas): <ul style="list-style-type: none"> ○ Sistema operativo del equipo ○ Serial number del equipo ○ Pertenencia al dominio corporativo ○ Software antivirus instalado y/o habilitado en tiempo real ○ Software antivirus con la base de datos de firmas actualizada ○ Marca del software antivirus ○ Parche de seguridad instalado, según su nivel de criticidad ○ Firewall de host habilitado ○ Software de cifrado de disco instalado ○ Software de DLP instalado o se podrá añadir validaciones de aplicaciones personalizadas añadiendo la Clave de Registro (en caso de Windows) o Plist (en caso de MacOS) ● Todos los parámetros indicados deberán poder ser realizados desde la consola gráfica de la plataforma. No se aceptarán configuraciones a través de CLI ● Incluir el licenciamiento al menos para 2000 equipos conectados de manera concurrente.
SD-WAN	<ul style="list-style-type: none"> ● La solución debe soportar una consola de monitoreo con la capacidad de poder identificar fácilmente las aplicaciones y enlaces sus estados dentro de la red de SD-WAN (aplicaciones con problemas de jitter, latencia, pérdida de paquetes y sus diferentes estados dentro de la red) pudiendo ver el estado de estas en por lo menos en los últimos 5 minutos, última hora, último día o bien haciendo filtros personalizados.



	<ul style="list-style-type: none"> • La solución debe soportar la capacidad de poder monitorear la salud de los enlaces en términos de jitter, latencia y pérdida de paquetes, tomando decisiones inteligentes de enrutamiento basado en la condición de los enlaces de manera dinámica. • La solución debe soportar con la posibilidad de hacer reportes del estado de los enlaces y aplicaciones, indicando volúmenes de datos con respecto a las veces que fueron degradados o afectados. • Soportar la opción de cambiar dinámicamente de camino al detectar alguna degradación del enlace sin afectar o cortar la sesión establecida de la aplicación, es decir, que el usuario no perciba corte en la aplicación, ni tener que reiniciar la sesión. • Soportar de algoritmo de corrección de errores (FEC - Forward Error Correction) con el objetivo de poder garantizar una buena experiencia en el uso de aplicaciones de voz y video a través de la red de SD-WAN. • Soportar la transmisión de paquetes duplicados por diferentes enlaces al utilizar la red de SD-WAN con el objetivo de mantener una calidad de experiencia alta al usar aplicaciones de misión crítica y prevenir la pérdida de paquetes, incremento de latencia, jitter, etc. • Soportar la opción de monitorear la salud de los enlaces a través de aplicaciones de SaaS y aplicaciones de Cloud, para poder determinar si esas aplicaciones son enviadas a internet de manera directa o bien a través de algún camino de la red de SD-WAN. • Soportar la capacidad de definir el tiempo de intercambio de heartbeats entre los puntos del túnel SD-WAN. • Debe soportar configuraciones de SDWAN en IPv6 • Soportar fail over a nivel de sub segundos • Soportar dashboards de monitoreo basado en el rendimiento de una aplicación y/o del enlace físico.
CAPACIDADES DE OPTIMIZACIÓN	<ul style="list-style-type: none"> • Se deberá incluir una herramienta integrada y/o externa que genere alertas si existen problemas de salud del equipo en materia de hardware y software, como mínimo: consumo de memoria, problemas de la alta disponibilidad (HA), problemas de disco duro, firmware vulnerable, expiración de licencias. • Con el objetivo de que la Entidad cuente con autonomía para evaluar si el NGFW se encuentra configurado acorde a las buenas prácticas y evitar que el contratista sea juez y parte del control de calidad de ésta, se deberá incluir una herramienta que permita evaluar automáticamente si el NGFW se encuentra configurado acorde a las buenas prácticas del fabricante en materia de los diferentes módulos de seguridad que se le haya activado.





	<ul style="list-style-type: none"> • Esta herramienta deberá ser única y consolidar la información de todos los NGFW por adquirir en el presente proyecto. • Debe contar con gráficos ejecutivos que permitan mostrar el nivel de adopción de los módulos de seguridad del NGFW en las políticas de seguridad. • Debe contar con un módulo que permita filtrar y depurar las políticas de NGFW sin uso en la red. • Debe identificar automáticamente las políticas abiertas que no tengan restricciones de puertos y/o aplicaciones (ANY o ALL), con el objetivo de corregirlas y hacer cumplir el principio de mínimo privilegio. • Debe identificar las reglas superpuestas (shadowed rules), los cuales representen un riesgo de seguridad al permitir mayores accesos que los autorizados. • La herramienta podrá estar integrada al NGFW o externa, ya sea de la misma marca u otra que se puede integrar. • La herramienta deberá ser dedicada para la Entidad, no se aceptarán plataformas compartidas con otras empresas o clientes del postor. • La herramienta de evaluación de buenas prácticas deberá ser específica para la configuración del NGFW implementado, no se aceptarán portales con guías de usuarios genéricas. • Deberá contar con un módulo predictivo de problemas del equipamiento, que permita evaluar si los equipos tendrán problemas de performance en un futuro cercano. De tal forma que permita tomar acciones preventivas antes de que ocurra la falla. • Se debe proporcionar acceso a la base de datos de inteligencia de amenazas del fabricante, el cual debe permitir hacer consultas de Hashes, Dominios y Direcciones IP, para mostrar información sobre la amenaza, a nivel de clasificación, reputación, familia de malware, comportamiento.
ADMINISTRACIÓN	<ul style="list-style-type: none"> • Deberá tener una capacidad de almacenamiento de 48 TB utilizables en formato RAID1 o superior (es decir, deberá tener 96 TB, pero al estar en RAID solo es utilizable la mitad). • Deberá estar desplegado en Alta Disponibilidad, considerando dos equipos de las mismas características detalladas. • Permitir exportar las reglas de seguridad del NGFW en formato CSV y PDF • Debe contar con un dashboard interactivo y gráfico que permita monitorear el uso de las aplicaciones en capa 7, sitios web visitados, actividad de los usuarios, actividad por IP (origen y destino), países origen y destino del tráfico, uso de las reglas de seguridad, actividad del tráfico malicioso, actividad de los usuarios VPN. Esta información podrá ser vista en base a Bytes y Sesiones,



y ser filtrado en base a un rango de tiempo, IP, usuario, país y regla de seguridad.

- Debe permitir el control de acceso a la gestión del equipo a través de roles personalizables.
- Debe permitir la captura de paquetes en formato PCAP para poder ser leídos por una herramienta tercera. La captura de paquetes deberá poder ser filtrada antes del proceso de ejecución en base a la interfaz, IP y Puerto (origen y destino)
- Ante escenarios donde existan dos o más administradores en el equipo, logueados y realizando cambios en simultáneo en la consola de gestión, la solución deberá de ser capaz de solo aplicar los cambios realizados por cada administrador individual, sin afectar o sobrescribir los cambios del otro administrador.
- Contar con un módulo que permita comparar y que indique específicamente que cambio se hizo a una política de seguridad respecto a una versión anterior de dicha política.
- Debe poder realizar una copia de seguridad (backup) automática de las configuraciones y rollback de configuración a la última configuración salvada.
- Debe permitir el monitoreo de eventos basados en SNMP, integración con SIEM a través de Syslog, y envío de alertas por correo electrónico (integrándose a un servidor SMTP).
- Debe permitir la generación de logs de auditoría detallados, informando de la configuración realizada, el administrador que la realizó, su IP y el horario de la alteración.
- La gestión de NGFW debe permitir la asignación de una cuota de uso de disco para definir una capacidad máxima de almacenamiento de logs de tráfico de datos, amenazas, auditoría de configuraciones, eventos de sistema.
- Debe soportar la personalización de reportes, permitiendo mostrar información de eventos de antivirus, antispyware, IPS, navegación a internet, aplicaciones, malware de día cero, debe permitir seleccionar las columnas a mostrar, filtrar la información en base a usuarios, grupos de usuarios, direcciones IP, el rango de fechas de los datos, deben poder ser exportados en PDF y enviados automáticamente vía correo electrónico.
- Debe permitir configurar reportes para ver el tiempo de navegación de los usuarios en internet, clasificado por tipo de página web y URL.
- Debe contar con reportes predeterminados que muestren información y diversas estadísticas sobre el uso de aplicaciones SaaS.
- La gestión de NGFW debe permitir realizar tareas de gestión a través del API basado en XML.

La administración de todas las soluciones y equipamiento solicitado por la Entidad, serán de administración compartida, en ese sentido, el contratista entregará credenciales de usuarios a nivel de read/write a personal de la Sección Redes y Seguridad Informática que estará a cargo del monitoreo y administración, usuarios que serán designados por la Entidad. El contratista está obligado a considerar todos los componentes, dispositivos y materiales que requiera para la integración de la solución adquirida con la red de la Entidad, así como para el cumplimiento de la finalidad del servicio requerido.

5.2.1.5.4.1.14 DETECCIÓN Y CONTROL DE MALWARE AVANZADO.

Sistema de detección y control de malware avanzado para nodos principal y secundario.

- La infraestructura (hardware/software) deberá cubrir la funcionalidad de la capa de detección de intrusos a nivel de red (IPS de red) con control de tráfico por reputación dentro de la funcionalidad misma en un hardware.
- Los equipos deben ser nuevos, de primer uso y que no se encuentren en End of Support declarados por su fabricante.
- La solución IPS deberá ser basada en Hardware de propósito único para realizar inspección profunda ya que no se aceptarán soluciones basadas en hardware y software de propósito común, el IPS debe tener la capacidad de inspeccionar los paquetes de capa 2 a capa 7 del modelo sin afectar el desempeño de la red. La solución de protección contra ataques de nueva generación (IPS) deberá contar como mínimo con las siguientes:

Características y funcionalidades:

- Se deben instalar dos equipos en redundancia, a través de la fibra oscura, uno en cada nodo.
- El equipo debe tener una capacidad de procesamiento de 10Gbps, 20Gbps, 30Gbps, 40Gbps, 60 Gbps de tráfico agregado, considerando el 10% del tráfico SSL entrante utilizando claves de tamaño 1.024 bits (ARC4 de 128 bits).
- El equipo deberá soportar una tasa de al menos 10.000.000 (diez millones) de conexiones concurrentes y una tasa de al menos 450.000 (cuatrocientos cincuenta mil) nuevas conexiones TCP por segundo.
- El equipo debe soportar la tasa de al menos 260.000 nuevas conexiones HTTP.
- El equipo debe soportar un rendimiento máximo de 100 µs (cien microsegundos) de latencia para el tráfico de paquetes UDP.
- La conexión debe ser por fibra, con capacidades no menores a 8x10GB SFP+

Características de Seguridad

- Los filtros del IPS deben soportar al menos las siguientes acciones de red: Block (bloqueo de paquetes), Block (reset TCP), Permit (permitir paquete), Trust (tráfico confiable), Notify (notificar), Trace (captura del paquete)
- Los filtros de la solución IPS deben ser agrupados en categorías, para facilitar la administración contando con al menos las siguientes

categorias: Exploits, Reconocimiento, Política de Seguridad, Spyware, Virus, Vulnerabilidades, mensajería instantánea, P2P y Streaming media.

- La solución de IPS propuesta debe contar con un programa de descubrimiento de vulnerabilidades de día cero (Zero Day Vulnerability) reconocido en la industria de Seguridad.
- El IPS deberá brindar protección contra ataques de día cero (nuevos ataques conocidos) y con la opción de contar con un sistema de monitoreo global reconocido para el manejo de este tipo de ataques a nivel mundial el cual debe ser referenciable públicamente para conocer la criticidad de los eventos que están ocurriendo en el mundo, así mismo deberá existir la opción de contar con un servicio que permita el acceso/consulta a una base de datos privada de vulnerabilidades, que permita ser personalizable.
- El IPS deberá contar con la capacidad de realizar modelado de protocolo para analizar cualquier protocolo, existente y/o propietario sin necesidad de hacer actualizaciones al sistema operativo del IPS.
- El IPS propuesto debe ser capaz de soportar políticas de Seguridad granular, basado en los siguientes métodos:
 - Por dispositivo IPS (todos los segmentos)
 - Por segmento físico
 - Por VLAN TAG 802.1Q,
 - Por rango de direcciones IP – CIDR
- La solución IPS propuesta debe soportar la capacidad de bloquear ataques de reconocimiento.
- El IPS debe contar con capacidades que permitan detectar brechas de seguridad que no pueden ser descubiertas por las soluciones de detección tradicionales basadas en firmas: contenido HTML malicioso incluyendo JavaScript, archivos maliciosos y objetos maliciosos de Adobe incluyendo Flash y PDF.
- La solución debe contar con la capacidad de monitoreo de tráfico encapsulado por lo menos de los siguientes tipos: VLANs, incluyendo frames 802.1q, GRE, Mobile IPv4 (IP-in-IP), IPv6 (6-in-4, 4-in-6, 6-in-6), Túneles Authentication Header (AH), GPRS
- Realizar un monitoreo transparente para los usuarios donde de forma automática bloquee ataques maliciosos preservando la disponibilidad del ancho de banda de red.
- La solución IPS propuesta debe permitir identificar y bloquear la comunicación con servidores, y deberá poder realizar la detección de amenazas avanzadas tales como Back Orifice, port scans, sensitive data, datos predefinidos y que aplique los controles directamente a la consola de administración de la solución para automatizar el proceso de detección y contención.
- La solución IPS propuesta debe permitir alertar y bloquear comunicaciones desde y hacia determinados países
- El equipo debe soportar análisis y decodificación de al menos 150 (ciento cincuenta) protocolos de red, entre la capa 2 (Layer-2) y la capa 7 (Layer-7) del modelo OSI (Open System Interconnection), de manera que no : ARP, BOOTP, DCCP, DHCP, DNS, EIGRP, FINGER, FTP, HTTP, HTTPS, ICMP (versión 4 y versión 6), IMAP, IP (versión 4 y versión 6), LDAP, NetBIOS, NFS, POP3, RADIUS , SMTP, SNMP, SSH, RPC, TCP, TELNET, TFTP y UDP.





- El equipo debe soportar identificación de ataques por protocolos de red independientemente de los puertos de comunicación utilizados, de manera automática, por lo menos para los siguientes protocolos: DCERPC, DNS, FTP, HTTP, IMAP, IRC, POP3, PORTMAPPER, SIP, SMTP, SNMP, SUNRPC y UPNP.
- La solución debe proveer protección como mínimo contra ataques de tipo SQL Injection, Command Injection, Cross Site Scripting, Buffer/Heap Overflow, DDoS
- Debe permitir el re-ensamblado de paquetes y sesiones fragmentadas
- Se deberá incluir el acceso al portal de información de Investigación en Seguridad e Inteligencia de Amenaza Global.
- La solución propuesta debe contar con la actualización automática de filtros y firmas al menos una vez por semana conforme las libere el fabricante del IPS y durante 1 año de soporte.
- Licenciamiento para servicios de Reputación por IP
- A fin de poder escalar en tiempo, el vendor oferente deberá poder ofrecer una capa de XDR donde nativamente se pueda ofrecer integración con al menos 500 fabricantes distintos de forma nativa. De no poder contar con esta característica deberá ofrecerse al menos 200 horas de servicios de fabricante para este fin.
- Como centro de reputación global, el fabricante ofrecido deberá contar con asociación directa de proveedores de servicios de análisis forense como Mandiant al menos. Se deberá confirmar que existe un contrato de sharing de IOCs de alguna de estas compañías en sus servicios. De no contarse con este partnership se aceptará personal dedicado (como mínimo 2 recursos) para realizar tareas de hunting 24/7 de IOCs publicados por empresas similares en el servicio.
- El IPS debe soportar reputación basado tanto en dirección IP como en nombre del dominio.
- La base de datos de reputación debe ser alimentada con diferentes fuentes de reputación.
- Las políticas de reputación deben tener la flexibilidad para ser aplicado en modo Permitir o Bloquear.
- Deberá mostrar para cualquier evento el origen y el destino del ataque o incidente de seguridad.
- Deberá soportar la descarga de paquetes, al generarse un evento de intrusión, para protecciones específicas con el fin de realizar análisis forenses.

Sistema de Administración y Configuración

Administración Local

- El IPS propuesto debe contar con una interfaz de administración vía Línea de Comandos (CLI) que siempre esté disponible en caso de que la interfaz de administración web esté inhabilitada

Administración Centralizada

- El IPS propuesto debe soportar un servidor de administración centralizada para administrar todos los dispositivos IPS.
- La solución de administración debe permitir configurar se para buscar, descargar y distribuir automáticamente las actualizaciones de los filtros en los IPS.

- Se debe contar con un Dashboard accesible vía Web, que permita supervisar todas las aplicaciones y alertas de seguridad, permitiendo priorizar los problemas de seguridad para su resolución mediante el resumen de filtros de Día Cero que se han estado activando, los Host con Brechas de Seguridad, los Servidores con Vulnerabilidades atacados.
- La solución debe permitir la definición y asignación de políticas de seguridad en función de segmentos físicos, VLAN's, rango de IP's, flujo de tráfico, etc.
- El servidor de administración debe contar con capacidad integrada de reporte incluyendo reportes para Top N de ataques, origen de los ataques, destino de los ataques, top de aplicaciones, Top reputación por País.
- El servidor de administración centralizado debe soportar la generación de reportes manual o calendarizados diariamente, semanalmente, mensualmente, etc.
- El servidor de administración centralizado debe permitir exportar el reporte al menos en los formatos PDF
- El servidor de administración debe soportar archivar y hacer backup de eventos.
- El sistema de administración propuesto debe ser capaz de proveer diferentes niveles de cuentas de usuarios y acceso de administración con al menos 3 perfiles.
- La solución debe poder como opción el soportar integración con herramientas SIEM y enviar logs en formato Syslog.
- La solución de administración centralizada debe permitir la administración de los IPS parte de la solución requerida.
- La solución de administración centralizada debe permitir importar los resultados de soluciones de detección de brechas de seguridad a través de API's, permitiendo integrar las URL's y las Direcciones IP's maliciosas descubiertas para robustecer el esquema de protección de los IPS.
- La solución de administración debe proporcionar visibilidad, contexto mejorado e informes sobre el tráfico de un usuario en particular a través de la integración de Active Directory (AD). Se debe tener visibilidad al menos del nombre de usuario, dominio, grupo de usuarios, entre otros, se deben poder rastrear y tener la información para funcionalidades forenses y generación de informes.



5.2.1.5.4.1.15 PROTECCIÓN DE PORTALES WEB Y BASE DE DATOS:

Actualmente la entidad cuenta con los siguientes portales web administrados por la Entidad:

- *.pnp.gob.pe
- *.policia.gob.pe

La Entidad también cuenta con los siguientes motores de base de datos:

- SQL Server
- Oracle

a. Protección de portales web:

La solución debe estar conformada por equipamiento basado en plataforma appliance (hardware y software de propósito específico) del mismo fabricante, que proporciona las funcionalidades de la protección de portales web o Firewall de aplicaciones web (WAF) y consola de gestión; sin necesidad de la instalación de software y/o hardware en algún equipo adicional que no forme parte de la solución.

Los equipos que requiera instalar el contratista para la prestación del servicio deben ser nuevos, de primer uso y que no se encuentren en End of Support declarados por su fabricante. Así mismo, funcionar con la última versión de software del sistema operativo vigente en el mercado, debiendo tener un buen estado de conservación, no presentando partes con raspadura, rajadura, rotura, abolladura, perforación, ni óxido.

La solución debe implementar en formato de alta disponibilidad, a través de la fibra oscura, uno por cada site (01 protección de portales web + 01 protección de base de datos).

Proporcionar, el correspondiente respaldo del fabricante, los servicios de garantía de hardware, mantenimiento software y soporte técnico, para la solución por el periodo de tres (03) años

Características y Funcionalidades del WAF:

- El equipo WAF perteneciente a la solución debe poseer como mínimo de 02 appliance. Cada WAF debe cumplir con las siguientes características:
- Contar con cuatro (04) interfaces como mínimo de tipo 10G SR.
- Poseer una (01) interface como mínimo independiente para administración, de tipo Ethernet.
- El appliance debe contar con fuente de poder redundante e intercambiable en caliente
- La solución deberá tener un throughput de aplicación y protección WAF sobre protocolo https de mínimo 5 Gbps, este throughput no debe ser de balanceo o red y se debe medir específicamente para tráfico aplicativo.
- Soporta bypass de dos (02) segmentos como mínimo ante fallas.
- Debe Soportar aceleración SSL basada en hardware con módulos o tarjetas específicas de descarga de negociación SSL
- De Factor de forma 2 RU como mínimo
- Soportar varios modos de operación, tales como puente transparente en línea (Transparent inline bridge) y fuera de línea (non-inline).
- Capacidad de integrarse a la red en modo bridge (capa 2 del Modelo OSI, las interfaces no requieren de una dirección IP). Las interfaces incluyen bypass/failopen/failclose configurable tanto para fallas de hardware.
- Permitir la integración en los modos reverse proxy y reverse proxy transparente.
- Protección de aplicaciones web
- Permitir bloquear las transacciones web en forma preventiva, antes de que estas lleguen al servidor.
- Capacidad de detectar, alertar y opcionalmente bloquear, en tiempo real, cualquier comportamiento malicioso conocido y/o desconocido.
- Contar con un modo de aprendizaje que permite definir cuáles son las acciones esperadas y aceptadas para los usuarios.
- El modo aprendizaje, debe aprender la estructura y elementos de la aplicación y esta información estará disponible para automatizar la configuración del



modelo positivo de seguridad. Como mínimo debe aprender sobre: Hosts, URLs, parámetros, tipo de contenidos de los parámetros y cookies.

- En modo aprendizaje, debe aprender también en base al comportamiento esperado del usuario y esta información estará disponible para automatizar la configuración del modelo positivo de seguridad.
- La solución debe tener capacidad de proteger frente ataques DDOS o DOS y antibot que no superen las capacidades de red e internet de la entidad y que estén dedicadas a las aplicaciones, proporcionar protección para todas las vulnerabilidades expresadas en OWASP, SQL INJECTION, CROSS SITE SCRIPTING entre otros.
- Capacidad de efectuar el parchado virtual de las aplicaciones web, para remediar las vulnerabilidades detectadas y debe permitir tener integración con software de detección de vulnerabilidades (la solución debe permitir integrarse como mínimo con dos vendor de scanner de vulnerabilidades que debe ser indicado mediante una carta del fabricante que se debe presentar para el perfeccionamiento del contrato), permitiendo utilizar los resultados de la ejecución de dichos programas para generar los parches virtuales.
- Para el caso de la implementación en la Entidad, la solución debe ser integrada con un scanner de vulnerabilidades especializado en aplicaciones web, para ejecutar sus procesos de tarea hacia los servidores de aplicaciones web de la Entidad, la cantidad de estos servidores serán definidos en una visita técnica realizada a la Entidad por el contratista previa coordinación con el responsable de Tecnología de la Información, con el fin de una mejor presentación de propuestas técnicas.
- La solución debe efectuar verificación de falsos positivos, este comportamiento examinará varios factores mínimos tales como: HTTP Protocol, Violación de Profiles, firmas, caracteres especiales, reputación de usuarios para precisar alertas o bloqueo de ataques con la finalidad de minimizar los falsos positivos.
- La solución debe contar con un sistema avanzado de alertas que reconozca y proteja contra ataques web de tipo avanzado.
- La solución debe contener un conjunto de firmas de aplicaciones y políticas disponibles, para las más avanzadas vulnerabilidades, también debe entregar inteligencia de amenazas y permitir el control de protección contra ataques de aplicaciones web
- A fin de asegurar la calidad de los datos auditados, al operar en modo bridge la solución no debe modificar las conexiones entre los clientes y el servidor, por lo que se asegura que los mismos paquetes (IP origen, IP destino, puerto origen, puerto destino, número de secuencia y datos de TCP) sean idénticos en ambos extremos.
- Respecto de algún ataque o alguna otra actividad no autorizada, la solución debe ser capaz de tomar las acciones adecuadas, como mínimo: Terminar las solicitudes y respuestas, bloquear la sesión TCP y bloquear la dirección IP.
- Contar con un conjunto de patrones correspondientes a los ataques conocidos. Esta base de datos de patrones se actualiza periódicamente en forma automática y no asistida.
- Permitir la creación de reglas lógicas que permiten identificar condiciones definidas por los usuarios, como una expresión regular o un valor determinado, en cualquier de los siguientes elementos: Encabezado y cuerpo del requerimiento HTTP, encabezado y cuerpo de la respuesta HTTP.
- Permitir definir las alarmas condiciones lógicas, en la cual la alarma no se dispara si no ha ocurrido por lo menos una cantidad de veces definida, en un período de tiempo definido.





- Capacidad de automatización para políticas de seguridad XML en protección de Servicios Web, SOAP, HTML 5 Web Sockets y Aplicaciones Web 2.0 como mínimo.
- Capacidad de proteger Servicios Web basados en SOAP y de aprender las estructuras de los elementos SOAP y su contenido, proponiendo la configuración.
- Capacidad de recibir y utilizar los certificados y pares de llaves público/privadas para los servidores web protegidos.
- Deberá contar con las siguientes funcionalidades:
 - Inspeccionar y monitorear todos los datos HTTP/S de la aplicación, incluyendo, los encabezados HTTP, campos de formularios, y el cuerpo HTTP/S.
 - Inspeccionar las peticiones y respuestas HTTP/S.
 - Capacidad de decodificar datos a su mínima expresión y validarla.
- Disponer de una funcionalidad de búsqueda de servidores web en la red y la capacidad para configurar automáticamente la protección para los servidores encontrados.
- Capacidad de identificar el usuario de la aplicación web. La identificación persiste hasta que el usuario haya abandonado la aplicación.
- Permitir identificar y mantener un registro de las sesiones web a nivel aplicativo, por medio del seguimiento de cookies o parámetros de aplicación.
- Implementar en forma nativa controles anti-scraping, permitiendo bloquear intentos reiterados sobre un mismo URL o parte de un URL.
- La solución debe contar con funcionalidades que permitan:
 - Rastrear e identificar las fuentes de los ataques originadas desde proxies anónimos, direcciones ip maliciosas, botnets y sitios de phishing.
 - Actualizar las fuentes de ataque para identificar y bloquear el tráfico malicioso.
 - Ajustar dinámicamente las políticas de seguridad con base en la identificación de las fuentes de ataque o de las fuentes que denoten actividad sospechosa.
 - Bloquear solicitudes de acceso basado en la reputación de la fuente del tráfico, como direcciones IP conocidas por su comportamiento malicioso por Botnet, DDoS, Phishing o redes de Anonimización (TOR y Proxis Anónimos).
 - Bloquear solicitudes de acceso basado en el país de origen de la conexión.
 - Realice un análisis automático de distribución de alertas en relación al país de origen, con opción a representar la información a través de un mapa mundial
 - Debe proveer protección contra toma de cuenta.
- La solución deberá monitorear y proteger las APIs desplegadas validando y monitoreando el tráfico de API y detectando actividad maliciosa
- La protección de API, de manera opcional, deberá incluir rate limiting, validación de sesión, seguimiento de usuarios, validación de certificados de clientes y validación de protocolos
- La protección de API deberá incluir un servicio de reputación para identificar IPs reconocidas como atacantes
- La protección de API, de manera opcional, deberá proteger contra manipulación de parámetros y uso de campos maliciosos perfilando y aprendiendo los llamados a las API y bloqueando llamados mal formados

- La solución deberá permitir crear un modelo positivo de seguridad para las APIs a partir del archivo swagger de las APIs
- La solución deberá proteger contra ataques DDOS o DOS y antibot que no superen las capacidades de red e internet de la entidad y que estén dedicadas a las aplicaciones.

b. Firewall de base de datos

Condiciones Generales

La solución estará conformada por equipamiento basado en plataforma appliance (hardware y software de propósito específico) del mismo fabricante, que proporcione la funcionalidad de protección de Bases de Datos (DBF).

Los equipos deben ser nuevos, de primer uso y que no se encuentren en End of Support declarados por su fabricante.

Proporcionar, con el correspondiente respaldo del fabricante, los servicios de garantía de hardware, mantenimiento software y soporte técnico, para la solución por el periodo de tres (03) años.

Contar con autorización del fabricante o su representante para comercializar la marca y brindar los servicios solicitados. Dicha autorización deberá ser presentada para la firma del contrato.

Funcionalidades del firewall de base de datos

- Cada equipo perteneciente a la solución debe poseer como mínimo las siguientes Características:
 - Debe soportar al menos 25,000TPS
 - Debe incluir el licenciamiento de 100 agentes para el monitoreo de la base de datos.
 - Debe contar como mínimo con 128GB de RAM
 - Debe contar como mínimo con 8 TB de capacidad de disco
 - Debe contar con fuente de poder redundante.
 - Debe contar con 8 interfaces 100/1000BASE-T Cobre.
 - El hardware debe soportar agregar placas de fibra, tanto de 1GbE como de 10GbE.
 - Debe contar con una interface independiente del tipo RJ45 para administración.
 - Debe contar con un factor de forma de 2U y rackable en gabinete estándar.
 - Debe contar mínimo con un puerto USB.
 - Debe instalarse en modo de alta disponibilidad, por cada centro de datos.
- La solución debe tener varios mecanismos de despliegue basado en agentes para monitoreo o bloqueo, siendo capaz de auditar las comunicaciones hacia las bases de datos interceptando las mismas en el agente. La implementación será en modo bloqueo, no sólo en modo monitoreo.
- Debe ser posible la instalación de agentes sólo para el monitoreo de todo el tráfico o poder excluir solamente la auditoría para tráfico local.
- Protección de Servidores de Base de Datos
- La solución no debe requerir la activación de la auditoría nativa de las bases de datos a proteger.





- La solución debe estar basada appliance con un sistema operativo robusto y específico para la función.
- La solución debe incluir agentes livianos de software para monitoreo de actividad sobre el servidor, sin depender de eventos nativos como registros de auditoría o logs de los servidores a proteger.
- Los equipos deben soportar el protocolo de gestión de red SNMP para ser monitoreados por las herramientas propias y generar alertas o traps hacia el servidor correspondiente.
- El sistema debe permitir la integración y envío de alertas a terceros u herramientas de correlación (SIEM).
- El sistema debe soportar protocolo de sincronización de hora NTP.
- La solución debe permitir aplicar políticas de seguridad a las distintas bases de datos en forma independiente y por conjunto de aplicaciones definidas por el administrador.
- La solución debe detectar analizar y clasificar información sensible sobre las bases de datos a proteger.
- Permitir registrar todas las pistas de auditoría de manera detallada de todas las actividades referentes a las bases de datos.
- Las políticas de seguridad deben permitir definir los siguientes tipos de violaciones de accesos:
 - Acceso denegado a un método determinado por parte de una o varias direcciones IP.
 - Acceso a base de datos, esquemas, tablas y comandos SQL no permitidos.
 - Operaciones sobre los datos no permitidas.
 - Operaciones DDL críticas no permitidas.
 - El manejo de políticas de seguridad debe cumplir los siguientes requerimientos:
 - Capacidad de aprender las políticas de seguridad adecuadas en base a la observación del tráfico existente.
 - Permitir la aceptación de peticiones legítimas que son consideradas como falsos positivos por la solución.
 - La solución debe tener los siguientes modos de operación: normal y simulación, este último no debe aplicar ninguna restricción sobre el tráfico cursante.
 - La solución debe detectar, alertar y opcionalmente bloquear, en tiempo real, cualquier comportamiento malicioso conocido y/o desconocido.
 - La solución debe soportar des encriptación de las conexiones de SQL sin instalar ningún software en el servidor de base de datos.
 - La solución debe notificar por medio una alerta cuando no pueda desencryptar el tráfico SSL por no tener el certificado y clave privada correctos.
 - La solución debe soportar la interpretación de los usuarios ocultos de Kerberos en MSSQL sin instalar ningún software en el servidor de base de datos.
 - La solución debe soportar las siguientes bases de datos, como mínimo:
 - Microsoft SQL Server
 - Oracle
 - Sybase.
 - Informix

■ MySQL

- Debe soportar el Negative Security Model, es decir, permitir todas las transacciones menos aquellas especificadas como ataques y/o Positive Security Model, es decir, solo permitir aquellas transacciones definidas como válidas.
- En el Positive Security Model debe soportar configuración manual y automática. Esta última debe ser implementado mediante técnicas de aprendizaje automático.
- Permitir la definición del uso de aprendizaje automático y manual en forma individual para cada aplicación de base de datos.
- El aprendizaje automático debe alcanzar los siguientes datos:
 - Usuarios de base de datos
 - Aplicaciones de base de datos
 - Equipo donde reside la aplicación de base de datos
 - Base de datos y esquemas consultados
 - Comandos DML ejecutados (SELECT, UPDATE, INSERT y DELETE)
- La solución debe soportar la protección contra ataques conocidos mediante la utilización de firmas de ataques.
- La solución debe soportar la creación manual de firmas mediante expresiones regulares.
- Las firmas podrán ser aplicados sobre un subconjunto de la aplicación base de datos y o políticas. Dicho subconjunto debe poder ser definidos mediante la definición de base de datos, esquema, tablas y o columnas. La solución debe realizar actualizaciones automáticos de firmas.
- La solución debe contener firmas propias las cuales se deben actualizar de manera automatizada.
- La solución debe controlar la consistencia del protocolo de base de datos, identificando ataques a la integridad de la conexión y la evasión de auditoría.
- La solución debe incluir un analizador de vulnerabilidades que se podrá ejecutar en forma manual y/o automatizada sobre las bases de datos a proteger.
- La solución debe estar compuesta por todos los componentes de hardware y software necesario para su completo funcionamiento sin necesidad de instalación de software ni hardware en algún equipo que no forme parte de la solución.
- La solución debe incluir reportes, políticas de seguridad y de auditoría predefinidas, además de que se deben actualizar de manera periódica

c. Consola de Administración

- La consola centralizada deberá ser entregada como appliance físico. La solución debe ser administrada por consolas separadas, tanto para WAF como para DBF.
- La solución permitirá generar archivos de respaldo automáticos y ser copiados en un servidor externo usando protocolos FTP o SCP. El SSH y HTTPS, son usados para administración y/o gestión del equipo
- Debe permitir la definición de distintas políticas de seguridad, entendiéndose como tal, al conjunto de reglas bajo el cual estará controlada una determinada aplicación.



- Debe permitir elegir la política de seguridad a ser implementada en una aplicación, como así también la aplicación de políticas distintas para aplicaciones distintas.
- Debe contemplar mecanismos que permitan fácilmente deshacer cambios efectuados por una política de seguridad implementada en una aplicación.
- Toda la configuración, administración y monitoreo de la solución se efectuará a través de las consolas de la solución.
- La comunicación entre las estaciones de trabajo y la consola de administración debe establecerse a través de un protocolo seguro con cifrado y autenticación por medio de usuarios locales, certificados digitales.
- Debe permitir la notificación de un determinado evento, producto de la aplicación de una política de seguridad mediante: Email, Syslog, SNMP, además de su visualización en la consola.
- La solución de administración debe permitir asignación de perfiles de administración por usuarios y estos perfiles deben permitir separar roles de administración y monitoreo.

Gestión de logs

- Proporcionar una vista centralizada de los logs, entendiendo como tal, la unificación de los logs de la totalidad de los componentes que conforman la solución.
- Los logs de todos los componentes de la solución deben cumplir con las siguientes características:
- Poder ser transferido hacia el servidor de administración externo.
- Capacidad de ser exportados desde el servidor de administración, a un formato para poder utilizar herramientas de análisis de terceros.
- En caso utilizar un servidor administración externo, los equipos deben poder almacenar en forma local los logs, para aquellos casos que existan inconvenientes en la comunicación con el servidor central.
- La administración debe permitir la visualización en tiempo real de los logs de actividad de la solución WAF y las modificaciones de configuración que los administradores pudieran efectuar.
- La solución permitirá seleccionar si es factible o no acceder a los logs del sistema. Asimismo, éstos pueden ser enviados a un servidor externo syslog o con Traps SNMP.
- Permitir especificar el tamaño máximo dedicado al almacenamiento de logs como opcional.
- Permitir que un usuario de la solución defina que transacciones serán registradas.
- La solución permitirá almacenar los logs tanto de forma cifrada o en caso no se requiera puede ser almacenada sin cifrado. Es una configuración que será permitida para la solución ofrecida.
- La solución permitirá integración con un conjunto de herramientas SIEM del mercado, asimismo, el envío de los logs se puede realizar usando el formato CEF u otros.
- La administración debe permitir, como mínimo, lo siguiente:
 - Agregar, eliminar o modificar la configuración en un entorno gráfico
 - Modificar las reglas de los diferentes equipos que conforman la solución.
 - Efectuar la configuración de los componentes de la solución.
 - Visualizar los registros de auditoría, alertas de seguridad y eventos del sistema (opcional).
 - Generar reportes ajustables por el usuario

Monitoreo y alertas



- Soportar SNMP v2 y v3 para control y monitoreo.
- Soportar la generación de alarmas mediante los siguientes protocolos:
 - SNMP.
 - Email.
 - Syslog.
- Se deben generar dashboard que provean, en tiempo real, vistas de:
 - Estado del Sistema.
 - Eventos de Seguridad.
- La solución permite generar notificación de alertas del sistema ante determinados eventos propios del equipo, tales como llenado de disco duro, reducción de performance, fallas en el equipo en general, etc. Estas notificaciones no son automáticas, se generan en base a la configuración del usuario haciéndose esto de forma opcional
- Poseer alarmas automáticas con la información completa (detalle del problema, configuración, log). La administración debe permitir la visualización en tiempo real de los logs de monitoreo correspondientes a los eventos que hayan violado una política de seguridad determinada, detallando como mínimo:
 - IP Origen
 - Puerto de origen y destino
 - Nombre del evento
 - Severidad del evento
 - Fecha y hora de ocurrencia
 - Nombre de la aplicación asociada al evento.
 - IP destino
 - Usuario de base de datos y sistema operativo (opcional)
 - Base de datos, esquema y tablas afectadas (opcional)
 - Descripción del evento o incidente de seguridad detectado
- Las alertas deben ser fácilmente buscadas, ordenadas y relacionadas a las reglas de seguridad.
- El administrador podrá categorizar los distintos eventos en función de distintos criterios a ser definidos.
- La administración debe permitir la notificación de un determinado evento, producto de la aplicación de una política de seguridad mediante: Email, syslog y SNMP, además de su visualización en la consola.

Reportes

- Permitir la generación de reportes, de toda la actividad registrada en los logs, en los formatos PDF, CSV como mínimo.
- Capacidad de automatizar la generación de reportes y su posterior remisión por email.
- Capacidad de generar reportes gráficos de fácil entendimiento sobre estado de seguridad, cumplimiento de regulaciones entre otros, la forma de generarlos puede ser predefinidos o customizados.
- Permitir la elección de información a ser incluida en los reportes.
- La generación de estos reportes me debe permitir revisar el cumplimiento de estándar relacionado a cualquiera de estas regulaciones: PCI, SOX, FISMA.

Otros Consideraciones:

- El Postor adjudicatario de la buena pro debe asegurar que la solución cuente con un servicio de investigación sobre vulnerabilidades y amenazas informáticas, para lo cual presenta la documentación respectiva en el descubrimiento de éstas (documentación que será entregada en la etapa de perfeccionamiento del contrato).



- El Postor debe presentar el modelo de la solución propuesta que debe contar con la certificación o reconocimiento como líder en firewall de base de datos, en reportes de analistas como Gartner y/o forrester, documentación que se debe presentar en el momento de la presentación de la oferta.

La administración de todas las soluciones y equipamiento solicitado por la Entidad, serán de administración compartida, en ese sentido, el contratista entregará credenciales de usuarios a nivel de read/write a usuarios designados por la Entidad. El contratista está obligado a considerar todos los componentes, dispositivos y materiales que requiera para la integración de la solución adquirida con la red de la Entidad, así como para el cumplimiento de la finalidad del servicio requerido

5.2.1.5.4.1.16 SPAM FIREWALL y PROTECCION ANTE PHISHING DIRIGIDO:

SPAM FIREWALL

La Entidad tiene más de 20000 buzones de correo, basados en una plataforma de Exchange.

Se debe suministrar el equipamiento y/o licencias necesarias para proporcionar el servicio de filtrado de correo y cifrado de correo electrónico a nivel de Gateway u otro medio alternativo, para al menos 30000 usuarios.

La solución debe soportar 5.000 dominios con configuraciones independientes o garantizar la protección independiente de todos los dominios que entidad necesite proteger.

La solución debe ofrecer protección del servicio de correo en múltiples capas, utilizando técnicas de filtrado de conexiones y escaneo profundo en los mensajes.

Protección que permita rechazar el correo no deseado (spam), mediante la previa verificación y comprobación de las direcciones ip de mensajería entrante, en bases de datos especializadas con registros de sitios considerados como altamente generadores de "spam"

Las características de protección requeridas son las siguientes:

- Detección en tiempo real de malware moderno en correos electrónicos. Debe tener un centro de inteligencia que se nutra con telemetría de las propias soluciones que administra el fabricante, al menos con las siguientes: endpoint security, SIEM, NDR, Sandboxing, cifrado, DLP, firewall de base de datos, análisis de vulnerabilidades de base de datos, FIM, Firewall de escritorio, y además el partnership de Mandiant. En el caso de no tenerse estas capacidades de forma nativa, debe ser contemplarse una equipo de personas que 24/7 administren la inteligencia de estas fuentes solicitadas.
- Análisis detallado de amenazas con información específica sobre la comunicación, IP, encabezado, y cambios en el sistema operativo.
- Capacidad de detectar amenazas sin firmas conocidas.
- Módulo de detección de AV/AS. Debe presentar 100% de eficacia en detecciones en el SE Labs Award de Q1 2023. Si no se cumple se debe agregar un servicio de monitoreo 24x7 dedicado a analizar muestras de manera diaria para identificar GAPS de seguridad y plan de cobertura. Si no se tiene participación o resultados esperados en este cuadrante se podrá incluir horas dentro del servicio propuesto de un red team que evalúe trimestralmente los rates de protección para lograr resultados como los esperados.
- Implementación en modo de protección activa, MX y monitor BCC con posibilidad de integrarse activamente a la solución de XDR del mismo

fabricante con el fin de lograr mayores casos de uso con al menos 1000 integraciones nativas. De no cumplirse se deberá agregar en la propuesta una solución de XDR del mercado que soporte esta cantidad de integraciones nativas.

- Cuarentena y notificación de correos maliciosos.
- Debe tener capacidades nativas de sandboxing en la misma solución o agregadas como complemento.
- Soporte para Reescritura de URLs, correlación de cabecera y cuerpo del email, y detección de spoofing de dominios.
- Portal para visualización en tiempo real y generación de reportes.
- Integración con soluciones de correos en la nube y protección de amenazas avanzadas a nivel web.
- Debe contarse con un partnership con Mandiant con el fin de compartir indicadores de compromiso únicos entre ambos vendors. En el caso de no tenerse, se deberá incluir un servicio de inteligencia de terceros como Mandiant o IBM Watson.
- Certificación "Safety act" del DHS, FEDRAMP, ISO 27001 y certificación SOC 2 Type II. Se no tenerse estas certificaciones se considerará un servicio trimestral de personal incluido en la propuesta dedicado a auditar controles de estas normativas.
- Funcionalidades avanzadas de Mail Transfer Agent (MTA).
- Soporte para gestión de congestión y varias opciones de despacho de correos.
- Configuración de tamaño máximo de correo.
- Análisis de URLs acortadas y en Sandbox. Sandbox propio o agregado en la propuesta.
- Inclusión de encabezado de correo con resultados de análisis.
- Creación y gestión de listas blancas y negras con múltiples criterios.
- Capacidad de importar y exportar listas en formato CSV.
- Debe tener la capacidad de remediar actividades maliciosas detectadas post delivery a través de integración nativa por API al servicio de correo. Propia de la solución o como servicio 24x7 incluido en la propuesta para este proposito.
- Notificaciones configurables en varios formatos.
- Detección de código malicioso en documentos y archivos comunes.
- Análisis de URLs embebidas en documentos PDF.
- Sincronización de tiempo a través de NTP.
- Soporte para SNMP con seguimiento detallado.
- Alertas retroactivas y detección de URL ocultas. Si la solución no posee estas características de forma nativa se podrá ofrecer un XDR integrable nativamente con la solución para tomar estas acciones.
- Sistema de cuarentena con configuraciones de almacenamiento y alertas.
- Descarga de correos en cuarentena en su forma original.
- Capacidades de búsqueda y listado en el sistema de cuarentena.
- Generación de reportes estadísticos detallados.
- Soporte para la creación de reglas en formato YARA, versión 3.4 o superior

5.2.1.5.4.1.17 PROTECCIÓN CONTRA ATAQUES DE DENEGACIÓN DE SERVICIO DISTRIBUIDO

El proveedor debe suministrar dos (02) equipos AntiDDoS (01 datacenter principal y 01 en el datacenter secundario), en los cuales se implementen reglas que evite la indisponibilidad del Servicio. Este bloque permitirá proteger los enlaces del

datacenter principal y secundario; asimismo, este bloque debe ser instalado encima del ROUTER de cada Cabecera Internet, la solución debe estar implementado con fibra 10Gbps y es responsabilidad del proveedor proveer todo lo necesario para que la solución funcione. Dichos equipos del Bloque Seguridad AntiDDoS deben ser On-Premise y del mismo fabricante para los equipos a instalarse en los centros de datos mencionados, debe tener al menos las siguientes características

- Debe estar licenciada para un throughput de tráfico legítimo de al menos 5 Gbps.
- Los equipos deben ser nuevos, de primer uso y que no se encuentren en End of Support declarados por su fabricante.
- Debe soportar crecimiento de throughput por licenciamiento sobre el mismo hardware de hasta 40 Gbps por equipo.
- Debe estar licenciada para soportar una capacidad de mitigación de al menos 5 Millones de PPS.
- Debe tener la siguiente configuración de interfaces para su integración a la red.
 - 4 Interfaces de fibra 10 Gbps LR.
- Debe contar con módulos de Bypass internos para las interfaces de fibra 10 Gbps LR
- El dispositivo debe incluir al menos dos interfaces de gestión (Management Ports) y administración por consola RJ45.
- Sin límite en la cantidad de sesiones concurrentes, al menos bajo las condiciones de ataque (Debe ser Stateless)
- Debe tener la capacidad de bloquear tráfico usando firmas de cabecera o contenido de paquetes o cualquier otra técnica que resulte adecuada para bloquear los distintos tipos de ataques de denegación de servicio conocidos ya sean volumétricos, de agotamiento de estado o de aplicación. Las firmas pueden ser actualizadas periódicamente por un servicio de inteligencia informática provisto por el fabricante de acuerdo con la actividad reciente monitoreada en internet
- Mitigar únicamente tráfico de ataque afectando lo menos posible al tráfico considerado legítimo
- No se aceptará que los equipos solo utilicen técnicas basadas en rate-limit. Debe permitir aplicar las técnicas adecuadas para cada técnica de ataque detectado
- Debe mitigar ataques en capa TLS/SSL permitiendo para ello la instalación de certificados de seguridad en el dispositivo con soporte TLS 1.3.
- Contar con firmas que protejan ante ataques que aprovechen vulnerabilidades que puedan ser explotadas con el fin de denegar servicios.
- El equipo no debe agregar una latencia superior a los 100 microsegundos de forma de no afectar considerablemente el tiempo de respuesta de los servidores
- Sincronizar con la base de datos del fabricante para el bloqueo efectivo de orígenes maliciosos con mala reputación y geolocalización.
- Deberá permitir la configuración de listas de filtros de cabecera L2/L3/L4 en forma manual.
- Debe ser capaz de detectar fuentes que envíen cantidades excesivas de tráfico bajo umbrales configurables, para después colocar esas fuentes en listas de hosts bloqueados temporalmente (bloqueo basado en la tasa de tráfico).



- Debe ser capaz de suprimir paquetes HTTP específicos según los encabezados HTTP coincidentes con expresiones REGEX configurables.
- Deberá de identificar web crawlers, darle tratamiento diferencial y monitorear su uso.
- Debe soportar la importación de IOCs (Indicadores de compromiso) de fuentes externas en formato STIX and TAXII.
- Debe soportar hasta 2 Millones de IOC.

Así mismo, el operador debe prestar a la entidad un servicio de protección contra ataques de DDoS volumétricos que cumpla con las siguientes características:

a) Sistema de detección:

- La solución utilizada para prestar el servicio debe ser capaz de detectar ataques DDoS volumétricos en los routers de Peer del operador, que constituyen su punto de entrada a internet, de manera que las amenazas puedan identificarse de forma temprana y su impacto mitigado antes de que el tráfico malicioso afecte la red interna.
- Alineado con el requerimiento anterior, el operador debe ser capaz de detectar y mitigar de forma proactiva ataques volumétricos dirigidos a cualquier IP que atravesase estos enrutadores, incluso si no pertenece a la PNP, de manera que este última no resulte afectada como daño colateral de un ataque hacia terceros.
- El mecanismo de detección de ataques de la solución del operador debe basarse en telemetría de flujos (Netflow, Jflow, Netstream), de manera que el crecimiento del tráfico en su red no comprometa la precisión en la identificación de ataques volumétricos de DDoS hacia la infraestructura con la que presta el servicio a la entidad
- La solución debe estar implementada físicamente en la red del operador, de forma que la información de la entidad permanezca local dentro del país, garantizando un mayor control sobre la privacidad, la seguridad y la configuración de los datos.
- La solución debe operar en modalidad de desvío y reinyección, de manera que, en ausencia de un ataque DDoS volumétrico, el tráfico dirigido hacia la PNP fluya a través de su ruta habitual desde internet. En caso de detectar un ataque, el tráfico debe desviarse al centro de mitigación en la nube del operador, garantizando así una reducción de puntos de falla durante el período normal de operación y evitando la intercepción innecesaria del tráfico.
- Para garantizar que el mecanismo de desviación hacia el centro de limpieza no sea evadible, el operador debe emplear su protocolo de enrutamiento, BGP, como medio para realizar dicha desviación.
- La solución debe estar en capacidad de detectar los siguientes tipos de ataques:
 - Ataques de Amplificación. (Chargen, CLDAP, DNS, NTP, MEMCACHED, MS SQL RS, SNMP, SSDP, TCP SYN/ACK)
 - Inundaciones (ICMP, Fragmentos IP, Tráfico de direcciones IP Privadas, IPv4 protocol 0, L2TP, mDNS, RIPv1, NETBIOS, RCPBind).
 - Inundaciones con paquetes TCP (NULL, RST, SYN, SYN/ACK, combinación de banderas) y agotamiento de estado volumétrico.
 - Inundaciones de tráfico UDP



b) Centro de mitigación:

- Para la protección contra ataques volumétricos dirigidos hacia la entidad, el centro de mitigación de DDoS debe estar conectado a los routers de Peer del operador, de manera que el tráfico malicioso sea desviado en el punto más cercano posible a la entrada de internet de la red.
- El operador debe disponer de un centro de mitigación con 100 Gbps de capacidad efectiva, utilizada exclusivamente para la gestión de ataques DDoS volumétricos. Esta capacidad debe ser independiente de cualquier tráfico desviado de clientes en modalidad "always on" o siempre activa, asegurando que no se vea comprometida durante tiempos de paz por tráfico legítimo.
- La solución del operador que realice la mitigación de ataques de DDoS volumétricos no debe verse limitada por el número de sesiones simultáneas, ni para tráfico total, ni para tráfico legítimo.
- Para la mitigación de ataques, la solución debe integrar mecanismos de protección enriquecidos con fuentes de inteligencia del fabricante (feeds). Estas fuentes deben ser cuidadosamente curadas, por lo que se requiere que provengan del monitoreo de la actividad de ataques de DDoS en al menos el 40% del tráfico de internet.
- El centro de mitigación debe implementar por los menos las siguientes técnicas para responder a las amenazas de DDoS:
 - Filtrado de tráfico que utiliza paquetes inválidos por malformaciones en capas 3, 4 y 7.
 - Listas de filtros para permitir o denegar tráfico, dependiendo de los recursos protegidos, de forma se limite la superficie de exposición y se implementen BCPs.
 - Mecanismos anti-inundación que permiten identificar cada IP individual atacante y evitar floods de tráfico en capa 3 (Incluyendo fragmentación) y 4. Por ejemplo: Floods de tráfico UDP, ICMP e inundación con distintas combinaciones de banderas de tráfico TCP.
 - Mecanismos anti-inundación de peticiones en capa 7 para distintos protocolos. Por ejemplo: HTTP, SIP, DNS.
 - Mecanismos de Challenge Response tanto en capa de transporte (TCP) como en capa de aplicación (HTTP, DNS) para evitar la falsificación de direcciones IP en las solicitudes y que la red protegida se convierta en fuente de ataques de reflexión/amplificación.
 - Mecanismos anti-Ataques de agotamiento de estados, no solo a niveles básicos como inundaciones de paquetes TCP con una bandera en particular o con una combinación de banderas, sino a nivel avanzado como envejecimiento agresivo de conexiones o limitar conexiones establecidas por orígenes individuales.
 - Mecanismos contra ataques que explotan vulnerabilidades de protocolos de cifrado como TLS o SSL para denegar el servicio (Enviando cryptobasura o solicitando miles de renegociaciones simultáneas)
 - Protección contra Botnets y contra comportamientos maliciosos.
 - Feeds de inteligencia para mitigar distintos tipos de amenazas identificando bots, herramientas de ataque y open resolvers usados activamente como reflectores/amplificadores.



- Mecanismos de filtrado, que usan expresiones regulares, para aplicaciones como HTTP y DNS.
- Policing y dropeo de tráfico utilizando geolocalización.
- Algoritmos de filtrado de ataques de reflexión/amplificación: Chargen, CLDAP, L2TP, mDNS, memcached, MS SQL RS, Netbios, NTP, RIPv1, RCPBIND, SNMP, SSDP.

c) Integración con AntiDDoS On premise

La solución propuesta por el operador para protección contra ataques de denegación de servicios volumétricos debe integrarse de la siguiente forma:

- Debe aceptar solicitudes de mitigación desde los dispositivos on premise, generar una alerta en su consola de gestión y permitir la mitigación del ataque de forma manual o automática.
- El sistema del operador debe recibir de manera autónoma las listas de filtros globales implementadas en el componente on-premise y asociarlas de forma automática a la mitigación. Estas listas de filtros deben incluir, como mínimo, los siguientes elementos:
 - a) hosts en la lista de permitidos
 - b) hosts en la lista de denegados/prohibidos
 - c) URLs en la lista de denegados.
- El sistema debe adaptarse automáticamente a los cambios en las solicitudes de mitigación, por ejemplo: Si en una solicitud automática desde el componente on premise se actualizan los prefijos para los cuales se requiere desvío o, si se actualizan las listas de filtros.
- La solución del operador debe proporcionar retroalimentación a los componentes on-premise, de manera que el estado y el progreso de la mitigación en la nube se muestren en la interfaz gráfica de estos últimos.
- En caso de que los componentes on-premise soliciten detener la mitigación en la nube, el sistema debe ser capaz de hacerlo de forma automática

d) Acceso a la herramienta para generación de reportes:

El operador debe proporcionar a la entidad un perfil de acceso a su herramienta de protección contra ataques de denegación de servicio (AntiDDoS), de manera que la PNP pueda generar reportes directamente desde la plataforma. Este acceso debe incluir, como mínimo, la visualización de los siguientes reportes:

- Alertas de DDoS: Acceso a la visibilidad de las alertas asociadas a las mitigaciones relacionadas con la policía. Las alertas de DDoS deben poder mostrar distinta información de los patrones del tráfico, como son: Dirección IP de destino, Direcciones IP de origen (Si no es altamente distribuido), puertos de destino, puertos de origen (Si no son altamente distribuidos), ASNs de origen, ASNs de destino, banderas TCP, Tipos ICMP o protocolo, top de patrones de tráfico o Nombre del ataque, categoría de DDoS o categoría de amenaza, impacto, severidad.
- Mitigaciones de DDoS: Acceso a la visibilidad de cada mitigación individual relacionada con la policía. Cada mitigación debe mostrar, como mínimo, la siguiente información: políticas que están descartando tráfico, volumen de tráfico descartado por política, estado de las políticas (activas/inactivas), dirección IP de destino, y un resumen general de la



mitigación, incluyendo el promedio de tráfico total, tráfico permitido y tráfico bloqueado.

- Reportes donde se muestren, en una misma gráfica, las relaciones de tráfico de la entidad, filtrando por la combinación de los siguientes elementos: país de origen, sistema autónomo, direcciones IP (origen y destino), puertos (origen y destino) y recurso protegido.
- Reportes donde se muestren, en una misma gráfica, las relaciones de tráfico de la institución, filtrando por la combinación de los siguientes elementos: categoría de DDoS, país de origen, sistema autónomo de origen, interfaz de ingreso y salida del router, y recurso protegido.
- A petición de la institución, el operador debe permitir la configuración de un reporte personalizado que incluya hasta siete elementos, filtrando por la combinación de cualquiera de los siguientes elementos: países de origen y destino, puertos de origen y destino, protocolos, sistemas autónomos de origen y destino, Top Talkers, categoría de DDoS, router monitoreado del operador, interfaces de ingreso/salida del tráfico y direcciones IP de origen y/o destino.

El proveedor debe entregar credenciales de acceso con roles o perfiles de lectura/escritura al Scrubbing Center dedicado, sin restricción alguna, de manera que los administradores de la PNP puedan verificar las configuraciones del dispositivo, así como poder generar reportes y alertas. Credenciales que serán entregados al inicio del servicio.

5.2.1.5.4.1.18 ANÁLISIS DE VULNERABILIDAD Y ANÁLISIS DE CIBERSEGURIDAD

Análisis de Vulnerabilidad

Objetivo

El objetivo es contar con las herramientas necesarias para identificar las vulnerabilidades en los dispositivos finales o páginas de la entidad por intranet e internet, realizando las tareas adecuadas y pruebas técnicas necesarias para así encontrar las debilidades en la infraestructura y poder determinar recomendaciones para su solución. Asimismo, tiene como funcionalidad el descubrimiento de las vulnerabilidades existentes en la red de la entidad desde el punto de vista DEFENSIVO, con el objetivo de categorizar y priorizar los riesgos asociados a los activos de la entidad.

Requerimiento

- Se requiere una solución de gestión de vulnerabilidades y auditoría de configuraciones de infraestructura basada en cloud y/o on-premise, en modalidad software como servicio.
- Deberá realizar escaneos de vulnerabilidades y evaluación de configuraciones (políticas) en forma programada y automática. Los resultados de estos deberán estar consolidados en un único sistema de gestión.
- No deberá ser disruptivo ante ningún servicio informático que la institución brinde, es decir; no deberá bloquear ningún tráfico, no deberá agregar latencia ni deberá operar "en línea", bajo ninguna circunstancia, sobre ningún paquete de red.
- Deberá realizar escaneos de vulnerabilidades y evaluación de configuraciones (políticas) en forma programada y automática. Los

resultados de estos deberán estar consolidados en un único sistema de gestión.

- Deberá coleccionar datos mediante escáneres activos, escáneres pasivos (análisis de tráfico de red). No deberá haber límites en la cantidad de escáneres a desplegar en forma distribuida. Además, deberá contar con motores de escaneo públicos para escanear ambientes publicados a Internet.
- La recepción y análisis del tráfico de red deberá ser posible sin la necesidad de integración con ningún servicio o infraestructura de la institución, y sin la necesidad de instalar agentes de software en ningún dispositivo a monitorear.
- Deberá estar basado en un catálogo propio de vulnerabilidades que incluyan más de 160 mil evaluaciones diferentes y al menos 64 mil vulnerabilidades conocidas por un período no menor a 15 años.
- Deberá proveer un mecanismo de priorización de vulnerabilidades automático basado en la probabilidad de explotación y que ofrezca información alternativa al CVSS (Common Vulnerability Scoring System) basada en Inteligencia de amenazas reales recabada de diversas fuentes como Deep Web, Dark Web, redes sociales, sitios de divulgación y otros centros de investigación.
- Deberá ser capaz de evaluar, no solo vulnerabilidades, sino auditar configuraciones y compararlas contra las mejores prácticas y frameworks de seguridad tales como CIS, CERT, CISA STIG, PCI y otros para la totalidad de activos licenciados, incluidos equipos de red, infraestructura de virtualización, Windows, Linux, Bases de Datos, Aplicaciones y otros sistemas. Estas auditorías podrán ser personalizables por la organización. Esta funcionalidad es también conocida como Policy Compliance. Se requiere esta capacidad sin límites de licenciamiento.
- Deberá tener la capacidad de detectar y analizar, dentro del tráfico entregado por la institución:
 - Deberá reportar vulnerabilidades que sean explotables, establecer el nivel de madurez del código de exploit (si aplica), documentar de que forma se explota (malware, acceso remoto, con o sin credenciales), si el exploit está presente en frameworks reconocidos tales como Metasploit, Canvas, Core y otras.
 - Vulnerabilidades relacionadas con posibles ataques dirigidos con el objetivo de extraer, robar u obtener por medios digitales información.
- Deberá brindar todos los elementos de inteligencia de amenazas necesarios para poder determinar el origen, las acciones y el impacto de la misma con el objetivo de implementar recomendaciones en la infraestructura analizada para poder responder a la vulnerabilidad.
- Deberá brindar un servicio de supervisión y monitoreo de la superficie de ataque, para complementar el servicio de análisis de vulnerabilidades externo.
- La solución deberá tener la capacidad de identificar IP y nombre del sistema.
- La solución deberá ser capaz de identificar activos mediante escaneos de descubrimiento y escaneos pasivos. Además, deberá detectar el sistema operativo, los servicios que se ejecutan, el software instalado y datos que permitan identificarlo tales como IP, MAC Address, hostname/DNS Name. Deberá permitir aplicar etiquetas que designen criterios de clasificación



tales como criticidad, área o departamento, dueño, ubicación física, ambiente. Estas etiquetas deberán ser completamente personalizables y permitir crear reglas que las apliquen automáticamente. También deberá registrar el día y hora que se vio al activo por primera y última vez y la última vez que fue escaneado con credenciales.

- La solución deberá poder notificar de sus hallazgos mediante el envío de mensajes de logs en formatos Syslog y/o SNMP y/o correo electrónico.

Características de la consola de administración de la solución:

- La consola de administración de la solución deberá tener capacidad de ser accedida a través de una página web segura (https).
- La consola deberá contar con un dashboard o panel de información personalizable, que permita configurar la presentación de la información recopilada de acuerdo a las necesidades de la entidad.
- Deberá contener los siguientes indicadores:
 - Lista de dispositivos (hosts) más afectados en la última hora, últimas 24 horas, últimos 7 días y últimos 30 días.
- Tener la capacidad de mostrar las vulnerabilidades en la última hora, últimas 24 horas, últimos 7 días y últimos 30 días.
- Lista de dispositivos (hosts) vulnerables de sistema operativo o aplicación en la última hora, últimas 24 horas, últimos 7 días y últimos 30 días.
- Deberá mantener registro de estado de vulnerabilidades por activo, de modo de identificar vulnerabilidades que, habiendo sido remediadas, volvieron a surgir en nuevos escaneos. Deberán registrarse las fechas de primera aparición, última aparición y reaparición. Además, se deberá contar con una vista de vulnerabilidades remediadas.
- Integraciones vía API
- Una API pública debe poder ser usada por clientes para integrarse con SIEM y herramientas SOAR.
- Deberá ser capaz de integrarse a un Centro de Operaciones de Seguridad (SOC) mediante alertas automatizadas independientes y nativas en el producto como así también integrarse a una solución de SIEM y de Orquestación (SOAR). Indicar la capacidad de integración con Splunk, IBM QRadar, LogRhythm, Siemplify, Simlane y otros. Se espera que la solución alerte cuando se detecten nuevas vulnerabilidades críticas en sistemas relevantes, nuevas vulnerabilidades asociadas a una amenaza conocida y otras reglas personalizables.
- Debe dar sugerencias de remediación de vulnerabilidades y/o aplicar parches de remediación.
- Deberá contar con opciones para configurar la performance del escaneo tales como:
 - Máximo número de conexiones HTTP concurrentes
 - Máximo número de requerimientos HTTP por segundo
 - Detectar red congestionada y reducir la carga
 - Especificar el tiempo máximo de espera de las respuestas
 - Especificar el tiempo máximo de espera de un browser antes de abortar el escaneo
 - Especificar el número consecutivo de vencimientos de tiempo de espera (timeouts) antes de abortar el escaneo
- Deberá mostrar en los paneles de control, cuantas vulnerabilidades existen agrupadas por categoría de OWASP.



- Deberá contar con paneles de control que muestren estadísticas de vulnerabilidades por aplicación, por categoría de OWASP y por severidad.
- Deberá contar con un módulo que automatice el descubrimiento de problemas de seguridades comunes tales como Cross-Site Scripting, SQL Injection, Directory Traversal,
 - Configuraciones inseguras y otras vulnerabilidades y debilidades en aplicaciones Web.

5.2.1.5.4.1.19 HERRAMIENTA INFORMÁTICA PARA PREVENCIÓN DE PÉRDIDA DE INFORMACIÓN, AUDITORÍA Y ANTICORRUPCIÓN.

PLATAFORMA DE PREVENCIÓN DE FUGA DE INFORMACIÓN

Debe efectuarse una actualización a los Inventarios de Activos de TI que posee actualmente la Entidad.

1. Aspectos Generales de la Solución

- Cada solución de seguridad propuesta debe ser proporcionada por un solo fabricante para que tanto el soporte como la funcionalidad de la solución estén completamente integrados y administrados a través de una única consola de administración.
- Se deberá licencia para 1000 dispositivos.
- Los equipos deben ser nuevos, de primer uso y que no se encuentren en End of Support declarados por su fabricante.
- Debe ser capaz de proteger la información crítica integrando en una solución las capacidades de clasificación de datos, cifrado, monitoreo y bloqueo.
- Debe poder compartir políticas y visibilidad de la información entre estaciones y servidores administrados e información en tránsito a través de la red.
- Debe proteger los canales principales de fugas, como dispositivos de almacenamiento extraíbles, mensajes de correo electrónico, mensajería instantánea, publicación web, impresión, portapapeles, capturas de pantalla, compartidores de archivos, comunicación de red y acceso por aplicaciones no autorizadas.
- Debe permitir a los usuarios iniciar análisis y correcciones al encontrar archivos clasificados.
- Tener una clasificación flexible que incluya diccionarios, expresiones regulares, documentos registrados, tipo MIME, propiedades de documentos creadas por el conjunto de aplicaciones de Office.
- Capacidad para etiquetar documentos según el origen, evitando que la información de las aplicaciones web, las aplicaciones de red y los recursos compartidos de red se copien y filtren.
- Debe tener capacidad de protección de escritorio físico y virtual (VDI).
- Debe permitir la visibilidad a través de informes y / o cuadros de mando que permitan a los auditores y a la alta dirección que se están aplicando medidas de normas de cumplimiento.
- Habilitar la educación del usuario a través de alertas, basadas en políticas impuestas.
- Permitir la personalización de los mensajes de notificación al usuario para cada regla aplicada para incluir como mínimo:



- Logotipo de la empresa
 - Texto personalizado
- Permitir la aplicación de estándares de cumplimiento que aborden las acciones cotidianas de los usuarios, como enviar correos electrónicos, publicar en la web, copiar archivos en dispositivos extraíbles.
- Debe utilizar técnicas de toma de huellas dactilares para clasificar y marcar datos sensibles y no estructurados.
- Debe tener al menos los siguientes módulos de protección:
 - Protección contra fugas de datos y agente de control de dispositivos para la familia Windows y macOS.
 - Equipo con sistema operativo propio de la solución capaz de integrarse con soluciones de filtro de contenido web a través del protocolo ICAP y SMTP.
 - Equipo con sistema operativo propio de la solución capaz de recibir tráfico duplicado de switches de red o a través de TAP.
- Debe tener integración con herramientas de administración de derechos, como: Microsoft Windows Rights Management Services y Seclore FileSecure.
- La consola debe forzar la actualización de las directivas, sin necesidad de actuar sobre el agente dlp instalado;
- La eliminación del agente DLP en los endpoints instalados debe realizarse a través de la consola de administración, sin necesidad de realizar ninguna acción manual en los dispositivos afectados;
- La actualización de los agentes debe ocurrir automáticamente, sin necesidad de instalación adicional;
- El agente de prevención de fugas debe ser compatible con las siguientes plataformas Windows:
 - Windows 11
 - Windows 10
 - Windows Server 2016
 - Windows Server 2019
 - Windows Server 2022
- El agente de prevención de fugas debe ser compatible con las siguientes plataformas macOS

2. Aspectos de protección contra fugas de datos

- La solución debe ser capaz de detectar e identificar los datos a los que accede el usuario, en tránsito fuera o dentro de la red y almacenarse localmente o en un recurso compartido de red
- A través de agentes instalados la solución debe permitir el control de los datos en uso, tales como acciones del usuario relacionadas con copiar información, imprimir archivos clasificados y captura de pantalla basada en datos sensibles, permitiendo la realización de la captura de pantalla de la aplicación si no contiene información clasificada;
- El agente debe emplear reglas para proteger los datos clasificados de fugas en los siguientes vectores:
 - Copiar software (Portapapeles)
 - Correo electrónico
 - Uso compartido de red
 - Impresión
 - Aplicaciones y navegadores específicos

- Publicaciones Web

- Debe poder restringir las reglas de protección de datos a grupos de usuarios de Active Directory;
- Debe poder restringir las reglas de protección de datos en función del sistema operativo en ejecución
- La solución debe poder replicar contenido confidencial que haya infringido una regla de protección de datos en su totalidad con al menos la siguiente información:
 - Documento completo, accesible a través de la consola de administración
 - Lista de términos que se encuentran en el documento
 - Mensaje de correo electrónico en formato completo, cuando corresponda
 - Captura de pantalla de contenido sensible, cuando corresponda
- Debe permitir la ejecución de acciones diferenciadas si el usuario está fuera de la red local
- La solución debe emplear técnicas de reconocimiento de patrones de texto predefinidos y diccionarios.
- La política de la solución debe permitir abarcar el alcance de la clasificación, el seguimiento, el monitoreo y la protección;
- Debe permitirle configurar en la solución las clasificaciones deseadas, siendo aceptadas al menos: Confidencial, Restringida, Pública.
- Para cada clasificación, debe permitirse definir la información que debe protegerse. Los métodos de definición incluirán:
 - Estándares avanzados (ejemplo: Regex)
 - Diccionarios
 - Archivos TrueType
 - Origen o destino
 - Grupos de aplicaciones
- Debe permitir que se agreguen grupos de aplicaciones a la solución como criterio de clasificación de datos
- Debe contener de forma predeterminada al menos 150 objetos predefinidos entre diccionarios y definiciones de texto
- Debe permitir la integración con herramientas de clasificación de información de terceros, como Titus, entre otros.
- Debe tener un método avanzado para identificar y rastrear el contenido mediante la creación de firmas (huella digital) de contenido, lo que permite usar las firmas para rastrear no solo el contenido total del archivo, sino también partes de él.
 - Dichas firmas deben almacenarse en los atributos extendidos del archivo o en flujos de datos alternativos, lo que permite a la solución mantener la persistencia de la clasificación de datos
- Debe tener la capacidad de realizar análisis (escaneo) de todos los archivos almacenados en un repositorio determinado (ejemplo: Fileserver) y crear firmas automáticamente para proteger el contenido clasificado.
 - Debe poder cargar manualmente los archivos para que la solución cree las firmas automáticas.
- Debe permitir la clasificación manual de archivos, agregando marcado y permitiendo su seguimiento;
- Debe tener la capacidad de crear reglas para la identificación de contenido sensible y la toma de una determinada acción;



- Debe permitir la creación de reglas que permitan el control de la distribución no autorizada de datos clasificados;
- Debe contener mecanismos de protección que impidan la desinstalación del agente localmente
- Debe permitir a los usuarios solicitar excepciones temporales a las reglas de protección con el tiempo establecido por los administradores de soluciones
- Debe permitir que el agente se ejecute en modo seguro en el sistema operativo Windows
- Debe permitir el control del uso máximo de RAM localmente
- Debe permitir que los módulos específicos de la solución se deshabiliten si no se utilizan en las reglas de protección

3. Funciones de control de dispositivos

- La solución debe permitir el bloqueo total del dispositivo o solo el monitoreo
- Debe permitir el control de los siguientes dispositivos:
 - Dispositivos de almacenamiento extraíbles
 - Dispositivos Bluetooth
 - Reproductores MP3
 - Dispositivos Plug and Play
- Debe controlar qué datos se pueden copiar en medios extraíbles
- Debe permitir bloquear la ejecución de aplicaciones desde dispositivos extraíbles, y puede crear excepciones al bloqueo.
- Debe permitir la agrupación de dispositivos a través de propiedades comunes, como: VendorID, ProductID, Device Class.
- Debe poder identificar el dispositivo (plug and play) a través de la siguiente información:
 - Tipo de BUS;
 - Clase de Dispositivo (Device Class)
 - ID de fabricante (Vendor ID)
 - ID del producto
- Debe ser posible habilitar o deshabilitar una determinada regla de protección una vez que esté dentro de la red (Ejemplo: Cuando está conectado a la red de la organización libera el uso de pen-drive);
- Debe tener las siguientes clases de dispositivos de forma nativa:
 - Batería
 - Biometría
 - Bluetooth
 - unidades de CD/DVD
 - Decodificadores
 - Adaptadores de vídeo
 - Disco Fijo
 - Controladoras de Disquete
 - Disqueteras
 - GPS
 - Infrarrojo
 - IEEE 1394
 - Ratón
 - Módem
 - Fax



- Adaptadores de red
 - PCMCIA
- Debe tener las siguientes plantillas:
 - Dispositivos Apple
 - Dispositivos BlueTooth
 - Unidades CD/DVD
 - Dispositivos de almacenamiento extraíbles
 - Lector de tarjetas SD
 - Dispositivos Windows Portable
 - Dispositivos USB Plug-n-Play
- Debería ser posible crear plantillas personalizadas.
- Al identificar un nuevo dispositivo conectado en el equipo cliente cuyo hardware es desconocido, la solución debe emitir una alerta en la consola centralizada que indique una nueva clase de dispositivo encontrado;
- Debe permitirle vincular un Usuario o Todos los Usuarios a un dispositivo específico a través de su GUID;
- Debe permitir, en la consola centralizada, la creación de los siguientes controles:
 - Regla para el control del disco duro fijo
 - Regla para dispositivos Plug-n-Play
 - Regla para dispositivos de almacenamiento extraíbles
 - Regla de acceso a archivos para dispositivos de almacenamiento extraíbles
 - Regla de dispositivo TrueCrypt
- Para cada norma, debe ser posible aplicar a:
 - Cualquier usuario
 - Pertener a un determinado grupo
 - Pertener a todos los grupos
 - Usuario local o usuario no LDAP
- Durante la definición de la regla, debe permitir la elección de la identificación del objeto LDAP, como mínimo:
 - Nombre del objeto
 - Dominio\Nombre de objeto
- Para cada regla, debe poder configurar exclusiones durante al menos:
 - Usuarios
 - Dispositivos
- Para cada regla debe ser posible configurar la gravedad entre al menos:
 - Información
 - Advertencia
 - Menor o medio
 - Destacado o alto
 - Crítico
- Para cada regla, la solución debe permitir la configuración de distintas reacciones entre:
 - Ordenador conectado y desconectado a la red corporativa
 - Ordenador desconectado de la red corporativa
- Debe tener la capacidad de controlar (bloquear) el acceso a ciertas extensiones o archivos TrueType a dispositivos de almacenamiento extraíbles.
- Cuando corresponda, debería permitirle aplicar la regla de control tanto a entornos de la familia Windows como a la familia macOS/OS X;



- La solución debe permitirle deshabilitar una regla de entre el conjunto de reglas.

4. Aspectos de la clasificación de datos

- Debe tener clasificaciones definidas por defecto incluyendo, como mínimo:
 - HIPAA
 - PCI
 - NO
 - SOX
 - PII de EE. UU.
- Debe tener la capacidad de identificar información confidencial basada en estándares avanzados (expresión regular), incluyendo al menos por defecto:
 - ABA RTN
 - Número Nacional Completo Australiano (FNN)
 - Número de teléfono fijo australiano
 - Número de tarjeta australiana de Medicare
 - Número de teléfono móvil australiano
 - Número de archivo de impuestos australiano
 - Números de cuentas bancarias austriacas
 - Número de seguro social austriaco
 - Número de identificación a efectos del IVA (UID) de Austria
 - Número de documento de identidad belga
 - Número de registro nacional belga (BIS)
 - Número BIS belga no nacional
 - Brasil CNPJ (Registro Nacional de Personas Jurídicas)
 - Brasil CPF (Registro Tributario)
 - Número de seguro social canadiense
 - Número de identificación nacional de China
 - Número de tarjeta de crédito (American Express)
 - Número de tarjeta de crédito (China UnionPay)
 - Número de tarjeta de crédito (Diner's Club)
 - Número de tarjeta de crédito (Discover)
 - Número de tarjeta de crédito (JCB)
 - Número de tarjeta de crédito (Mastercard)
 - Número de tarjeta de crédito (simple, delimitado por guiones)
 - Número de tarjeta de crédito (Visa)
 - Número de identificación personal croata (OIB)
 - Número de ciudadano maestro único croata (JMBG)
 - Número de serie electrónico (ESN, 8 dígitos hexadecimales)
 - Dirección de correo electrónico
 - Código de identidad personal finlandés
 - Código INSEE francés
 - Número de identificación alemán
 - Número de seguridad social alemán
 - Identificador/Código fiscal alemán
 - Número de identificación griego
 - Número de seguridad social griego (AMKA)
 - Número de identificación fiscal griego (AFM)
 - Código HMRC
 - Número de documento de identidad de Hong Kong
 - Número de identificación personal húngaro



- Número de seguridad social húngaro (TAJ)
- Dirección IP (notación decimal)
- Número irlandés de servicio público personal (PPS/PRSI)
- Número de identificación israelí
- Número de identificación fiscal/SSN italiano (Código Tributario)
- Japonés Mi número corporativo
- Código personal japonés My Number
- Número de registro de residente coreano
- Dirección MAC
- Estándar bancario de México (CLABE)
- Clave de producto de Microsoft Windows
- Múltiples tarjetas PCI comunes
- Identificador Nacional de Proveedores (HIPAA)
- Número de índice de los ministerios de salud de Nueva Zelanda
- CUSIP Norteamericano
- Debe poseer la capacidad de identificar información confidencial a través de diccionarios, incluyendo, como mínimo:
 - Documento farmacéutico
 - Lista de precios
 - Ganancias Pro
 - Profanidad
 - Pérdida de beneficios
 - Horario del programa
 - Reanudar
 - Pronóstico de ventas
 - Sarbanes-Oxley Sensible
 - Términos de presentación de la SEC
 - Agencias de Seguridad
 - Enfermedad sensible
 - Lenguaje sexual
 - Etiquetas del Seguro Social
 - Código fuente CPP
 - Código fuente Java
 - Código fuente Python
 - SPAM
 - Deportivo
 - SSN Bajo
 - Abuso
 - Informe de actividad sospechosa
 - Nombre de usuario
 - Violencia
 - Armas
 - Transferencia bancaria
 - Los 1000 apellidos más comunes de EE. UU.
 - Adquisición
 - Alta de admisión
 - Banco ABA
 - Banco ACNT
 - Banco STMT
 - Entrada de blog
 - Reunión de la Junta Directiva
 - Registro de llamadas del operador celular
 - Clasificado





- Códigos de medicamentos clasificados
- Enfermedad común
- Compensación y beneficios
- Informe de cumplimiento
- Confidencial
- Informe de crédito
- Fecha de nacimiento
- Descontento
- Licencia de conducir
- Número de identificación del empleador
- Origen étnico
- Búsquedas de empleo para ejecutivos
- Reglamento de Administración de Exportaciones (EAR)
- Auditorías Financieras
- Informe financiero
- Informe financiero - Español
- Juego
- Gnutella
- Grados
- Odio al racismo
- HIPAA - Enfermedades
- HIPAA HCPCS
- HIPAA CIE10
- HIPAA CIE9
- Clases de NDC de HIPAA
- Dosis de HIPAA NDC
- Listado de NDC de HIPAA
- Rutas NDC de HIPAA
- IExplorer
- Drogas ilegales
- Instrucciones
- Reglamento sobre el tráfico internacional de armas (ITAR)
- Apellido
- Legal
- Diagnóstico médico
- Números de registros médicos
- MEMORÁNDUM
- Mozilla (en inglés)
- Seguridad de red
- Contraseña
- PCI GLBA
- Permitirá definir la clasificación sobre la base del origen o el destino, que admita al menos:
 - Aplicación
 - Grupo de usuarios
 - Uso compartido de red
 - URL
- Debe tener plantillas definidas por el fabricante, incluyendo al menos:
 - 3ds Max
 - Lector Adobe Acrobat
 - Compiladores de Dev Studio y Microsoft
 - Aplicaciones cliente de correo electrónico
 - Aplicaciones de cifrado

- Explorador
- Aplicaciones de mensajería instantánea
- Instaladores
- Cumplidor de Java
- Notas de Lotus
- Aplicaciones de grabadora de medios
- Compiladores de Microsoft
- Aplicaciones de Microsoft Office
- Aplicaciones P2P
- Rdpclip
- Navegador Safari
- Escáneres e indexadores
- Navegadores web compatibles
- Navegadores Web
- WinAce Archiver
- Archivos del sistema operativo Windows
- WinRar Archiver
- Aplicaciones Zip
- Además de las plantillas ya incluidas en la solución, el administrador puede crear libremente estándares y diccionarios avanzados para la identificación de información confidencial en puntos finales;
- Debe permitir la inclusión de documentos que no deben ser detectados por la solución (Lista blanca)
- Permitirá el registro de documentos sensibles, incluidos, como mínimo:
 - Inclusión manual
 - Inclusión automática

5. DLP DISCOVERY

- Debe ser capaz de realizar búsquedas de información clasificada (por ejemplo, restringida, confidencial, secreta) almacenada localmente.
- Debe identificar la ubicación donde se almacenan los datos confidenciales e identificar al propietario del contenido
- Debe permitir la visualización de todos los datos indicados en el escaneo mediante una consola intuitiva;
- El porcentaje máximo de consumo de memoria y CPU debe establecerse a través de la consola;
- La tarea de búsqueda debe detenerse si la máquina está en uso;
- La tarea de búsqueda debe tener la opción de ser iniciada por el propio usuario a través del agente DLP;
- Debe soportar la clasificación de más de 300 tipos de contenido, tales como:
 - Documentos Microsoft Office
 - Adobe de archivos
 - Archivos multimedia
 - Código fuente
 - Archivos de proyecto
 - Archivos comprimidos
- Debe permitir la programación de tareas periódicas para escanear repositorios;





- Debe admitir la detección de información confidencial en las siguientes ubicaciones:
 - Archivo:
 - Caja
 - CIFS
 - Bases
 - Microsoft SQL
 - MySQL
 - Oráculo
- Debe permitir al administrador configurar al menos cuatro análisis independientes, incluidos:
 - Inventario;
 - Clasificación;
 - Remediación
 - Registro
- El análisis de inventario debe permitir al administrador una visión general de los tipos de archivo que existen en cada repositorio ejecutando solamente:
 - Solo recopilación de metadatos
 - Clasifica los metadatos analizados en diferentes tipos de contenido y analiza atributos, como el tamaño del archivo, la ubicación de almacenamiento y la extensión.
- El análisis de clasificación debe permitir al administrador comprender qué tipos de datos existen en los repositorios.
 - Debe comparar el contenido analizado con clasificaciones establecidas, como estándares de texto o diccionarios.
 - Debe detectar contenido cifrado, incluidos:
 - Cifrado de Microsoft Rights Management;
 - Seclore Rights Management Encryption
 - Protección con contraseña;
 - Sin cifrar.
- El análisis de corrección debe permitir al administrador encontrar datos que infrinjan una determinada directiva de confidencialidad de datos establecida.
 - Debe permitir este análisis en el repositorio de archivos y bases de datos compatibles;
 - Debe permitirle aplicar directivas de, por ejemplo, Rights Management, copiar o mover el archivo;
 - Para el análisis de bases de datos, la solución debe admitir mínimamente la supervisión, el registro de incidentes y el almacenamiento de pruebas
- El análisis del registro debe permitir al administrador extraer contenido de los archivos y crear automáticamente firmas para identificar la fuga de información insertada en los archivos.
- Debe tener la capacidad de realizar el descubrimiento en agentes distribuidos en estaciones de trabajo, lo que permite el descubrimiento de contenido en:
 - Sistema de archivos local en estaciones con sistema operativo Windows
 - Correo electrónico local (PST e OST)
 - Servidor de archivos

- Al encontrar un archivo confidencial en estaciones del sistema operativo Windows, debería poder hacer al menos lo siguiente:
 - Monitorización
 - Cifrado a través de la integración de la solución de cifrado del mismo fabricante
 - Aplicación de la directiva de gestión de derechos (RM)
 - Enviar al área de cuarentena
- La herramienta de punto final debe permitir al usuario realizar, a través de un comando local, el análisis de la estación de trabajo para el descubrimiento de archivos clasificados
 - Debe permitir al usuario la opción de corrección local (autocorrección);
- La solución de punto final debe permitir que cuando detecte un archivo confidencial, la solución lo clasifique automáticamente;
- La base de datos de soluciones debe admitir al menos 250 millones de firmas (huellas digitales);
- Debe permitir establecer el ancho de banda al realizar un análisis.

6. Consola central - Monitoreo

- Debe tener un módulo capaz de monitorear la red para conocer la cantidad y los tipos de datos transferidos por la red;
- Para este módulo no requiere bloqueo de flujos de red, solo visibilidad;
- Debe recopilar los datos en la red de forma pasiva, sin introducir latencia en la red, a través de la redirección de flujo de red (SPAN);
- Si la solución no admite la redirección a través de SPAN, se debe proporcionar una red TAP para redirigir el flujo de red para su análisis.
- Debe supervisar mínimamente los siguientes protocolos:
 - SMTP
 - IMAP
 - POP3
 - HTTP
 - LDAP
 - TELNET
 - FTP
 - IRC
 - SMB
- Debe permitir la inspección del protocolo SMTP utilizando las mismas reglas creadas para el módulo de prevención;
- Debe permitir la inspección del tráfico HTTP y FTP utilizando las mismas reglas creadas para el módulo de prevención;
- Debe permitir la inspección de los protocolos de red utilizando reglas específicas, utilizando información específica de los protocolos monitoreados;
- Debe permitir clasificar más de 300 tipos de contenido, incluyendo:
 - Documentos Office
 - Archivos multimedia
 - P2P
 - Código fuente
- Debe permitir la identificación del tipo real del archivo que viaja en la red, independientemente de la extensión informada o la compresión aplicada



- Los mecanismos de clasificación de objetos tendrán las siguientes características mínimas:
 - Clasificación multicapa: cubre el contenido contextual y la información en formato jerárquico.
 - Registro de documentos: incluye firmas de información a través de carga manual;
 - Clasificación de archivos: identifica los tipos de contenido independientemente de la extensión o compresión aplicada al archivo.

7. Políticas de Protección de Datos

- Debe tener reglas predefinidas por el fabricante para la protección de datos;
- El panel de creación de reglas debe tener los siguientes campos como una forma de facilitar la visualización de la regla:
 - Estado de la regla
 - Regla
 - Descripción
 - Severidad
 - Incidentes detectados;
 - Dado a ser protegido
 - Aplicable
- Debe permitirle crear una regla de protección de datos mediante las siguientes reglas:
 - Protección de acceso a aplicaciones
 - Protección del portapapeles
 - Protección de correo electrónico
 - Protección de uso compartido de red
 - Protección de impresión
 - Protección de almacenamiento extraíble
 - Protección de captura de pantalla
 - Protección web
- Para cada definición de regla, debe permitir los siguientes campos:
 - Clasificación de los datos que deben protegerse
 - Usuario o grupo que aplica
 - Excepciones de usuario o clasificación
 - Reacción a los datos sensibles identificados
 - Severidad
- Debe poder aplicar directivas distintas para los agentes conectados a la red interna y los agentes conectados a una red externa o a través de VPN.
- Si el administrador no desea almacenar la evidencia, la solución debe permitir dicha configuración.
- Debería permitirle ordenar el contenido por:
 - Origen
 - Destino
- Debe permitir la protección de archivos para al menos los siguientes destinos:
 - Correo electrónico
 - Impresión
 - Almacenamiento extraíble
 - Protección Web



- Debe proteger al menos los siguientes campos de correo electrónico:
 - Encabezado
 - Cuerpo
 - Anexos

8. Características de la consola DLP

- Debe proteger al menos los siguientes campos de correo electrónico:
- La gestión de la herramienta debe entregarse en formato "on-premise", manteniendo la operatividad.
- Debe permitir el envío de pruebas a la consola del producto como una forma de mejorar la investigación del incidente.
- Debe permitir, a través de la consola, identificar con precisión, de manera fácil, el contenido sensible que causó la generación del evento.
 - Debe almacenar el texto generador en un archivo cifrado
- La solución debe permitir la creación de distintos roles por usuario (RBAC), con al menos tres (3) permisos:
 - Lectura
 - Personalizado
 - Acceso total
- Debe permitir la configuración de distintos perfiles para acceder a diferentes secciones de la consola.
- La consola debe tener:
 - Tareas del cliente: Tareas para la automatización de las rutinas de gestión y mantenimiento;
 - Dashboards: Monitorea el entorno;
 - Directivas: configuración de la solución.
 - Perfiles de permisos: establecer los permisos de los usuarios de la solución;
 - Informes: Gestión de informes;
 - Protección de datos: Gestión de la solución contra la fuga de datos;
 - Help Desk: Soporte para desinstalar la aplicación, eliminar archivos de la cuarentena, omisión de seguridad temporal
- Debe tener una consola de incidentes para ver mejor todos los eventos detectados;
- Debe tener filtros capaces de identificar rápidamente el siguiente uso:
 - Datos en movimiento
 - Dado en reposo (Red)
 - Dado en reposo (Endpoint)
- Debe permitir el uso de filtros, entre ellos:
 - Regla
 - Tipo de incidente
 - Usuario
 - Destino
 - Calificaciones
- Debe presentar fácilmente:
 - Las reglas con más ocurrencias (Top 10)
 - Los incidentes con más ocurrencias (Top 10)
 - Usuarios con el mayor número de infracciones (Top 10)
 - Número de incidentes por semana
 - Rankings (Top 10)



- Debe tener la capacidad de presentar el historial de un incidente en particular, que contenga:
 - ID del incidente;
 - Producto que generó el evento;
 - Hora del evento (UTC)
 - Severidad
 - Tipo de Incidente
 - Nombre de usuario;
 - Inicio de sesión
 - Nombre del equipo;
 - Compartir;
 - Menstruación;
 - Clasificación
 - Destino
- Debe permitir ver la lista completa de incidentes relacionados;
- Debe permitir el enmascaramiento de los datos que se presentan en la consola, dependiendo del usuario, ya que ciertos usuarios no pueden ver la información de los incidentes de forma clara;
- Para el manejo de incidentes, la solución debe permitir escalar para la creación de casos.
- Para la gestión de la solución, debe permitir la visualización a través de cuadros de mando, con al menos los siguientes monitores:
 - Resumen de la política
 - Resumen de las operaciones
 - Resumen de incidentes
- Debe permitir el enmascaramiento de datos confidenciales en la base de datos de la solución.
- Debe permitir la instalación de Discovery Servers a través de la consola centralizada
- La consola centralizada debe tener una sección que permita la creación de claves de excepción para:
 - Client Bypass: Permitir la no aplicación de reglas durante un tiempo determinado, y el operador, introducir la justificación adecuada para la liberación, durante un tiempo determinado (ejemplo: 30 minutos)
 - Liberación de archivos enviados al área de cuarentena
 - Clave de desinstalación del agente



5.2.1.5.4.1.20 SOLUCIÓN DE ANTIVIRUS PARA SERVIDORES Y ENDPOINT DEL DATACENTER

1. Protección para equipos finales.

Se requiere contar con una solución de Protección Avanzada para puestos de Servicio Endpoint. Todos los componentes que forman parte de la solución deben ser parte de un fabricante único. Se requerirán 500 licencias por 36 meses.

Proveer detección y respuesta de amenazas automatizadas contra una variedad de amenazas de malware avanzadas, incluidos ataques sin archivos (fileless), cryptomining y ransomware.

Proporcionar parches virtuales (es decir, capacidad para bloquear los intentos de explotación de vulnerabilidades de sistemas operativos no parchados),

control de aplicaciones, control de acceso a dispositivos, antimalware en un solo agente.

Permitir que los programas de terceros se integren con la solución a través de una interfaz de programación de aplicaciones (API)

Admitir la instalación del agente en sistemas operativos Windows, Linux y MAC OS, así como el entorno de escritorio virtual

Permitir una fácil implementación del agente utilizando varios procedimientos compatibles (por ejemplo, Active Directory GPO, Microsoft System Center, Software de Deployment de tercero, Script MSI, entre otros)

Proveer la consola de administración centralizada sea bajo un esquema SaaS para una administración más eficiente de todos los componentes de protección en el panorama de amenazas en constante cambio.

Deberá haber logrado una efectividad de protección de ataques de 100%, según la evaluación del 2023 de MITRE ATT&CK

Deberá haber logrado una efectividad de Detección de Técnicas de Ataque de al menos 98% y 100% de Prevención, según la evaluación del 2023 de MITRE ATT&CK

Deberá estar ubicado como Líder en el Cuadrante Mágico de Gartner para soluciones EPP (Endpoint Protection Platform) del año 2024.

Deberá estar ubicado como Líder en la evaluación Forrester Wave para soluciones XDR (Extended Detection and Response) del año 2024.

Deberá estar ubicado como Líder en el reporte de Gigaom Radar para soluciones XDR (Extended Detection and Response) del año 2023.



1.1 Protección antimalware.

- Debe estar integrada a una consola maestra para poder centralizar la administración y gestión de bitácoras.
- Deberá contar con funcionalidades de antimalware de siguiente generación, entendiéndose antimalware de siguiente generación como plataformas que utilizan algoritmos de aprendizaje de máquina (machine learning) para detectar y bloquear el malware; no deberá tener ningún componente que requiera actualizar una base de datos de firmas de antivirus.
- El algoritmo de machine learning deberá operar de manera local en el endpoint sin depender de una conexión permanente a la consola.
- Deberá ser capaz de detectar y bloquear cambios sospechosos en la imagen UEFI, que intenten comprometer el proceso de arranque del host, antes de que se cargue el sistema operativo.
- Debe prevenir el robo de contraseña a partir de la lectura de la memoria RAM (mimikatz)
- Contar con un módulo de prevención contra ransomware que podrá ser configurado en modo normal y riguroso.
- Capacidad de prevenir ataques de Cryptomining a partir del comportamiento del objeto ejecutado.
- Deberá ofrecer protección contra scripts de tipo webshell.
- Deberá ser capaz de prevenir ataques basados en el Bypass del UAC (User Account Control) que intenten escalar privilegios.
- Deberá ser capaz de analizar datos de paquetes de red para detectar comportamientos maliciosos

- Capacidad habilitada para eliminar (restablecer) los cambios de malware en el registro del sistema operativo, eliminar los archivos caídos y finalizar la ejecución de procesos maliciosos.
- Capacidad habilitada para detectar y eliminar malware, incluso aquel que ya se encuentre en el endpoint.
- Capacidad habilitada para restaurar archivos modificados automáticamente por ransomware.
- Tener integrado nativamente un componente de sandboxing para el endpoint. El agente deberá ser capaz de enviar automáticamente el archivo a un entorno de sandbox para ser emulado. Esta capacidad deberá estar disponible para sistemas Windows, MacOS, Linux.
- El sandbox podrá ser del mismo fabricante que el agente de seguridad o un fabricante tercero integrado.
- El sandbox deberá estar basado en nube y debe tener una disponibilidad del servicio de al menos 99.9% contabilizados mensualmente.
- El sandbox deberá soportar el análisis de al menos 300 mil archivos por día. El sandbox deberá tener capacidad de analizar archivos de hasta 100 MB de peso o superior.

1.2 Ataques de día cero.

- Contar con tecnología de aprendizaje automático (machine learning) para la detección de amenazas de día cero.
- Proveer funciones de machine learning para un análisis estático y en ejecución de una amenaza (pre y run-time machine learning).
- Capacidad de monitorear el comportamiento de los endpoints en busca de modificaciones inusuales en el sistema operativo como procesos, registros, explorador, etc.

1.3 Protección contra Vulnerabilidades.

- Capacidad habilitada para proteger a los endpoints de las vulnerabilidades explotables dirigidas al su sistema operativo final sin necesidad de modificar su integridad.
- Capacidad habilitada para reducir o mitigar la exposición al riesgo debido a parches faltantes.
- Bloquear ataques contra vulnerabilidades conocidas o asociadas a un CVE.
- Debe identificar y bloquear técnicas de explotación sin necesidad de utilizar firmas y/o heurísticas. La solución no deberá tener ningún componente que requiera actualizar una base de datos de firmas.
- El bloqueo de exploits deberá ser posible incluso en procesos desarrollados inhouse, la solución deberá permitir especificar los nombres de los procesos que serán protegidos contra exploits.
- Bloquear técnicas de explotación de vulnerabilidades, como mínimo Return Oriented Programming (ROP), Heap Spray, Jit Spray, Shell link, Structured Exception Handler, CPL Execution Process.
- Identificación y prevención de intentos de escalación de privilegios a nivel de Kernel.

- Capacidad de crear un snapshot (dump) de la memoria RAM al momento de prevenir la ejecución de una técnica de explotación, con la finalidad de proporcionar información forense sobre el evento.
- Prevención de técnicas de explotación que utilizan Java Deserialization, Kernel Integrity Monitor (KIM), Local Threat Evaluation Engine (LTEE), Reverse Shell Protection, Shellcode Protection, SO Hijacking Protection, Webshell.

1.4 Control de dispositivos.

- La configuración para el control de acceso del dispositivo debe realizarse desde una consola central de administración.
- Mostrar un mensaje de notificación en el endpoint cuando ocurra una violación.
- La solución debe de registrar en una base de datos la violación de un endpoint.
- Dispositivos de almacenamiento USB
- Recursos compartidos de red.
- Debe permitir controlar también los dispositivos con conexión Bluetooth.
- Debe de permitir generar perfiles de excepciones para poder conectar dispositivos en puertos USB utilizando los siguientes parámetros: tipo de dispositivo, tipo de permiso a asignar (lectura/escritura o sólo lectura), fabricante (debe de contener una lista predeterminada), producto (debe de contener una lista predeterminada) y número de serie.
- Las políticas generadas deben de poder asignarse a un endpoint en particular, a un grupo de endpoints.
- Debe de permitir la creación de excepciones temporales a partir de una alerta registrada, para permitir el dispositivo solo durante un tiempo configurable.
- Capacidad de añadir nuevos tipos de dispositivos agregando el GUID de Windows correspondiente.

1.5 Firewall a nivel de host.

- Capacidad habilitada para crear políticas de firewall administradas centralmente.
- Capacidad habilitada para definir diferentes políticas de firewall para clientes en línea.
- Capacidad habilitada para generar registros de firewall cuando ocurre una violación.

1.6 Control de aplicaciones.

- Capacidad habilitada para bloquear la ejecución de software mediante políticas de seguridad.
- Capacidad habilitada para proporcionar la funcionalidad de control de la aplicación sin necesidad de un agente adicional o integración de terceros.
- Capacidad habilitada para bloquear manualmente (por el administrador) las aplicaciones sospechosas.

- Capacidad habilitada para bloquear aplicaciones con al menos en base a los siguientes criterios: Hash, Firma Digital, Ruta, Nombre del Archivo.

1.7 Administración y Gestión

- La solución debería poder proporcionar una vista central de las detecciones de amenazas registradas en los endpoints.
- La solución debe proporcionar control de acceso basado en roles para fines de administración, investigación y operación.
- La solución debe proporcionar la función de registro de auditoría para una vista histórica de las actividades del usuario
- La solución debería poder generar informes descargables a partir de plantillas existentes y personalizables
- La solución deberá poder permitir un inicio de sesión único desde la plataforma avanzada de detección y respuesta extendida.
- La solución permite a los administradores llevar una gestión centralizada de las políticas de seguridad.
- La solución debería poder administrar e implementar centralmente actualizaciones de productos del agente, incluidos parches, revisiones y actualizaciones de firmware para todos los productos administrados.
- La solución deberá contar con la opción de poder monitorear los comandos ejecutados por la consola de gestión centralizada a través del entorno web.
- Capaz de admitir la autenticación multifactor (MFA). El Postor deberá incluir el módulo de MFA para la autenticación a la consola para al menos 30 analistas.
- La solución podrá ser soportada en los navegadores de Internet Explorer, Edge, Edge (Chromium) y Chrome).
- Deberá contar con diferentes pestañas con tableros y widgets.
- La solución deberá contar con un API que permita:
 - Listar agentes
 - Obtener data de alertas e incidentes
 - Crear paquetes de actualizaciones de agentes
 - Listar servidores administrados

1.8 Plataformas soportadas en estaciones de trabajo.

Todos los componentes que forman parte de la solución deben ser parte de un fabricante único. Se requerirán un total de 1000 licencias, distribuidas de la siguiente manera: 500 licencias para endpoint y 500 licencias para servidores, con una duración de 36 meses

- El agente debe ser compatible con las siguientes versiones de sistema operativo al menos:
- Windows 8.1 (32-bit / 64-bit) (opcional)
- Windows 10 (32-bit / 64-bit)
- Windows 11 (32-bit / 64-bit)
- MacOS 11.x, 12.x, 13.x y 14.x

2. Protección para Servidores

Todos los componentes que forman parte de la solución deben ser parte de un fabricante único. Se requerirán 500 licencias para servidores por 36 meses.

Compatibilidad con las siguientes versiones de sistema operativo:

- Windows Server 2016 y superior
- MacOS 11.x, 12.x, 13.x y 14.x
- CentOS 7, Debian 9, Red Hat Enterprise Linux 7 y Oracle Linux 7 en adelante.

Consola De Gestión

- La consola debe tener capacidades de estar en Nube modo SaaS, permitiendo tener un ambiente híbrido que permita administrar los agentes instalados en la red de equipos. Permitiendo conocer el estado de los agentes.
- La consola de administración debe permitir agrupar los agentes en grupos para facilitar la configuración y administración de los mismos.
- La consola de administración debe permitir configurar notificaciones sobre riesgos de seguridad y ver los Logs enviados por los agentes sobre los eventos de los mismos.
- La consola de administración debe proporcionar un Dashboard que brinde información global sobre los agentes, usuarios afectados, eventos de comando y control, incidentes de filtración de datos, entre otros e igualmente debe permitir que secciones o widgets sean agregados o eliminados según se requiera.
- La consola de administración debe permitir consultar los Logs de instalación tanto del agente como el del servidor de administración.
- La consola de administración debe permitir visualizar estadísticas de históricos de actualizaciones de patrones de análisis de antivirus, antispymware, análisis de comportamiento, conexiones sospechosas y exploits de los navegadores de internet.
- La consola de administración debe permitir visualizar los logs de los eventos sobre los equipos donde se encuentra instalado el agente, dichos eventos deben estar relacionados a temas de malware, spyware, -+conexiones sospechosas, archivos sospechosos, Command & Control Callbacks, Behavior Monitoring, Machine Learning y escaneos. Adicionalmente la solución debe permitir filtrar dichos logs por periodos de tiempo preestablecidos, por rangos de fechas y por tipo de escaneo y/o ataque.
- La consola de administración debe permitir la visualización de los logs de registro de los eventos de la actualización del servidor de actualizaciones.
- La consola debe poder operarse en la nube sin requerir recursos de infraestructura y entregarse como software como servicio
- La solución debe permitir la creación de políticas globales para todas las máquinas, por perfil e individualmente para cada host
- La solución deberá ser administrada por consola web y debe soportar certificado digital para su administración
- Es requisito contar con la habilidad de configurar permisos granulares en la consola de administración para delegar operaciones y trabajos específicos a diversos usuarios o grupos de usuarios, así como perfiles de auditoría que solo permitan visualizar datos, pero sin la capacidad de modificar ninguna configuración





- La consola de gestión debe contar con doble factor de autenticación.
- La solución permite la generación de reportes bajo demanda o calendarizados permitiendo el envío de dichos reportes vía e-mail
- Debe contar con un módulo de virtual patching (es decir, capacidad para bloquear los intentos de explotación de vulnerabilidades de sistemas operativos no parchados) y debe permitir la administración de todos los agentes instalados en servidores sin importar el tipo de infraestructura ya sea en nube, virtual o física.
- La consola de administración debe tener la capacidad de generar reportes relacionados a las vulnerabilidades recomendadas que afecten tanto al sistema operativo, así como a las aplicaciones instaladas en el sistema operativo.
- La consola de administración debe tener la capacidad de generar reporte en formato PDF protegidos con contraseña.
- La consola de administración deberá contar con la capacidad de etiquetar eventos importantes de seguridad.
- La comunicación entre la consola de administración y los agentes debe estar cifrada.
- La consola de administración debe contar con dashboards que permitan monitorear los equipos de forma sencilla y estos pueden ser personalizados por el administrador
- La administración de todas las soluciones y equipamiento solicitado por la Entidad, serán de administración compartida, en ese sentido, el contratista entregará credenciales de usuarios a nivel de read/write a usuarios designados por la Entidad. El contratista está obligado a considerar todos los componentes, dispositivos y materiales que requiera para la integración de la solución adquirida con la red de la Entidad, así como para el cumplimiento de la finalidad del servicio requerido.

Antimalware de Nueva Generación

- La solución debe tener la capacidad de brindar protección contra malware, Ransomware, virus de red, conexiones sospechosas, spyware, monitoreo de comportamiento, ataques combinados y ataques de día cero para servidor.
- no deberá tener ningún componente que requiera actualizar una base de datos de firmas de antivirus.
- El algoritmo de machine learning deberá operar de manera local en el endpoint sin depender de una conexión permanente a la consola.
- Deberá ser capaz de detectar y bloquear cambios sospechosos en la imagen UEFI, que intenten comprometer el proceso de arranque del host, antes de que se cargue el sistema operativo.
- Debe prevenir el robo de contraseña a partir de la lectura de la memoria RAM (mimikatz)
- Capacidad de prevenir ataques de Cryptomining a partir del comportamiento del objeto ejecutado.
- Deberá ofrecer protección contra scripts de tipo webshell.
- Deberá ser capaz de prevenir ataques basados en el Bypass del UAC (User Account Control) que intenten escalar privilegios.
- Deberá ser capaz de analizar datos de paquetes de red para detectar comportamientos maliciosos

- Capacidad para bloquear ataques que permitan a un contenedor tener acceso al sistema operativo del host (container escaping) para sistemas Linux.
- La solución debe permitir la detección de amenazas tipo Fileless a través de la exploración de memoria mejorada para detectar comportamientos de procesos sospechosos. El agente debe tener la capacidad de terminar los procesos sospechosos antes de que se pueda hacer cualquier daño.
- Debe permitir la detección de malware oculto, polimórfico o variantes de malware usando fragmentos de malware visto anteriormente y algoritmos de detección
- La solución debe contar con motores de Machine Learning y monitoreo de comportamiento para examinar un elemento desconocido mientras se carga y analiza comportamientos sospechosos en el sistema operativo, aplicaciones, secuencias de comandos,
- La solución debe contar con firewall (reglas de conexiones de aplicación, IP, puerto y protocolo).
- La solución debe permitir realizar escaneos de los endpoint de forma manual, programada y en tiempo real.
- La solución debe permitir la integración con Active Directory.
- La solución debe permitir recuperar los archivos que sean enviados a cuarentena.
- La solución debe proporcionar protección a los agentes contra Ransomware.
- La solución debe proporcionar una consola de administración que pueda ser utilizada desde un entorno web.
- La solución debe tener la capacidad de analizar la reputación de archivos en base a su hash.
- La solución debe tener la capacidad de proteger los equipos que se encuentren dentro de la red y fuera de ella.
- La solución debe tener la capacidad de programar la actualización de agentes instalados en los equipos para horas y fechas específicas.
- La solución debe permitir seleccionar el criterio de las notificaciones para ser enviadas a la administración, cuando una amenaza sea detectada.
- La solución debe permitir la configuración de los tipos de eventos que serán notificados y visualizados en el agente, y adicionalmente configurar el mensaje de las alertas dependiendo de la criticidad del evento (High, Medium, Low)
- La solución debe permitir la configuración de proxy para los agentes.
- La solución debe tener la capacidad de finalizar sesiones en la consola de administración por tiempo de inactividad.

Amenazas de Día Zero

- Se tiene la capacidad de enviar muestras de archivos sospechosos para detectar amenazas de día cero, a través de la integración nativa y automática con una plataforma de sandbox.
- Deberá contar con técnicas avanzadas de Machine Learning para la detección de amenazas desconocidas, a través de análisis estáticos y dinámicos de archivos y procesos mediante el motor de aprendizaje automático, el cual correlaciona información de amenazas para detectar riesgos de seguridad a través de huellas digitales, mapeo de librerías, entre otras propiedades de los archivos.

- El agente deberá ser capaz de enviar automáticamente el archivo a un entorno de sandbox para ser emulado. Esta capacidad deberá estar disponible para sistemas Windows, MacOS, Linux.
- El sandbox deberá estar basado en nube y debe tener una disponibilidad del servicio de al menos 99.9% contabilizados mensualmente.
- El sandbox deberá soportar el análisis de al menos 300 mil archivos por día. El sandbox deberá tener capacidad de analizar archivos de hasta 100 MB de peso o superior.

Firewall

- El servicio de administración deberá contener un firewall que proteja servidores físicos y virtuales administrados desde la misma consola, permitiendo sólo las comunicaciones requeridas entre ellos. Este filtrado debe ser bidireccional y hacerse al menos sobre los siguientes parámetros:
 - Protocolos: ICMP, TCP, UDP
 - Direcciones IP
 - Puertos TCP & UDP
- Es deseable que el servicio de administración sea capaz de configurar la prioridad de la tarjeta de red cuando el servidor tenga múltiples tarjetas de conexión, en el caso de que el esquema de despliegue, aplique.
- Deberá haber logrado una efectividad de protección de ataques de 100%, según la evaluación del 2023 de MITRE ATT&CK
- Deberá haber logrado una efectividad de Detección de Técnicas de Ataque de al menos 98% y 100% de Prevención, según la evaluación del 2023 de MITRE ATT&CK
- Deberá estar ubicado como Líder en el Cuadrante Mágico de Gartner para soluciones EPP (Endpoint Protection Platform) del año 2024.
- Deberá estar ubicado como Líder en la evaluación Forrester Wave para soluciones XDR (Extended Detection and Response) del año 2024.
- Deberá estar ubicado como Líder en el reporte de Gigaom Radar para soluciones XDR (Extended Detection and Response) del año 2023.

IPS de Host

- El servicio deberá ser capaz de realizar una inspección bidireccional profunda de los paquetes para analizar y prevenir ataques a vulnerabilidades en las aplicaciones instaladas en cada servidor, incluidas vulnerabilidades de día cero.
- El proveedor del servicio deberá monitorear el tráfico para registrar algún ataque, y además tener la capacidad de realizar acciones de bloqueo.
- El proveedor del servicio deberá monitorear el tráfico para registrar algún ataque y bloquear el tráfico relacionado con él sin afectar el tráfico normal no relacionado con el ataque, permitiendo que continúen disponibles los servicios del servidor.
- El servicio de administración deberá ser capaz de monitorear y detectar técnicas de ransomware para el cifrado de archivos en recursos compartidos (Windows o Linux- Samba), protegiendo al servidor de clientes infectados, así como la capacidad de detectar y limitar el renombre de archivos en un periodo específico de tiempo.



- La solución deberá monitorear e inspeccionar el tráfico de un servidor virtual hacia a otro servidor virtual incluso cuando dicha comunicación no alcance la red física del cliente.
- La solución deberá tener la capacidad de reconocer los agentes desplegados en la red por medio de una tarea manual o programada
- La solución debe analizar, controlar y radicar los códigos maliciosos, entre ellos: Rootkits, Gusanos, Troyanos, Spyware, Malware Fileless, Virus, Ransomware, Malware Crypto (Monederos), otros
- Debe permitir monitorear los cambios no autorizados en llaves de registro, archivos propios, rutas específicas entre otros y generar alerta respecto a estos cambios o modificaciones
- Debe permitir detectar conexiones sospechosas o relacionadas con C&C y urls de baja reputación.
- La solución debe contar con la capacidad de generar paquetes de auto-diagnostico que permita la recolección de archivos relevantes para envío al fabricante en caso de requerir soporte del producto

Monitoreo de cambios de archivos y carpetas críticas (Integrity Monitoring)

- El proveedor del servicio deberá identificar los cambios en archivos críticos, cambios a la configuración de archivos, carpetas, servicios y llaves de registro tanto del sistema operativo como de las aplicaciones instaladas en el servidor. Bajo las plataformas de Windows y Linux soportadas.
- El proveedor del servicio debe ser capaz de identificar y aplicar automáticamente reglas de monitoreo sobre cambios realizados en archivos, carpetas y llaves de registro críticas del sistema operativo y las aplicaciones instaladas en el servidor.
- La solución deberá permitir identificar el usuario que realice cambios sobre los archivos, servicios o llaves de registros dentro del servidor.
- La solución deberá permitir etiquetar eventos importantes de seguridad y de duplicar esas etiquetas para eventos futuros.
- La solución deberá tener la capacidad de poder crear folders y/o grupos Inteligentes para llevar a cabo una agrupación que permita la administración y visibilidad de los servidores con base a una serie de criterios como nombre, Sistema Operativo, Versión, Rango de Red.
- La solución debe permitir doble o múltiple factor de autenticación utilizando SAML.

Control de Aplicaciones

El servicio deberá de garantizar:

- Debe de ser capaz de una vez habilitado el componente, realizar un escaneo que permita buscar el inventario de programas instalados para crear un conjunto de reglas locales, permitiendo la ejecución de los programas identificados.
- Debe de monitorear de forma continua con el fin de detectar cualquier cambio tanto a nivel del kernel y archivos de sistema realizados por los programas al momento de la instalación o nuevas ejecuciones.
- Debe de registrar todos los cambios de software. Los eventos se generan cuando el control de aplicaciones detecta software nuevo o modificado en el sistema de archivos, y cada vez que el software intenta ejecutarse.

- Debe de crear reglas para permitir o bloquear un software específico cuando intenta iniciarse. Igualmente, se debe de tener la capacidad de editar o eliminar reglas utilizando el editor del conjunto de reglas o el registro de decisiones.
- Capacidad habilitada para bloquear aplicaciones con al menos en base a los siguientes criterios: Hash, Firma Digital, Ruta, Nombre del Archivo.

Monitoreo de bitácoras del sistema operativo y aplicaciones

- La solución debe inspeccionar bitácoras o directorios de sistema operativo y aplicaciones para identificar malware dormido (es decir, malware que no se ejecuta) en el equipo.
- Las alertas podrán ser enviadas por correo electrónico o por syslog con el fin de poder ser explotadas.

REST API

- La solución deberá tener documentado un API que permita automatizar tareas administrativas, incluyendo funcionalidades de autenticación, monitoreo de usuarios, eventos de seguridad.

AGENTE

- Los agentes deben actualizar automáticamente su contenido, es decir, algoritmos y motores de análisis de comportamiento.
- El agente debe tener la capacidad de realizar un escaneo por servidor para determinar las vulnerabilidades presentes en el sistema operativo y las aplicaciones instaladas.

3. Capacidades de detección y respuesta en endpoint para la atención de incidentes

Se requiere contar con la capacidad de detección y respuesta tanto para los endpoint y servidores. Todos los componentes que forman parte de la solución deben ser parte de un fabricante único.

Colección de Telemetría de Endpoints

- El agente deberá poder capturar, como mínimo, las siguientes acciones en equipos Windows:
 - Proceso ejecutado, incluyendo el tiempo de inicio, el tamaño del archivo asociado.
 - Actividades de creación, escritura, renombre, eliminación, modificación de archivos.
 - Archivos DLL: ruta completa, dirección base, id del proceso, tamaño de la imagen, firma, valores hash calculados con los algoritmos MD5 y SHA256 del archivo DLL.
 - Creación y terminación de los procesos, incluyendo los siguientes atributos: nombre del proceso padre, ID del proceso, ruta completa, argumentos de la línea de comando, nivel de integridad, valores hash calculados con los algoritmos MD5 y SHA256, detalles de la firma o el certificado utilizado para firmar el archivo.

- Inyecciones en hilos de procesos: ID del hilo padre, ID del hilo nuevo o que se ha terminado, proceso que inició el hilo (en caso de ser un proceso distinto).
- Interacciones de red de cada endpoint: IP y puerto origen y destino, estado de conexión (exitosa o fallida), protocolo usado (TCP, UDP), solicitudes DNS, conexiones y desconexiones HTTP.
- Estadísticas de red: volumen de tráfico en eventos de subida y descarga de tráfico TCP.
- Acciones sobre los registros de Windows: Configuración o eliminación de valores del registro. Creación, modificación, eliminación, adición, restauración y guardado de llaves del registro. Con los siguientes parámetros: ruta del registro del valor o llave que fue modificado; nombre del valor o llave modificado; datos del valor modificado.
- Sesiones del sistema operativo: inicio de sesión, cierre de sesión, conexión y desconexión. Considerando los siguientes atributos: inicio de sesión interactivo, id de la sesión, estado de la sesión, y si la sesión es local o remota.
- Llamadas (calls) RPC y llamadas de Sistema (Syscall)
- Logs de eventos de Windows, incluyendo eventos de Seguridad, Aplicación.
- El agente deberá poder capturar, como mínimo, las siguientes acciones en equipos Linux:
 - Para los archivos: las acciones de creación, apertura, escritura y eliminación, incluyendo la ruta completa del archivo y el hash del archivo (para ciertos archivos y sólo si el archivo fue escrito). Información del copiado o renombrado de los archivos, incluyendo las rutas completas tanto del archivo original como del modificado. Las acciones para cambiar el dueño (chown) y el modo (chmod) de los archivos, incluyendo la ruta completa del archivo, así como el nuevo dueño o nuevos atributos.
 - Inicio y detención de procesos, con los siguientes parámetros: PID de proceso del proceso padre, PID del proceso, ruta completa, argumentos de la línea de comando, nivel de integridad para determinar si el proceso está siendo ejecutado con privilegios elevados, valores hash calculados con los algoritmos MD5 y SHA256, detalles de la firma o el certificado utilizado para firmar el archivo.
 - Interacciones de red de cada endpoint: IP y puerto origen y destino, estado de conexión (exitosa o fallida), protocolo usado (TCP, UDP).
 - Las siguientes acciones de red: accept, connect, connect failure, disconnect, listen, statistics.
 - Logs de eventos de autenticación.
- Todo el almacenamiento de la telemetría recolectada de los endpoints en formato "hot storage" por al menos 30 días deberá aplicarse durante toda la duración del servicio, garantizando así la disponibilidad de la información para fines de auditoría y análisis de seguridad.
- Todos estos eventos deberán ser colectados por el agente de manera continua, así exista o no una alerta de seguridad asociada.



- El contratista deberá incluir el licenciamiento correspondiente para que toda la telemetría colectada de los endpoints pueda ser enviada hacia la plataforma de **"Análisis de Incidentes y Correlación de Logs de Seguridad"**, con el objetivo de tener capacidades avanzadas de analítica y correlación, tanto automática (basada en inteligencia artificial) y personalizada.

Modelos de Correlación

- La solución debe contar con modelos de detección avanzados que detectan actividades sospechosas en los equipos.
- Los modelos de correlación deben combinar múltiples reglas y filtros usando una variedad de técnicas de análisis como, pero no limitándose, a Data Stacking y Machine Learning.
- Debe proveer la posibilidad de encender y apagar modelos según la tolerancia al riesgo y preferencias de la entidad.
- Deberá contar con capacidades de UEBA (User and Entity Behavior Analytics), siendo capaz de retener los eventos recolectados durante al menos 30 días y aprender una línea base o perfil de comportamiento de cada dispositivo y usuario.
- Los perfiles de comportamiento deberán de ser generados mediante el uso de algoritmos de aprendizaje de máquina no supervisado.
- A partir del comportamiento aprendido, el módulo de UEBA deberá ser capaz de alertar los siguientes comportamientos inusuales, que estén fuera del perfil base aprendido:
 - User agent sospechoso
 - Ejecución de comando Powershell sospechoso
 - Uso inusual de herramientas Systemals
 - Uso sospechoso de CURL
 - Servicio remoto iniciado desde una fuente inusual
 - Cantidad de interacciones de red inusuales
 - Query LDAP inusual
 - Creación de reglas de firewall inusuales
 - Sesión WinRM anómala
 - Proceso raro ejecutado en la institución
 - Elevación de privilegios con usuario SYSTEM de manera anómala
 - Firewall de Linux desactivado de manera anómala
 - Tarea programada creada de forma inusual
 - Ejecución de arp.exe anómala
 - Cantidad inusual de screenshots tomados
 - Conexión RDP inusual
 - Escaneo de puertos sospechoso
 - Creación de una máquina en el dominio
 - Creación de usuario con permisos de domain admin
 - Usuario imprime una cantidad inusual de archivos
 - Uso de aplicación no habitual
 - Cantidad inusual de solicitudes DNS generadas
 - Tráfico Kerberos y/o SMB generado desde un proceso no estándar
 - Subida de información anómala hacia internet

Workbench y priorización de alertas

- Debe proveer una vista de alertas para analizar la amenaza granularmente.
- Las alertas deben permitir ver un análisis de causa raíz identificar el alcance del impacto y permitir tomar acciones de respuesta.
- Debe priorizar las alertas y llevar registro de lo que se ha hecho y la fase de la alerta (nuevo, en progreso, finalizado/cerrado).

Visualización del ataque

- Debe contar con gráficas: una representación visual de los objetos que levantaron la alerta y la relación entre ellos.
- Debe permitir entender la historia del ataque con una representación visual e interactiva de los eventos.
- Debe tener la capacidad de verificar el perfil de ejecución/análisis de causa raíz para ver las acciones que una amenaza llevó a cabo en un servidor o endpoint.
- Debe permitir investigar adicionalmente desde la perspectiva de red (Network Analysis) para mostrar todas las interacciones de red de un endpoint.

Búsqueda/Threat hunting

- Debe permitir hacer un barrido con IoC (indicadores de compromiso) o búsquedas personalizadas usando múltiples parámetros, y filtrar los resultados añadiendo criterios adicionales de búsqueda.
- Desde el resultado de una búsqueda se debe poder ejecutar acciones de respuesta y generar un análisis de causa raíz.
- Se debe poder construir, guardar y reutilizar búsquedas para Threat Hunting básico.
- Deberá contar con un lenguaje propio para realizar consultas de la telemetría almacenada, deberá incluir al menos los siguientes criterios: Filtros por cada atributo recolectado del endpoint (procesos, archivos interacciones de red, login/logout, actividad en claves de registro y DLLs) con coincidencia total o parcial de cada atributo; uso operadores booleanos (and, or, not); operadores de comparación (igual, no igual, mayor que, menor que, mayor o igual que, menor o igual que); capacidad para especificar un límite de resultados (top 10, 20, 100, 500, 1000, personalización en general); operadores de comparación de datos; operadores matemáticos (promedio, contar, contar-distinto, máximo, mínimo, sumar); uso de expresiones regulares.
- Las búsquedas deberán estar disponibles tanto para endpoints en línea y fuera de línea.
- Permitir seleccionar las columnas y orden de los datos mostrados como resultados de las búsquedas.
- La solución debe contar con columnas de los dashboards de visualización de datos y deberán de ser configurables, para poder seleccionar las que sean del interés del analista.
- Las búsquedas deberán de poder programarse para ser ejecutadas en un día y hora determinados durante una sola ocasión y también de manera recurrente.
- Deberá contar con una librería predeterminada de búsquedas habituales realizadas en una labor de threat hunting. Esta librería podrá ser editada según la labor del investigador.



Built-in threat intelligence

- Debe detectar proactivamente con búsquedas automáticas de IoC publicados por el vendor
- Capacidad de alimentar la plataforma de Indicadores de Compromiso (IOC) de manera manual o automática vía API
- Los IOC soportados deberán ser de tipo Hash, Ruta, Nombre de archivo, Dominio, Dirección IP.
- Capacidad de agregar IOC de manera individual o masiva (por ejemplo, subiendo un archivo CSV)
- Capacidad de colocar un nivel de reputación, confiabilidad del IOC y una fecha de expiración.
- Debe poder integrarse a una plataforma tercera de Threat Intelligence como Virus Total.
- La capacidad de Threat Intelligence embebida debe ser capaz de identificar la campana asociada, la Plataforma atacada, las Técnicas, Tácticas y Procedimientos (TTPs) alineadas a MITRE ATT&CK™ y debe proveer enlaces/links a entradas de blog relacionados si están disponibles

MITRE ATT&CK mapping

- Enlaces desde el workbench a la documentación del framework de MITRE ATT&CK.

Acciones de respuesta integrada

- En una sola ubicación debe poder iniciar y ver estado de respuesta en endpoint y servidores.
- Debe permitir ejecutar acciones de respuesta rápidamente gatilladas desde el mismo incidente.
- Capacidad de extraer el malware o archivo sospechoso del endpoint hacia la consola, para poder ser analizado por el investigador
- Deberá ser capaz de hacer una búsqueda masiva en todos los endpoints en base al hash de un archivo o el path, con el objetivo de borrar dichos archivos de todos los endpoints.
- Debe ser posible aislar el endpoint de la red para que no tenga comunicación con ningún dispositivo de la red interna o externa.
- Capacidad de configurar reglas de automatización que permitan ejecutar una acción determinada en los endpoints en base condiciones de alertas de seguridad, como mínimo estas reglas deberán permitir las siguientes acciones de manera automática: aislar el endpoint, hacer un escaneo de malware, extraer el malware desde el endpoint.
- Deberá ser posible realizar una conexión remota a cada endpoint que forme parte de una investigación para ejecutar las siguientes acciones:
 - Listar procesos y archivos
 - Ejecutar instrucciones por línea de comandos (CMD y Powershell para el caso de Windows; Bash para el caso de Linux y MacOS).
 - Ejecutar scripts basados en Python
- Capacidad de ejecutar scripts remotamente a múltiples endpoints de manera concurrentes.

Integraciones vía API

- Una API pública debe poder ser usada por clientes para integrarse con SIEM y herramientas SOAR.

Software-as-a-Service solution

- Debe ser una solución hospedada y administrada en Nube (SaaS) para tomar ventaja de tecnologías Cloud.
- No debe requerir desplegar ninguna plataforma on-premise para su funcionamiento, únicamente los agentes conectados a la consola Cloud.

Apps - Detection Model Management

- Los modelos de detección deben consistir en uno o mes conjunto de filtros que integran recursos internos y externos como las técnicas y tácticas de MITRE ATT&CK
- El vendor debe constantemente refinar y añadir modelos de detección y filtros para mejorar las capacidades de detección y reducir falsos positivos.
- Los modelos deben priorizar la respuesta del administrador en base a puntajes (score). El score debe funcionar basado en Machine Learning.
- Los modelos deben tener una severidad asociada dependiendo del tipo de evento y la información de MITRE:
 - Critical: Hay fuerte evidencia de compromiso por un ataque dirigido, APT u operaciones de cibercrimen.
 - High: Hay indicadores altamente sospechosos de compromiso por un ataque dirigido, APT u operaciones de cibercrimen
 - Medium: Hay indicadores sospechosos posiblemente relacionados con infección de malware, violación de políticas u operaciones de cibercrimen.
 - Low: Hay indicadores levemente sospechosos. Usado para monitoreo y Threat Hunting.
- Los modelos deben especificar para que productor en específico (Workstation/Server) aplica una alerta
- Los modelos deben especificar y permitir modificar "status": encendido/apagado
- Debe permitir añadir excepciones durante la investigación de una alerta.
- En el proceso de añadir una excepción se debe poder definir una descripción para documentar la excepción.

Workbench

- Deberá mostrar una secuencia gráfica del incidente de seguridad que correlacione las alertas individuales con el objetivo de identificar la causa raíz. Esta secuencia gráfica deberá ser construida de manera automática a partir de la inteligencia artificial de la plataforma.
- Deberá mostrar información de los procesos correlacionados en la secuencia gráfica, mostrando los siguientes datos: ruta de ejecución, nombre de usuario que ejecutó el proceso, entidad que firmó el proceso, valor SHA256 del ejecutable relacionado con el proceso, veredicto del análisis del sandbox y línea de comandos de la ejecución.
- Por cada proceso correlacionado en la secuencia gráfica del incidente se deberá mostrar lo siguiente:
 - Fecha, hora, hostname, dirección IP, nombre del usuario, sistema operativo del equipo que generó el proceso.
 - Alertas relacionadas al proceso analizado con su respectiva descripción, acción tomada sobre la alerta, categoría de la amenaza, ejecutable que lo inicializó, táctica y técnica del ataque según el framework MITRE ATT&CK.



- Actividad de la red del proceso: IP y puerto origen, IP y puerto destino, resolución del DNS, país destino, indicar si la conexión fue exitosa o fallida.
- Creación, escritura, lectura, eliminación, renombre, cambio de atributos, hash en SHA256 y MD5 de los archivos relacionados al proceso analizado. En caso del renombre deberá mostrar el nombre anterior y actual para facilitar la investigación del analista.
- Creación, apertura, escritura, eliminación, renombre, cambio de atributos de los directorios relacionados al proceso analizado.
- Actividad sobre la clave y valores de registros, tales como creación, eliminación, carga, apertura, renombre, escritura, del proceso analizado.
- Mostrar los system calls, rpc calls y procesos inyectados sobre cada proceso analizado.
- Deberá contar con un mecanismo inteligente que separe de manera automática los binarios y DLLs no significados de la secuencia gráfica del incidente.

Response Management

- Response Management app: Debe permitir tomar acciones y llevar registro de las acciones tomadas.
- Debe haber distintas acciones que se puedan tomar en los objetos maliciosos/sospechosos
- Añadir a lista de bloqueo
- Eliminar de lista de bloqueo
- Terminar procesos en endpoints
- Recolectar archivos en endpoints
- Aislar un equipo
- Restaurar la conexión en equipos aislados
- Después de activar una respuesta a un evento u objeto, debe ver el estado de la tarea de respuesta y los detalles en la consola.

Search

- Debe permitir realizar barridos de loC, personalizar búsquedas especificando parámetros, filtros y otros criterios, y buscar múltiples eventos que ocurrieron en el mismo punto final.
- Debe permitir guardar búsquedas para encontrar nueva data relacionada a los mismos criterios.
- El administrador debe poder ver los queries guardados
- Debe ser fácil limpiar los criterios de búsqueda
- Los resultados deben ser exportables a CSV o JSON
- Los resultados deben mostrar origen de los datos (workstation/servidor)
- El administrador debe ser capaz de ver los logs en RAW
- Debe permitir diferentes tipos de búsquedas, filtros, y un lenguaje de consultas basado para identificar, categorizar y obtener los resultados de búsqueda.

Administración

- La consola deberá estar basada 100% en nube, con el objetivo de no depender ni administrar infraestructura física local. La nube del fabricante deberá contar con las siguientes características:



- Contar con la certificación SOC2 Tipo II o SOC2 Plus de AICPA, ISO 27001, ISO 27017, ISO 27018.
- Contar con doble factor de autenticación para el login.
- Permitir el acceso solo desde un rango de IP pública de la Entidad.
- La consola debe permitir la gestión de usuarios mediante roles preconfigurados y debe ser capaz de crear roles personalizados.
- Permite utilizar cualquier aplicación de un tercero para poder realizar la instalación del agente.
- Cuenta con la capacidad de crear grupos que pueden alimentarse de forma estática y dinámica.
- Capacidad de personalización del dashboard para mostrar los widgets según las necesidades de la Entidad.
- Capacidad de almacenar una auditoría de eventos sobre las acciones realizadas en la consola
- Deberá permitir el envío automático de alertas al correo electrónico cuando se identifica una actividad maliciosa. Podrán aplicarse filtros a dichas alertas para solo mostrar las de mayor relevancia.
- Tener la capacidad de generar reportes personalizados, eligiendo los tipos de gráficos a incluir y personalizando los datos, filtros y atributos a incluir en cada gráfico o tabla.
- Mantener un historial de los reportes que han sido generados para su posterior consulta.
- Los reportes podrán ser enviados de forma automática y programada a una o más direcciones de correos electrónicos.



5.2.1.5.4.1.21 SERVICIO DE SOC GESTIONADO, HERRAMIENTA DE ANÁLISIS DE INCIDENTES Y CORRELACIÓN DE LOGS DE SEGURIDAD

a. SOC GESTIONADO:

- El CONTRATISTA debe ofrecer un servicio de SOC para la Entidad. El Centro de Operaciones de Seguridad (SOC en sus siglas en inglés), tiene como finalidad automatizar y orquestar las diferentes soluciones de ciberseguridad implementadas para la protección de los activos de la entidad. Este servicio de SOC debe estar alineado a las mejores prácticas del mercado, como mínimo se solicita:
 - Punto único de contacto para gestionar la seguridad de la información en cuanto a Integridad, disponibilidad y confidencialidad, dicho punto único será el personal autorizado por la Entidad para reportar eventos/incidentes de seguridad.
 - Monitoreo y gestión en tiempo real.
 - Auditoría de los servicios de SOC requeridos por la Entidad, según término de referencia.
 - Actualización de los procesos de SOC requeridos por la Entidad, según término de referencia.
 - Gestión de informes y análisis de incidentes.
- La Entidad requiere contratar el servicio que incluya una solución SOAR (security orchestration, automation and response) que cuente con al menos 700 integraciones ya disponibles con distintas herramientas (de seguridad, forense, TI, colaboración) de la Entidad,

y automatizar acciones de respuesta a incidentes. La solución debe incluir las siguientes funcionalidades:

- La plataforma debe permitir realizar investigaciones interactivas que permitan colaboración, revisión histórica y ejecución en tiempo real y documentación de todas las acciones.
- La solución de SOAR a considerar deberá al menos haber sido elegida como líder de productos y en innovación en al menos dos reportes reconocidos de analistas en alguno de los 3 últimos años.
- Para cualquier acción de seguridad, debe ofrecer flexibilidad para automatizar o manualmente ejecutar en tiempo real según los requisitos del caso de uso.
- Los flujos de trabajo que la plataforma de SOAR utiliza para automatizar y ejecutar acciones deben ser compatibles al menos con Python y JavaScript.
- Debe incluir una función "Bring Your Own Integration" o similar que permita a los analistas escribir sus propias integraciones a través de un SDK interno y un wizard.
- La solución debe incluir nuevas integraciones de productos y automatizaciones automáticas como parte de actualizaciones de contenido.
- La solución debe integrar las funciones de Threat Intelligence Management (TIM). Deberá también automatizar y orquestar las labores de un equipo de Threat Intelligence.
- La solución debe integrarse, sin la necesidad de ningún desarrollo extra, con al menos 700 soluciones del mercado, entre ellas herramientas forenses, herramientas de TI, colaboración, SIEMs, soluciones de endpoint, firewalls, análisis de vulnerabilidades. Esto deberá ser demostrado a través del link público del fabricante que corrobore su cumplimiento, debiendo adjuntarse esto a la propuesta.
- La Plataforma debe poder admitir formatos de código abierto estándar como OpenIOC, Yara, STIX 1.0, STIX 1.2, STIX 2.0, XML, CSV, JSON
- La plataforma debe poder mapear los Indicadores de Compromiso (IoC) que ingiere a distintas técnicas, tácticas y procedimientos de ataque (TTPs), y debe mapear el TTP específico a grupos de Ataques Persistentes Avanzados (APT) para reducir el nivel de riesgo basado en grupos de APT.
- La solución deberá contar con su propia fuente de inteligencia de amenazas el cual provea IoC. Además, la solución deberá estar en capacidad de gestionar otras soluciones de fuente de Inteligencia de Amenazas de terceros que la Entidad pueda haber contratado con la finalidad de enriquecer de más IoC la solución.
- La plataforma debe facilitar la atribución de amenazas con nombre: mapeo de TTP a actores de amenazas, grupos, y el marco de MITRE ATT&CK
- La plataforma debe realizar la deduplicación y normalización automática de indicadores de compromiso provenientes de distintas fuentes.
- La plataforma debe admitir la inclusión de indicadores internos como IP y URL en la lista blanca, para garantizar que no sean marcados como maliciosos



- La herramienta debe contar con un mínimo de 600 casos de usos y playbooks de respuesta a incidentes, debe contar con una comunidad o Marketplace que permita consumir dichos playbooks sin depender de un desarrollo de la marca. Se define a un playbook como el conjunto de acciones definidas como un flujo de trabajo que ejecutan procedimientos de clasificación y respuesta a un incidente. Esto deberá ser demostrado a través del link público del fabricante que corrobore su cumplimiento, debiendo adjuntarse esto a la propuesta.
- Debe permitir crear playbooks copiando flujos existentes existentes, debe poseer una interface sencilla de utilizar que permita realizar drag-and-drop de acciones u otros flujos/playbooks y contar con un playbook debugger
- Debe permitir embeber un playbook dentro de otro, de forma de que este sea reutilizado continuamente
- Un playbook puede contener acciones totalmente automatizadas o tareas manuales, tareas de colección de datos o tareas condicionadas
- Los playbooks pueden ser ejecutadas automáticamente al crear un incidente y asociando al playbook correspondiente
- Los playbooks deben poder ser ejecutados como tareas y también ejecutados en tiempo real
- La ejecución de los playbooks y la actividad relacionada por el analista debe ser automáticamente documentada para cada incidente de seguridad
- La herramienta debe incluir una instancia donde usuarios puedan ver evidencia y documentación de incidentes anteriores, la herramienta debe agregar información de investigaciones pasadas
- Debe incluir un War Room donde los incidentes se auto-documenten, ofreciendo una vista detallada de registros basada en una línea de tiempo con cada actividad realizada durante la investigación de un incidente
- Como parte de un incidente, la herramienta debe documentar cualquier cambio, los analistas parte del incidente, tareas terminadas, comandos de interacción, evidencia, chats, notas y tareas de playbooks
- Los usuarios pueden marcar resultados de comandos o notas como evidencia, o automatizar la recolección de evidencia dentro de un playbook.
- Toda la información recolectada debe ser inmutable y no debe ser modificada, la documentación debe ser exportable para producir un documento de cadena de custodia
- Los analistas deben poder ver todos los indicadores de compromiso y el detalle alrededor de ellos.
- Los analistas deben ser capaces de utilizar campos customizados para por ejemplo atribuir indicadores a campañas de ataque
- La herramienta debe integrarse con sistemas de ticketing de TI, debe ser compatible con Jira, ServiceNow, HP Service Manager, Remedy).
- Los usuarios deberán poder tener comunicación bi-direccional con estas herramientas para iniciar acciones de creación de





- notificaciones (tickets) como también buscar y actualizar notificaciones(tickets) con información de investigación
- Debe contar con API autenticado (validado por el fabricante) capaz de ejecutar las mismas funciones que están disponibles a través de GUI
 - La herramienta debe estandarizar o escalar la administración de SLAs
 - La solución debe soportar aprendizaje automático (machine learning) para:
 - Identificar incidentes o casos relacionados
 - Recomendaciones o próximos pasos de casos y/o priorización de casos
 - Sugerir analistas.
 - Debe manejar campos obligatorios a ser llenados antes de cerrar un incidente de seguridad
 - Debe enviar notificaciones mediante herramientas de integración de mensajes tales como Okta, Slack y correos sobre cambios en incidentes, alertas, SLAs, etc.
 - Debe poseer la capacidad de asignar tags o características personalizables a los incidentes, estas características deberán poder utilizarse para distintos usos, entre ellos medir KPIs, medir estadísticas, ejecutar atomizaciones basadas en ellas, etc.
 - La solución debe permitir la delegación de tareas a otro usuario y asignar SLAs
 - La solución debe ser capaz de sugerir próximos pasos de acuerdo con el aprendizaje de máquina realizado durante investigaciones previas.
 - Debe incluir la capacidad de generar informes de incidentes, informes de estadísticas (tales como MTTR – tiempo medio de resolución) y los resúmenes o informes por incidente.
 - Debe ser capaz de aprender qué analistas son contactados usualmente por tipo de incidente y puede sugerir a los nuevos analistas a quien ellos pueden querer contactar para recibir ayuda.
 - La solución debe soportar un despliegue on-premise permitiendo que toda la data que se produzca en la organización no salga de las premisas
 - La solución debe soportar un despliegue en nube, capaz de conectarse a las premisas del cliente
 - Toda la información que esté en tránsito, debe estar cifrada usando TLS.
 - La solución debe proveer RBAC (control de acceso basado en usuarios) y se debe poder determinar acciones particulares usando RBAC. RBAC debe poder conectarse a AD (LDAP) y SAML a través de mapeo de grupos en roles.
 - La solución debe cifrar todas las Comunicaciones entre el usuario (browser) y el Servidor y debe proporcionar seguridad utilizando un certificado digital para:
 - Conexión segura (SSL) entre la plataforma y el servidor SOAR y la conexión interna entre los servicios.
 - Cifrar todos los datos de integración sensibles en la base de datos, p. ej. nombre de usuario, contraseña.

- Proporcionar una conexión segura a nivel de aplicación entre Servidor SOAR y la integración que estén en la nube o sea remota. Para cifrar datos sensibles de los archivos de configuración.

- La solución SOAR debe incluir 4 usuarios concurrentes con privilegios totales y soporte por 3 años. Se debe incluir el servicio de implementación de la solución y Servicios especializados de soporte y Transferencia de conocimientos hacia la Entidad.
- La solución deberá ser implementada en un servidor provisto por la Entidad para lo cual deberán indicar las características requeridas para tal fin.
- La solución deberá ser dedicada al 100% para la Entidad por lo que ningún componente de la misma deberá ser compartida ni podrá depender de un super-usuario superior a los usuarios de la Entidad. Es decir, no se podrá configurar un tenant para la Entidad toda vez que la plataforma que se requiere debe ser totalmente dedicada a la Entidad.

b. Herramienta para análisis de incidentes y correlación de logs de seguridad:

La Entidad requiere un servicio que incluya una solución que permita correlacionar los eventos de los Firewalls, la solución de seguridad de endpoints, entre otras soluciones que este soporte con el fin de identificar amenazas sofisticadas, movimientos laterales, Exfiltración de datos, comunicaciones de comando y control, entre otros difícilmente identificables por soluciones de forma independiente; debiendo considerar para tal fin una cantidad de 2000 GB (dos mil gigabytes) de logs a correlacionar diariamente o en su defecto, capacidad para poder recibir 24,000 logs por segundo. Adicionalmente, a esta capacidad, deberá estar dimensionado para recolectar toda la telemetría generada por los endpoints incluidos en el componente "Antivirus para servidores y endpoint del DataCenter", considerar que por cada endpoint se generan entre 100,000 a 120,000 eventos al día de telemetría.

Para este componente se requiere de una solución que permita lo siguiente:

Análisis de alertas e investigación de actividad sospechosa

- Deberá de contar con un dashboard en nube que permite visualizar alertas generadas de distintas fuentes.
- Deberá permitir la personalización de reglas de correlación que permitan configurar casos de uso utilizando los eventos recolectados de las diversas fuentes.
- Deberá permitir configurar motores de detección en tiempo real de la data colectada de distintas fuentes, así como motores de detección que se ejecuten de manera periódica sobre la data colectada.
- Deberá permitir enriquecer las reglas de correlación con atributos asociados a Tácticas y Técnicas de Ataque, Tipo de Amenaza, Severidad.
- La solución debe contemplar el uso de motores de detección basados en IOC's.



- La solución debe contemplar el uso de motores de correlación basados en el comportamiento de usuarios y dispositivos.
- La plataforma debe soportar el uso de machine learning en los casos de detección analíticos.
- Los perfiles de comportamiento deberán de ser generados mediante el uso de algoritmos de aprendizaje de máquina no supervisado.
- La plataforma debe contar con al menos 100 casos de uso de analítica para las distintas fuentes a integrar.
- Deberá agrupar automáticamente las alertas de seguridad similares en un solo incidente.
- Debe asociar cada alerta e incidente de seguridad descubierto a tácticas y técnicas de MITRE ATT&CK.
- La plataforma debe contemplar al menos los siguientes casos de correlación y detección:
 - Acceso a aplicaciones SaaS y de Red inusuales
 - Subida masiva de información a sitios de storage
 - Conexiones a múltiples puertos
 - Conexiones fallidas sospechosas
 - Sesiones SMTP anómalas
 - Subida de información anómala y excesiva por HTTPS, FTP u otro puerto no estándar.
 - Recurrente acceso a un Dominio y/o IP inusual
 - Acceso no-web a un sitio como Pastebin o similar
 - Proceso no-web accediendo a un website
 - Conexiones a Github desde Powershell
 - Conexión inusual de túnel de red
 - Anomalía de viajero imposible para logueos en VPN, Office 365, AWS, Azure, GCP
 - Logueo VPN con una cuenta de servicio
 - Logueo VPN desde un país inusual
 - Logueo VPN en un horario no habitual.
 - Intento de logueo VPN con un usuario inactivo o cuenta de servicio
 - Múltiples conexiones fallidas de DNS que puedan representar C&C
 - Exportación de múltiples cloud snapshots
 - Enumeración de contenedores Kubernetes
 - Modificación sospechosa de claves SSH de entornos cloud service provider
 - Snifer de red detectado en entornos cloud service provider
 - Inusual modificación/creación de recursos cloud
 - Actividad de herramientas de pentesting en entornos cloud
 - Excesivo bloqueo de cuentas de dominio
 - Ataques de fuerza bruta
 - Enumeración remota de usuarios
 - Intento de reseteo de password de usuario administrador
 - Login interactivo de una cuenta de servicio
 - Posible pass the hash
 - Habilitación de usuarios por defecto de Windows
 - Creación sospechosa de usuario domain admin
 - Configuraciones anómalas en Office 365 y Google Workspace

- La plataforma deberá poder integrarse con el Directorio activo ya sean On-prem así como también en la nube.
- La alerta deberá de formar parte de los incidentes que se hayan generado.
- Deberá ser capaz de recibir y procesar los eventos de telemetría generado por la solución de "Antivirus para servidores y endpoint del DataCenter" con el objetivo de enriquecer la investigación. Deberá ser capaz de mostrar gráficamente el proceso del endpoint que genera una conexión maliciosa de red que pasa por el NGFW, mostrando el detalle del proceso, interacción de archivos y registros ejecutados por el proceso, interacciones de red del proceso; regla, serial number y parámetros del NGFW que coincidieron con la interacción de red ejecutada por el proceso del endpoint.

Capacidades de detección basada en datos de la red

- La solución debe ser capaz de ingestar alarmas de red de cualquier marca de Firewall, incorporándolas dentro de los incidentes encontrados ofreciendo mayor contexto al analista
- La solución debe ser capaz de capturar logs de red y en conjunto con los datos del endpoint, debe generar perfiles de comportamiento utilizando algoritmos supervisados y no supervisados
- Debe detectar un intento de colección de datos, identificando el uso de un archivo protegido por contraseña
- Debe detectar intentos de exfiltración mediante el uso de exfiltración de tráfico a través de tuneleo por DNS
- Debe detectar intentos de descubrimiento, resaltando conexiones fallidas de un dispositivo hacia otros
- Debe detectar intentos de comando y control mediante la identificación de resoluciones hacia dominios creados por DGAs, resaltando desviaciones en el comportamiento de resoluciones de DNS de un dispositivo
- Debe identificar internos de exfiltración de datos resaltando grandes cantidades de información desde un dispositivo a través de tráfico http, FTP o SMTP
- Debe identificar intentos de comando y control y evasión resaltando procesos sospechosos enmascarados como Google
- Debe resaltar intentos de comando y control resaltando conexiones esporádicas de forma dinámica hacia dominios DNS
- Debe identificar potencial comando y control, resaltando conexiones extrañas hacia dominios terceros desde procesos no firmados
- Debe identificar potencial comando y control, resaltando conexiones extrañas hacia dominios categorizados como maliciosos de forma recursiva
- Debe identificar potencial comando y control resaltando conexiones recursivas específicas hacia direcciones IP externas
- Debe resaltar la técnicas y tácticas de ataque según el framework de MITRE ATT&CK
- Debe resaltar cuando una cuenta de usuario, servicio o administrador intentó autenticarse usando NTLM de forma excesiva en un período corto



- Debe identificar intentos de recolección de hashes NTLM resaltando un número inusual de usuarios tratando de autenticarse contra un target en la última hora.
- Debe identificar escaneos de puertos y reconocimiento, resaltando cuando un endpoint se conectó, o intentó conectarse, a varios puertos privilegiados (inferiores al puerto 1024), que son utilizados con poca frecuencia por otros puntos finales
- Debe identificar cuando un host busque registrarse como un nuevo controlador de dominio, y alertar cuando exista tráfico de sincronización de datos
- Debe identificar el robo de credenciales o tokens de acceso, resaltando un intento de autenticación NTLM inusual por parte de un usuario
- Debe identificar cuando un usuario trata de autenticarse a un host vía NTLM y no lo haya hecho en los últimos 30 días
- La solución provista deberá ser del mismo fabricante de los NGFW con la finalidad de tener una mejor integración y capacidad de detección más efectiva para la Entidad.

Capacidades de detección basada en datos de Identidad

- La solución debe ingestar datos de identidad de fuentes como Azure AD, Okta o PingOne
- Debe identificar cuando un usuario deshabilitado trata de autenticarse
- Debe identificar cuando un usuario busque autenticarse desde un nuevo ASN
- Debe resaltar cuando un usuario busca autenticarse de un país inusual por primera vez
- Debe resaltar cuando un usuario busca autenticarse de país distinto
- Debe identificar una anomalía cuando un usuario busca autenticarse desde múltiples países en un periodo de tiempo corto, que resultaría imposible
- Debe identificar cuando una cuenta de dispositivo y no de usuario trata de autenticarse
- Debe identificar cuando una cuenta de servicio y no de usuario trata de autenticarse
- Debe identificar cuando un usuario trata de autenticarse de forma sospechosa luego de no haberlo hecho en un periodo de tiempo
- Debe identificar cuando un usuario intentó autenticarse con un sistema operativo nuevo o anormal

Soporte de Fuentes para Ingesta de logs

- Capacidad de recolectar logs de Firewalls Fortinet, Palo Alto Networks, Cisco, Checkpoint, Sophos, entre otros.
- Deberá recolectar eventos de Google Workspace vía API, tales como: eventos de Google Chrome, acciones administrativas de la consola, chat, login, reglas, Google Drive, tokens, cuentas de usuarios, alertas, metadata de correos electrónicos.
- Deberá recolectar eventos de Office 365 vía API, tales como: auditoría de Office 365, Azure AD, Exchange, Sharepoint, metadata de correos electrónicos.



- Deberá recolectar eventos de Salesforce, tales como log de sesión, auditoría, flujo de eventos y transacciones, distribución de contenido, gestión de usuarios.
- Deberá recolectar eventos de Amazon S3, Amazon Cloudwatch, Azure Event Hub, Azure Network Watcher, GCP Flow Logs, GCP DNS Logs, GCP Audit Logs, GKE.
- Deberá recolectar eventos de AWS, Azure y GCP.
- Deberá recolectar eventos de Active Directory (Window Event Logs), tales como: búsquedas de LDAP, gestión de grupos y usuarios de dominio, gestionar de computadoras del dominio.
- Deberá recolectar eventos de Netflow.
- Deberá recolectar eventos de otras fuentes de diferentes marcas a través del protocolo Syslog, pudiendo soportar al menos los formatos CEF, LEEF, RAW.
- Deberá permitir la recepción de logs y/o eventos en distintos formatos o protocolos, alojados Servidores FTP/SFTP/FTPS y en carpetas compartidas de equipos Windows y Linux, tales como: CSV, PSV, TSV, texto plano, Archivos en formato CEF/LEEF, JSON.
- Para los archivos alojados en carpetas compartidas, la solución debe ser capaz de coleccionar los eventos en línea y/o vía batch definiendo la frecuencia en base a minutos, horas o días.
- Deberá contar con conectores directos a bases de datos MySQL, MSSQL, Oracle y PostgreSQL, para poder coleccionar información alojada en tablas de bases de datos.
- Deberá soportar el uso de agentes para equipos Linux, capaces de recolectar los logs nativos de sistemas Red Hat, Centos, Debian, Ubuntu, así como logs de Nginx.
- Deberá contar con agentes para equipos Linux, capaces de recolectar los logs nativos de sistemas Red Hat, Centos, Debian, Ubuntu, así como logs de Nginx.
- Deberá contar con agentes para equipos Windows, capaces de recolectar los logs de DNS, logs de DHCP, logs de servidores IIS y Nginx.
- Deberá contar con agentes para equipos Windows, capaces de recolectar los Event Log (que nativamente se ven en el Event Viewer).
- Deberá soportar el protocolo Windows Event Collector (WEC) para poder integrarse a los Active Directory y coleccionar los Event Log sin necesidad de instalar agentes.
- Deberá poder coleccionar logs o eventos utilizando API, ya sea mediante el uso de HTTP Collectors o Filebeat respetivamente.
- Deberá ser capaz de normalizar los eventos recibidos de las diferentes fuentes, utilizando parsing rules u otro método.
- Deberá realizar la colección de información de los dispositivos en las premisas mediante la implementación de una máquina virtual (colector). El colector también podrá ser desplegado en entornos nube.
- Los colectores deberán tener la capacidad de ser desplegados en Alta Disponibilidad.
- La plataforma deberá almacenar la información recolectada en formato raw log (log crudo) por al menos 3 años (todo el tiempo de duración del servicio), esto aplica para todos los logs recolectados por la solución de correlación de las diferentes plataformas de seguridad.



Se precisa, que para la telemetría de los endpoints, únicamente será necesario un periodo de retención de 30 días.

- La plataforma debe permitir el almacenamiento de información por cada tipo de fuente, con el fin de poder gestionar métricas y parámetros de almacenamiento.
- La plataforma debe permitir el indexado de los eventos colectados en un esquema de tablas que permitan la búsqueda y uso de estadísticas/métricas de cada campo normalizado.
- La plataforma debe permitir visualizar las métricas de espacio, promedio de ingesta diaria, promedio de ingesta total, fecha de última vez de colección, etc.
- La plataforma debe soportar un mínimo de 1000 datasets, asociados a cada fuente de datos

Casos de Uso Predefinidos

- La solución provista debe incluir al menos 300 casos de uso de correlación o analítica ya predefinidos, incluyendo entre otros los siguientes:
 - Escaneo de puertos
 - Conexiones fallidas
 - Usuarios accediendo a aplicaciones no comunes (no antes utilizados)
 - Gran cantidad de datos siendo transferidos a un sitio externo como correo o almacenamiento
 - Viajero Imposible (el conectarse vía VPN desde ciudades/países distintos en un tiempo muy corto).
 - Intentos de fuerza bruta de conexión a la VPN
 - Posibles Intentos de sniffing de red vía TCPdump o tshark
 - Posible búsqueda de archivos de passwords en los endpoints

Investigación, Threat Hunting y Visualización de Amenazas

- Permitir realizar búsquedas en base a cualquier dato recopilado por la plataforma.
- La solución debe permitir la correlación fuentes de terceros por medio de búsquedas personalizadas.
- La plataforma debe permitir la búsqueda de IOC's por medio de búsquedas personalizadas usando logica booleana, filtros o funciones propias de la solución de correlación.
- Deberá contar con un lenguaje propio para realizar consultas de cada dataset, que incluya al menos los siguientes criterios: Filtros por cada atributo del dataset con coincidencia total o parcial de cada atributo; uso operadores booleanos (and, or, not); operadores de comparación (igual, no igual, mayor que, menor que, mayor o igual que, menor o igual que); capacidad para especificar un límite de resultados (top 10, 20, 100, 500, 1000, personalización en general); operadores de comparación de datos; operadores matemáticos (promedio, contar, contar-distinto, máximo, mínimo, sumar); combinar búsquedas de dos o más datasets.
- Permitir seleccionar las columnas y orden de los datos mostrados como resultados de las búsquedas.



- La solución debe contar con columnas de los dashboards de visualización de datos y deberán de ser configurables, para poder seleccionar las que sean del interés del analista.
- Las búsquedas deberán de poder programarse para ser ejecutadas en un día y hora determinados durante una sola ocasión y también de manera recurrente.
- Deberá contar con una librería predeterminada de búsquedas habituales realizadas en una labor de threat hunting. Esta librería podrá ser editada según la labor del investigador.
- Todas las opciones de búsqueda anteriormente detalladas deberán poder ser utilizadas para configurar reglas personalizadas de seguridad, que permitan generar una alerta cuando exista alguna coincidencia en el log (o logs) recolectados con la regla de búsqueda.
- Deberá permitir exportar los resultados de la búsqueda en archivo CSV.
- Los resultados de las búsquedas deberán poder ser mostrados en una tabla o una gráfica de tipo pie, columnas, burbuja y área, con la finalidad de facilitar el análisis del investigador.
- Deberá permitir la personalización de los dashboard y agregar varios dashboards de monitoreo
- Por cada dashboard se podrá añadir diferentes gráficos de tipo pie, columnas, burbuja, área, entre otros mostrando información extraída de los diferentes datasets a través de las opciones de búsqueda granular que tenga la plataforma.

Gestión de Incidentes

- Las alertas e incidentes de seguridad deberán tener una valoración cualitativa de al menos 4 niveles de severidad: bajo, medio, alto y crítico. Estos niveles de severidad podrán ser modificados de manera manual o automática.
- Tener la capacidad de poder agrupar las alertas relacionadas en incidentes, así como proporcionar un contexto de este.
- Debe tener la capacidad de poder extraer los elementos importantes o relevantes de las alertas, y mostrarlos a manera de resumen en la pantalla de análisis del incidente.
- Debe contar con un dashboard donde se muestran los incidentes de seguridad que no han sido atendidos (clasificados de acuerdo con su criticidad en alta, media y baja), un resumen sobre los incidentes de seguridad (clasificados por su plataforma, etc.)
- Debe permitir asignar cada alerta de seguridad a un analista administrador de la consola, esta asignación se puede hacer de forma manual o automática en base a ciertos criterios de la alerta. Por cada asignación que se realice se deberá notificar vía correo al analista.
- Cada incidente de seguridad debe tener un estado, tales como abierto, en proceso, cerrado, resuelto, o estados equivalentes.
- Debe permitir colocar un comentario por cada incidente, con el objetivo de llevar un seguimiento de este durante la investigación.
- Debe contar con un dashboard donde se describen las características de los incidentes de seguridad que se han generado. Este dashboard debe de permitir analizar a mayor detalle las alertas de seguridad, incluyendo los reportes generados por el agente.

- Debe tener un dashboard para monitorear el MTTR (mean time to response) en la gestión de incidentes.
- Deberá tener un motor automático de scoring de incidentes, que permitan dar una valoración cuantitativa en un puntaje de 0 a 100 en base a determinados criterios de cada alerta de seguridad, éste deberá de funcionar de manera paralela a la valoración cualitativa de los incidentes y alertas de seguridad.
- Mostrar un mapa geográfico que permita analizar la dirección IP detectada como parte de incidente, como mínimo deberá mostrar lo siguiente: fecha de registro, ISP (Internet Service Provider), país. La información deberá poder ser mostrada en base al país, proceso, puerto e IP destino.
- Deberá contar con un dashboard que permita analizar el comportamiento del hash de un archivo en particular, mostrando su nivel de reputación y si dicho hash ha sido detectado en otras alertas e incidentes.

Consola de Gestión

- Administración de políticas centralizada, vía una consola web.
- La solución debe estar basada en la nube como servicio SaaS (Software as a Service), esto implica que los recursos de almacenamiento y procesamiento deberán estar alojados en nube, con la finalidad de no tener limitaciones de hardware para las tareas de correlación y búsqueda de datos.
- La nube del fabricante deberá contar con las siguientes características:
 - Contar con la certificación SOC2 Tipo II Plus o SOC2 Plus de AICPA
 - Contar con certificaciones ISO 27001, ISO 27017, ISO 27018, ISO 27031, ISO 27701
 - Contar con doble factor de autenticación para el login.
 - Permitir el acceso solo desde un rango de IP pública de la Entidad.
- La solución debe permitir la visualización del licenciamiento adquirido desde la Consola en una ventana específica.
- La solución debe mostrar en promedio cuantos Gigabytes de Logs por Día recolecta por cada fuente o en su defecto el promedio de los Eventos/Logs por Segundo.
- La solución debe proveer una consola de administración en la nube que permita la gestión de cada uno de los componentes aquí descritos, adicionalmente debe permitir administrar cada uno de los componentes encargados de la colección de eventos.
- La solución deberá ser capaz de almacenar la información de alertas e incidentes de seguridad durante al menos 360 días
- La consola debe clasificar los eventos al menos en tres niveles de acuerdo a su severidad: bajo, medio y alto.
- Capacidad de poder agrupar las alertas relacionadas en incidentes, así como proporcionar un contexto del mismo.
- Capacidad de poder extraer los elementos importantes o relevantes de las alertas, y mostrarlos a manera de resumen en la pantalla de análisis del incidente.





- La consola deberá de proporcionar información detallada bajo demanda de los eventos identificados como exploits siempre y cuando la solución propuesta sea del mismo fabricante de la solución de Seguridad de Endpoint.
- Cuenta con integración con Active Directory para la gestión de computadoras y configuración de políticas.
- Cuenta con la capacidad de poder crear perfiles granulares.
- Cuenta con la capacidad de poder crear políticas basadas en los perfiles creados.
- La consola deberá de ser proporcionada bajo un esquema software as a service.
- Cuenta con un dashboard donde se describen las características de los incidentes de seguridad que se han generado.
- Deberá de contar con un dashboard que permite visualizar alertas generadas de distintas fuentes
- Las columnas del dashboard deberán de ser configurables, para poder seleccionar las que sean del interés del analista.
- Debe resaltar las técnicas y tácticas de ataques identificados según el framework de MITRE ATT&CK.
- La solución debe incluir el almacenamiento histórico de los logs durante el periodo del contrato.
- La consola debe permitir la gestión de usuarios que acceden a la consola mediante roles.
- La plataforma debe permitir integrarse con feeds de reputación externos, de manera automática vía API o de manera manual-masiva subiendo un archivo con los IOC.
- Debe contar con una capa de administración vía API, para automatizar acciones integradas con herramientas externas como un SOAR.

c. Herramienta de Monitoreo de Gestión de Disponibilidad para 7500 elementos.

ALCANCE

- Herramienta orientada al monitoreo de la red a nivel LAN/WAN.
- Instalación y funcionamiento en la red del cliente (on-premise)
- Capacidad de monitoreo integral del desempeño de la infraestructura, la red y las aplicaciones hasta un total de 7500 elementos
- Monitoreo de hosts y dispositivos físicos y virtuales
- Detección automatizada y asignación de dependencias
- Paneles históricos y en tiempo real
- Correlación inteligente, alertas e informes personalizables
- Administración de configuraciones para redes, virtualización, servidores y aplicaciones

MONITOREO DE GESTIÓN DE RED INTEGRADO

- El POSTOR suministrará la activación del licenciamiento de software de gestión de red integrado con toda la solución, para monitorear la disponibilidad de nodos, volúmenes e interfaces (elementos de la red con SNMP habilitado)

- La herramienta de monitoreo debe operar sobre todos los elementos de red y servidores instalados en el cliente, permitiendo obtener en tiempo real los reportes y graficas de por lo menos las siguientes métricas:
 - Disponibilidad.
 - Tendencia de parámetros monitoreados en el tiempo.
 - Capacidad y utilización de ancho de banda.
 - Utilización y errores de buffer.
 - Utilización de CPU, memoria y disco duro (en equipos físicos y virtualizados).
 - Errores y descartes de Interfaces, multicast y broadcast en gráficas fáciles de personalizar.
 - Latencia de la red.
 - Estatus de equipos, interfaces y volúmenes (interfaces virtuales o Vlans).
 - Utilización de volúmenes virtuales.
 - Consumo de ancho de banda agrupados por dispositivos, aplicaciones y protocolos.
- Tener la capacidad de diagramar una vista gráfica de la arquitectura de la red con los datos obtenidos dinámicamente por el propio sistema y con datos adicionales definidos por el usuario.
- Diferenciar claramente a través de iconos, todos los dispositivos que conforman la red (switches, routers, servidores, etc.).
- Descubrir la Red en forma automática a través de SNMP (V1, V2, V3), WMI e por ICMP para los dispositivos que no respondan a los primeros protocolos. Lo hará de acuerdo a un rango de direcciones definido y conformará la topología exacta de conexión.
- Tener la capacidad de realizar gráficas de la topología que muestre conexiones y estados de dispositivos.
- Posibilitar la definición de grupos, identificados claramente por iconos, conformados por agrupación de elementos (dispositivos y aplicaciones). Dichos grupos deberán resumir el estado de situación de cada uno de los elementos que lo componen mostrándolo gráficamente.
- Indicar con diferentes colores, el traspaso de umbrales definidos sobre las variables a monitorear de cada elemento.
- Configurar vistas de acuerdo a las necesidades del usuario.
- Definir umbrales de funcionamiento que en caso de ser superados ejecuten las alarmas por tiempo medio de permanencia en red para los dispositivos afectados.
- Almacenar en la base de datos la información referente a la causa que provocó la ejecución de una alarma.
- Combinar umbrales de disparo de alarmas: El disparo de alarmas podrá ser configurado combinando el traspaso de umbrales de cualquiera de las variables.
- Paleta de análisis de métricas monitoreadas basado en "drag and drop" permite correlación de diversas métricas para análisis de incidencia entre las mismas, exportación de data y compartir paletas de análisis.
- Soporte de monitoreo para dispositivo cisco ACI, permite monitoreo lógico de componente de entornos SDN incluyendo APICs, tenants, perfiles de aplicación, grupos de endpoint, spien y leaf switches



- Soporte de monitoreo para cloud environment Microsoft Azure (nombre de gateway, status, tipo, location, tunnel traffic entrante y saliente, etc) y Amazon Web Services

MONITOREO DEL ANCHO DE BANDA Y ANALIZADOR DE TRÁFICO

- El POSTOR suministrará la activación del licenciamiento de software de monitoreo de tráfico integrado con toda la solución para el análisis de tráfico mediante NetFlow en interfaces.
- Brindar control y análisis por medio de la presentación de los datos extraídos en cuadros fáciles de interpretar y tablas que los cuantifican.
- Permitir la visualización de los datos capturados en tiempo real (acorde con el intervalo de medición y almacenamiento) y de los datos históricos.
- Salvar los datos recolectados en la base de datos del sistema dedicados para este fin.
- Asegurar el refresco de toda la información capturada cada minuto.
- Permitir trabajar con los protocolos NetFlow v5/v9, sFlow v2/v4/v5, J-flow, Huawei Netstream, IPFIX y NBAR2 para recopilar datos de tráfico de red.
- Indicar los patrones de uso a través del tiempo mediante gráficos de fácil entendimiento.
- Efectuar identificación y seguimiento del tráfico externo.
- Deberá realizar una integración rigurosa con estadísticas de rendimiento de la interfaz detalladas.
- Incluir recursos que permiten granularidad sobre la composición del tráfico en términos de conversaciones top, grupos de direcciones IP, fuentes de tráfico por dominios y top de destinos de tráfico.
- Generar informes sobre el tráfico de red.
- Permitir visualizar la granularidad del tráfico NetFlow por minuto hasta un mínimo de 30 días para análisis de incidencias, cambios y patrones, y permitiendo que las gráficas con granularidad de 1 minuto solo puedan generarse para periodos de hasta 5 horas, fomentando una mayor pluralidad de postores en el proceso.
- Generar informes detallados e históricos de utilización del tráfico de los enlaces a nivel WAN.
- Soporte de monitoreo de tráfico para redes IPv4 e IPv6
- Monitoreo de tráfico malicioso TCP o UDP port 0

MONITOREO DE SERVIDORES Y APLICACIONES

- Realizar ciertas configuraciones de aplicaciones y servidores de línea de referencia en Windows y Linux
- Comparar las configuraciones actuales con las versiones previas
- Correlacionar los cambios de configuración con indicadores de rendimiento
- Permitir configurar alertas avanzadas para eventos relacionados, condiciones continuadas y combinaciones complejas de estados de los dispositivos
- La herramienta debe estar en capacidad de trabajar en una interfaz web totalmente personalizable que permite a los usuarios de TI ver de forma remota el estado de la red



- Ver mapas con las dependencias de los dispositivos, sus componentes y aplicaciones.
- La herramienta de monitoreo debe permitir ser instalada en servidores virtuales o físicos.
- La herramienta de monitoreo debe soportar IPV4 y IPV6
- Permitir la visualización de los datos capturados en tiempo real (acorde con el intervalo de medición y almacenamiento) y de los datos históricos.
- Salvar los datos recolectados a la base de datos del sistema.
- Asegurar el refresco de toda la información capturada cada 5 minutos o menos
- Obtener patrones de uso de dispositivos de red a través del tiempo
- Permitir la visualización de los datos capturados en tiempo real (acorde con el intervalo de medición y almacenamiento) y de los datos históricos.
- Salvar los datos recolectados a la Base de Datos del sistema.
- Supervisión de procesos mediante WMI, RPC, SSH y SNMP, así como la supervisión de aplicaciones por medio de scripts personalizados.
- Supervisar cualquier puerto TCP y UDP disponible de la red
- Supervisar servidores Windows, Unix, AIX, Solaris y Linux realizando el seguimiento de las estadísticas clave relativas al rendimiento, como son los servicios en ejecución, la disponibilidad de procesos, el uso de la memoria, la utilización de la CPU y el tiempo de respuesta.
- Supervise el estado del hardware para clústeres Nutanix
- Supervisar remotamente contadores de rendimiento vía WMI o agente.
- Supervisar activamente la disponibilidad y la capacidad de respuesta de servicios de red esenciales con monitores para DNS (en TCP y UDP), HTTP, HTTPS, IMAP4, POP3, SMTP y NNTP. Además, debe permitir crear monitores personalizados para puertos TCP con los que comprobar la disponibilidad y la capacidad de respuestas de aplicaciones que dependen de la red.

MONITOREO Y GESTIÓN DE EQUIPO DE RED

- Administrar y controlar centralmente los cambios de configuración de la red de la entidad
- Recibir alertas en tiempo real cuando se efectúen cambios en la configuración de la red de la entidad
- Detectar infracciones de las políticas de configuración de la red de la entidad
- Realizar automática copias de seguridad de la configuración de los dispositivos de la red de la entidad
- Visualizar simultáneamente configuraciones, cambiar cadenas de la comunidad, actualización de ACL y bloqueo de direcciones MAC.
- Comparar los archivos de configuración de arranque y de ejecución de los equipos de la red de la entidad
- Detección y copia de seguridad de VDC
- Visualización de listas de control de acceso (ACL)

- Permitir la visualización de los datos capturados en tiempo real (acorde con el intervalo de medición y almacenamiento) y de los datos históricos.

MONITOREO DE EQUIPOS VIRTUALES

- Soportar y administrar entornos VMware, Microsoft Hyper-V y Nutanix a través de un único panel de administración.
- Proporcionar recomendaciones de rendimiento y colocación activas o predictivas que se pueden ejecutar inmediatamente o programarse para ejecutarse en un momento determinado para VMware y Hyper-V.
- Supervisar y analizar proactivamente los problemas de rendimiento específicos de la virtualización en entornos virtuales.
- Brindar una comparación y análisis de rendimiento y métricas en una sola vista incluidos el estado, los eventos y las estadísticas a través de PerfStack.
- Intercalar datos de rendimiento y métricas en sus sistemas de virtualización, almacenamiento, aplicaciones, sistemas y redes, lo que permite una identificación más rápida de los problemas a través de PerfStack.
- Crear mapas de dependencias entre objetos virtuales mediante AppStack.
- Administrar, planificar y optimizar la capacidad de infraestructura de sus equipos virtuales encontrando desbalances de recursos (CPU, Memoria RAM y Espacio en Discos) otorgados a sus equipos para VMware y Hyper-V.
- Visión general del rendimiento, la capacidad, la configuración y el uso de su infraestructura virtualizada.
- Encontrar máquinas virtuales asignadas, agregue o quite CPU y RAM y elimine VMDKs huérfanos, para VMware y Hyper-V.
- Encontrar máquinas inactivas (zombis) y equipos apagadas en el tiempo, para su desuso o mejor uso de sus recursos, para VMware y Hyper-V.

MONITOREO DE TRAFICO WAN Y TELEFONIA VoIP

- El Ofrecer una solución de monitoreo de red de gran alcance la cual utilizando una configuración automática de la tecnología IP SLA de Cisco, identifique los problemas de rendimiento específicos del sitio y WAN relacionados desde la perspectiva de cada uno de los sitios remotos.
- Mantener una estrecha vigilancia sobre sus indicadores clave de rendimiento de la WAN, incluyendo CISCO VoIP jitter y MOS.
- Capacidad de controlar, informar y alertar en operaciones adicionales de IP SLA, incluyendo: Ruta de ICMP Echo, Ruta ICMP Jitter, DHCP, DNS, FTP, HTTP, ICMP Echo, TCP Conectar, UDP Echo, UDP Jitter.
- Capacidad de analizar, proactivamente el desempeño de la infraestructura de red, servidores y VoIP, el consumo de la red, dispositivos inalámbricos, y servidores.
- Configurar fácilmente las operaciones de IP SLA en múltiples dispositivos Cisco, al mismo tiempo usando la consola web intuitiva
- Ver el estado de funcionamiento IP SLA en mapas personalizados

- Capacidad de alerta en todos los umbrales sobre el estado de la operación de IP SLA.
- Posibilidad de asignar un codec de voz específico
- Poder especificar las fuentes de voz y su ruta por cada interface IP
- Soporte para múltiples pollers de VoIP
- Ofrecer métricas de rendimiento de jitter, latencia, pérdida de paquetes para los sitios y rutas de llamadas.

MONITOREO Y GESTIÓN DE LOGS

- Recopilar datos de capturas syslog y SNMP que su infraestructura haya generado para ayudar a obtener un conocimiento más exhaustivo y ayudar con la detección y solución de problemas.
- Acotar sus búsquedas de datos de registro mediante filtros listos para usar, y encontrar entradas de registros relevantes a través de un eficaz motor de búsqueda.
- Visualizar rápidamente volúmenes de registros, resultados de búsquedas y redefinir marcos de tiempo mediante cuadros interactivos.
- Integrar sus datos de registro directamente en la consola de la plataforma de monitoreo para verlos fácilmente junto con las mediciones de desempeño de la red y los sistemas.

REPORTERIA

- Informes comprensivos y análisis de tendencias que destaquen las tendencias de rendimiento clave a través de la interfaz de informes fácil de usar. Los informes y gráficos cubren áreas como actividad de input/output de CPU, actividad de disco físico, peor rendimiento por aplicación y usuario, inicios de sesión (incluidos inicios de sesión fallidos).
- El sistema también proporciona una serie de informes de pronóstico que permiten a los usuarios pronosticar el crecimiento de bases de datos, unidades y tablas en función del rendimiento pasado.
- Realizar reportes en forma automática, pudiendo configurarse el envío de los mismos vía e-mail en horarios determinados por el usuario.
- El sistema también proporciona una serie de informes de pronóstico que permiten a los usuarios pronosticar el crecimiento de bases de datos, unidades y tablas en función del rendimiento pasado.
- Crear/almacenar un informe personalizado basado en cualquier métrica recopilada para identificar problemas recurrentes y prevenir futuras ocurrencias. Estos deben poder enviarse por correos electrónicos programados fácilmente a través de la consola de administración.

ALERTAS

- Las Alertas deben ser adaptables, automatizadas.
- Debe proporcionar alertas predefinidas y configurables basadas en las mejores prácticas de la industria con configuraciones de configuración avanzadas que permiten una mayor flexibilidad.



- Variedad de acciones para notificar al personal encargado de lo que está ocurriendo.

d. Plataforma para el descubrimiento e identificación de servicios en servidores PNP (200 servidores)

Se requiere una solución de seguridad, cuyo objetivo principal es la contención de la proliferación de brechas y ataques de ransomware sobre una superficie de ataque de entornos híbridos (On-Prem y Cloud) mediante la visualización continua de los patrones de comunicación entre las cargas de trabajo y dispositivos (Ej. OT/IoT), y que permita la creación de políticas de seguridad granulares que solo permitan el tráfico requerido y necesario, y que permita el aislamiento automático de brechas al restringir el movimiento lateral tanto de forma proactiva o durante un ataque activo. Se deberán considerar 200 servidores que estarán alojados en el data center principal de la Entidad. Las políticas de operación serán coordinadas con la Entidad. La solución deberá contar con las siguientes características:

- Deberá ser una solución basada en únicamente 2 capas:
 - Capa de Protección de carga de trabajo: a través de un agente liviano que colectione metadatos, flujos y telemetría de la carga de trabajo e instrumente el control de tráfico nativo.
 - Capa Central de Cómputo y Procesamiento de Políticas de seguridad: a través de una consola SaaS y/o on-premise que centralice, procese y analice los flujos y telemetría del entorno distribuido de protección, consola gráfica para el análisis de flujos, metadatos, definición y programación de políticas de seguridad y aplicación y envío de las mismas
- El agente de protección de la carga de trabajo deberá específicamente instrumentar el control de tráfico nativo del sistema operativo donde se instala, es decir el agente NO deberá estar en-línea en el flujo de comunicación del activo protegido.
- La instalación y desinstalación del agente de protección deberá ser llevada a cabo sin la necesidad de reiniciar el sistema operativo en ninguna circunstancia.
- El agente o software deberá tener mecanismos internos de protección ante ataques (Anti-tampering), con la capacidad de detectar, corregir y registrar eventos de:
 - Manipulación de políticas de control de tráfico
 - Manipulación y/o fallas de procesos y servicios propios del agente
 - Protección mediante token de autenticación para realizar tareas de mantenimiento o desinstalación.
 - Registro de eventos Anti-tampering para poder ser monitoreados y analizados por una plataforma o SIEM externo.
- El agente o software deberá ser capaz de co-existir en entornos desplegados que ya contengan políticas de seguridad y tráfico pre-existentes en el sistema operativo, escenarios comunes:
 - Hosts orquestados por Kubernetes
 - Soluciones que hagan uso del Firewall de Host, ej. EDR.



- El software/agente deberá soportar su instalación como mínimo en los siguientes sistemas operativos/plataformas:
 - IBM AIX 7.1 TL4 o posterior
 - Amazon Linux 2016 o posterior
 - Red Hat Enterprise Linux (RHEL) 5.0, 6.2, 7, 8, 9 o posterior
 - CentOS 6.2, 7, 8
 - CentOS Stream 8, 9
 - Rocky Linux 8, 9
 - Alma Linux 8, 9
 - Oracle Linux 6.2, 7, 8, 9 o posterior con Kernel RedHat
 - Oracle Linux 5.8, 6.2, 7, 8, 9 o posterior con Kernel Unbreakable (UEK)
 - Debian 7 o posterior
 - Solaris 10 U8, 11.1 o posterior (Arquitectura x86 y SPARC 64 bit)
 - SUSE Linux (SLES) 11 SP3, 12, 15 o posterior
 - Ubuntu LTS 12.04 o posterior
 - Ubuntu Non-LTS 20.10 o posterior
 - Windows Server 2003 SP1, SP2
 - Windows 2008 SP1, SP2
 - Windows 2008 R2 SP1 o posteriores
 - Windows 7 o posteriores
 - MacOS 11 o posteriores
- La consola deberá generar en todo momentos registros de auditoria y trazabilidad de los eventos operativos, administrativos, así como los generados por los agentes instalados en las cargas de trabajo.
- Deberá contar con paneles gráficos o Dashboards que permitan saber la situación y estado de la plataforma ZTS con respecto a:
 - Estado y modo de protección de las cargas de trabajo protegidas, versiones del agente, sistemas operativos, cantidad de políticas definidas
 - Estado situacional y superficie de exposición al ransomware sobre puertos y protocolos inseguros, aplicaciones y servicios inseguros.
- Deberá permitir la creación de reportes calendarizados bajo las siguientes categorías:
 - Sumario Ejecutivo
 - Reporte detallado por aplicativo deseado
 - Reporte de hits de reglas
 - Exportación de tráfico
 - Reporte de exposición al ransomware.

5.2.1.5.4.1.22 SOLUCION DE RETROALIMENTACION (FEEDS) DE CIBERINTELIGENCIA DE AMENAZAS, INTEGRADA A LOS DISPOSITIVOS DE PROTECCIÓN PERIMETRAL

Se debe proveer de una solución de software que permita recibir retroalimentación de Indicadores de compromiso (IoC) de amenazas informáticas. Estas deberán poder integrarse a los dispositivos firewalls perimetrales, optimizando así las capacidades de detección y respuesta de amenazas en dichos dispositivos de protección perimetral. Asimismo, la presente solución de propósito específico (Feeds de Inteligencia), tiene como objetivo maximizar y potenciar el enriquecimiento de indicadores de compromiso.

Requerimientos Generales

- El fabricante de la solución debe tener un representante local o distribuidor en el país que opere localmente durante al menos 10 años.
- El fabricante debe proporcionar soporte técnico 24x7.
- El fabricante de la solución debe contar con la certificación ISO 9001-2011.
- El fabricante de la solución debe cumplir con la certificación ISO / IEC 27001: 2013.

Capacidad de despliegue de casos de uso

- La solución debe prevenir contra brechas de datos confidenciales mediante la aplicación de IoC conocidas de feeds de reputación de IP y hashes maliciosos.
- La solución debe prevenir el fraude mediante la aplicación de IoC conocidas de feeds de reputación de IP, hashes maliciosos, Botnet C&C URL.
- La solución debe reconocer amenazas internas mediante la aplicación de IoC conocidas de feeds de URL maliciosas, URL de phishing.
- La solución debe ser capaz de detectar incidentes de Ransomware mediante la aplicación de IoC conocidas de feeds de URL de Ransomware.
- Los requisitos previos incluyen fuentes de registro relevantes configuradas para proporcionar datos a tecnologías SIEM y los logs enviados a la solución especializada de feeds del fabricante, implementados dentro de la infraestructura local.

Requerimientos funcionales

Los feeds de datos de amenazas (TDF) deben proporcionar información actualizada sobre los objetos más frecuentes y peligrosos, específicamente:

- La solución debe proporcionar información sobre amenazas activas durante los últimos 2 meses como mínimo.
- La solución debe proporcionar información desde la perspectiva global del fabricante de antimalware.
- La solución debe utilizar una red global de sensores como fuente de inteligencia para los feeds.
- La solución debe proporcionar información en JSON, exportable en formatos CSV, OpenIOC o STIX.
- La solución debe proporcionar información a través de protocolos de comunicación seguros (por ejemplo, HTTPS) con autenticación basada en certificados.
- La solución debe proporcionar información contextual adicional.

La solución debe proporcionar información en las siguientes categorías como mínimo

- El feed de reputación IP debe cumplir con los siguientes requisitos:
 - La solución debe proporcionar una frecuencia de actualización promedio inferior a 1 hora.
 - La solución debe proporcionar más de 70,000 registros.
 - La información se proporcionará con un contexto adicional que incluya popularidad, geolocalización, categoría, puntaje de amenaza, etc.
 - Las categorías deben incluir al menos lo siguiente: IP maliciosa, IP de spam, nodo de salida TOR, VPN, proxies.
- El feed de URL maliciosas debe cumplir con los siguientes requisitos:
 - La solución debe proporcionar una frecuencia de actualización promedio inferior a 1 hora;
 - La solución debe proporcionar más de 60,000 registros.
 - La información se proporcionará con un contexto adicional que incluya popularidad, geolocalización, direcciones IP principales, máscara o URL, etc., si esta información está disponible en la base de datos del fabricante.



- El feed de URL de suplantación de identidad debe cumplir con los siguientes requisitos:
 - La solución debe proporcionar una frecuencia de actualización promedio inferior a 1 hora.
 - La solución debe proporcionar más de 100,000 registros.
 - La información se proporcionará con un contexto adicional que incluya popularidad, geolocalización, direcciones IP principales, máscara o URL, etc.
- El feed de Botnet C&C URLs debe cumplir con los siguientes requisitos:
 - La solución debe proporcionar una frecuencia de actualización promedio inferior a 1 hora.
 - La solución debe proporcionar más de 200,000 registros.
 - La información se proporcionará con un contexto adicional que incluya popularidad, geolocalización, direcciones IP principales, máscara o URL, etc.
- **Requisitos de estructura de datos:**
 - La solución debe incluir indicadores de amenazas de diferentes tipos: hashes; IP con la reputación correspondiente; URLs; URL comodín; URL que contienen scripts con parámetros específicos; URL que cubren el contenido de la carpeta con subcarpetas, Dominios y subdominios.
 - La solución debe tener la capacidad de entregar indicadores de amenaza de URL / Dominios como reglas de Snort / Suricata.
 - La solución debe proporcionar un período de actualización de IoC de no más de 8 horas.
- **Requisitos de arquitectura:**
 - La solución debe incluir un módulo de detección en tiempo real que realice el escaneo de logs en conjunto con SIEM, lo que implica la normalización de la URL, la comparación y match con los feeds y la creación de un evento con información de contexto del feed en el SIEM en caso de una coincidencia.
 - La solución debe poder integrarse con marcas SIEM conocidas y sistemas desarrollados a medida similares a SIEM (desarrollo propio o personalizado), que incluyen los siguientes: Alien Vault, MicroFocus ArcSight, IBM QRadar, Splunk, LogRhythm y RSA NetWitness.
 - La solución debe poder integrarse con marcas conocidas de Threat Intelligence Platform, incluidas las siguientes: ThreatQ, Threat Connect, Anomali, MISP, EclecticIQ.
 - La solución debe poder escanear entradas personalizadas, como retro-logs.
 - La solución debe poder proporcionar un motor de correlación externo para los feeds de datos, que debe funcionar sin acceso a Internet.
 - La solución debe tener capacidades para admitir fuentes de datos adicionales de OSINT y otros proveedores comerciales en formatos comunes (STIX a través de TAXII, CSV, JSON).
 - La solución debe tener capacidades para admitir fuentes de logs personalizadas para recibir eventos a través del protocolo TCP para el matching.
 - La solución debe tener la capacidad de crear cuentas para usuarios con al menos dos roles: administrador para cambiar la configuración, analista para trabajar con las características de la solución sin la capacidad de reconfigurarla.
 - Los paquetes de instalación de la solución deben estar disponibles tanto para Windows como para plataformas Linux.



- La solución debe tener una interfaz web para la configuración y el monitoreo.

Servicio de Ciberseguridad Ofensiva

El servicio debe realizar una prueba de seguridad ofensiva que ejecute un ciber ataque real en un entorno controlado. El objetivo es identificar las debilidades que podrían ser aprovechadas por un atacante externo y completar así amenazas de tipo robo de información, acceso indebido, provocar caídas de servicios, instalación de malware, entre otros. Asimismo, tiene como funcionalidad emular el escenario de ataque real de un atacante desde el punto de vista OFENSIVO, con el objetivo de explotar las vulnerabilidades descubiertas, operando en un entorno controlado.

El servicio deberá cubrir el siguiente alcance:

- ✓ Servidores Web publicados: 10
- ✓ Direcciones IP externas: 10
- ✓ Cantidad de ejecuciones de análisis: 2 veces por año y un re-test a los 3 meses después de cada ejecución.

El contratista debe brindar el servicio haciendo uso de plataformas de software profesional licenciadas. (No se aceptará el uso de plataformas Open Source como Kali Linux, nmap, o versiones limitadas (trial) de herramientas de seguridad ofensiva). El lanzamiento de ataques debe ser desde fuera de la red hacia los activos de acceso público, como sitios web organizacionales, recursos web compartidos de archivos o servicios alojados en la nube pública.

La tecnología debe contener como mínimo las siguientes características:

Arquitectura del sistema

- La solución propuesta debe ofrecerse como un Producto de software y deberá poder ejecutarse en una plataforma x86 general.
- La solución propuesta debe contar con una arquitectura de sistema unificado y una interfaz de usuario de management para realizar pruebas de ataques reales (pruebas de penetración) y pruebas de ataques simulados (emulación cibernética del adversario).
- La solución propuesta debe admitir un proceso totalmente automatizado que pueda minimizar el comportamiento de un hacker real para escanear/descubrir las exposiciones de la superficie de ataque de los objetivos, las vulnerabilidades del sistema y luego explotar automáticamente las vulnerabilidades del sistema para validar el riesgo real de los objetivos.
- La solución propuesta debe tener una arquitectura escalable para realizar escaneos de sistemas/redes a gran escala y creación de perfiles de activos, descubrimiento de vulnerabilidades y extracción de bases de conocimientos, auto-explotación de vulnerabilidades, post-explotación y priorización, e informes de riesgos.
- La solución propuesta debe permitir como mínimo 4 niveles de control de nivel sigiloso para tareas de pruebas de penetración, que incluyen: modo sigiloso, modo intermedio, modo normal y modo ruidoso.

Instalación

- La solución propuesta debe poder ejecutarse en una plataforma x86 general y deberá estar montada sobre un sistema operativo de 64 bits.
- La solución propuesta debe poder implementarse en servidores bare metal y en entornos virtuales VMware y Microsoft Hyper-V.
- La solución propuesta debe poder implementarse en plataformas de nube populares, por ejemplo, Amazon Web Service, Microsoft Azure y Google Cloud Platform.

Performance

- La solución propuesta debe utilizar la capacidad de multiprocesamiento simétrico de la plataforma de servidor x86 para aumentar el rendimiento de un servidor independiente.



- La solución propuesta debe poder ejecutar múltiples instancias de bot de software en un servidor y cada instancia de bot puede ejecutar sus propias tareas de prueba para mejorar el rendimiento general del sistema.
- La solución propuesta debe contar al menos con 100 instancias de bot simultáneas en el servidor si la configuración del hardware del servidor lo permite. La cantidad de instancias de bot permitidas se basará en los recursos informáticos del servidor.

Cobertura de Pruebas de Penetración

- La solución propuesta debe permitir la arquitectura de complementos para el descubrimiento y la explotación de vulnerabilidades, y la base de conocimientos del complemento debe ser 100% local y puede actualizarse fuera de línea en entornos donde el acceso a Internet no esté disponible.
- La solución propuesta debe permitir un entorno de TI más amplio, las plataformas Target compatible debe incluir hosts de servidores, servidores web, sistemas de gestión de contenido web, servidores de aplicaciones, sistemas de gestión de bases de datos, equipos de red, equipos de IoT, equipos SCADA, etc.
- La solución propuesta debe tener una base de conocimiento de plugins de vulnerabilidad/explotación con más de 35.000 técnicas de penetración agregadas (plugins).
 - ✓ Cada plugin debe incluir puntuación CVSS, vector CVSS e información del número CVE si está disponible
 - ✓ Cada plugin debe contar con un nivel de gravedad de vulnerabilidad y un nivel de control de riesgo de explotación asociado.
 - ✓ El nivel de severidad del plugin deberá ser Alto, Medio, Bajo e Informativo
- La solución propuesta debe permitir la agregación de plugins de vulnerabilidades/exploits desarrollados por el usuario.
- La solución propuesta debe permitir el modo de intervención del usuario y tener registros de ataques para pruebas de penetración de alto impacto.
- La solución propuesta debe contar con la capacidad de descubrimiento de activos y superficies de ataque sin necesidad de licencia. El usuario puede usarlo para descubrir la infraestructura de TI e identificar activos críticos y superficies de ataque de puerto abierto del servidor y superficies de ataque de URL del sitio web.
- La solución propuesta debe contar con plantillas predefinidas con los siguientes Casos de Uso: WebSite Penetration, Intranet Penetration, Host Penetration, Ransomware Penetration, Weak Password Bruteforce, como mínimo, simplificando la operación de pentest para los administradores de sistemas.
- La solución propuesta debe contar con el Caso de Uso de pruebas de penetración de Ransomware y deberá simular técnicas populares de intrusión de Ransomware para explotar y validar los riesgos de los sistemas Target ante posibles ataques de Ransomware.
- La solución propuesta debe contar con el tipo Host Scan y el tipo Web Scan y el administrador del sistema podrá configurar los parámetros de red (por ejemplo, rango de puertos, método de escaneo) y parámetros de Crawling (por ejemplo, modo crawler, profundidad de URL, política de páginas 404, filtro de sufijo, filtro URL, Lista blanca de URL) para trabajos de escaneo.
- La solución propuesta debe ser capaz de realizar pruebas de penetración de Sitios Web con autenticación. Para sitios web no estándar, la solución propuesta proporcionará una utilidad de registro de secuencia de Logins en sitios web que se pueda utilizar para Logins automáticos en sitios web no estándar durante una tarea de prueba.
- La solución propuesta debe contar con la opción Web Scan tanto para páginas web estáticas como para páginas web dinámicas para el descubrimiento de vulnerabilidades y la validación de riesgos.



- La solución propuesta debe tener un modo inteligente para el escaneo Web. El sistema debe seleccionar automáticamente Crawling de páginas web dinámicas o Crawling de páginas web estáticas en función del Framework utilizado por el sitio web objetivo.
- La solución propuesta debe soportar el uso de Bypass de contraseñas de Sitios Web y debe descubrir superficies de ataque de sitios web protegidos con contraseña.
- La solución propuesta debe permitir al administrador del sistema configurar el modo proxy para Crawling inteligente.
- La solución propuesta debe tener la capacidad de búsqueda de plugins de vulnerabilidades/exploits en su interfaz de usuario web.
- La solución propuesta debe contar con integración con un scanner VA (Vulnerability Assessment) de terceros y tendrá una plantilla de tareas dedicada para validar los resultados del escaneo. Como mínimo deberá soportar: Tenable Nessus Pro, Rapid7 Nexpose.
- La solución propuesta debe realizar ataques de fuerza bruta a los siguientes servicios: DB2, FTP, Microsoft SQL Server, MySQL, PostgreSQL, RDP, Redis, Microsoft SMB, SNMP, SSH, Telnet, Web User Login, VNC, InfluxDb, Vmware. ESXi, Weblogic, Drupal, Joomla, Apache CouchDB, Apache Tomcat, Apache ActiveMQ, Apache Axis2, RabbitMQ, SonarQube, como mínimo.
- La solución propuesta debe permitir credenciales personalizadas e importación de diccionarios para ataques de fuerza bruta.
- La solución propuesta debe ayudar al usuario a cumplir con los estándares OWASP Top-10 (2017 y 2021), ISO27001 y PCI-DSS.

Explotación de vulnerabilidades

- La solución propuesta debe realizar la explotación automática de vulnerabilidades y debe poder mostrar el progreso de la explotación en tiempo real desde la interfaz de administración.
- La solución propuesta debe permitir al administrador del sistema configurar la explotación según el tipo de sistema operativo, niveles de severidad de la vulnerabilidad, niveles de control del riesgo de explotación y Keywords definidas por el usuario.
- La solución propuesta debe permitir al administrador del sistema desactivar la funcionalidad de explotación automática para proporcionar más flexibilidad en el control de riesgos.
- La solución propuesta debe contar con un plugin de exploit individual basado en la configuración del administrador del sistema en la interfaz de administración web.
- La solución propuesta debe permitir visualizar la topología de ataque del entorno del objetivo con al menos 5 capas de información durante la explotación. Debe incluir: Dirección IP del target, Servicio, Superficie de ataque, Vulnerabilidad y el riesgo del negocio.
- La solución propuesta debe permitir visualizar toda la secuencia del Kill Chain de una vulnerabilidad explotada.
- La solución propuesta debe soportar la configuración de Reverse Shell para validar la explotación de la vulnerabilidad RCE (Remote Code Execution).
- La solución propuesta debe estar en la capacidad de soportar la implementación de oyentes persistentes en un nodo designado para permitir que los hosts explotados se conecten nuevamente y validen la filtración de datos.
- La solución propuesta debe proporcionar pruebas de una explotación exitosa, incluidas Snapshots de bases de datos, WebConsole Outputs, directorios de FileSystem y credenciales.
- La solución propuesta debe proporcionar validación con un solo clic para revalidar la vulnerabilidad y la solución.



- La solución propuesta debe proporcionar una funcionalidad de limpieza del seguimiento de ataques con un solo clic.

Movimiento Lateral -Post explotación

- La solución propuesta debe realizar movimiento lateral post-explotación y utilizar un activo comprometido como pivot para descubrir y explotar activos adicionales en redes adyacentes.

Priorización de Riesgo en el negocio

- La solución propuesta debe calcular el riesgo del sistema objetivo basado en el impacto de la vulnerabilidad explotada y la información del Kill Chain.
- La solución propuesta debe poder calcular la puntuación de salud (Health Score) total del sistema objetivo basado en la cantidad de superficies de ataque encontradas, los números y severidad de las vulnerabilidades y los riesgos, así como el Rate de conversión de las superficies de ataque en vulnerabilidades y de las vulnerabilidades en riesgos.

Gestión de Vulnerabilidades

- La solución propuesta debe contar con una plantilla de tareas dedicada para identificar y documentar la exposición de la superficie de ataque de las máquinas objetivo.
- La solución propuesta debe permitir la priorización de vulnerabilidades basada en riesgos, proporcionar una tabla de riesgos simple, de riesgo de alta prioridad que el usuario necesita mitigar lo antes posible.
- La solución propuesta debe contar con información detallada para cada vulnerabilidad descubierta, como mínimo debe contar con: tipo de vulnerabilidad, severidad, el Score CVSS (Common Vulnerability Scoring System), vector CVSS, descripción, solución, el enlace de referencia, así como la máquina target vulnerable y la superficie de ataque y ruta de ataque para esta vulnerabilidad. La solución también debe proporcionar una herramienta de validación de vulnerabilidades que ayude al usuario a revalidar la vulnerabilidad después de parchar el software.
- La solución propuesta debe proporcionar información detallada para cada riesgo validado, incluyendo: el tipo de riesgo, la máquina del target comprometido y su versión del sistema operativo, la superficie de ataque comprometida, la ruta de ataque, privilegios de usuario y el tipo de shell que el hacker puede obtener.
- La solución propuesta debe proporcionar un informe de prueba que incluya información de riesgo sobre el Kill Chain que el usuario pueda utilizar para mitigarlo.
- La solución propuesta debe proporcionar informes históricos y de tendencias para el score de salud de las máquinas target, el número total de riesgos, el número total de vulnerabilidades, el número total de superficie de ataque y la lista de riesgos de pruebas anteriores.
- La solución propuesta debe proporcionar informes comparativos para evaluar los cambios en la postura de seguridad de las máquinas de destino a lo largo del tiempo. Estos informes comparativos deberán permitir comparar como mínimo los siguientes cambios: Puntuación de salud, diferencia de riesgo del negocio, vulnerabilidad y exposición de la superficie de ataque de dos pruebas de validación de seguridad.

Gestión de Activos

- La solución propuesta debe contar con una base de datos centralizada para gestionar los activos de TI para la validación de la seguridad. Los activos administrados deben incluir información de la versión del sistema operativo, puertos abiertos del servidor e información de aplicaciones activas, sitios web e información de aplicaciones, nombres de dominio y direcciones IP.

Integración con APIs

- La solución propuesta debe soportar API RESTful para la integración de sistemas de terceros.



- La solución propuesta debe permitir la autenticación basada en tokens para API.

Administración

- La solución propuesta debe contar con una consola de administración local para una configuración segura del sistema, por ejemplo reset de passwords, reinicio del proceso del sistema, y apagado/reinicio del servidor.
- La solución propuesta debe contar con una interfaz de usuario de gestión basada en Web sobre tráfico cifrado. No será permitido el acceso en texto claro.
- La solución propuesta debe contar con autenticación de doble factor (2FA) para el inicio de sesión de los usuarios web.
- La solución propuesta debe permitir actualizaciones en línea para el sistema y la base de conocimientos sobre vulnerabilidades/exploits cuando esté disponible el acceso a Internet.
- La solución propuesta debe actualizar el sistema y la base de conocimientos sobre vulnerabilidades/exploits en un entorno donde no hay acceso a Internet disponible.
- La solución propuesta debe contar con control de acceso basado en roles para que los operadores del sistema realicen diferentes tareas, por ejemplo, crear nuevas tareas de pentest, sistema/backups, revisar logs del sistema, etc.
- La solución propuesta debe realizar copias de seguridad manuales y automáticas para configuraciones de tareas de pruebas de penetración y bases de datos/logs del sistema.
- La solución propuesta debe permitir al administrador del sistema configurar notificaciones de correo electrónico y syslog, para tareas de pruebas de penetración.
- La solución propuesta debe enviar syslogs compatibles con CEF para integrarse con SIEM u otras plataformas de gestión centralizada.
- La solución propuesta debe poder integrarse con plataformas populares DevSecOps, Jira Cloud, Jira Data Center, ServiceNow y GitLab, para problemas de seguridad y seguimiento de errores.
- La solución propuesta debe respaldar al GDPR y el cumplimiento de la privacidad de datos en todo el mundo.

Reportes y exportación

- La solución propuesta debe brindar un informe integrado para los resultados de las pruebas de penetración.
- La solución propuesta debe brindar informes estándar y admitir funciones de informes personalizados para diferentes usuarios, por ejemplo, ejecutivo, operador de TI, operador de SOC, etc.
- La solución propuesta debe brindar informes estándar que prioricen los riesgos del negocio sobre las vulnerabilidades.
- La solución propuesta debe proporcionar un informe estándar de vulnerabilidades, mostrando los riesgos con detalles del Kill Chain e información general del estado de salud del sistema.
- La solución propuesta debe contar con un informe estándar para los resultados de la elaboración de perfiles de activos, incluidos los fingerprints del sistema.
- La solución propuesta debe contar con una plantilla de informe de superficie de ataque para informar todas las superficies de ataque públicas expuestas de los sistemas objetivo.
- La solución propuesta debe contar con plantillas de informes de cumplimiento OWASP Top-10:2017 y OWASP Top-10:2021 para tareas de pruebas de penetración web.
- La solución propuesta debe contar con múltiples formatos de informes, incluidos, entre otros, PDF, HTML y CSV.
- La solución propuesta debe tener soporte en varios idiomas para los informes, como mínimo deberá contar con: Inglés, italiano, español y coreano.

- La solución propuesta debe permitir al cliente agregar el logotipo de la entidad en la portada de los informes pentest.
- La solución propuesta debe poder cifrar el informe de prueba de penetración antes de descargarlo de la interfaz para proteger los datos confidenciales del usuario en el informe.
- La administración de todas las soluciones y equipamiento solicitado por la Entidad, serán de administración compartida, en ese sentido, el contratista entregará credenciales de usuarios a nivel de read/write a usuarios designados por la Entidad. El contratista está obligado a considerar todos los componentes, dispositivos y materiales que requiera para la integración de la solución adquirida con la red de la Entidad, así como para el cumplimiento de la finalidad del servicio requerido.

5.2.1.5.4.1.23 ADECUACION DEL DATACENTER (SEDE MININTER)

El contratista deberá adecuar el Datacenter (Sede Mininter – Sala de comunicaciones y Seguridad) para el óptimo funcionamiento de los servicios de la información de la PNP y cumplir los siguientes requisitos mínimos:

- Mantenimiento de pozos a tierra existentes.
- Acondicionamiento de aire acondicionado para sala de comunicaciones y seguridad.
- Acondicionamiento de tablero general existente para energización de equipamiento
- Provisión de piso técnico
- Pintado de paredes con pintura látex satinado y acabado con pintura Ignífuga P-25, retardante a fuego.
- Provisión de luminarias necesarias y luminarias de emergencia.
- Provisión de control de acceso.
- Provisión de tablero eléctrico.
- Provisión de sistema antiincendios.
- Provisión de 04 gabinetes de 42UR con PDU, bandeja, ventilador Cooler, barra a tierra de las dimensiones necesarias para el acondicionamiento de la solución a plantear por el Contratista.
- Provisión de bandejas portacable.

Adicionalmente, el contratista deberá brindar el soporte del sistema de aire acondicionado de la sala de servidores ubicada en el Datacenter Principal (Sede MNINTER) durante la vigencia del contrato.

5.2.1.5.5 COMPONENTE 5. SERVICIO DE SMS PARA NOTIFICACIONES DE LA PNP

El objetivo de este servicio es proporcionar a la Policía Nacional del Perú (PNP) una solución integral de gestión de identidad y autenticación que garantice la seguridad y el acceso controlado a los sistemas de la institución. La solución deberá incluir los siguientes componentes

DEL SERVICIO DE MENSAJERÍA SMS PARA NOTIFICACIONES DE LA PNP

Condiciones Generales.

- Se deberá proveer el servicio de envío de mensajes cortos de texto (SMS), de manera ilimitada para soluciones de gestión de identidades y autenticación.

- La bolsa de mensajes SMS deberá estar disponible para el consumo a demanda sin restricción
- La bolsa de mensajes de SMS permitirá la remisión masiva de información de seguridad a los usuarios
- El mensaje corto de texto (SMS) debe tener una capacidad de envío de hasta 160 caracteres por mensaje
- El mensaje corto de texto (SMS) no deberá tener fecha de caducidad (autoeliminación)

Condiciones específicas

- El servicio requerido deberá permitir envíos a todos los operadores de telefonía móvil del Perú.
- El servicio de mensajes cortos de texto (SMS) no incluye servicios de valor agregado. Además, se precisa que la entidad no asumirá costo adicional por este tipo de servicio
- Se encuentran excluidos los envíos de mensajes a números en zonas rurales con señal satelital a nivel local y nacional, así como también los destinos internacionales.
- El contratista debe cumplir con todas las disposiciones regulatorias que conducen a salvaguardar el secreto de las telecomunicaciones.
- El contratista garantizará el envío del sms al operador del usuario final, asimismo, proporcionará herramientas o similares que permitan verificar envíos y recepciones del sms.

De la herramienta de administración del servicio contratado

El proveedor proporcionará cuentas de administración para el acceso a una página web para que se puedan acceder al control y consultas del servicio contratado durante la ejecución contractual.

- Debe permitir el envío masivo de SMS mediante uso de bases de datos (Excel, CSV)
- Debe permitir generar y exportar reportes de respuesta y de entrega. Se aceptará el envío de reportes mediante correo electrónico.
- Debe permitir conocer el consumo del servicio
- Debe permitir realizar el tracking de las campañas
- Debe permitir gestionar la palabra clave para la recepción de respuestas por SMS. Se aceptará que la gestión de la palabra clave podrá realizarse mediante correo electrónico.
- Debe generar los reportes de consumo diario, semanal y mensual.

De la integración mediante interfaz de programación de aplicaciones (API)

Condiciones específicas

- Debe incluir una conexión directa mediante uso de Web Services, API SOAP o REST, la misma que deberá ser establecida mediante mecanismos de autenticación de usuario y dirección IP pública para garantizar la seguridad de acceso
- Debe permitir la automatización de procesos, así como el consumo de:
 - Método de envío de SMS
 - Método de estado de entrega de SMS
 - Método de recepción de SMS
- El servicio Web o API, debe ser compatible con las plataformas de desarrollo disponibles en el mercado
- Deberá ejecutarse la integración que garantizará la operatividad con los sistemas de la PNP, la entidad proporcionará la información requerida al contratista sobre los sistemas con los que cuenta la entidad, a fin de realizar la integración requerida, el contratista

debe proveer el o los API, acompañamiento, soporte y la documentación técnica y funcional. La integración es por parte de personal de la entidad.

- Con la finalidad de una mejor administración del servicio, debe permitir la configuración de un campo de bloqueo de nuevos envíos por el tiempo de periodo que determine la Entidad
- El contratista es libre de brindar servicios como mejora que cumpla con todas las especificaciones solicitadas en el COMPONENTE 5. Dicha mejora deberá ser probada mediante una prueba de concepto para comprobar que cumpla con las necesidades y objetivos de la entidad.

5.2.1.5.6 COMPONENTE 6: SERVICIO DE HOUSING PARA EL DATACENTER SECUNDARIO PNP

5.2.1.5.6.1 HABILITACIÓN DE LOS SERVICIOS DEL DATA CENTER SECUNDARIO.

- El servicio a contratar comprende la provisión de infraestructura de Centro de Datos (housing) y pase a producción de los servicios críticos de la PNP a un Datacenter secundario.
- La Mudanza de los equipos desde el Datacenter secundario de la PNP ubicados en el actual Housing (local del actual proveedor) hacia el Datacenter Secundario propiedad del CONTRATISTA (no rentado a terceros), es responsabilidad del contratista, el cual debe asegurar la desinstalación, transporte, seguros, instalación y otros que crea necesario para cumplir con lo solicitado en los términos de referencia. En caso el equipamiento de la entidad se dañe o pierda alguna información en el proceso de mudanza, el contratista será responsable de ello, por lo que debe considerar las contingencias necesarias (backups de información del equipamiento a trasladar), siempre y cuando el equipamiento tecnológico cuenta con soporte activo por parte de la entidad.
- El contratista debe proveer el seguro correspondiente para el traslado de los equipos de cómputo del sitio secundario actual al Datacenter propuesto por el contratista.
- El contratista debe realizar el apagado de los equipos de cómputo siguiendo el procedimiento que corresponda según la plataforma, desinstalar, embalar y trasladar al Datacenter del contratista, luego recibir, desembalar, instalar, encender y poner en funcionamiento el Datacenter secundario de la PNP propiedad del CONTRATISTA (no rentado a terceros).
- El RTO máximo debe ser de veinticuatro (24) horas.
- Habilitación del Datacenter secundario de la PNP, incluyendo el servicio de provisión de Infraestructura base necesaria para recibir y alojar los equipos de propiedad de la PNP. (El término "infraestructura base" es referido a los commodities que se requieren para el funcionamiento de un Centro de Cómputo o Datacenter y son parte del servicio esencial de un Datacenter de acuerdo a los estándares requeridos).
- El contratista deberá garantizar la disponibilidad y la continuidad del servicio requerido en el suministro de los medios indispensables para el funcionamiento del Datacenter secundario PNP propiedad del CONTRATISTA (no rentado a terceros), tales como suministro eléctrico estabilizado en alta disponibilidad, climatización del ambiente del Datacenter en alta disponibilidad, así como controles de acceso físico al Datacenter y sistemas contra incendios. Asimismo, esta exigencia se interpretará dentro de los parámetros de calidad establecidos y/o aceptados por OSIPTEL y el MTC, según corresponda.
- El contratista deberá atender los requerimientos de la Entidad en cuanto a provisión de equipamiento de cómputo, líneas de datos, entre otros necesarios para funcionalidad de los sistemas y servicios de la Entidad.
- Activación de los servicios de la PNP en el Centro de datos secundario.



- El contratista deberá proveer el servicio contratado de un Data Center secundario.
- El Data Center provisto debe contar con las siguientes características mínimas:
 - ✓ Proveer un sistema de energía ininterrumpida redundante.
 - ✓ Proveer los sistemas de instrumentación y control de procesamiento de datos (sensores de los sistemas de seguridad del Data Center).
 - ✓ Proveer un sistema de climatización de precisión para los equipos alojados, el cual debe ser redundante.
 - ✓ Proveer de los circuitos y enlaces de comunicación internos requeridos para el funcionamiento de las aplicaciones de PNP.
 - ✓ Proveer de seguridad de acceso físico al Centro de Datos el cual debe considerar una bitácora de acceso.
 - ✓ El contratista se obliga a efectuar la configuración, monitoreo y mantenimiento de los equipos del Datacenter secundario.
 - ✓ Las instalaciones del proveedor tendrán las siguientes características mínimas:

Edificación	Características de seguridad para protección contra actos vandálicos.
	Contar con una sala de Operadores, Sala de Equipos de Cómputo y ambientes de energía independientes.
	Sala de equipos de cómputo con falso piso, que considere el uso de baldosas perforadas o con rejilla que direccionen eficientemente el flujo del aire acondicionado
	Los accesos a la sala de equipos de Cómputo deben contar con un sistema automatizado de seguridad
	Contar con un sistema de cámaras de video de seguridad y su respectivo videograbador.
	Equipos UPS configurados en un esquema de "Alta Disponibilidad" del tipo N+1. Debe contar con un sistema de baterías redundantes. Debe contar con transformadores de aislamiento redundantes.
	Grupo electrógeno configurado en un esquema de "Alta Disponibilidad", que garantice la continuidad de data center secundario, ante interrupciones eléctricas. La transferencia o pase a operación del grupo electrógeno debe ser automática
	Debe contar con un sistema de aire acondicionado de precisión redundante, que garantice el enfriamiento estándar según las buenas prácticas.
Redes	Contar con un sistema de detección y extinción de incendios.
	Capacidad para proveer la infraestructura interna de comunicaciones para acceder desde sus Data Center a la WAN de la PNP. Capacidad en su infraestructura interna para incorporar durante el servicio contratado nuevos enlaces de cobre o fibra óptica que la PNP adquiera. Durante la prestación del servicio se debe contar con la capacidad de poder ampliar hasta en 02 enlaces de cobre y 04 enlaces de fibra, o hasta 06 enlaces de fibra.
	Las instalaciones deben tener facilidades para que múltiples proveedores de enlaces de datos provean servicios a la PNP.
Seguridad física	En la data center secundario se instalarán las cabeceras MPLS o MetroEthernet e inforternet requeridos en el componente 3 y 1, a fin de garantizar la conexión a la red privada de la PNP e INTERNET respectivamente.
	El CONTRATISTA será responsable de proteger el Centro de Datos secundario contra accesos no autorizados, actos vandálicos, fraude o robo, a todos los



	servidores y dispositivos de infraestructura de propiedad de la PNP o que le den el servicio.
	El CONTRATISTA debe realizar los controles de seguridad físicas en sus instalaciones.
	Se debe facilitar a PNP, su(s) representante(s) y/u organismos reguladores o de fiscalización, el acceso a las instalaciones y activos de uso exclusivo para la provisión de los servicios contratados, en casos de auditorías, investigaciones e inspecciones de verificación de cumplimiento de las condiciones del servicio. Estos accesos serán informados, autorizados y acordados con la PNP.

Servicio de Gestión de Requerimientos e Incidencias

A continuación, se establecen tiempos de respuesta (atención) para requerimientos e incidencias. El tiempo de resolución dependerá de la complejidad del requerimiento y/o incidente, no se comprometen tiempos de resolución.

Atención de Requerimientos:

- ✓ Las solicitudes de la Entidad son aquellas peticiones que implican gestión de cambios. En general se considera que existen labores de "gestión de cambios" en aquellas solicitudes de la Entidad que tienen las siguientes características:
- ✓ El trabajo solicitado debe ser ejecutado por el personal con perfil de administrador o de técnico especialista.
- ✓ Para la gestión de cambios se acordará e implementará un procedimiento que incluye herramientas y una serie de medidas de control para asegurar que los cambios se están ejecutando de manera eficiente.
- ✓ EL CONTRATISTA brindará al CLIENTE un formato standard de Solicitud de Cambios.
- ✓ Una vez presentada la necesidad del cambio, de la Entidad enviará el formato respectivo indicando los cambios solicitados y adjuntando los datos necesarios. EL CONTRATISTA analizará el requerimiento y evaluará el impacto, de proceder el cambio se ejecutará en coordinación con la Entidad. Se recomienda que la Entidad pruebe los cambios en un ambiente de testing previo al pase a producción. EL CONTRATISTA no se responsabiliza por los daños que estas actualizaciones o modificaciones puedan ocasionar al servicio.

La recepción de cambios es 24x7, sin embargo, las respuestas a la solicitud de cambio están sujetos a un horario de 5x8 (lunes a viernes de 9:00 am a 5:00 pm) para su revisión y aprobación.

Tiempo de respuesta para Requerimientos

Se define como Tiempo de Respuesta para requerimientos al tiempo transcurrido desde el momento en que la Entidad realiza un pedido AL CONTRATISTA y el momento en que el requerimiento ha sido recepcionado y el personal especializado se comunica con la Entidad para informar que el requerimiento ha sido recepcionado para su pronta atención.

Tiempo de respuesta: 2 horas en 8x5

Característica	Descripción
Horario de Atención	Los horarios de atención solicitados son: Gestión de Requerimientos 9:00 am a 5:00 pm (L-V) No aplica para días festivos, ni feriados.

Bolsa de requerimientos mensual:

- El Contratista brindara una bolsa de 10 requerimientos mensual no acumulables, según lo solicitado por la Entidad:
 - ✓ Operaciones básicas:
 - Apagado, encendido y reinicio de equipos
 - Verificación visual de equipos
- Los siguientes requerimientos deben ser solicitados con un plazo mínimo de 24 horas de lunes a viernes (9am a 5pm) para su atención:
 - Ingreso / Salida de equipos.
 - Incorporación de un procedimiento operativo.
 - Visitas o actividades programadas (trabajos de mantenimientos hardware o software)

Atención de Incidencias:

- El tiempo de respuesta se define como el tiempo transcurrido entre el momento en que la Entidad notifica la avería o si la avería es detectada internamente por EL CONTRATISTA y el momento en que un técnico del servicio empieza a trabajar en la resolución del problema y además se realiza la primera comunicación con la Entidad indicando la inicial evaluación y apreciación.
- Cada incidencia está asociada a un nivel de severidad descrito a continuación:
 - Severidad Nivel 1 (Graves): Fallos que involucran una indisponibilidad del servicio, tal como la falla en la conectividad LAN, energía, plataforma.
 - Severidad Nivel 2 (Medias): Fallos que involucran una degradación en la calidad del servicio, tal como la saturación de recursos, atención de servicios a una capacidad menor al 100%.
 - Severidad Nivel 3 (Leves): Fallos que involucran a funcionalidades secundarias del servicio y que no afectan su normal operatividad.
- Estos niveles de severidad servirán a los grupos de operación para priorizar las incidencias y atenderlas en base a los siguientes tiempos de respuesta:
 - Severidad Nivel 1: 30 min. en 7 x 24
 - Severidad Nivel 2: 1 hora en 7 x 24
 - Severidad Nivel 3: 2 horas en 8 x 5 y 4 horas 7 x 24
- Si ante una incidencia se genera un requerimiento de cambio, éste será atendido en el más breve plazo y no será contabilizado como parte de la bolsa de requerimientos.

Servicio de alojamiento de Gabinetes y equipos:

EL CONTRATISTA será responsable de brindar los siguientes servicios del Centro de Datos secundario de la PNP alojados en su Centro de Datos propiedad del Contratista (no rentado a terceros):

- Alojamiento de 06 Gabinetes (42 UR por gabinete como máximo) y equipos de cómputo (Hardware) y aprovisionamiento de suministro eléctrico continuo que garantice la continuidad operativa de los equipos de PNP.
- El contratista proveerá los gabinetes con sus respectivas consolas, PDU y Patch panels necesarios
- EL CONTRATISTA habilitará la energía especial específica para los racks, para un consumo de hasta 42 KVA repartidos entre los 06 Gabinetes (o 7KVA por gabinete)
- EL CONTRATISTA realizará Cableado externo y rackeo de equipos en los gabinetes (por única vez), de forma tal, que se permita la comunicación de datos requeridos
- EL CONTRATISTA brindará los servicios de cableado y acondicionamiento a los Gabinetes

- El CONTRATISTA brindará los Servicios propios de Data Center: Seguridad física, Aire acondicionado de precisión, Energía estabilizada, Grupo electrógeno, Servicio de manos y ojos remotos, (contar con el personal y las herramientas necesarias para las tareas de administración y mantenimiento del data center a proponer), hasta un máximo de 10 operaciones básicas al mes no acumulables.
- El contratista implementara los equipos de comunicaciones y seguridad, destinados para este servicio.
- LA PNP será responsable de la Instalación de sistema operativo y del software en sus equipos.

5.2.1.5.7 COMPONENTE 7: INDUCCION

SE LLEVARÁ EN LAS SIGUIENTES CONDICIONES:

CONDICIONES GENERALES

REUNION DE COORDINACIÓN

- Las fechas de inicio serán coordinadas entre la Entidad y el Contratista, a través del personal responsable por ambas partes, mediante reunión de coordinación que se llevará a cabo en un plazo máximo de quince (15) días calendarios contados a partir del día siguiente de la suscripción del Contrato, para cuyo efecto se suscribirá un Acta de reunión de coordinación.
- El contratista en un plazo de cinco (05) días calendario posteriores a la suscripción del Acta de Reunión de coordinación, entregará el cronograma de inducciones y la relación del personal a cargo de la inducción. Asimismo, adicionalmente a la información solicitada el contratista presentará la acreditación del personal técnico certificado especializado en cada inducción, o autorizado por el fabricante de la plataforma considerada (de ser el caso), a fin de ser evaluado y aprobado por la entidad. La Entidad dará su conformidad u observación al contratista a través de correo electrónico a los diez (10) días posteriores de recepcionado el cronograma.
- En relación a los cursos de inducción técnica y cursos con certificación oficial el contratista mantendrá reuniones de coordinación con la Entidad, a fin de evaluar el inicio de las inducciones por estar supeditadas a la disponibilidad del centro de inducción.
- Cabe señalar que el inicio de la inducción deberá realizarse dentro de los TREINTA (30) días calendarios posteriores a la firma del acta de conformidad por la implementación y puesta en marcha del servicio.
- Las inducciones podrán reprogramarse hasta una (01) vez durante el período de ejecución, siempre y cuando esto sea aceptado por ambas partes

5.2.1.5.7.1 SEGURIDAD DE LA INFORMACION

Consideraciones que deberá atender el contratista para el cumplimiento de las siguientes inducciones:

- Se desarrollará en la ciudad de Lima, en un ambiente que proveerá el contratista y que reúna las condiciones para el dictado de clases teórica-prácticas, con computadora para cada participante, ayudas audiovisuales, documentación teórica y dictado por un instructor certificado por el fabricante de los equipos, la inducción será para cinco (05) personas de la Entidad, cuya relación será proporcionada por la

Sección de Redes y Seguridad Informática del Departamento de Gestión de Centro de Datos DEPGCD-DIVINF-DIRTIC PNP.

- La curricula de inducción será observando el modelo curricular oficial, lo cual debe ser garantizado por el fabricante o su distribuidor local. El período de inducción no será menor a veinticuatro (24) horas.
- El contenido de los cursos y el material didáctico debe corresponder a la versión de la solución mediante la cual se llevará a cabo el servicio. Las inducciones serán dirigidas a nivel técnico, comprendiendo sesiones teóricas prácticas.
- Se debe entregar el material de estudio en formato electrónico (repositorio compartido durante el periodo de ejecución del servicio o USB) o impreso a los participantes y una copia a la Entidad.
- El contratista otorgará Diplomas o constancias de participación, al finalizar todos los cursos, en un plazo máximo de treinta (30) días calendario de finalizada cada inducción.
- Todos los SYLABUS deberán ser entregados antes de la inducción, por el Contratista, para ser validados y aceptado por la Entidad, asimismo este puede ser brindado en la modalidad de presencial o virtual en línea.

Objetivo de los cursos

Proveer de los conocimientos técnicos mínimos necesarios al personal técnico del Sección de Redes y Seguridad Informática del Departamento de Gestión de Centro de Datos -DIVINF-DIRITC PNP, para el aprovechamiento máximo del equipamiento en el presente servicio.

- a. Plataforma de balanceador de enlaces
- b. Plataforma de optimizador de tráfico y traffic shapping
- c. Plataforma de Balanceador de carga de sitios
- d. Plataforma de gestión de identidades
- e. Plataforma de Firewall para sedes policiales
- f. Plataforma de Firewall de próxima generación
- g. Protección de detección y control de malware avanzado
- h. Protección de portales Web y Base de datos
- i. Servicio de SOC Gestionado, Herramienta de Análisis de incidentes y Correlación de logs de seguridad.
- j. Servicios de seguridad de la información

5.2.1.5.7.2 INDUCCION CON CERTIFICACIÓN OFICIAL

Consideraciones de deberá atender el contratista para el cumplimiento de los siguientes cursos:

Debe ser dictado en un Centro de Inducción Autorizado en el dictado de cursos oficiales, siguiendo el modelo de inducción de la currícula oficial, lo cual debe ser garantizado por el Contratista. El contratista entregará los Boucher de los cursos con los nombres proporcionado por la Entidad según el curso y la distribución del área competente que a continuación se detalla:

- 
- 
- 
- 
- 
- 
- a. Curso Oficial de Certificación a nivel asociado o similar en la marca de los equipos routers y/o switches propuestos. Para siete (07) personas, (04 para la Sección de Operaciones y 03 para la Sección Redes y Seguridad Informática del DEPGCD-DIVINF-DIRTIC PNP).
 - b. Curso Oficial de Certificación a nivel profesional o similar en la marca de los equipos routers y/o switches propuestos. Para tres (03) personas, de la Sección de Redes y Seguridad Informática del DPGCD.
 - c. Curso Oficial de Certificación Hacker Ético (CEH, en inglés CERTIFIED ETHICAL HACKER), Para Cinco (05) personas, del Departamento de Gestión Centro de Datos de la División de Informática de la DIRTIC PNP.
 - d. Curso Oficial de Certificación en la plataforma de Protección de portales Web y Base de datos. Para tres (03) personas, de la Sección de Redes y Seguridad Informática del Departamento de Gestión Centro de Datos de la División de Informática de la DIRTIC PNP.
 - e. Curso Oficial de Certificación en la plataforma de Firewall de próxima generación. Para tres (03) personas, de la Sección de Redes y Seguridad Informática del Departamento de Gestión Centro de Datos de la División de Informática de la DIRTIC PNP.
 - f. Curso Oficial de Certificación en el Servicio de SOC Gestionado. Para tres (03) personas, de la Sección de Redes y Seguridad Informática del Departamento de Gestión Centro de Datos de la División de Informática de la DIRTIC PNP.
 - g. Curso Oficial de Certificación en la plataforma de Rendimiento de Aplicaciones. Para tres (03) personas, de la Sección de Redes y Seguridad Informática del Departamento de Gestión Centro de Datos de la División de Informática de la DIRTIC PNP.

5.3 ACTIVIDADES

A. PERSONAL RESIDENTE

Se requiere la atención de un grupo de seis (06) residentes laborando 8x5 para que el contratista pueda brindar una atención adecuada y efectiva en horarios rotativos de lunes a domingo, los cuales serán coordinados entre la PNP y el contratista.

1. 02 Residentes Monitores:

- Técnico, Bachiller o Ingeniero titulado en algunas de las profesiones siguientes: Electrónica o Telecomunicaciones o Electrónica y Telecomunicaciones o Redes o Redes y Comunicación de Datos o Sistemas o Sistemas e Informática o Empresarial y de Sistemas o Informática o Industrial o Telemática o Mecatrónica.
- Constancias o certificados de trabajo que acrediten experiencia mínima de un (01) año en configuración y/o soporte de servicios de redes LAN/WAN y/o servicios de transmisión de voz y/o servicios de transmisión de video y/o servicios de transmisión de internet.
- Curso o Taller en Routing, Switching y/o Seguridad.

2. 02 Residentes Analistas

- Técnico, Bachiller o Ingeniero titulado en algunas de las profesiones siguientes: Electrónica o Telecomunicaciones o electrónica y Telecomunicaciones o Redes o Redes y Comunicación de Datos o Sistemas o Sistemas e Informática o Empresarial y de Sistemas o Informática o Industrial o Telemática o Mecatrónica.
- Constancias o certificados de trabajo que acrediten experiencia mínima de dos (02) años en gestión de Seguridad Informática y/o Seguridad de Información.
- Los residentes deberán contar con al menos una certificación de las siguientes soluciones de seguridad propuestas por el Contratista:
 - o Firewall de nueva generación, para red externa y red interna.
 - o Detección y control de malware avanzado.
 - o Protección de portales web y base de datos
 - o Spam Firewall y protección ante phishing dirigido
 - o Protección contra ataques de denegación de servicios distribuido
 - o Análisis de vulnerabilidades de red
 - o Herramienta informática para prevención de pérdida de información, auditoría y anticorrupción.
 - o Solución de antivirus para servidores y endpoint de la DIRTIC PNP.
 - o Servicio de SOC Gestionado, Herramienta de Análisis de incidentes y Correlación de logs de seguridad.
 - o Servicios de seguridad de la información.

3. 02 Residentes de Remediación

- Técnico, Bachiller o Ingeniero titulado en algunas de las profesiones siguientes: Electrónica o Telecomunicaciones o electrónica y Telecomunicaciones o Redes o Redes y Comunicación de Datos o Sistemas o Sistemas e Informática o Empresarial y de Sistemas o Informática o Industrial o Telemática o Mecatrónica.
- Constancias o certificados de trabajo que acrediten experiencia mínima de tres (03) años en gestión de Seguridad Informática y/o Seguridad de Información.
- Los residentes deberán contar con al menos tres certificaciones de las siguientes soluciones de seguridad propuestas por el Contratista:
 - o Firewall de nueva generación, para red externa y red interna.
 - o Detección y control de malware avanzado.
 - o Protección de portales web y base de datos
 - o Spam Firewall y protección ante phishing dirigido
 - o Protección contra ataques de denegación de servicios distribuido
 - o Análisis de vulnerabilidades de red
 - o Herramienta informática para prevención de pérdida de información, auditoría y anticorrupción.
 - o Solución de antivirus para servidores y endpoint de la DIRTIC PNP.
 - o Servicio de SOC Gestionado, Herramienta de Análisis de incidentes y Correlación de logs de seguridad.
 - o Servicios de seguridad de la información.

4. 01 Residente Líder

- Técnico, Bachiller o Ingeniero titulado en algunas de las profesiones siguientes: Electrónica o Telecomunicaciones o electrónica y Telecomunicaciones o Redes o Redes y Comunicación de Datos

o Sistemas e Informática o Empresarial y de Sistemas o Informática o Industrial o Telemática o Mecatrónica.

- Constancias o certificados de trabajo que acrediten experiencia mínima de cuatro (04) años en gestión de Seguridad Informática y/o Seguridad de Información.
- Certificado oficial en Routing, Switching.
- El residente líder deberá contar con al menos cuatro certificaciones de las siguientes soluciones de seguridad propuestas por el Contratista:
 - o Firewall de nueva generación, para red externa y red interna.
 - o Detección y control de malware avanzado.
 - o Protección de portales web y base de datos
 - o Spam Firewall y protección ante phishing dirigido
 - o Protección contra ataques de denegación de servicios distribuido
 - o Análisis de vulnerabilidades de red
 - o Herramienta informática para prevención de pérdida de información, auditoría y anticorrupción.
 - o Solución de antivirus para servidores y endpoint de la DIRTIC PNP.
 - o Servicio de SOC Gestionado, Herramienta de Análisis de incidentes y Correlación de logs de seguridad.
 - o Servicios de seguridad de la información.

Nota: Se precisa que, para el cálculo del total del tiempo de experiencia mínima solicitada, será considerado el tiempo cuando desempeñaba sus funciones en las áreas indicadas, con el grado de bachiller y/o título profesional.

B. PERSONAL CLAVE (Durante la implementación)

Jefe de Proyecto

Actividades

- Planifica el proyecto en todos sus aspectos, identificando las actividades a realizar, los recursos y los plazos.
- Dirige y coordina todos los recursos empleados en el proyecto.
- Adopta las medidas correctivas pertinentes para remediar las desviaciones que se hayan detectado.
- Evalúa los cambios y riesgos del proyecto
- Coordina con La Entidad respecto a la información requerida.
- Mantenimiento permanente de las relaciones externas del proyecto.

Jefe de Servicio

Actividades

- Identifica las actividades a realizar, los recursos y los plazos.
- Dirige y coordina todos los recursos empleados en el ámbito asignado.
- Adopta las medidas correctivas pertinentes para remediar los imprevistos.
- Evalúa los cambios y riesgos del servicio
- Coordina con la Entidad respecto a la información requerida.

Especialista de Ciberseguridad

Actividades

- Gestionar la Arquitectura de la solución
- Gestionar la solución de incidentes de seguridad informática
- Administrar la plataforma integral de orquestación de seguridad informática

CONDICIONES GENERALES:

El personal que realizará la implementación debe estar certificado por el fabricante de los materiales y/o equipamiento a utilizar, con la finalidad de garantizar el Acuerdo de Nivel de Servicio contratado.

A la entrega del Plan de Trabajo el contratista entrega la lista del personal que realizará los trabajos descritos en los presentes términos de referencia. Este personal debe estar certificado por el fabricante (mediante una declaración jurada o carta simple del fabricante) de los materiales o equipamiento a emplearse.

El personal que asigne el contratista para los trabajos en cada sede deberá emplear uniforme y laborar con sus respectivos implementos de seguridad, de acuerdo con lo requerido en el cumplimiento de la Norma G.050 seguridad durante la construcción.

El Contratista debe contar con un Centro de atención de averías e incidencias, disponible durante la ejecución del servicio.

ACTIVIDADES PARA IMPLEMENTACIÓN

A partir del día de siguiente de suscrito el contrato se inicia el periodo de implementación, el mismo que comprende las siguientes consideraciones y actividades por el Contratista:

Los servicios de implementación incluyen la provisión y configuración y puesta en funcionamiento de los Servicio de conectividad de datos a Internet y fibra oscura para el Datacenter principal y de contingencia de la PNP, plataforma digital de servicios para transmisión de voz, video y datos para las sedes desconcentradas pnp, a nivel nacional; servicio de Gestión de Identidades; servicio de housing del datacenter de contingencia PNP y servicio de seguridad de la información y seguridad gestionada; entre otros según lo indicado en el presente ITEM de acuerdo al diseño propuesto por el contratista y aprobado en coordinación con el personal técnico del DEPGCD-DIVINF-DIRTIC PNP.

El Contratista deberá considerar la provisión de los gabinetes necesarios para albergar todo el equipamiento de las soluciones propuestas (router, switches, seguridad, servidores, entre otros requeridos en el presente TDR), considerando la provisión del cableado eléctrico desde el tablero de distribución hacia los gabinetes, PDU redundantes en diferentes líneas, acondicionamiento de tablero eléctrico de distribución, cableado estructurado de fibra y etiquetado según buenas prácticas para las soluciones o componentes propuestos.

Proveer los equipos de comunicación y seguridad a la Entidad en el lugar, de forma progresiva de acuerdo con el cronograma de implementación del servicio.

Componente 1

- Elaborar y entregar el plan de trabajo para el presente componente.
- Elaborar y entregar la topología inicial propuestas.
- Elaborar el diagrama de implementación del servicio de internet en los datacenter principal y secundario, considerando las líneas Backus para ambos sitios, cada uno con un ancho de banda de 2Gbps.
- Implementar el equipamiento necesario para brindar los servicios de acceso a Internet a través de líneas de datos redundante de banda ancha de 2Gbps en el Datacenter principal y secundario.
- Implementar la optimización de tráfico – traffic shapping en cada sitio principal y secundario
- Implementar el balanceador de enlaces entre los sitios principal y secundario de tal forma que se puede alternar las salidas a internet según requerimiento de la Entidad, o en caso de falla de un sitio el sitio disponible asumirá toda la carga de forma automática, asimismo, realizará el balanceo de sitios a nivel de registros DNS.
- Proveer y configurar equipos de comunicación (switches wan-lan), en el sitio principal y secundario de tal forma que brinden el soporte para la interconexión entre los sitios a fin de establecer la funcionalidad de balanceo de sitios y balanceo de enlaces.

- Proveer y configurar los switches wan/lan en el centro de datos y sitios adyacentes en el data center principal, proveyendo de todos los accesorios o componentes necesarias para la integración con la red de la Entidad
- Proveer y configurar las switches core Lan capa 3 en alta disponibilidad en cada uno de los datacenter principal y secundario, considerando todos los dispositivos necesarios para la interconexión con la totalidad de equipamiento comprendido en el presente ITEM y la red de la Entidad. El contratista realizará todas las configuraciones necesarias para integrar los equipos de comunicaciones, seguridad, servidores de la Entidad.
- Integrar todas las soluciones adquiridas en los diferentes componentes del presente ITEM a los SW Core LAN capa3.
- Proveer y configurar el optimizador de tráfico y traffic shapping en el data center principal y secundario de tal forma, que se pueda monitorear y administrar el ancho de banda de cada sitio.
- Realizar otras actividades que se requiere para el cumplimiento de la finalidad del servicio contratado.

Componente 2:

- Elaborar y entregar el plan de trabajo para el presente componente.
- Elaborar y entregar la topología inicial propuestas.
- Proveer y habilitar el servicio de fibra oscura principal y backup, por diferentes nodos, para los datacenter principal y secundario de la PNP.
- Proveer y configurar los equipos DWDM (multiplexores), de tal forma, que se integre a la fibra oscura y la red de datos de la Entidad, para ello considerará todo el equipamiento y accesorios necesarios (cableado estructurado, patch cord de fibra, bandejas, etiquetado, transceivers, entre otros) que requiera para cumplir con la finalidad del servicio contratado.
- Validar a través del OTDR los requerimientos mínimos solicitados para la fibra oscura.
- Realizar otras actividades que se requiere para el cumplimiento de la finalidad del servicio contratado.

Componente 3

- Elaborar y entregar el plan de trabajo para el presente componente.
- Elaborar y entregar la topología inicial propuestas.
- Implementar la plataforma digital de comunicaciones para la intranet de la PNP.
- Proveer y configurar los equipos routers que serán utilizados para la interconexión con la plataforma privada MPLS o Metroethernet.
- Elaborar etiquetas autoadhesivas que serán adheridas a la lámina de polietileno de los gabinetes donde proveeran los routers, la etiqueta contendrá información necesaria para brindar los canales de atención ante averías, La etiqueta será de 10x21cm y contendrá la siguiente información:
 - Telf. <0800 xxxxx.....>
 - Para presentar un reclamo o reporte de incidencia en la prestación del servicio enviar un correo a: (...centrodeatención@operador..)
 - Identificación del Circuito de Datos utilizados en la sede policial
 - La etiqueta autoadhesiva tendrá el siguiente formato y estructura

Lamina de Polietileno 21x29cmm ITEM

**SERVICIO DE RED PRIVADA (INTRANET) PARA LA UNIDADES
POLICIALES A NIVEL NACIONAL CON ACCESO A INTERNET**

En caso de falla en servicio enlace de internet /intranet llamar a la línea gratuita:

ITEM

10x21cm (información que contendrá la etiqueta autoadhesiva)

Telf. <0800 xxxxx.....>

Para presentar un reclamo o reporte de incidencia en la prestación del servicio enviar un correo a: (...centrodeatención@operador..)

Circuito de datos CD Principal CD Backup

La etiqueta deberá ser elaborada de material resistente e impresión legible a fin de mantenerse disponible durante la ejecución del presente servicio, de no mantenerse disponible, el contratista está obligado a cambiar la etiqueta en un breve plazo.

El contratista podrá registrar mayor información si lo requiera, para mejora del servicio de soporte técnico.

- Proveer y configurar los equipos de comunicación y seguridad en las sedes policiales a nivel nacional según indicación del anexo 1.
- Ejecutar los protocolos de pruebas para verificar la funcionalidad de plataforma de comunicaciones de la intranet PNP.
- Elaborar el diagrama de implementación del servicio de MPLS y/o METROETHERNET en los datacenter principal y secundario, considerando las líneas backups para ambos sitios, cada uno con un ancho de banda de 8Gbps.
- Implementar el equipamiento necesario para brindar los servicios de acceso a intranet a través de líneas de datos redundante de banda ancha de 8Gbps en el Datacenter principal y secundario.
- El servicio de plataforma de backbone y gabinetes por sede será brindado para mil dieciocho (1018) sedes de la Policía Nacional del Perú a nivel nacional y la sede principal del ministerio del interior, las mismas que se detallan en el Anexo N° 1 del presente.
- Considerará una bolsa de cableado de fibra óptica de 24 kilómetros para interconexión de los equipos de comunicación en las sedes policiales que la Entidad requiera, según Anexo 1.
- El contratista debe proporcionar los instrumentos de medida y certificación en cableado de fibra óptica (OTDR), u otro protocolo de pruebas que permita validar la operatividad del servicio solicitado en el presente ITEM. Con el cual se realizará la certificación del canal completo de cada punto de salida, para medir la pérdida de potencia e inserción (insertion loss, IL), lo que se ejecutará en conjunto por el personal del contratista y el que designe la Entidad.
- Implementar los equipos de seguridad (firewall) para sedes tipo 1 y 2 de las unidades policiales a nivel nacional.
- Elaborar y entregar la topología final propuesta.
- Realizar otras actividades que se requiera para el cumplimiento de la finalidad del servicio contratado.

Componente 4

- Elaborar y entregar el plan de trabajo para el presente componente.
- Elaborar y entregar la topología propuesta inicial.
- Proveer y configurar el equipamiento propuesto de comunicaciones, seguridad y appliance de uso exclusivo en los datacenter principal y secundario.

- Integrar el equipamiento propuesto a la red de la Entidad.
- Ejecutar los protocolos de pruebas para verificar la funcionalidad de plataforma de seguridad de la información y seguridad informática gestionada (todo el equipamiento considerado en el presente componente)
- Elaborar y entregar la topología propuesta final.
- Realizar otras actividades que se requiere para el cumplimiento de la finalidad del servicio contratado.
- Realizar otras actividades que se requiera para el cumplimiento de la finalidad del servicio contratado.

Componente 5

- Implementar los servicios web en los servidores de la DIRTIC PNP para el consumo del servicio SMS
- Establece hitos y plazos específicos para cada fase en coordinación con la Entidad.
- Realizar otras actividades que se requieran para el cumplimiento de la finalidad del servicio contratado.

Componente 6

- Elaborar y entregar el plan de trabajo para el presente componente.
- Proveer el servicio de housing para el equipamiento de computo, equipo de seguridad, gabinetes, cableado estructurado, facilities entre otros para el datacenter secundario de la DIRTIC PNP.
- Realizar el traslado de los equipos de cómputo del sitio secundario actual al Datacenter propuesto por el contratista, previa coordinación con la Entidad.
- Apagar el equipamiento de computo de la Entidad, siguiendo el procedimiento que corresponda según la plataforma, desinstalar, embalar y trasladar al Datacenter del contratista, luego de ser recepcionado, desembalar, instalar, encender y poner en funcionamiento el Datacenter secundario de la PNP.
- Realizar otras actividades que se requiera para el cumplimiento de la finalidad del servicio contratado.

Componente 7

- El contratista proporcionará inducción para la Entidad según requerimiento y condiciones descritas en los respectivos componentes, los mismos que no excederán como mínimo 30 días posteriores o máximo 24 meses de la firma del acta de conformidad de la implementación.

Las actividades referenciadas para los componentes son básicas para el cumplimiento del objeto del servicio a contratar, en ese sentido, el contratista deberá realizar todas las actividades requeridas necesarias a fin de cumplir con la finalidad de cumplimiento del servicio solicitado por la Entidad.

5.4 PROCEDIMIENTO

PROCEDIMIENTO DE EMISIÓN DE CONFORMIDAD DEL SERVICIO, DURANTE LA EJECUCION DEL CONTRATO

- Generación del reporte mensual por parte del Contratista:
A fin de emitir la conformidad, el sistema proporcionado por el contratista debe generar el reporte automático mensual que debe contar con la siguiente información:
 - Reporte de Estado de los circuitos de datos (en caso aplique), según el siguiente detalle:
 - Departamento.
 - Provincia.

- Distrito.
- Tipo de medio de transmisión del circuito.
- Porcentaje de operatividad por circuito de manera mensual.
- Reporte de atención de averías y su resultado, según el siguiente detalle:
 - Fecha y hora de la generación del ticket.
 - Tipo de avería.
 - Lugar de avería (rural o urbano).
 - Tiempo de atención desde la generación del ticket.
 - Tiempo de subsanación de la avería.
 - Cantidad de caídas de los componentes del servicio, mensual.
- Elaboración del acta de conformidad por el Jefe del Departamento de Gestión de Centro de Datos de la DIVINF-DIRTIC PNP.

Obtenida la información antes mencionada, el Jefe del Departamento de Gestión de Centro de Datos de la DIVINF-DIRTIC PNP, previo informe técnico emitirá el acta de conformidad, en la que se menciona las averías e incidencias ocurridas en el mes correspondiente, con la finalidad de penalizar en caso lo amerite, la aplicación de la misma se realizará teniendo en cuenta los cuadros de penalidad mencionadas en el presente documento.

El informe y acta de conformidad es remitida a la División de Logística PNP para el pago correspondiente, según corresponda.

PROCEDIMIENTO DE ATENCIÓN DE AVERÍAS EN LOS SERVICIOS DEL COMPONENTE 1,2 y 3

- Se entenderá por avería a una interrupción parcial, total y decremento en la calidad del Servicio.
- Toda actividad o provisión de bienes que tenga que ejecutar el contratista para subsanar la avería será sin costo alguno para LA ENTIDAD.
- El contratista debe asumir los costos de subsanación de averías cuando la causa sea imputable al contratista.
- Con respecto a la reposición de equipos solo corresponderá si la avería de equipos y/o suministros no es responsabilidad de LA ENTIDAD.
- En caso de situaciones tales como fenómenos externos (rayos o tormentas eléctricas entre otras) que averíen los equipos de conectividad, afectando el servicio, el CONTRATISTA está en la obligación de reponer dicho equipamiento de acuerdo a los alcances técnicos considerados en la contratación o con mejoras tecnológicas según corresponda, a fin de restablecer el servicio de acuerdo a los SLA establecidos en el presente requerimiento.
- Se entenderá por Tiempo de Subsanación, al tiempo transcurrido entre la comunicación al Contratista de la existencia de una avería en el servicio por parte de LA ENTIDAD y la subsanación de la misma a su satisfacción. Ésta no debe ser mayor a lo descrito en el numeral 7.10 según indicación del ITEM respectivo, si se supera este rango de tiempo sin subsanar será considerada como penalidad tal como se indica en el numeral antes indicado.
- El tiempo de subsanación incluye el tiempo de transporte y todo aquel relacionado con la atención, en aquellos casos que se presenten demoras por parte de la entidad, o no exista facilidades para el transporte (huelgas en carretera, deslizamientos, restricciones gubernamentales, emergencia sanitarias, aislamiento focalizado, inmovilización social, vandalismo, rondas campesinas y/o pobladores que no permitan el ingreso a sus localidades u otro ocasionado por terceros) este tiempo será considerado como parada de reloj, el cual no será considerado como parte del tiempo de atención de acuerdo a los SLA solicitados.

- El Contratista debe contar con un Network Operation Center o NOC y Centro de Averías, con personal capacitado en atención de averías y expertos en el equipamiento propuesto en los diferentes servicios, para la gestión y atención del **soporte técnico** del servicio, no pudiendo éste ser tercerizado, instalado de tal manera, que le asegure a LA ENTIDAD que se encuentra en condiciones de cumplir con lo estipulado en éstos términos de referencia. Asimismo, la atención del servicio brindado a través del NOC y Centro de Averías será 24x7x365.
- El Contratista deberá indicar cuántas personas serán las responsables de atender a la Entidad, debiendo demostrar que estas personas en su totalidad se encuentran certificadas en la marca de equipos de red (routers) sobre los cuales brindarán los servicios; La Entidad está contratando servicios en modalidad 24 x 7, por lo que la cantidad de personal debería cubrir tal necesidad, siendo esto evaluado por la Entidad.
- El monitoreo y control del servicio brindado será en línea a través del NOC 24x7x365. Este monitoreo debe incluir la evaluación de la performance, disponibilidad, uso de interfaces y estatus de procesamiento de las funcionalidades de los equipos, debe estar en capacidad de realizar detección de alarmas tempranas, acciones de control preventivos y correctivos, pruebas técnicas, cuya información debe ser entregada a la ENTIDAD, conjuntamente con los informes mensuales.
- LA ENTIDAD podrá constatar de ser necesario la información presentada por el contratista con visitas a su NOC, previa coordinación.
- El contratista notificará a los responsables de LA ENTIDAD, los eventos de interrupción parcial, total y decremento en la calidad del Servicio, así como del comportamiento anómalo, generando las acciones inmediatas de subsanación de la avería presentada para restaurar el servicio.
- Designar a una persona del NOC para la atención de reportes a solicitud de la entidad, esta persona será representante del Contratista ante la Entidad. Este responsable debe contar con los conocimientos y experiencia en el manejo y generación de reportes en los equipos propuestos. Los reportes serán enviados a la Entidad de manera mensual, así también se considerarán reportes a demanda cuando la Entidad así lo requiera.
- El Contratista está obligado a mantener respaldado la información del histórico del estado de los circuitos y de todas las soluciones propuestas en el presente contrato, con la finalidad de emitir reportes a requerimiento la Entidad, dentro de las 48 horas como máximo.
- El Contratista debe proveer una herramienta online con interfaz Web disponible 24x7x365 para la generación de tickets de atención de averías y de solicitudes por parte de personal de la entidad asimismo se debe poder visualizar su estado de atención, incluyendo el procedimiento para la generación de tickets de averías y la matriz de escalamiento. LA ENTIDAD en un plazo máximo de cinco (05) días calendarios posteriores a la suscripción del contrato debe hacer entrega al contratista el listado del personal autorizado para utilizar la herramienta online antes indicada, a fin de que el contratista le entregue las credenciales de acceso correspondiente.
- Los reportes y estado de las averías deben generarse a demanda por parte de la Entidad a través de una herramienta online con interface web disponible 24x7x365, el Contratista debe garantizar que la información antes mencionada tenga la información actualizada de forma permanente.
- El contratista debe proveer una herramienta online con interfaz Web disponible 24x7x365 para la generación de tickets de atención de averías y de solicitudes por parte de personal de la entidad; asimismo, se debe visualizar su estado de atención.
- Las atenciones del NOC y Centro de Averías del contratista deben ser en 24x7 de lunes a lunes, los 365 días del año.
- La entidad podrá aperturar de forma ilimitada tickets e incidentes durante el periodo de servicio contratado.



- La entidad antes de generar un ticket de avería previamente se realizará procedimientos básicos de revisión (verificación de fluido eléctrico, verificación del cableado estructurado, conexiones de equipamiento de comunicaciones y seguridad, y otros que pudieran ser necesarios para el diagnóstico del incidente), con el fin de describir correctamente la avería. En aquellos casos que se presenten demoras por parte de la entidad, el contratista debe coordinar con la Unidad Usuaria para que dicha demora sea considerada como parada de reloj y dicho tiempo será descontado del tiempo de atención de la avería. La parada del reloj entre el contratista y la unidad usuaria será necesario realizarla mediante el envío al correo electrónico institucional. Adicionalmente, se podrá adjuntar la evidencia mediante fotografía y/o videos para justificar las demoras por parte de la entidad; no serán exigidas constancias adicionales ni trámite burocráticos y/o legales.
- LA ENTIDAD, registrará las averías que se presenten incluyendo la siguiente información:
 - Fecha y hora
 - Descripción del problema
 - Contacto en la entidad
- El contratista informará a la entidad, de manera electrónica, de lo sucedido cada vez que se reporte una avería, en un plazo no mayor a un (01) día útil, sin perjuicio de remitir el informe mensual correspondiente (con la información mínima requerida). El informe (por avería y el mensual) debe contener como mínimo número de ticket de la avería, descripción, tráfico de consumo, hora de inicio y fin, persona contacto por parte de la entidad, el diagnóstico del problema, tiempo empleado, solución aplicada y recomendaciones, personal que dio conformidad del levantamiento si las hubiera.
- El contratista debe presentar a la entidad la relación del personal técnico autorizado para realizar labores en reparación y/o configuración en los locales donde se llevará a cabo la prestación del servicio. El contratista deberá presentar mensualmente la relación de su personal y en caso se produzca algún cambio de personal, deberá comunicarlo en forma oportuna, durante el periodo de ejecución contractual. El listado debe contener nombre completo y documento de identidad.
- La entidad no se encuentra obligada a permitir el acceso del personal no considerado en la referida relación.
- El acuerdo del nivel de Servicio debe ser igual o mayor al 99.5% o 99.7% por mes según lo referido en otras penalidades aplicables.
- El CONTRATISTA realizará los ajustes necesarios en la solución de tal manera que los archivos de logs sirvan para una rápida determinación y solución de los incidentes.
- El CONTRATISTA se obliga a garantizar en toda circunstancia la posibilidad de escalamiento de los eventos, de forma continua. Al inicio del servicio se permitirá realizar una reunión de presentación sobre el procedimiento de la atención de averías y la matriz de escalamiento. La Entidad al inicio del servicio, remitirá al contratista la relación de contactos por sede donde se deberá especificar los datos de las personas a ubicar en caso el contacto no se encuentre disponible, la entidad deberá comunicar los cambios de contactos que se produzcan durante la ejecución contractual.
- La entidad no se encuentra obligada a permitir el acceso del personal no considerado en la referida relación.
- El Acuerdo del Nivel de la Calidad del Servicio de conectividad de datos a Internet, fibra oscura para los Datacenter principal y de contingencia de la PNP y el servicio de housing del Datacenter de contingencia PNP, debe ser mayor o igual al 99.7% por mes.
- El CONTRATISTA realizará los ajustes necesarios en la solución de tal manera que los reportes sirvan para una rápida determinación y solución de los problemas



- Mediante el documento que aprueba el plan de trabajo, LA ENTIDAD remitirá al contratista el listado del personal autorizado para utilizar la herramienta online antes indicada, a fin de que el contratista le entregue las credenciales de acceso correspondiente, en un plazo máximo de diez (10) días calendario de recepcionado el precitado documento, listado que durante la ejecución del contrato pudiera variar solicitud de la Entidad. Ante la existencia en el cambio del personal policial, la entidad comunicará al contratista a fin de realizar las modificaciones correspondientes, bajo las mismas condiciones. Luego de informada la modificación, el plazo para entregar las credenciales será de 02 días calendarios.
- La entidad podrá solicitar la modificación o elaboración de un nuevo formato de informe para cada componente, según corresponda, a fin de que el área usuaria pueda evidenciar de manera eficiente la prestación del servicio brindado y emita su acta de conformidad según corresponda, dicha solicitud será realizada al contratista con una anticipación de 20 días calendarios próximos al siguiente reporte mensual.
- Proporcionado los informes y reportes mensuales antes mencionada, la Unidad Usuaria, previo informe técnico emitirá el acta de conformidad, en la que se menciona las averías e incidencias ocurridas en el mes correspondiente, con la finalidad de penalizar en caso lo amerite, la aplicación de la misma se realizará teniendo en cuenta los cuadros de penalidad mencionadas en el presente documento.
- El informe y acta de conformidad se remitirá a la División de Logística PNP para el pago correspondiente, según corresponda.

El servicio de la solución implementada debe garantizar el uso ininterrumpido de la misma por el periodo de treinta y seis (36) meses (plazo de prestación del servicio), sin que disminuyan ninguna de las funciones y capacidades desarrolladas durante el periodo de implementación; asimismo durante este periodo el uso de la solución no debe irrogar un costo adicional de licencias o permisos por parte de la ENTIDAD.



5.5 PLAN DE TRABAJO

La entrega del plan de trabajo se efectuará dentro de los SEIS (06) días calendarios, a partir del día siguiente de la suscripción del contrato, en la mesa de partes de la DIRTIC-PNP, con copia en la mesa de partes de la DIVLOG.PNP, en formato impreso y archivo digital. También se podrá realizar de manera digital a las siguientes direcciones virtuales: depaba.secejecon@policia.gob.pe; y dirtic.ayu@policia.gob.pe, con la finalidad que el personal de la DEPGCD-DIVINF-DIRTIC-PNP, realice la evaluación y aprobación del referido documento. El plan de trabajo podrá ser presentados por componente o como un solo documento para todos los componentes que forman parte de los términos de referencia

El Plan de Trabajo deberá desarrollar el cronograma de las actividades y procedimientos para la implementación y ejecución del servicio, incluyendo lo siguiente:

- La propuesta técnica para la implementación del servicio, que incluirá la documentación técnica detallada y explícita que sustente el cumplimiento de la totalidad de las especificaciones técnicas establecidos en los términos de referencia, adjuntando la descripción de la infraestructura del contratista que soportará el servicio, con indicación de la marca y modelo de las soluciones propuestas necesarios para asegurar el nivel de servicio, diagramas y esquemas de la topología de la solución tecnológica planteada.
- Project Charter.
- Plan de Gestión del Proyecto.
- Estructura de Detalle de Trabajo (WBS).
- Plan de Calidad.
- Plan de Recursos Humanos.
- Plan de Comunicaciones.
- Plan de Administración de Riesgos.
- Planos de arquitectura

- (j) Manual de resolución de problemas
- (k) Plan de traslado y activación del Datacenter secundario PNP
- (l) Plan de Control en la etapa de implementación y ejecución
- (m) Cronograma de actividades

Los entregables señalados entre los literales "b" y "j" deben cumplir con lo establecido en el Project Management Body of Knowledge (PMBOK) desarrollado por el Project Management Institute (PMI).

Para el perfeccionamiento del Contrato el postor ganador debe incluir los datasheets en idioma original de los dispositivos y/o equipamiento propuesto con su número de parte (part number) correspondiente, licenciamiento, accesorios y componentes necesarios para asegurar el nivel de servicio; el Diagrama técnico detallará la arquitectura y topología de la solución tecnológica propuesta, esto aplica para todos los componentes del ítem 1; asimismo, el contratista no podrá colocar equipos distintos a los indicados en su propuesta técnica durante la etapa de implementación y/o durante la prestación del servicio, a menos que sea por mejora tecnológica, previa aprobación por parte de LA ENTIDAD.

5.6 REQUISITOS SEGÚN LEYES, REGLAMENTOS TÉCNICOS, NORMAS METROLÓGICAS Y/O SANITARIAS, REGLAMENTOS Y DEMÁS NORMAS

Todos los elementos suministrados para ejecutar el trabajo, que se utilizarán en la implementación de la provisión de la Plataforma Digital de Servicios para la PNP deben cumplir con las siguientes Normas de Cableado de Sistemas de Comunicaciones:

- Tierras y aterramientos para los sistemas de telecomunicaciones de edificios comerciales
- Reglamento Nacional de Edificaciones del Perú.
- Código Nacional de Electricidad del Perú.
- Resolución Ministerial N° 175-2008-MEM/DM del 11ABR2008.
- Decreto Supremo N°020-2007-MTC; Texto Único Ordenado del Reglamento General de la Ley de Telecomunicaciones
- Reglamento Específico de Homologación de Aparatos y Equipos de Telecomunicaciones
- Norma G.050 seguridad durante la construcción
- Ley 29733 Ley de Protección de datos personales.
- Decreto Supremo 081-2017-PCM "Decreto que aprueba la formulación de un plan de transición al protocolo IPV6 en las entidades de la Administración Pública", de fecha 08 de agosto del 2017.
- Resolución Ministerial 004-2016-PCM Aprobación del uso obligatorio de la Norma técnica peruana "NTP ISO/IEC 27001:2014 Tecnología de la Información Técnicas de Seguridad Sistemas de Gestión de Seguridad de la Información Requisitos 2da Edición.

5.7 IMPACTO AMBIENTAL (no aplica)

5.8 SEGUROS

Seguro Complementario de Trabajo de Riesgo

La Entidad requiere que el Contratista cuente con el Seguro laboral obligatorio vigente para el personal propuesto, correspondiente a la tarea que desempeñará en el servicio a contratarse.

5.9 PRESTACIONES

5.10 LUGAR Y PLAZO DE PRESTACIÓN DEL SERVICIO

5.10.1 LUGAR

"SERVICIO DE TRANSMISION PARA LA RED PRIVADA DE LA PNP, EN LAS UNIDADES POLICIALES A NIVEL NACIONAL; SERVICIO DE SEGURIDAD GESTIONADA Y ACCESO A INTERNET", se brindará en las siguientes ubicaciones:

Servicio N° 1	DETALLE	UBICACION
COMPONENTE 1	DATACENTER PRINCIPAL Y SECUNDARIO	Plaza 30 de agosto s/n Urb. Corpac San Isidro, 2do piso de las instalaciones de la DIRTIC-PNP PNP y DATACENTER propuesto por el Contratista
COMPONENTE 2	DATACENTER PRINCIPAL Y SECUNDARIO	Plaza 30 de agosto s/n Urb. Corpac San Isidro, 2do piso de las instalaciones de la DIRTIC-PNP y DATACENTER propuesto por el Contratista
COMPONENTE 3	UNIDADES PNP	A nivel nacional, según indicación del anexo 01 adjunto.
COMPONENTE 4	DATACENTER PRINCIPAL Y SECUNDARIO	Plaza 30 de agosto s/n Urb. Corpac San Isidro, 2do piso de las instalaciones de la DIRTIC-PNP PNP y DATACENTER propuesto por el Contratista
COMPONENTE 5	COORDINACIÓN CON EL CONTRATISTA	Plaza 30 de agosto s/n Urb. Corpac San Isidro, 2do piso de las instalaciones de la DIRTIC-PNP PNP y DATACENTER propuesto por el Contratista
COMPONENTE 6	COORDINACIÓN CON EL CONTRATISTA	DATACENTER propuesto por el Contratista
COMPONENTE 7	COORDINACIÓN CON EL CONTRATISTA	Centro de inducción propuesto por el contratista

5.10.2 PLAZO DE EJECUCION DE LA PRESTACION

Plazo de implementación. - Inicia a partir del día del siguiente de suscrito el contrato, dándose inicio a la implementación y puesta en funcionamiento del servicio en un plazo máximo de SEIS (06) MESES.

Plazo para suscribir la Conformidad.- Culminada la etapa de implementación y puesta en funcionamiento, el Jefe del DEPGCD-DIVINF-DIRTIC PNP emitirá el Acta de Conformidad de la implementación realizada, previo informe del personal técnico responsable de las Secciones de Operaciones, Redes y Seguridad Informática, en un plazo máximo de SIETE (7) días calendarios.

Inicio del Servicio. - inicia a partir del día siguiente de suscrita el Acta de conformidad de implementación del servicio, dándose inicio a la ejecución contractual para la prestación del **"SERVICIO DE TRANSMISION PARA LA RED PRIVADA DE LA PNP, EN LAS UNIDADES POLICIALES A NIVEL NACIONAL; SERVICIO DE SEGURIDAD GESTIONADA Y ACCESO A INTERNET"**, por el período de treinta y seis (36) meses contados a partir del día siguiente de suscrito el Acta de Conformidad de la implementación y puesta en funcionamiento.

Se ha considerado los siguientes plazos:

Prestación de servicio

- 1) La implementación y puesta en funcionamiento se realizará en un plazo no mayor a SEIS (06) MESES, contados a partir del día siguiente de la suscripción del contrato.

- 2) El plazo de ejecución del servicio de transmisión para la red privada de la PNP, internet y fibra oscura para la data center principal y secundario PNP, es treinta y seis (36) meses, contabilizados desde el día siguiente de firmada el Acta de conformidad por parte del Jefe del DEPGCD-DIVINF-DIRTIC PNP, previo informe del personal técnico responsable según corresponda.
- 3) La implementación y prestación del servicio se ejecutará según los siguientes plazos y condiciones:

- **Plazo para reunión de coordinación para el inicio del proyecto:** El Contratista dentro de OCHO (08) días calendarios posteriores a la suscripción del contrato, coordinará con las personas encargadas de DIRTIC-PNP la reunión de coordinación para el inicio del proyecto.
- **Plazo para presentación del Plan de trabajo:** El Contratista dentro de SEIS (06) días calendarios posteriores a la suscripción del contrato, presentará en la mesa de partes de la DIRTIC-PNP, con copia en la mesa de martes de DIVLOG-PNP, el plan de trabajo para su evaluación y aprobación a cargo del Jefe del DEPGCD - DIVINF-PNP. También se podrá realizar de manera digital a las siguientes direcciones virtuales: depaba.secejecon@policia.gob.pe; y dirfic.ayu@policia.gob.pe.
- **Plazo para la Evaluación y Aprobación del Plan de Trabajo:** en un plazo máximo de DOS (02) días calendario de entregado el plan de trabajo, el Jefe del DEPGCD DIVINF-PNP, aprobará el referido plan. De existir observaciones la entidad comunicará al contratista el sentido de las mismas mediante correo electrónico, teniendo este último DOS (02) días calendario para la subsanación de las mismas, para cuyo efecto deberá realizar la presentación del plan de trabajo en las respectivas mesas de parte. También se podrá realizar de manera digital a las siguientes direcciones virtuales: depaba.secejecon@policia.gob.pe; y dirfic.ayu@policia.gob.pe.
- **Plazo para la presentación del Diseño de la Topología del Servicio de Conectividad y Protocolo de pruebas:** en un plazo máximo de SEIS (06) días calendarios posteriores al día siguiente de la suscripción del contrato, el contratista presentará en la mesa de partes de la DIRTIC-PNP, con copia en la mesa de partes de DIVLOG-PNP, el Diseño y protocolo de pruebas para su evaluación y aprobación a cargo del Jefe del DEPGCD DIVINF-PNP.
- **Plazo para la aprobación del Diseño de la Topología del Servicio de Conectividad y Protocolo de pruebas:** la entidad tendrá un plazo de aprobación hasta DOS (02) días calendario, contados a partir del día siguiente de presentado el Diseño y Protocolo de Pruebas. De existir observaciones el contratista tendrá DOS (02) días calendarios para levantar las observaciones presentadas, una vez subsanadas todas las observaciones que se hubiesen presentado, se suscribirá en Acta de conformidad del Diseño de la Topología del Servicio de Conectividad y Protocolo de pruebas, por parte del Jefe del DEPGCD-DIVINF-DIRTIC-PNP.
- **Plazo para la entrega de los manuales técnicos de los equipos:** hasta SEIS (06) MESES posteriores a la suscripción del contrato:
 - 1) Manual Técnico de equipos de conectividad (Router y switch)
 - 2) Manuales Técnicos de equipos de balanceo de enlaces y de sitios.
 - 3) Manuales Técnicos de equipos de traffic shapping.
 - 4) Manuales Técnicos del servicio de gestión de identidades.
 - 5) Documentos de garantías del equipamiento suministrado.
 Los manuales podrán ser entregados en el idioma original del fabricante.



- 4) El plazo de implementación es de SEIS (06) MESES contados a partir del día siguiente de la suscripción del contrato. Se suscribirá el Acta de conformidad de Implementación, previa entrega de los entregables descritos en el numeral 5.10.1 y el informe final por parte del Contratista, con esto se dará inicio al Servicio. El plazo máximo para la suscripción de la referida Acta de Implementación y puesta en funcionamiento es de SIETE (07) días calendario, posteriores a la verificación y recepción de la documentación correspondiente.
- 5) La Entidad brindara las facilidades de accesos y/o facilidades requeridas en la etapa de implementación, en el caso de imprevistos por parte de la Entidad, los plazos internos (antes mencionados) podrán ser cambiados en coordinación con el contratista, sin que ello genere la aplicación de ninguna penalidad en contra del contratista.
- 6) El contratista por fuerza mayor podrá solicitar variar los referidos plazos internos antes indicados, en coordinación con el área usuaria, pero sin extender los SEIS (06) MESES, del periodo de implementación, los cambios solicitados requerirán aprobación de LA ENTIDAD.
- 7) Para la inducción se considerará los siguientes plazos y condiciones:
 - o Plazo para coordinar cronograma de inducción: Dentro de los quince (15) días calendarios posteriores a la suscripción del contrato, el contratista y un representante del área del DEPGCD DIVINF DIRTIC PNP, deberán realizar una reunión de coordinación a fin de establecer el cronograma para el desarrollo de la inducción, suscribiendo el acta correspondiente.
 - o Las inducciones, se brindarán en las condiciones establecidas según el numeral 5.2.1.5.7 de los presentes términos de referencia.
 - o Las inducciones se iniciarán 30 días posteriores a la suscripción del acta de conformidad por la implementación y puesta en marcha del servicio, teniendo como plazo máximo de inicio 24 meses posteriores a la firma del del acta de conformidad por la implementación y puesta en marcha del servicio.



CRONOGRAMA DE ACTIVIDADES ACTIVIDADES	CRONOGRAMA DE ACTIVIDADES POR DÍA					
	Del 1 al 6	Del 7 al 8	Del 9 al 180	Del 181 al 187	Del 188 al 907	Del 907 al 1267
Reunión de coordinación para el inicio del proyecto. a partir del día siguiente de la suscripción del contrato.						
Presentación del Plan de Trabajo						
Evaluación y Aprobación del Plan de Trabajo						
Presentación del Diseño de la Topología del Servicio de Conectividad y Protocolo de pruebas						
Aprobación del Diseño de la Topología del Servicio de Conectividad y Protocolo de pruebas						
Entrega de Manuales Técnicos de los equipos						
Implementación del servicio total (considera todos los componentes)						
Acta de Conformidad de la Implementación del Servicio						
Inicio del servicio						
Inducción						

La ENTIDAD indicará el horario de trabajo para la provisión de los equipos, configuración y pruebas del servicio, garantizando por lo menos ocho (08) horas diarias de lunes a viernes en días laborables, en horarios diurnos o nocturnos para la realización de las actividades; asimismo, se podrá programar actividades de la implementación los sábados, domingos o feriados en coordinación con el responsable técnico de la Entidad.

Las actividades o reuniones de coordinación no se encuentran supeditadas al cumplimiento de la presentación del plan de trabajo dentro del plazo establecido. Dicha documentación se entregará según cronograma del cuadro antes indicado.

5.11 RESULTADOS ESPERADOS.

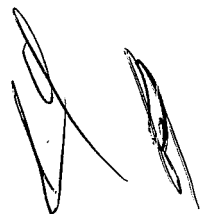



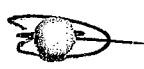
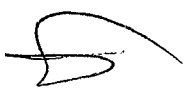
5.11.1 Entregables:

5.11.1.1

A fin de suscribir el Acta de Conformidad de la implementación y puesta en funcionamiento del Servicio de acceso a Internet en los data center principal y secundario, fibra oscura entre el Datacenter principal y secundario de la PNP, plataforma digital de servicios para transmisión de voz, video y datos para las sedes desconcentradas PNP, a nivel nacional; servicios de gestión de identidades; servicio de housing del datacenter secundario PNP y servicio de seguridad de la información y seguridad gestionada, el contratista deberá hacer entrega de la siguiente documentación al término del periodo de implementación del servicio según lo descrito el punto 5.9.2 Plazo

- a) Informes de instalación y puesta en funcionamiento según los requerimientos de la entidad de: acceso a Internet para el data center principal y secundario el mismo que deben contener como mínimo el siguiente detalle:
 - i. Reporte de pruebas acceso a internet de los sitios principal y de contingencia, evidenciando el balanceo de enlaces entre los sitios.
 - ii. Reporte de pruebas de implementación del DNS autoritativo para la PNP y el balanceo de sitios de a través de los registros DNS.
 - iii. Reporte de pruebas de administración de ancho de banda para los diferentes servicios brindados por la DIRTIC PNP.
 - iv. Reporte de la configuración y funcionamiento en los servicio de DDoS
 - v. Reporte de pruebas del funcionamiento del balanceo de servicios y/o aplicaciones brindados por la DIRTIC PNP.
- b) Informe de instalación y puesta en funcionamiento según los requerimientos de la entidad de: Servicio de fibra oscura entre el datacenter principal y secundario de la PNP el mismo que deben contener como mínimo el siguiente detalle:
 - i. Reporte de pruebas de conectividad a través de la fibra oscura entre el datacenter principal y secundario
 - ii. Reporte de integración de la solución con la red de la Entidad, observando el ancho de banda requerido en el presente servicio.
 - iii. Reporte de pruebas de funcionamiento de alta disponibilidad entre la línea principal y backup, evidenciando las rutas físicas diferentes de la fibra oscura.
- c) Informe de instalación y puesta en funcionamiento según los requerimientos de la entidad de: la plataforma digital de servicios para transmisión de voz, video y datos para las sedes desconcentradas PNP, a nivel nacional, el mismo que deben contener como mínimo el siguiente detalle:
 - i. Reporte de pruebas realizadas de interconexión entre las diferentes unidades policiales a nivel nacional con los centros de datos principal y secundario, así como la interconexión entre las mismas unidades policiales, evidenciando full mesh de la MPLS y/o Metroethernet.



- 
- 
- 
- 
- 
- 
- ii. Reporte de pruebas de unidades PNP, validando la operatividad de las líneas backups.
 - iii. Reporte de pruebas de la salida a internet de las unidades policiales a través de la MPLS y/o Metroethernet, evidenciando configuraciones de NAT y no de Proxy o semejante.
 - iv. Reporte de pruebas de conectividad entre el centro de datos principal y secundario y las diferentes unidades PNP a nivel nacional, observando tiempos de repuesta, el ancho de banda solicitado (8Gbps) y disponibilidad de la línea backup en ambos sitios.
 - v. Reporte de pruebas de interconexión de las plataformas de backbone de fibra y validación de provisión de gabinetes para las sedes desconcentradas pnp, a nivel nacional.
 - vi. Diagrama del gabinete principal y de distribución si correspondiera, con descripción de componentes, accesorios, medios de comunicación y tendido utilizado (aéreo o ductos), este debe contener leyendas para mejor comprensión de los datos gráficos.
 - vii. Acta de la instalación con indicación del metraje de fibra óptica, suscritas por responsable de la Unidad Policial y el responsable técnico del contratista.
 - viii. Documento Excel de recursos utilizados en cada una de las Unidades Policiales y Complejos en referencia al metraje de fibra óptica en el cual deberá señalar el nombre de la unidad policial, el metraje utilizado, cantidad de gabinetes con indicación del lugar físico (departamento, oficina, sección, entre otro) en la unidad PNP. Asimismo, el documento debe señalar los códigos o números de identificación de los gabinetes en cada Unidad PNP, de forma que se puede identificar el lugar o ambiente donde se encuentra en la sede policial.
 - ix. Diagrama de distribución del sistema eléctrico realizado para la provisión de los gabinetes.
 - x. Diagrama de la plataforma de backbone de fibra implementada en cada sede policial.
 - xi. Reporte de implementación y puesta en funcionamiento de la seguridad informática en las unidades PNP comprometidas en el presente servicio a través de la instalación y configuración de firewall.
- d) Informe de instalación y puesta en funcionamiento según los requerimientos de la entidad de: servicio de seguridad de la información y seguridad gestionada, el mismo que deben contener como mínimo el siguiente detalle:
- i. Reporte de pruebas de instalación, configuración y funcionamiento del siguiente equipamiento:
 - Firewall de nueva generación, para red externa y red interna.
 - Detección y control de malware avanzado.
 - Protección de portales web y base de datos
 - Spam Firewall y protección ante phishing dirigido
 - Protección contra ataques de denegación de servicios distribuido
 - Análisis de vulnerabilidades de red
 - Herramienta informática para prevención de pérdida de información, auditoría y anticorrupción.
 - Solución de antivirus para servidores y endpoint de la DIRITC PNP.
 - Servicio de SOC Gestionado, Herramienta de Análisis de incidentes y Correlación de logs de seguridad

- e) Informe de instalación y puesta en funcionamiento según los requerimientos de la entidad de servicios de gestión de identidades, el mismo que deben contener como mínimo el siguiente detalle:
 - i. Reporte de pruebas de funcionamiento del servicio SMS, con las características mínimas solicitadas.
 - ii. Reporte de pruebas de acceso a la herramienta de administración del presente servicio.
 - iii. Reporte de integración con los sistemas de la Entidad.
- f) Informe de instalación y puesta en funcionamiento según los requerimientos de la entidad de: servicio de housing del datacenter secundario PNP, el mismo que deben contener como mínimo el siguiente detalle:
 - i. Reporte de pruebas de funcionamiento de la infraestructura de la DIRTIC PNP en las instalaciones propuesta por el contratista para el funcionamiento del centro de datos secundario.
 - ii. Información detallada de la actualización, soporte y mantenimiento de la solución de servidores de la Entidad.
 - iii. Información del licenciamiento del software.
 - iv. Reporte de pruebas de funcionamiento de la solución de respaldo y archivamiento.
- g) Procedimientos y formatos para solicitud de incremento/decremento de servicios.
- h) Informe de reporte mensual, el cual reporta el uso de los servicios, atenciones realizadas, incidencias presentadas y resueltas dentro del plazo máximo permitido, incidencias presentadas y resueltas fuera del plazo máximo permitido, incidencias presentadas y no resueltas, situación del equipamiento, Inventarios, garantías y los niveles de servicio alcanzados, así como las recomendaciones para la mejora de los mismos.
- i) Inventario de Hardware y Software que forma parte del SERVICIO DE TRANSMISION PARA LA RED PRIVADA DE LA PNP, EN LAS UNIDADES POLICIALES A NIVEL NACIONAL; SERVICIO DE SEGURIDAD GESTIONADA Y ACCESO A INTERNET; servicio sms para la PNP; servicio de housing del datacenter de secundario PNP y servicio de seguridad de la información y seguridad gestionada, brindado a la ENTIDAD.
- j) Documentación de la configuración de cada uno de los equipos implementados y esquema del cableado de conexiones entre ellos, con indicación del número de puerto, IP, van, tipo de medio, equipos entre otros considerados en el presente ITEM.
- k) Topología de red lógica y física de los Centro de datos Principal y secundario, Complejos Policiales y comisarias PNP a nivel nacional de forma individual.
- l) Topología de red lógica y física de la red privada de la PNP.
- m) Formato de reporte de rendimiento de cada uno de los circuitos dedicados.
- n) Cuadro de direccionamiento IP de todos los servicios.
- o) Cuadro que señale los códigos o números de identificación de los circuitos digitales, IP wan, IP lan, Redes, Gateway de las sedes a nivel nacional con indicación de anchos de banda y medios de transmisión usados.
- p) Entrega de credenciales con nivel de administración de todas las soluciones implementadas en el presente ITEM para usuarios PNP involucrados y responsables de las soluciones propuestas.
- q) Toda la documentación deberá ser entregada en formato digital e impreso

Todos los entregables deben ser firmados por el Jefe de Proyecto del contratista, y serán entregados al Responsable Técnico del Departamento de Gestión de Centros de Datos de la División de Informática PNP - DIRTIC-PNP el día en que se realice la verificación de la



implementación, dicha documentación resulta necesaria para la suscripción del Acta de Conformidad de la implementación del **SERVICIO DE TRANSMISION PARA LA RED PRIVADA DE LA PNP, EN LAS UNIDADES POLICIALES A NIVEL NACIONAL; SERVICIO DE SEGURIDAD GESTIONADA Y ACCESO A INTERNET**; servicio de housing del Datacenter secundario PNP; servicio de gestión de identidades y servicio de seguridad de información y seguridad informática gestionada.

5.11.1.2 Del uso del Servicio

La prestación debe garantizar el uso ininterrumpido del Servicio de internet y fibra oscura en los Datacenter PNP principal y secundario, transmisión de datos y seguridad de la información e informática; servicio de cableado estructurado de fibra en los complejos de multi unidades policiales y en las comisarías PNP; y el servicio de housing para el datacenter secundario, así como de la totalidad del equipamiento y soluciones propuestos por el CONTRATISTA, por el periodo de treinta y seis (36) meses, sin que disminuyan ninguna de las funcionalidades y capacidades desarrolladas durante el periodo de ejecución del servicio, conforme el Acuerdo de Nivel de Servicio contratado 99.5% a excepción de los componentes 1, 2 y 4 que será del 99.7% por considerarse servicios críticos para la Entidad; asimismo, no debe irrogar costos adicionales para la entidad.

Como parte del servicio se debe entregar un informe detallado en forma mensual (en formato digital con firma de los comprometidos y en formato físico cuando la entidad lo requiera, previa coordinación) de la siguiente información, teniendo como plazo máximo diez (10) días calendario posterior al último día de cada mes a partir de la finalización del periodo mensual del servicio:

- Programación de mantenimientos del siguiente mes; está referida a los mantenimientos preventivos que se encuentren programados para los equipos que conforman los componentes contratados por la Entidad
- Reporte de Incidencias.
- Reporte de averías. Número de circuitos averiados, número y fecha del ticket de avería, solución ejecutada, tiempo de atención, gráfico de circuitos averiados, observaciones y recomendaciones.
- Ajustes de parámetros en el sistema.
- Cambios en el ambiente de operación (Direcciones IP, Redes, etc.).
- Inclusión de nuevos dispositivos de cómputo, nuevos usuarios.
- Análisis de rendimiento.
- Detalles de los niveles de servicio comprometidos en la Operación.
- Programación de mantenimientos del siguiente mes.
- Reporte de Estado de los Circuitos.
- Reporte de Consumo de Ancho de Banda, gráficas de consumo, enlaces con saturación, enlaces sin uso, enlaces normales, observaciones y recomendaciones.
- Reporte de la operatividad de los equipos de conectividad.
- Reporte de operatividad de la totalidad del equipamiento y soluciones propuestos por el contratista según componente.

6 OTRAS CONSIDERACIONES PARA LA EJECUCION DE LA PRESTACION

6.1 OTRAS OBLIGACIONES

6.1.1 OTRAS OBLIGACIONES DEL CONTRATISTA

Otras consideraciones para la ejecución de la prestación

Debe disponer, de manera opcional, de un sistema de gestión de seguridad de la información conforme con la Norma ISO/IEC 27001

6.1.2 RECURSOS Y FACILIDADES A SER PROVISTAS POR LA ENTIDAD

La Entidad, proporcionará acceso a las instalaciones de los Datacenter principal y de contingencia, así como a las Unidades policiales a nivel nacional consideradas en el Anexo N° 01 del presente, para que en dicho lugar sea instalado el equipamiento y líneas de datos correspondientes al presente servicio de acuerdo con el diseño que propondrá el contratista.

La Entidad suministrará la energía eléctrica para los equipos de conectividad y de cómputo suministrados por el contratista

6.2 ADELANTOS

La Entidad no cuenta con recursos presupuestales para atender adelantos.

6.3 SUBCONTRATACIÓN.

El contratista podrá subcontratar parte de las prestaciones a su cargo de acuerdo a las condiciones establecidas. La subcontratación podrá ser aplicada siempre y cuando se trate de la subcontratación de tareas NO ESENCIALES

6.4 CONFIDENCIALIDAD.

El contratista se compromete a mantener en reserva y no revelar a tercero alguno sin previa conformidad escrita de LA ENTIDAD, toda información que le sea suministrada por este último, excepto en cuanto resultare estrictamente necesario para el cumplimiento del Contrato y que restringirá la revelación de dicha información sólo a sus empleados, sobre la base de "necesidad de conocer".

En la necesidad de revelar información que sea de propiedad de la Entidad, recibida por la propia entidad o por terceros, y que tenga relación con el contrato y/o servicio contratado, esto deberá ser tratado previamente y por escrito con la Entidad.

El contratista se compromete a no revelar ni permitir la revelación de cualquier detalle a los medios de prensa o a terceros, y a no usar el nombre de LA ENTIDAD en cualquier promoción, publicidad o anuncio, sin previa autorización escrita de LA ENTIDAD.

El contratista, o sus empleados, no podrá vulnerar, copiar, almacenar, publicar, o capturar la información de LA ENTIDAD de información acerca de las Unidades y Nodos a ser interconectados, cantidad de circuitos digitales, configuración de la red de la Policía Nacional del Perú, direcciones IP, protocolos, equipamiento, dato o cualquier información de la PNP a que el contratista tenga acceso como parte del suministro del Servicio de conectividad de datos a Internet, fibra oscura para los Datacenter principal y secundario de la PNP y servicio de housing del Datacenter secundario de la PNP, en ninguna circunstancia, salvo pedido expreso de LA ENTIDAD.

Las condiciones del servicio a contratar están reguladas por las disposiciones legales en lo referente a los contratos y sujeto a las disposiciones del código penal en lo referente a la Ley 30096 y su modificatoria Ley No. 30171 de Delitos Informáticos.

La obligación de confidencialidad no aplicará a la información que:

Resulte accesible al público por causa distinta del incumplimiento de la obligación de confidencialidad por la parte receptora.

Haya sido publicada con anterioridad a la fecha de la firma de contrato.

Se encuentre en poder de la Parte receptora y no esté sujeta a cualquier otro impedimento o restricción puesto de manifiesto a la otra Parte en el momento de la revelación o luego de ella.

Sea recibida a través de terceros sin restricciones y sin que implique incumplimiento del Contrato.

Sea independientemente desarrollada por la Parte receptora, siempre que no se hubiese utilizado para ello la información confidencial proporcionada por la otra Parte.

Deba ser revelada para dar cumplimiento de una orden de naturaleza judicial o administrativa, en cuyo caso la Parte receptora deberá informar a la otra Parte en forma inmediata a la sola recepción de la citada orden.

6.5 PROPIEDAD INTELECTUAL.

El contratista debe indemnizar y eximir de cualquier responsabilidad a LA ENTIDAD y a sus empleados y funcionarios, por cualquier litigio, acción legal o procedimiento administrativo, reclamación, demanda, pérdida, daño, costo y gasto; cualquiera sea su naturaleza, incluidos los honorarios y gastos de representación legal, en los cuales pueda incurrir LA ENTIDAD como resultado de cualquier trasgresión o supuesta trasgresión de cualquier patente, uso de modelo, diseño registrado, marca registrada, derechos de autor o cualquier otro derecho de propiedad intelectual que estuviese registrado o de alguna otra forma existente a la fecha del contrato debido a la provisión de los bienes por parte del Contratista o el uso de los mismos por parte de LA ENTIDAD.

Dicha indemnización no procederá si los bienes o cualquiera de sus partes fuesen utilizados para fines no previstos en el contrato o para fines que no pudiesen razonablemente inferirse de dicho contrato.

Si el Contratista no cumpliera con la obligación de informar a LA ENTIDAD dentro del plazo de ley contado a partir de la fecha del recibo de tal notificación, de su intención de proceder con cualquier acción legal o reclamación, LA ENTIDAD tendrá derecho a emprender dichas acciones o reclamaciones a nombre propio.

LA ENTIDAD se compromete a brindarle al Contratista, cuando éste así lo solicite, cualquier asistencia que estuviese a su alcance para que el Contratista pueda contestar las citadas acciones legales o reclamaciones. LA ENTIDAD será reembolsada por el Contratista por todos los gastos razonables en que hubiera incurrido.

De existir demandas o reclamos por parte de un tercero en contra de la Entidad, por motivos de propiedad intelectual trasgresión o supuesta trasgresión de cualquier patente, uso de modelo, diseño registrado, marca registrada, derechos de autor o cualquier otro derecho de propiedad intelectual, el Contratista a favor de la entidad, asumirá los costos del proceso, o cualquier otro medio de resolución de conflictos.

6.6 MEDIDAS DE CONTROL DURANTE LA EJECUCIÓN CONTRACTUAL.

Inspección y Pruebas

El contratista estará obligado a elaborar y entregar a la ENTIDAD, el PROTOCOLO DE PRUEBAS, que servirá de instrumento técnico para la recepción del servicio y permitirá garantizar que el servicio cumple con las exigencias técnicas y condiciones establecidas en las bases, así como, realizar las pruebas necesarias en número y tiempo antes de dar la conformidad correspondiente, debiéndose incluir en el protocolo, las características de los instrumentos, insumos y medios físicos que suministrará y empleará el contratista para efectos de la prueba.

Para su aplicación, el mencionado protocolo debe contar con la aprobación previa de la Entidad.

En base al Protocolo de pruebas antes indicado, el Contratista y LA ENTIDAD realizarán en forma conjunta los procedimientos de inspección, verificación y pruebas sobre la infraestructura implementados por el Contratista, de tal forma que le permita a LA ENTIDAD establecer que los servicios serán brindados de conformidad con lo solicitado en las presentes bases y a las prestaciones adicionales establecidas por el Contratista en su oferta.

Las pruebas se realizarán en los lugares de instalación.

Los insumos que demanden estas pruebas, ya sea en concepto de horas-máquina, personal, materiales, programas y/o equipos de medición de performance, no implicarán en ningún caso, reconocimiento de gastos por parte de LA ENTIDAD y deben ser provistos por el Contratista.

La omisión en la oferta de algún dispositivo, producto y/o servicio que, al momento de las pruebas, resulte necesario para el normal funcionamiento del servicio o para el cumplimiento de las especificaciones funcionales y/o técnicas ofrecidas, obligará al Contratista a proveerlo de inmediato y sin cargo alguno para LA ENTIDAD.

Las observaciones notificadas por LA ENTIDAD al Contratista durante la realización de pruebas de aceptación será absuelta por este último, sin cargo en un plazo máximo de CINCO (05) días calendario.

Los requisitos para la firma del Acta de Implementación del servicio son los siguientes:

- Que el contratista implemente en su totalidad los componentes del servicio de acceso a internet para los sitios principal y secundario, fibra oscura entre el datacenter principal y secundario de la PNP, plataforma digital de servicios para transmisión de voz, video y datos para las sedes desconcentradas PNP, a nivel nacional, servicio de seguridad de la información y seguridad informática gestionada, servicio de gestión de identidades y servicio de housing para el datacenter secundario PNP ofertados por el CONTRATISTA, considerados en el presente proceso funcionando óptimamente de acuerdo con la configuración y condiciones establecidas en las bases y haciendo entrega de la documentación requerida correspondiente.
- Que el contratista entregue el informe final, acerca de la provisión del Servicio de plataforma de backbone de fibra y gabinetes de las sedes PNP a nivel nacional.
- Que el contratista entregue el informe final acerca de la provisión del Servicio de acceso a internet para los sitios principal y secundario, fibra oscura entre el datacenter principal y secundario de la PNP, plataforma digital de servicios para transmisión de voz, video y datos para las sedes desconcentradas pnp, a nivel nacional, servicio de seguridad de la información y seguridad informática gestionada, servicio de gestión de identidades y servicio de housing para el datacenter secundario PNP.
- Una vez realizados los procedimientos de inspección y pruebas a su conformidad, el Departamento de Gestión de Centro de Datos de la División de Informática PNP o la que haga sus veces en LA ENTIDAD, levantará y entregará al Contratista el Acta de Conformidad de la



implementación del **"SERVICIO DE TRANSMISION PARA LA RED PRIVADA DE LA PNP, EN LAS UNIDADES POLICIALES A NIVEL NACIONAL; SERVICIO DE SEGURIDAD GESTIONADA Y ACCESO A INTERNET"** en un plazo máximo de siete (07) días calendario.

Supervisión

El área que coordinará con el contratista y supervisará las labores es el Departamento de Gestión de Centro de Datos de la División de Informática PNP.

6.7 CONFORMIDAD DE LA PRESTACIÓN

De la prestación

Habiendo culminado la etapa de implementación, el servicio iniciará desde el día siguiente de firmada el acta de conformidad por el Jefe del DEPGCD-DIVINF-DIRTIC PNP y el Jefe Departamento de Redes e Ingeniería de la División de Infraestructura, Tecnológica y Redes de la DIRTIC-PNP, según corresponda, previo informe del personal encargado.

A fin de emitir la conformidad del servicio de manera mensual, el contratista emitirá un informe mensual en cual se evidenciará el servicio prestado con el detalle solicitado por la Entidad, previa revisión de la información proporcionada por el Contratista, el área usuaria según su competencia, formulará el informe técnico respectivo en un plazo máximo de SIETE (7) días calendarios de recepcionado el Informe Mensual; al elaborar acta de conformidad en él se mencionará las averías e incidencias ocurridas en el mes correspondiente, con la finalidad de penalizar en caso lo amerite, la aplicación de la misma se realizará teniendo en cuenta los cuadros de penalidad mencionadas en el presente documento.

El contratista proporcionará dos reportes, el primero de la herramienta de monitoreo y el segundo con el sistema de generación de tickets. Para aplicación de las penalidades se considerará con el segundo reporte obtenido "sistema de generación de tickets para la atención de averías".

El informe y acta de conformidad deberá ser remitida a la División de Logística PNP para el pago correspondiente, según corresponda.

De la Inducción

La inducción culminará previo informe final del contratista y entrega de los certificados correspondientes, se precisa que para los cursos de certificación los certificados serán coordinados por el área usuario ante el centro de inducción.

6.8 FORMA DE PAGO

El pago de la prestación del servicio se realizará en TREINTA Y SEIS (36) pagos periódicos mensuales, al final de cada ciclo de facturación, dentro de los diez (10) días calendarios siguiente de otorgada la conformidad de los servicios. Para efectos del pago de las contraprestaciones ejecutadas por el contratista, la Entidad debe contar con la siguiente documentación:

- Comprobante de pago
- Acta de conformidad firmada por el Jefe del DEPGCD-DIVINF-DIRTIC PNP, previo informe de las áreas competentes según sus funciones (DEPGCD-DIVINF-DIRTIC PNP de la DIRTIC-PNP)

Para el caso del primer pago se solicitará de manera adicional, el acta de conformidad de implementación y puesta en marcha del servicio, y en el caso del veinticuatroavo pago, se solicitará adicionalmente la

constancia y/o certificado de Inducción según lo indicado en el numeral 5.2.1.5.7 de los presentes términos de referencia.

Dicha documentación se debe presentar en Mesa de Partes de la Sección de Ejecución Contractual del Departamento de Abastecimiento de la DIVLOG PNP, sito en Calle San Germán N° 200 – Rímac, de lunes a viernes en el horario de 08:00 a 16:00 horas.

PENALIDAD POR MORA EN LA EJECUCIÓN DE LA PRESTACIÓN.

La aplicación de penalidades por retraso injustificado en la ejecución de las prestaciones objeto del contrato y las causales para la resolución del contrato, serán aplicadas de conformidad con el artículo 161° y 162° del reglamento de ley de Contrataciones del Estado.

De existir observaciones, la Entidad las comunica al contratista, indicando claramente el sentido de estas, otorgándole un plazo para subsanar no menor de dos (2) ni mayor de ocho (08) días. Dependiendo de la complejidad o sofisticación de las subsanaciones a realizar, o si se trata de consultorías, el plazo para subsanar no puede ser menor de cinco (5) ni mayor de quince (15) días. Subsanadas las observaciones dentro del plazo otorgado, no corresponde la aplicación de penalidades de conformidad al artículo 168ª numeral 4 del reglamento de ley de Contrataciones del Estado.

6.9 REAJUSTE DURANTE LA EJECUCION DEL SERVICIO

6.10 OTRAS PENALIDADES APLICABLES.

Asimismo, conforme al artículo 163° del Reglamento de la Ley de Contrataciones del Estado, y a las características del servicio a contratar, se considera necesario establecer penalidades distintas a la penalidad por mora conforme al siguiente detalle:

6.10.1 SERVICIO BRINDADO

6.10.1.1 DISPONIBILIDAD DE ACUERDOS

Para el cálculo de la penalidad se considerará como sigue:

Penalidad Disponibilidad (DIS) ITEM1 = Penalidad Disponibilidad (DIS) $C_{1,2,4,5} +$

Penalidad Disponibilidad (DIS) C_3

6.10.1.1.1 PARA COMPONENTES 1, 2, 4 y 5 ($C_{1,2,4,5}$):

Disponibilidad de acuerdo al SLA (99.7%): El contratista será responsable de la operatividad de los servicios por cada componente 1, 2, 4 y 5 necesarios para la prestación del servicio (implica a cada equipamiento instalado), los cuales deben estar disponibles y operativos las veinticuatro (24) horas del día, los siete (07) días a la semana y trescientos sesenta y cinco (365) días del año. El nivel de disponibilidad debe ser como mínimo del 99.7% (SLA) para los siguientes servicios:

N°	DISPONIBILIDAD PROMEDIO MEDIDOS MES A MES (DIS)	PENALIDAD	PROCEDIMIENTO
01	$\leq 99.7\% \text{ y } > 95\%$	20% de 4UIT	Personal técnico de la DIRTIC PNP a través del acceso web, monitorea,

02	$\leq 95\%$ y $> 90\%$	30% de 4UIT	registra e informa la disponibilidad de los enlaces y en comparación con la información descrita en la presente tabla, LA ENTIDAD procede a solicitar la penalización, emitiendo el informe correspondiente.
03	$\leq 90\%$ y $> 80\%$	40% de 4UIT	
04	$\leq 80\%$	50% de 4UIT	

6.10.1.1.2 PARA COMPONENTES 3 C₃:

Disponibilidad de acuerdo al SLA (99.5%): El contratista será responsable de la disponibilidad de los servicios brindados en el componente 3 necesarios para la prestación del servicio (implica a cada equipamiento instalado), los cuales deben estar disponibles y operativos las veinticuatro (24) horas del día, los siete (07) días a la semana y trescientos sesenta y cinco (365) días del año. El nivel de disponibilidad debe ser como mínimo del 99.5% (SLA) para los siguientes servicios:

N°	DISPONIBILIDAD PROMEDIO MEDIDOS MES A MES (DIS)	PENALIDAD	PROCEDIMIENTO
01	$\leq 99.5\%$ y $> 93\%$	20% de 3UIT	Personal técnico de la DIRTIC PNP a través del acceso web, monitorea, registra e informa la disponibilidad de los enlaces. LA ENTIDAD procede a solicitar la penalización, emitiendo el informe correspondiente, tomando en consideración la información indicada en el presente cuadro.
02	$\leq 93\%$ y $> 90\%$	30% de 3UIT	
03	$\leq 90\%$ y $> 80\%$	40% de 3UIT	
04	$\leq 80\%$	50% de 3UIT	

6.10.1.2 CALIDAD DE ATENCIÓN ANTE AVERÍAS

6.10.1.2.1 PARA COMPONENTE 1,2, 4 Y 5:

N°	CONCEPTO- THE	PENALIDAD	PROCEDIMIENTO
01	Demora de mayor a una (01) horas hasta cinco (05) horas para la subsanación de averías de los siguientes servicios: COMPONENTE 1: Servicio de acceso de internet para la sede principal y secundario (sitio principal y secundario). COMPONENTE 2: Servicio de fibra oscura entre el Datacenter principal y secundario de la PNP COMPONENTE 4: Servicio de seguridad de la información y seguridad informática gestionada. COMPONENTE 5: Servicio de housing para el Datacenter secundario PNP	20% de 4UIT por ocurrencia	Cuando La Entidad reporte una falla en los enlaces y/o equipamientos de los Data Center, registrara la fecha y hora de la llamada. El contratista deberá crear un ticket por cada incidente reportado y resolverlo dentro de una (01) hora. Si no se soluciona, el personal de la DIRTIC PNP

02	<p>Demora de mayor a cinco (05) horas para la subsanación de averías de los siguientes servicios:</p> <p>COMPONENTE 1: Servicio de acceso de internet para la sede principal y secundario (sitio principal y secundario).</p> <p>COMPONENTE 2: Servicio de fibra oscura entre el Datacenter principal y secundario de la PNP</p> <p>COMPONENTE 4: Servicio de seguridad de la información y seguridad informática gestionada.</p> <p>COMPONENTE 5: Servicio de housing para el Datacenter secundario PNP</p>	30% de 4UIT por ocurrencia	informará sobre la demora y emitirá un informe solicitando la penalización correspondiente, según lo establecido. Además, se pedirá la penalización si ocurre otra falla similar.
03	El personal designado para los trabajos necesarios para la implementación del servicio no cuenta con uniforme o implementos de seguridad y seguro complementario de trabajo de riesgo.	20% de 1UIT por ocurrencia, asimismo, no se permitirá el ingreso del personal del contratista en los Datacenter PNP	

6.10.1.2.2 PARA COMPONENTE 3:

N°	CONCEPTO- THE	PENALIDAD	PROCEDIMIENTO
----	---------------	-----------	---------------



01	<p>COMPONENTE 3: "Plataforma digital de servicios para transmisión de voz, video y datos para las sedes desconcentradas PNP, a nivel nacional"; en la que se debe considerar, para la subsanación de averías de las líneas de conexión a internet, intranet y sus equipos de conectividad, así como los equipos de seguridad gestionada:</p> <ul style="list-style-type: none"> • Demora de mayor a cuatro (04) horas hasta nueve (09) horas para la subsanación de averías en zonas urbanas. • Demora de mayor a doce (12) horas hasta dieciséis (16) horas para la subsanación de averías en zonas rurales. 	20% de 2UIT por ocurrencia	La Entidad anotará el día y la hora en la cual realiza la llamada reportando la ocurrencia, falla y/o avería en el servicio. Ante cada falla en el servicio el contratista debe generar un ticket por el incidente reportado y solucionarlo en cuatro (04) hora, de no darse la solución del incidente, el personal de la DIRTIC PNP informará la demora de la solución de la avería, emitiendo el informe correspondiente solicitando la penalización respectiva considerando la información descrita en el presente cuadro.
02	<p>COMPONENTE 3: "Plataforma digital de servicios para transmisión de voz, video y datos para las sedes desconcentradas PNP, a nivel nacional"; en la que se debe considerar, para la subsanación de averías de las líneas de conexión a internet, intranet y sus equipos de conectividad, así como los equipos de seguridad gestionada:</p> <ul style="list-style-type: none"> • Demora de mayor a nueve (09) horas hasta catorce (14) horas para la subsanación de averías en zonas urbanas. • Demora de mayor a dieciséis (16) horas hasta veinte (20) horas para la subsanación de averías en zonas rurales. 	30% de 2UIT por ocurrencia	La Entidad anotará el día y la hora en la cual realiza la llamada reportando la ocurrencia, falla y/o avería en el servicio. Ante cada falla en el servicio el contratista debe generar un ticket por el incidente reportado y solucionarlo en cuatro (04) horas, de no darse la solución del incidente, el personal de la DIRTIC PNP informará la demora de la solución de la avería, emitiendo el informe correspondiente solicitando la penalización respectiva considerando la información descrita en el presente cuadro.
03	<p>COMPONENTE 3: "Plataforma digital de servicios para transmisión de voz, video y datos para las sedes desconcentradas PNP, a nivel nacional"; por lo que se debe considerar, para la subsanación de averías de las líneas de conexión a internet, intranet y sus equipos</p>	40% de 2UIT por ocurrencia	La Entidad anotará el día y la hora en la cual realiza la llamada reportando la ocurrencia, falla y/o avería en el servicio. Ante cada falla en el servicio el contratista debe generar un ticket por el incidente reportado y solucionarlo en cuatro (04) horas, de no darse la solución del incidente, el personal de la DIRTIC PNP informará la demora de la solución de la avería, emitiendo el informe correspondiente solicitando la penalización respectiva considerando la información descrita en el presente cuadro.



	de conectividad, así como los equipos de seguridad gestionada: <ul style="list-style-type: none"> • Demora de mayor a catorce (14) horas para la subsanación de averías en zonas urbanas. • Demora de mayor a veinte (20) horas para la subsanación de averías en zonas rurales. 		
04	El personal designado para los trabajos necesarios para la implementación del servicio no cuenta con uniforme o implementos de seguridad y seguro complementario de trabajo de riesgo.	20% de 3UIT por ocurrencia. Asimismo, no se permitirá el ingreso del personal del contratista en los Datacenter PNP	De verificar esta ocurrencia, se solicitará la penalización emitiendo el informe correspondiente solicitando la penalización respectiva considerando la información descrita en el presente cuadro (punto 04).



*El cálculo de penalidad se realizará por cada sobre el cual no se cumpla el acuerdo de nivel de servicio. La penalidad se calculará de acuerdo con la siguiente fórmula:

$$\text{Tiempo de solución} = \text{Fecha y hora de solución del incidente} - \text{Fecha y hora de generación del ticket de Incidente} - \text{Duración de parada de reloj}$$

Dónde: Parada de Reloj es el retraso en la atención de averías por motivos no atribuibles al contratista, y que se encuentran específicamente detallados en las Bases Integradas, el cual será registrado en la herramienta de gestión de averías.

La penalidad total mensual por este concepto se obtiene sumando las penalidades obtenidas de las líneas de conexión a internet, fibra oscura, plataforma digital de servicios para transmisión de voz, video y datos para las sedes desconcentrada PNP a nivel nacional, servicio de seguridad de la información, servicio sms y servicio de autenticación, servicio de housing para el datacenter secundario. Por ejemplo:

Penalidad Total (THE) ITEM1 = THE por Equipo1 * penalidad +

THE por Equipo2 * penalidad + THE por EquipoXX * penalidadXX

Frecuencia de caída Mensual (FCM) del servicio, al mes: Medido por la cantidad de veces en que está fuera de servicio la línea a internet e intranet, la fibra oscura o los equipos de comunicación y seguridad de las sedes a nivel nacional, así como los comprendidos en el servicio de seguridad gestionada.

Cuadro de penalidad

FCM	Penalidad	PROCEDIMIENTO
-----	-----------	---------------

3 o 4	10% de una UIT	El personal de la DIRTIC PNP informará de las caídas mensuales del servicio (contados según ticket de avería) emitiendo el informe respectivo solicitando la penalización del servicio considerando la información indicada en el presente cuadro.
5 o 6	20% de una UIT	
7 u 8	30% de una UIT	
Mayor a 8	35% de una UIT	

Si la FCM es mayor a 4 caídas del servicio, se considera como una falta grave, y se acumula para efectos de resolver el Contrato.

De presentarse una situación excepcional que impida al CONTRATISTA cumplir con los plazos de respuesta establecidos, éste podrá enviar una Carta y un correo electrónico a LA ENTIDAD y a la Unidad Usuaria (DIRTIC PNP) en un plazo no mayor a cuarenta y ocho (48) horas de comunicado la avería, exponiendo los motivos técnicos que originaron la situación. LA ENTIDAD evaluará dicha justificación en un plazo no mayor a setenta y dos (72) horas. Si LA ENTIDAD encuentra justificadas y aprueba las razones expuestas, no se contabilizarán las horas de exceso incurridas para el cálculo del UPTIME.

Del mismo modo, si la Entidad excede el plazo máximo de setenta y dos (72) horas en dar respuesta a las razones expuestas en la comunicación del contratista, no se contabilizarán las horas de exceso incurridas para el cálculo del UPTIME y se procederá a la parada de reloj.

Pérdida de Paquetes (PPKT)

La pérdida de paquetes se calcula producto de la ejecución del comando ping en el circuito de datos (Entre el equipo de comunicación del circuito de datos de la Unidad Remota y el equipo de comunicación del circuito de datos del Nodo Central), sobre una muestra de 1,000 paquetes de tamaño estándar (32 Bytes), la pérdida de paquetes no debe ser mayor al 1 %.

Las pruebas se realizarán sobre un enlace que no exceda un consumo del 80%, en cuanto al periodo de muestreo este podrá ser mayor a tres minutos, la medición de pérdida de paquetes se deberá realizar una (01) vez al mes por cada enlace de datos.

La medición de este factor de calidad será medida en condiciones climáticas normales.

Cuadro de Penalidad:

PPKT	Penalidad	PROCEDIMIENTO
>1% y < 2%	5% de una UIT	El personal de la DIRTIC PNP informará sobre la pérdida de paquetes de acuerdo al reporte obtenido del sistema de monitoreo o de acuerdo el reporte brindado por el contratista, la DIRTIC PNP emitirá un informe solicitando la penalización tomando en consideración la información indicada en el presente cuadro.
>= 2% y < 3%	10% de una UIT	
>= 3% y < 4%	20% de una UIT	
>= 4%	30% de una UIT	

Si el PPKT es mayor a 4%, se considera como una falta grave, y se acumula para efectos de resolver el Contrato. Ante una caída total del servicio, no se considerará la penalidad por pérdida de paquetes.



ya que esta penalidad se aplica cuando el enlace está operativo, pero con ciertas limitantes de conectividad.

6.10.1.2.3 PARA EL COMPONENTE 3 LATENCIA

El contratista será responsable de mantener la latencia según lo solicitado por la entidad, los servicios brindados en el componente 3 necesarios para la prestación del servicio implica la implementación de un red corporativa la misma que requiere mantener latencia bajas para el normal funcionamiento de los sistemas policiales, interoperabilidad entre entidades nacionales e internacionales, soluciones de videoconferencia y acceso a herramientas de investigación propias de las Unidades Operativas PNP, servicio que debe estar controlado las veinticuatro (24) horas del día, los siete (07) días a la semana y trescientos sesenta y cinco (365) días del año.

N°	LATENCIA	PENALIDAD	PROCEDIMIENTO
01	>20ms y 40ms> (Lima Metropolitana F.O.) >40ms y 60ms> (Provincia F.O.) ≥60ms y 120ms> (Radio Enlace)	10% de 3UIT	El personal de la DIRTIC PNP informara sobre la perdida de paquetes de acuerdo al reporte obtenido del sistema de monitoreo o de acuerdo al reporte brindado por le contratista. La DIRTIC PNP emitirá un informe solicitando la penalización tomando en consideración la informacion indicada en el presente cuadro.
02	≥40ms y 60ms> (Lima Metropolitana F.O.) ≥60ms y 90ms> (Provincia F.O.) ≥120ms y 180ms> (Radio Enlace)	20% de 3UIT	
03	≥60ms y 90ms> (Lima Metropolitana F.O.) ≥90ms y 130ms> (Provincia F.O.) ≥180ms y 240ms> (Radio Enlace)	40% de 3UIT	
04	≥90ms y 150ms> (Lima Metropolitana F.O.) ≥130ms y 210ms> (Provincia F.O.) ≥240ms y 300ms> (Radio Enlace)	50% de 3UIT	
05	≥150ms (Lima Metropolitana F.O.) ≥210ms (Provincia F.O.) ≥300ms (Radio Enlace)	60% de 3UIT	

6.10.2 CAUSALES DE RESOLUCIÓN DE CONTRATO

De conformidad con el artículo 164° del Reglamento de la Ley de Contrataciones del Estado, respecto a causales de resolución de contrato por incumplimiento.

Las partes acuerdan que todas las controversias entre las partes durante la ejecución del contrato se resuelvan mediante conciliación o arbitraje, según el acuerdo de las partes.

El arbitraje será institucional y administrado por el Centro de Arbitraje del Ilustre Colegio de Abogados de Lima o por el Centro de Análisis y Resolución de Conflictos de la Pontificia Universidad Católica del Perú, a fin de resolver dichas controversias dentro del plazo de caducidad previsto en la Ley de Contrataciones del Estado y su Reglamento, el mismo que será resuelto por un Tribunal Arbitral Unipersonal o Árbitro Único.

Facultativamente, cualquiera de las partes tiene el derecho a solicitar una conciliación dentro del plazo de caducidad correspondiente, según lo señalado en el artículo 224 del Reglamento de la Ley de Contrataciones del Estado, sin perjuicio de recurrir al arbitraje, en caso no se llegue a un acuerdo entre ambas partes o se llegue a un acuerdo parcial. Las controversias sobre nulidad del contrato solo pueden ser sometidas a arbitraje.

El Laudo arbitral emitido es inapelable, definitivo y obligatorio para las partes desde el momento de su notificación, según lo previsto en el numeral 45.21 del artículo 45 de la Ley de Contrataciones del Estado.

Las partes se someten al fuero jurisdiccional de Lima.

6.10.3 RESPONSABILIDAD POR VICIOS OCULTOS.

El contratista será responsable por la calidad ofrecida y los vicios ocultos del servicio ofertado, conforme a lo indicado en el Artículo 40° de la Ley de Contrataciones y 173° del Reglamento de la Ley de Contrataciones del Estado, que deberá ser considerada por treinta y seis (36) meses de vigencia del contrato, hasta 30 días después de la última conformidad otorgada por la Entidad; esta responsabilidad se considerará a partir de la conformidad de la implementación del servicio otorgada por parte del Jefe del DEPGCD-DIVINF-DIRTIC-PNP Yel Jefe Departamento de Redes e Ingeniería de la División de Infraestructura, Tecnológica y Redes de la DIRTIC-PNP según corresponda funcionalmente.

7 CLÁUSULA ANTICORRUPCIÓN

EL CONTRATISTA declara y garantiza no haber, directa o indirectamente, o tratándose de una persona jurídica a través de sus socios, integrantes de los órganos de administración, apoderados, representantes legales, funcionarios, asesores o personas vinculadas a las que se refiere el artículo 7 del Reglamento de la Ley de Contrataciones del Estado, ofrecido, negociado o efectuado, cualquier pago o, en general, cualquier beneficio o incentivo ilegal en relación al contrato.

Asimismo, el CONTRATISTA se obliga a conducirse en todo momento, durante la ejecución del contrato, con honestidad, probidad, veracidad e integridad y de no cometer actos ilegales o de corrupción, directa o indirectamente o a través de sus socios, accionistas, participacionistas, integrantes de los órganos de administración, apoderados, representantes legales, funcionarios, asesores y personas vinculadas a las que se refiere el artículo 7 del Reglamento de la Ley de Contrataciones del Estado.

Además, EL CONTRATISTA se compromete a i) comunicar a las autoridades competentes, de manera directa y oportuna, cualquier acto o conducta ilícita o corrupta de la que tuviera conocimiento; y ii) adoptar medidas técnicas, organizativas y/o de personal apropiadas para evitar los referidos actos o prácticas.

Finalmente, EL CONTRATISTA se compromete a no colocar a los funcionarios públicos con los que deba interactuar, en situaciones reñidas con la ética. En tal sentido, reconoce y acepta la prohibición de ofrecerles a éstos cualquier tipo de obsequio, donación, beneficio y/o gratificación, ya sea de bienes o servicios, cualquiera sea la finalidad con la que se lo haga.

8 REQUISITOS DE CALIFICACIÓN

A	CAPACIDAD LEGAL
	HABILITACIÓN
	<u>Requisitos:</u> <ul style="list-style-type: none"> Autorización o registro del ministerio de Transporte y Comunicaciones (MTC) para brindar los servicios de internet y transmisión de datos o Registros de Empresas prestadoras de Servicios de Valor añadido.
	<u>Acreditación:</u>

- Copia simple del documento en el cual se acredite que cuenta con la autorización del Ministerio de Transporte y Comunicaciones (Certificado de Registro de Empresas prestadoras de servicios de Valor añadido)

Importante

En el caso de consorcios, cada integrante del consorcio que se hubiera comprometido a ejecutar las obligaciones vinculadas directamente al objeto de la convocatoria debe acreditar este requisito.

B	CAPACIDAD TÉCNICA Y PROFESIONAL
B.1	CALIFICACIONES DEL PERSONAL CLAVE
B.1.1	FORMACIÓN ACADÉMICA
	<p><u>Requisitos:</u></p> <p>UN (01) JEFE DEL PROYECTO Ingeniero titulado, en algunas de las especialidades siguientes: Eléctrica o Electrónica o Telecomunicaciones o sistemas o informática o industrial o telemática o mecatrónica o sistemas e informática o redes.</p> <p><u>Acreditación:</u> El Ingeniero titulado, en algunas de las especialidades siguientes: Eléctrica o Electrónica o Telecomunicaciones o sistemas o informática o industrial o telemática o mecatrónica o sistemas e informática o redes, será verificado por el comité de selección en el Registro Nacional de Grados Académicos y Títulos Profesionales en el portal web de la Superintendencia Nacional de Educación Superior Universitaria - SUNEDU a través del siguiente link: https://enlinea.sunedu.gob.pe/ o en el Registro Nacional de Certificados, Grados y Títulos a cargo del Ministerio de Educación a través del siguiente link: https://titulosinstitutos.minedu.gob.pe/, según corresponda. En caso que, el grado o título profesional requerido, no se encuentre inscrito en el referido registro, el postor debe presentar la copia del diploma respectivo a fin de acreditar la formación académica requerida.</p> <p>UN (01) JEFE DE SERVICIO Ingeniero titulado, en algunas de las especialidades siguientes: Electrónica o Telecomunicaciones o sistemas o informática o industrial o telemática o empresarial o mecatrónica o Sistemas e Informática o Redes y Comunicaciones.</p> <p><u>Acreditación:</u> El ingeniero titulado, en algunas de las especialidades siguientes: Electrónica o Telecomunicaciones o sistemas o informática o industrial o telemática o empresarial o mecatrónica o Sistemas e Informática o Redes y Comunicaciones, será verificado por el comité de selección en el Registro Nacional de Grados Académicos y Títulos Profesionales en el portal web de la Superintendencia Nacional de Educación Superior Universitaria - SUNEDU a través del siguiente link: https://enlinea.sunedu.gob.pe/ o en el Registro Nacional de Certificados, Grados y Títulos a cargo del Ministerio de Educación a través del siguiente link: https://titulosinstitutos.minedu.gob.pe/, según corresponda. En caso que, el grado o título profesional requerido, no se encuentre inscrito en el referido registro, el postor debe presentar la copia del diploma respectivo a fin de acreditar la formación académica requerida.</p> <p>DOS (02) ESPECIALISTAS DE CIBERSEGURIDAD Tecnico, Bachiller o Ingeniero titulado en algunas de las profesiones siguientes: Electrónica o Telecomunicaciones o Electrónica y Telecomunicaciones o Redes o Redes y Comunicación de Datos o Sistemas o Sistemas e Informática o Empresarial y de Sistemas o Informática o Industrial o Telemática o Mecatrónica.</p> <p><u>Acreditación:</u> Tecnico, Bachiller o Ingeniero titulado en algunas de las profesiones siguientes: Electrónica o Telecomunicaciones o Electrónica y Telecomunicaciones o Redes o Redes y Comunicación de Datos o Sistemas o Sistemas e Informática o Empresarial y de Sistemas o Informática o Industrial o Telemática o Mecatrónica, será verificado por el comité de selección en el Registro Nacional de Grados Académicos y Títulos Profesionales en el portal web de la Superintendencia Nacional de Educación Superior Universitaria - SUNEDU a través del siguiente link: https://enlinea.sunedu.gob.pe/ o en el Registro Nacional de Certificados, Grados y Títulos a cargo del Ministerio de Educación a través del siguiente link: https://titulosinstitutos.minedu.gob.pe/, según corresponda. En caso que, el grado o título profesional requerido, no se encuentre inscrito en el referido registro, el postor debe presentar la copia del diploma respectivo a fin de acreditar la formación académica requerida.</p>



B.1.2	CAPACITACIÓN
	<p><u>Requisitos:</u> UN (01) JEFE DEL PROYECTO Capacitación en Project Management Professional, de ciento veinte (120) horas lectivas <u>Acreditación:</u> Se acreditará con copia simple del certificado o Constancia oficial.</p> <p>UN (01) JEFE DE SERVICIO Capacitación en Gestión de servicios y/o proyectos, de ciento veinte (120) horas lectivas y/o. <u>Acreditación:</u> Se acreditará con copia simple del certificado o Constancia oficial</p> <p>DOS (02) ESPECIALISTAS DE CIBERSEGURIDAD</p> <p>Duración mínima de VEINTE (20) horas por cada solución.</p> <p>Certificación o Constancia oficial en mínimo 06 soluciones de la siguiente lista:</p> <ul style="list-style-type: none"> • Firewall de nueva generación, para red externa y red interna. • Detección y control de malware avanzado. • Protección de portales web y base de datos • Spam Firewall y protección ante phishing dirigido • Protección contra ataques de denegación de servicios distribuido • Análisis de vulnerabilidades de red • Herramienta informática para prevención de pérdida de información, auditoría y anticorrupción. • Solución de antivirus para servidores y endpoint de la DIRTIC PNP. • Servicio de SOC Gestionado, Herramienta de Análisis de incidentes y Correlación de logs de seguridad. • Servicios de seguridad de la información. <p><u>Acreditación:</u> Se acreditará con copia simple del certificado o Constancia oficial.</p> <div data-bbox="379 1205 1426 1352" style="border: 1px solid black; padding: 5px;"> <p>Importante</p> <p><i>Se podrá acreditar la capacitación mediante certificados de estudios de postgrado, considerando que cada crédito del curso que acredita la capacitación equivale a dieciséis horas lectivas, según la normativa de la materia.</i></p> </div>
B.2	<p>EXPERIENCIA DEL PERSONAL CLAVE</p> <p><u>Requisitos:</u></p> <p>UN (01) JEFE DEL PROYECTO Experiencia laboral mínimo de tres (03) años como jefe o gerente o especialista en implementación y/o supervisión y/o gestión y/o instalación de servicios de líneas de comunicación y/o fibra óptica y/o equipos de red (networking) y/o infraestructura de telecomunicaciones y/o interconexión de voz y datos y/o VPN y/o Internet.</p> <p>UN (01) JEFE DE SERVICIO Experiencia laboral mínimo de tres (03) años como jefe o gerente o especialista o coordinador en implementación y/o supervisión y/o gestión y/o instalación de servicios de líneas de comunicación y/o fibra óptica y/o equipos de red (networking) y/o infraestructura de telecomunicaciones y/o interconexión de voz y datos y/o VPN y/o Internet.</p> <p>DOS (02) ESPECIALISTAS DE CIBERSEGURIDAD Experiencia laboral mínimo de dos (02) años como especialista, implementador, coordinador en implementación y/o configuración y/o instalación de servicios de redes LAN/WAN y/o servicios de transmisión de voz y/o servicios de transmisión de video y/o servicios de transmisión de internet.</p>



B.3

EXPERIENCIA DEL PERSONAL CLAVE**Acreditación:**

La experiencia del personal clave se acreditará con cualquiera de los siguientes documentos: (i) copia simple de contratos y su respectiva conformidad o (ii) constancias o (iii) certificados o (iv) cualquier otra documentación que, de manera fehaciente demuestre la experiencia del personal propuesto.

Importante

- Los documentos que acreditan la experiencia deben incluir los nombres y apellidos del personal clave, el cargo desempeñado, el plazo de la prestación indicando el día, mes y año de inicio y culminación, el nombre de la Entidad u organización que emite el documento, la fecha de emisión y nombres y apellidos de quien suscribe el documento.
- En caso los documentos para acreditar la experiencia establezcan el plazo de la experiencia adquirida por el personal clave en meses sin especificar los días se debe considerar el mes completo.
- Se considerará aquella experiencia que no tenga una antigüedad mayor a veinticinco (25) años anteriores a la fecha de la presentación de ofertas.
- Al calificar la experiencia del personal, se debe valorar de manera integral los documentos presentados por el postor para acreditar dicha experiencia. En tal sentido, aun cuando en los documentos presentados la denominación del cargo o puesto no coincida literalmente con aquella prevista en las bases, se deberá validar la experiencia si las actividades que realizó el personal corresponden con la función propia del cargo o puesto requerido en las bases.

C

EXPERIENCIA DEL POSTOR EN LA ESPECIALIDAD**Requisitos:**

El postor debe acreditar un monto facturado acumulado equivalente a DIEZ MILLONES CON 00/100 SOLES (S/ 10,000,000.00) por la contratación de servicios iguales o similares al objeto de la convocatoria, durante los OCHO (08) años anteriores a la fecha de la presentación de ofertas que se computarán desde la fecha de la conformidad o emisión del comprobante de pago, según corresponda.

Se consideran servicios iguales o similares al objeto de la convocatoria:

- Servicio de transmisión de datos
- Servicio de internet
- Servicio de internet dedicado
- Servicio de Plan de Datos
- Servicio de Telecomunicaciones
- Servicio de líneas IP
- Servicio de conectividad
- Servicio de interconexión
- Servicio de voz y datos
- Servicio de Construcción, Instalación y Tendido de cable de Fibra Óptica
- Servicio de instalación de fibra óptica
- Servicio de despliegue de fibra óptica
- Servicio de tendido de fibra óptica

Acreditación

La experiencia del postor en la especialidad se acreditará con copia simple de (i) contratos u órdenes de servicios, y su respectiva conformidad o constancia de prestación; o (ii) comprobantes de pago cuya cancelación se acredite documental y fehacientemente, con voucher de depósito, nota de abono, reporte de estado de cuenta, cualquier otro documento emitido por Entidad del sistema financiero que acredite el abono o mediante cancelación en el mismo comprobante de pago¹, correspondientes a un

¹ Cabe precisar que, de acuerdo con la Resolución N° 0065-2018-TCE-S1 del Tribunal de Contrataciones del Estado:

máximo de veinte (20) contrataciones.

En caso los postores presenten varios comprobantes de pago para acreditar una sola contratación, se debe acreditar que corresponden a dicha contratación; de lo contrario, se asumirá que los comprobantes acreditan contrataciones independientes, en cuyo caso solo se considerará, para la evaluación, las veinte (20) primeras contrataciones indicadas en el **Anexo N° 8** referido a la Experiencia del Postor en la Especialidad.

En el caso de servicios de ejecución periódica o continuada, solo se considera como experiencia la parte del contrato que haya sido ejecutada durante los ocho (8) años anteriores a la fecha de presentación de ofertas, debiendo adjuntarse copia de las conformidades correspondientes a tal parte o los respectivos comprobantes de pago cancelados.

En los casos que se acredite experiencia adquirida en consorcio, debe presentarse la promesa de consorcio o el contrato de consorcio del cual se desprenda fehacientemente el porcentaje de las obligaciones que se asumió en el contrato presentado; de lo contrario, no se computará la experiencia proveniente de dicho contrato.

Asimismo, cuando se presenten contratos derivados de procesos de selección convocados antes del 20.09.2012, la calificación se ceñirá al método descrito en la Directiva "Participación de Proveedores en Consorcio en las Contrataciones del Estado", debiendo presumirse que el porcentaje de las obligaciones equivale al porcentaje de participación de la promesa de consorcio o del contrato de consorcio. En caso que en dichos documentos no se consigne el porcentaje de participación se presumirá que las obligaciones se ejecutaron en partes iguales.

Si el titular de la experiencia no es el postor, consignar si dicha experiencia corresponde a la matriz en caso que el postor sea sucursal, o fue transmitida por reorganización societaria, debiendo acompañar la documentación sustentatoria correspondiente.

Si el postor acredita experiencia de otra persona jurídica como consecuencia de una reorganización societaria, debe presentar adicionalmente el **Anexo N° 9**.

Cuando en los contratos, órdenes de servicios o comprobantes de pago el monto facturado se encuentre expresado en moneda extranjera, debe indicarse el tipo de cambio venta publicado por la Superintendencia de Banca, Seguros y AFP correspondiente a la fecha de suscripción del contrato, de emisión de la orden de servicios o de cancelación del comprobante de pago, según corresponda.

Sin perjuicio de lo anterior, los postores deben llenar y presentar el **Anexo N° 8** referido a la Experiencia del Postor en la Especialidad.

Importante

- *Al calificar la experiencia del postor, se debe valorar de manera integral los documentos presentados por el postor para acreditar dicha experiencia. En tal sentido, aun cuando en los documentos presentados la denominación del objeto contractual no coincida literalmente con el previsto en las bases, se deberá validar la experiencia si las actividades que ejecutó el postor corresponden a la experiencia requerida.*
- *En el caso de consorcios, solo se considera la experiencia de aquellos integrantes que se hayan comprometido, según la promesa de consorcio, a ejecutar el objeto materia de la convocatoria, conforme a la Directiva "Participación de Proveedores en Consorcio en las Contrataciones del Estado".*

9 NOTIFICACIÓN ELECTRÓNICA

Constituye forma válida de notificación, la que efectúe la Entidad a través del correo electrónico (domicilio virtual) consignado por el contratista en su cotización y ratificado en la orden de compra o de servicio. Para dichos efectos, el contratista declara y asume dicho domicilio como su ubicación habitual en la red de Internet, autorizando a la Entidad a utilizar esta modalidad de notificación oficial. La suscripción de la cotización por parte del contratista implica su "autorización expresa" para el uso de esta modalidad de notificación.

"... el solo sello de cancelado en el comprobante, cuando ha sido colocado por el propio postor, no puede ser considerado como una acreditación que produzca fehaciencia en relación a que se encuentra cancelado. Admitir ello equivaldría a considerar como válida la sola declaración del postor afirmando que el comprobante de pago ha sido cancelado"
(...)

"Situación diferente se suscita ante el sello colocado por el cliente del postor [sea utilizando el término "cancelado" o "pagado"] supuesto en el cual sí se contaría con la declaración de un tercero que brinde certeza, ante la cual debiera reconocerse la validez de la experiencia".

La notificación dirigida a la dirección de correo electrónico señalada por el contratista, se entiende válidamente efectuada cuando la Entidad reciba respuesta de recepción de la dirección electrónica indicada por el contratista. Dicha notificación surte efectos el día en que conste haber sido recibida.

Si la entidad no recibe respuesta en un plazo máximo de DOS (02) días hábiles contados desde el día siguiente efectuado el acto de notificación por correo electrónico, procede a notificar en forma física al contratista en su domicilio, teniendo en cuenta lo dispuesto en el artículo 21 del Decreto Supremo N° 274447, Ley del Procedimiento Administrativo General.

El contratista es responsable de mantener oportunamente los medios de recepción de notificación, debiendo comunicar a la Dirección de Administración, la Unidad de Administración o la que haga sus veces en las UE de la PNP cualquier cambio de domicilio o dirección, con una anticipación no menor a quince (15) días calendario

Anexo A – Ubicación de sedes policiales y ancho de banda de transmisión de las líneas de datos

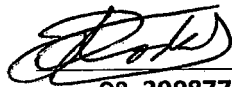
Anexo A1 Circuitos de DATACENTER

Anexo B1 Sedes policiales tipos 1 consideradas

Anexo B2 Sedes policiales tipos 2 consideradas

Anexo C – Diseño de red propuesto.

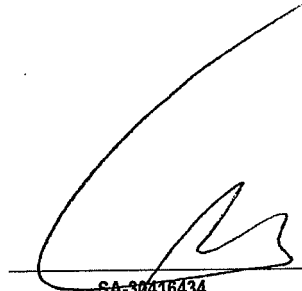
Anexo D Para la prestación del servicio -



OS- 390877

Donaire DURAN JANAMPA
MAYOR S PNP

JEFE DE LA SECCION OPERACIONES DEL
DEPGCD - DIVINF - DIRTIC PNP



SA-30416434

Juan Carlos LINARES ARAUJO
SUB OFICIAL SUPERIOR PNP

SECCION DE REDES Y SEGURIDAD INFORMÁTICA
DEPGCD - DIVINF - DIRTIC PNP




OS- 368083

Jesús SEQUEIROS ARONE
MAYOR PNP

JEFE (E) DEL DEPARTAMENTO DE GESTION
DE CENTRO DE DATOS DIVINF - DIRTIC PNP

Handwritten signature and initials in the top left corner.



Handwritten signature and initials in the middle left margin.

Handwritten signature and initials in the middle left margin.

Handwritten signature and initials in the middle left margin.

ANEXOS

[Handwritten signature]

[Handwritten signature]

[Handwritten signature]

[Handwritten signature]

[Handwritten signature]



ANEXO A

UBICACIÓN, VELOCIDAD DE TRANSMISIÓN Y PUNTOS DE RED DE LOS 1018 SEDES POLICIALES A
NIVEL NACIONAL

N°	SEDE	DIRECCIÓN ACTUAL	DISTRITO	PROVINCIA	DPTO	LATITUD	LONGITUD	ANCH O BANDA	SWITCH CORE LAN Y GABINETE PRINCIPAL	SWITCH H LAN 48 PUERTOS Y GABINETE PRINCIPAL	SWITCH LAN DE DISTRIBUCION 48 PUERTOS Y GABINETE PRINCIPAL	FIREWALL	FIREW ALL DE PROXIMA GENE RACION	N° DE ACC POI NT	Zonificación	TIPO DE UNIDAD	TIPO
1	CPNP SECTORIAL BAGUA	AV. HEROES DEL CENÉPA # 1000	BAGUA	BAGUA	AMAZONAS	-5.639849	-78.531008	100M			0	1	1	0	2	URBANO B	TIPO 1
2	CPNP SECTORIAL JAZAN	AV. MARGINAL # 121	JAZAN	BONGARA	AMAZONAS	222291	-77.978215	100M			0	1	1	0	2	URBANO B	TIPO 1
3	DESPPCAR PEDRO RUIZ GALLO	CARRETERA FERNANDO BELAUNDE TERRY # SN	JAZAN	BONGARA	AMAZONAS	-5.941878	-77.976206	100M			0	0	1	0	0	URBANO CARRETERAS	TIPO 1
4	COMISARIA DE TURISMO AMAZONAS - COMTUR AMAZONAS	JR. PUNO N° 571 - CHACHAPOYAS	CHACHAPOYAS	CHACHAPOYAS	AMAZONAS	6.2294947	-77.87544326	100M			0	0	1	0	1	URBANO TURISMO	TIPO 1
5	CPNP SECTORIAL CHACHAPOYAS / OFICRI	JIRÓN AMAZONAS # 1320	CHACHAPOYAS	CHACHAPOYAS	AMAZONAS	-6.229875	-77.874661	100M			0	1	1	0	3	URBANO A	TIPO 1
6	DIRCOCOR AMAZONAS	JR. LIBERTAD N° 1353-1357	CHACHAPOYAS	CHACHAPOYAS	AMAZONAS	-6.228788	-77.875471	100M			0	1	1	0	1	URBANO DIRCOCOR	TIPO 1
7	DIV MEDIO AMBIENTE (D.V. UNI. ESP.)	JR. SANTO DOMINGO 876	CHACHAPOYAS	CHACHAPOYAS	AMAZONAS	-6.232306	-77.874628	100M			0	0	1	0	1	URBANO AMBIENTE	TIPO 1
8	REGPOL AMAZONAS	JIRÓN AVACUCHO C 10	CHACHAPOYAS	CHACHAPOYAS	AMAZONAS	-6.228955	-77.873369	100M	1		1	0	1	0	5	URBANO UNIDAD PNP	TIPO 2
9	CPNP SECTORIAL LAMUD	JIRÓN GRAU # 451	LAMUD	LUYA	AMAZONAS	6.1392107 04	-77.95205355	100M			0	1	1	0	1	URBANO B	TIPO 1
10	CPNP LUYA - CRUZ SANTIAGO VALQUI OROSCO	JIRÓN SAN MARTÍN # 910	LUYA	LUYA	AMAZONAS	6.1633433 33	-77.94431667	100M			0	1	1	0	1	URBANO C	TIPO 1
11	CPNP SECTORIAL SAN NICOLAS	JIRÓN HUAMBO # 316	SAN NICOLAS	RODRIGUEZ DE MENDOZA	AMAZONAS	6.3948683 33	-77.48277833	100M			0	1	1	0	1	URBANO B	TIPO 1
12	CP UTUBAMBABA - CPNP SECTORIAL UTUBAMBABA (O BAGUA GRANDE)/POLICINICO BAGUA GRANDE/DEPINCRI BAGUA GRANDE	AV. CHACHAPOYAS 2318	BAGUA GRANDE	UTUBAMBABA	AMAZONAS	5.7574516 67	-78.44050833	400M			2	1	1	0	2	URBANO UNIDAD PNP	TIPO 1
13	CPNP CAJARURO	JIRÓN EL COMERCIO # 407	CAJARURO	UTUBAMBABA	AMAZONAS	-5.75741	-78.42963	100M			0	1	1	0	1	URBANO D	TIPO 1
14	CPNP SECTORIAL AUA	AV. TUPAC AMARU - PEDRO PABLO ATUSPARIA # SN	AUA	AUA	ANCASH	-9.78324	-77.60937667	100M			0	1	1	0	1	RURAL C	TIPO 1
15	CPNP SECTORIAL ASUNCION - CHACAS	JIRÓN RAYMONDI # SN	CHACAS	ASUNCION	ANCASH	-9.18347	-77.36637833	100M			0	1	1	0	1	RURAL C	TIPO 1
16	CPNP SECTORIAL BOLOGNESI CHIQUEJAN	JIRÓN COMERCIO # SN	CHIQUEJAN	BOLOGNESI	ANCASH	10.154715	-77.45747667	100M			0	1	1	0	1	RURAL B	TIPO 1
17	CPNP SECTORIAL CARHUAZ	JIRÓN RIO BUIN # SN	CARHUAZ	CARHUAZ	ANCASH	-9.282405	-77.64595333	100M			0	1	1	0	1	URBANO B	TIPO 1
18	CPNP SECTORIAL SAN LUIS	JIRÓN DANIEL ALCIDES CARRION # 310	SAN LUIS	CARLOS FERMIN FITZCARRALD	ANCASH	-9.0946	-77.33010167	100M			0	1	1	0	1	RURAL C	TIPO 1
19	CPNP SECTORIAL CASMA/DESPPCAR CASMA	AV. MAGDALENA SN. CASMA	CASMA	CASMA	ANCASH	9.4756016 67	-78.30602667	100M			0	1	1	0	2	URBANO A	TIPO 1
20	CPNP YAUTAN	AV. CASMA S/N MZ.1 LT.1	YAUTAN	CASMA	ANCASH	9.5118616 67	-77.99693167	100M			0	1	1	0	1	RURAL C	TIPO 1
21	DIV. POL. CHIMBOTE	JR. LEONCIO PRADO 401 - CERCADO	CERCADO	CHIMBOTE	ANCASH	9.0739664	-78.5937685	100M			0	1	1	0	1	URBANO DIVPOL	TIPO 1
22	CPNP SECTORIAL CORONGO	JIRÓN LIMA # SN	CORONGO	CORONGO	ANCASH	8.5705816 67	-77.89835167	100M			0	1	1	0	1	RURAL B	TIPO 1

[Handwritten signature]



[Handwritten signature]

23	CPNP HUARAZ	JIRON JOSE DE SUCRE # SN	HUARAZ	HUARAZ	ANCASH	9.5293483 43	-77.52987184	100M			0	1	1	0	1	URBANO	A	TIPO 1
24	CPNP SAN GERONIMO	AV. FRANCISCO BOLOGNESI # SN	HUARAZ	HUARAZ	ANCASH	9.5270966 67	-77.535465	100M			0	1	1	0	1	URBANO	C	TIPO 1
25	CPNP TACLAN	CARRERA PENETRACION PATIVILCA HUARAZ # SN	HUARAZ	HUARAZ	ANCASH	-9.542485	-77.533225	100M			0	1	1	0	1	URBANO	C	TIPO 1
26	REGPOL ANCASH	JIRON 28 DE JULIO 755	HUARAZ	HUARAZ	ANCASH	-9.53109	-77.52825	200M			0	1	1	0	1	URBANO	REGPOL	TIPO 1
27	COMISARIA DE TURISMO HUARAZ	JR. MARIANO MELGAR N° 453- CENTENARIO	INDEPENDENCIA	HUARAZ	ANCASH	-9.519668	-77.527482	100M			0	0	1	0	1	URBANO	TURISMO	TIPO 1
28	CPNP PARIACOTO	JR. GONZALO SALAZAR MIGUELA MORAN SN	PARIACOTO	HUARAZ	ANCASH	9.5597166 67	-77.89026167	100M			0	1	1	0	1	RURAL	C	TIPO 1
51	DEPNEME-DEPSEPN-DEPTA-DEPSESP- DEPEPROC-DEPROVE-DEPAIUS	AV. JOSE PARDO CUADRA 26	CHIMBOTE	SANTA	ANCASH	-9.086921	-78.572428	200M		1	1	0	1	0	5	URBANO	UNIDAD PNP	TIPO 2
30	CPNP RURAL CHAVIN DE HUANTAR	JIRON 17 DE ENERO # SN	CHAVIN DE HUANTAR	HUARI	ANCASH	9.5835983 33	-77.17781167	100M			0	1	1	0	1	RURAL	C	TIPO 1
31	CPNP SECTORIAL HUARI/DIVPOL HUARI	JR. ANCASH CDRA. 10 Y JR. ELIAZAR	CHAVIN DE HUANTAR	HUARI	ANCASH	-9.348804	-77.173099	100M			0	1	1	0	2	RURAL	B	TIPO 1
32	DESPCAR HUARI	JR. LAS FLORES S/N CHAVIN DE HUANTAR (COSO TAURINO)	HUARI	HUARI	ANCASH	-9.582573	-77.177715	100M			0	0	1	0	0	RURAL	CARRERAS	TIPO 1
33	CPNP RURAL SAN MARCOS	JIRON GRAU # SN	SAN MARCOS	HUARI	ANCASH	9.5239516 67	-77.15768167	100M			0	1	1	0	1	RURAL	C	TIPO 1
34	CPNP SECTORIAL HUARMY	AV. CABO ALBERTO REYES # 224	HUARMY	HUARMY	ANCASH	10.069089	-78.15456972	100M			0	1	1	0	2	URBANO	A	TIPO 1
35	CPNP CANON DEL PATO HUALLANCA	AV. 14 DE ABRIL # 171	HUALLANCA	HUAYLAS	ANCASH	-8.81843	-77.86193	100M			0	1	1	0	1	RURAL	DIRCOCOR	TIPO 1
36	CPNP SECTORIAL MARISCAL LUZURIAGA - PISCOBAMBA	JIRON MARISCAL LUZURIAGA # 125	PISCOBAMBA	MARISCAL LUZURIAGA	ANCASH	8.8883796 62	-77.35507965	100M			0	1	1	0	1	RURAL	C	TIPO 1
37	CPNP SECTORIAL CABANA	CALLE PLAZA DE ARMAS # SN	CABANA	PALLASCA	ANCASH	8.3931431	-78.0087637	100M			0	1	1	0	1	RURAL	B	TIPO 1
38	CPNP SECTORIAL POMABAMBA	OTRO PLAZUELA CONVENTO # SN	POMABAMBA	POMABAMBA	ANCASH	8.8194850 31	-77.46140309	100M			0	1	1	0	1	RURAL	B	TIPO 1
39	CPNP CATAC	AV. 31 DE MAYO SN	CATAC	RECUAY	ANCASH	9.7979666 67	-77.432525	100M			0	1	1	0	1	URBANO	C	TIPO 1
40	DESPCAR CATAC	AV. 31 DE MAYO # SN	CATAC	RECUAY	ANCASH	9.8014633 33	-77.43131333	100M			0	0	1	0	0	URBANO	CARRERAS	TIPO 1
41	CPNP SECTORIAL RECUAY	JIRON LA SOLEDAD # SN	RECUAY	RECUAY	ANCASH	9.7188891 84	-77.45635986	100M			0	1	1	0	2	URBANO	B	TIPO 1
42	COMISARIA DE TURISMO CHIMBOTE	JR. TUPAC AMARU MZ. 8 LT. 9 (URBANIZACION LA LIBERTAD)	CHIMBOTE	SANTA	ANCASH	-9.09608	-78.56856	100M			0	0	1	0	1	URBANO	TURISMO	TIPO 1
43	DIVPOL CHIMBOTE	JIRON LEONCIO PRADO N° 401	CHIMBOTE	SANTA	ANCASH	9.0737789 77	-78.59377898	100M			0	1	1	0	1	URBANO	DIVPOL	TIPO 1
44	CPNP 21 DE ABRIL	AV. JOSE BALTA CDR 11. UR. 21 DE ABRIL ZN -B. CHIMBOTE	CHIMBOTE	SANTA	ANCASH	9.0681366 67	-78.58992833	100M			0	1	1	0	2	URBANO	A	TIPO 1
45	CPNP ALTO PERU	JR. MOQUEGUA S/N CDR 9 AH. ALTO PERU. CHIMBOTE	CHIMBOTE	SANTA	ANCASH	-9.07828	-78.57349	100M			0	1	1	0	1	URBANO	B	TIPO 1



46	CPNP CHIMBOTE	AV. VICTOR RAUL HAYA DE LA TORRE # 296	CHIMBOTE	SANTA	ANCASH	9.0732064 48	-78.5978288	100M		0	1	1	0	2	URBANO	A	TIPO 1
47	CPNP LA LIBERTAD	AV. ENRIQUE MEIGGS # 1535	CHIMBOTE	SANTA	ANCASH	9.0868783 33	-78.57503833	100M		0	1	1	0	2	URBANO	A	TIPO 1
48	CPNP RINCONADA	AV. VICTOR RAUL HAYA DE LA TORRE SN MZ LT.3	CHIMBOTE	SANTA	ANCASH	8.8932039	-78.5662873	100M		0	0	1	0	1	URBANO		TIPO 1
49	CPNP SAN PEDRO CHIMBOTE	CLL. LOS ALAMOS SN MZ Y LT.9	CHIMBOTE	SANTA	ANCASH	9.0490582	-78.596830	100M		0	1	1	0	2	URBANO	COMISARIA	TIPO 1
50	CPNP TAMBO REAL	AV. AMERICAS S/N CASERIO TAMBO REAL NUEVO	CHIMBOTE	SANTA	ANCASH	8.5649542	-78.585519	100M		0	1	1	0	0	URBANO	E	TIPO 1
57	CP SANTA ROSA DE LIMA / OFICRI AREQUIPA	AV. GOYENECHE 317	CERCADO	AREQUIPA	AREQUIPA	16.400265	-71.526808	150M		0	1	1	0	4	URBANO	UNIDAD PNP	TIPO 1
52	DEPINCRI CHIMBOTE	JR. LADISLAO ESPINAR 181	CHIMBOTE	SANTA	ANCASH	9.0722173	-78.5958651	100M		0	1	1	0	1	URBANO	DIVINCI	TIPO 1
53	POL PNP CHIMBOTE	AV. PARDO 292	CHIMBOTE	SANTA	ANCASH	-9.073091	-78.599419	100M		0	1	1	0	1	URBANO	POLICINICO	TIPO 1
54	CPNP COISHCO	AV. PANAMERICANA ANTIGUA # 410	COISHCO	SANTA	ANCASH	9.0207798	-78.6152822	100M		0	1	1	0	1	URBANO	C	TIPO 1
55	CPNP NEPEÑA	CLL. HIPOLITO UNANUE SN MZA LT.8	NEPEÑA	SANTA	ANCASH	-9.172025	-78.361235	100M		0	1	1	0	1	RURAL	C	TIPO 1
56	CPNP SAN JACINTO ANCASH	AV. PROGRESO SN	NEPEÑA	SANTA	ANCASH	-9.15164	-78.27908167	100M		0	1	1	0	1	RURAL	C	TIPO 1
57	CPNP DE LA FAMILIA CHIMBOTE	CENTRO CIVICO SECTOR 7A-7S MZ.-D LOTE 02 - NVO. CHIMBOTE-SANTA	CHIMBOTE	SANTA	ANCASH	9.1273283 33	-78.52198167	100M		0	1	1	0	1	URBANO	FAMILIA	TIPO 1
58	CPNP SECTORIAL BUENOS AIRES	AV. PACIFICO SN MZE LT.45	CHIMBOTE	SANTA	ANCASH	9.1281216 67	-78.52114	100M		0	1	1	0	2	URBANO	A	TIPO 1
59	CPNP VILLA MARIA / OFICRI	JR. LOS ANGELES CRUCE CON CALLE INDEPENDENCIA	CHIMBOTE	SANTA	ANCASH	9.1170283 33	-78.54481667	150M		0	1	1	0	2	URBANO	B	TIPO 1
60	DESPICAR CHIMBOTE	JIRON NEPEÑA # 100	CHIMBOTE	SANTA	ANCASH	9.1265966 67	-78.52760333	100M		0	0	1	0	0	URBANO	CARRETERAS	TIPO 1
61	CPNP SAMANCO	JIRON PASCUAL CORCINO CUETO # 237	SAMANCO	SANTA	ANCASH	9.2616533 33	-78.49572167	100M		0	1	1	0	1	URBANO	C	TIPO 1
62	CPNP SECTORIAL SANTA	JIRON UCAVALI # 142	SANTA	SANTA	ANCASH	8.9870816 67	-78.61310667	100M		0	1	1	0	1	URBANO	B	TIPO 1
63	CPNP SECTORIAL SIHUAS	JIRON SAN MARTIN # 130	SIHUAS	SIHUAS	ANCASH	8.5542862 61	-77.63150007	100M		0	1	1	0	1	RURAL	C	TIPO 1
64	DESPICAR SIHUAS	JIRON LAS PONCIANAS # 240	SIHUAS	SIHUAS	ANCASH	-8.552275	-77.63134	100M		0	0	1	0	0	RURAL	CARRETERAS	TIPO 1
65	CPNP SECTORIAL YUNGAY	AV. 28 DE JULIO Y ARIAS GRACIANI # SN	YUNGAY	YUNGAY	ANCASH	-9.14086	-77.74472333	100M		0	1	1	0	2	URBANO	B	TIPO 1
66	CPNP ABANCAY/DEPINCRI/OFICRI	JIRON HUANCAMELCA # 215	ABANCAY	ABANCAY	APURIMAC	13.636633 33	-72.87791167	150M		0	1	1	0	3	URBANO	C	TIPO 1
67	CPNP BELLA VISTA ABANCAY	AV. PANAMERICANA # 1600	ABANCAY	ABANCAY	APURIMAC	-13.63699	-72.89771667	100M		0	1	1	0	1	URBANO	C	TIPO 1
68	CPNP FAMILIA DE ABANCAY	JIRON LIMA # 1000	ABANCAY	ABANCAY	APURIMAC	13.635951 67	-72.88465833	200M		0	1	1	0	1	URBANO	FRENTE Y FAMILIA	TIPO 1
69	CPNP VILLA AMPAY	AV. MAGISTERIAL S/N CENTRO POBLADO PUEBLO JOVEN AV PERU REF. PARQUE PICHICHA	ABANCAY	ABANCAY	APURIMAC	13.631715	-72.88478333	100M		0	1	1	0	1	RURAL	D	TIPO 1
70	INSPECTORIA / OFICINA DE DISCIPLINA ABANCAY	AV. BELLA ABANQUINA N° 409	ABANCAY	ABANCAY	APURIMAC	13.633577	-72.867265	100M		0	0	1	0	1	URBANO	UNIDAD	TIPO 1
71	MEDIO AMBIENTE	PROLONGACION CUSCO A-12	ABANCAY	ABANCAY	APURIMAC	13.627745	-72.878455	100M		0	0	1	0	1	URBANO	MEDIO AMBIENTE	TIPO 1

[Handwritten signatures and marks at the top left of the page]



72	REGPOL APURIMAC / OFICIA ABANCAY	JR LIMA N° 1000	ABANCAY	ABANCAY	APURIMAC	-13.63587	-72.88447	150M		0	1	1	0	1	URBANO	REGPOL	TIPO 1
73	CPNP TAMBURCO	AV. 14 DE SEPTIEMBRE / SN	TAMBURCO	ABANCAY	APURIMAC	13.622459 41	72°52'34.0	100M		0	1	1	0	1	URBANO	D	TIPO 1
74	CPNP ANDAHUAYLAS	AV. PERU # 198	ANDAHUAYLAS	ANDAHUAYLAS	APURIMAC	13.656515	-73.384836	100M		0	1	1	0	2	RURAL	A	TIPO 1
75	CPNP HUANCABAMBA ANDAHUAYLAS	AV. HUANCABAMBA # SN	ANDAHUAYLAS	ANDAHUAYLAS	APURIMAC	13.729873 33	-73.35364167	100M		0	1	1	0	0	RURAL	E	TIPO 1
76	DESPCAR ANDAHUAYLAS	AV. SESQUICENTENARIO # 1845	ANDAHUAYLAS	ANDAHUAYLAS	APURIMAC	13.665235	-73.41374833	100M		0	0	1	0	0	RURAL	CARRERAS	TIPO 1
77	CPNP FAMILIA ANDAHUAYLAS	JR. CARMEN N° 542	SAN JERONIMO	ANDAHUAYLAS	APURIMAC	13.653143	-73.370081	100M		0	1	1	0	1	URBANO	FAMILIA	TIPO 1
78	CPNP SAN JERONIMO ANDAHUAYLAS	AV. ALFONSO UGARTE # 112	SAN JERONIMO	ANDAHUAYLAS	APURIMAC	13.651791 67	-73.36528167	100M		0	1	1	0	1	RURAL	C	TIPO 1
79	CPNP TALAVERA	AV. MANCO CAPAC # 505	TALAVERA	ANDAHUAYLAS	APURIMAC	13.656250	-73.43043667	100M		0	1	1	0	1	URBANO	D	TIPO 1
80	CPNP ANTABAMBA	JIRÓN APURIMAC # SN	ANTABAMBA	ANTABAMBA	APURIMAC	14.366306	-72.876796	100M		0	1	1	0	0	URBANO	E	TIPO 1
81	CPNP CHALHUANCA	AV. PANAMERICANA # SN	CHALHUANCA	CHALHUANCA	APURIMAC	14.295323 33	-73.24764	100M		0	1	1	0	2	RURAL	COMISARIA	TIPO 1
82	DESPCAR CHALHUANCA	JIRÓN MARISCAL CASTILLA # SN	CHALHUANCA	CHALHUANCA	APURIMAC	14.295158	-73.2474833	100M		0	0	1	0	1	URBANO	CARRERAS	TIPO 1
83	CPNP SECTORIAL CHINCHEROS	AV. FERNANDO BELAUDE TERRY # SN - CHINCHEROS	CHINCHEROS	CHINCHEROS	APURIMAC	13.517078	-73.72023667	150M		0	1	1	0	1	URBANO	D	TIPO 1
84	CPNP CHALHUAHUACHO	PLAZA DE ARMAS DE CHALHUAHUACHO N° 138	CHALHUAHUACHO	COTABAMBA	APURIMAC	14.118430	-72.24624333	100M		0	1	1	0	1	URBANO	D	TIPO 1
85	CPNP SECTORIAL TAMBOMBAMBA	CALLE BOLIVAR # SN	TAMBOMBAMBA	COTABAMBA	APURIMAC	13.948511 67	-72.17540333	100M		0	1	1	0	1	RURAL	C	TIPO 1
86	CPNP CHUQUIBAMBILLA	CALLE PASOS VALERA # SN	CHUQUIBAMBILLA	GRAU	APURIMAC	14.103182	-72.7068758	100M		0	1	1	0	1	URBANO	D	TIPO 1
87	CPNP ALTO SELVA ALEGRE	CALLE LOS ANDES NRO. 215	ALTO SELVA ALEGRE	AREQUIPA	AREQUIPA	16.383329	-71.517913	100M		0	1	1	0	2	URBANO	A	TIPO 1
88	CPNP INDEPENDENCIA	PI. JORGE CHAVEZ SN MZ.15 LT.15	ALTO SELVA ALEGRE	AREQUIPA	AREQUIPA	16.365998 33	-71.51990667	100M		0	1	1	0	2	URBANO	B	TIPO 1
89	ESCUADRON MISTI (SECCION DE EMERGENCIA MOTORIZADA HALCONES)	AV. FCO. MOSTAJO 119	ALTO SELVA ALEGRE	AREQUIPA	AREQUIPA	16.371363	-71.52818	100M		0	1	1	0	1	URBANO	UUEE	TIPO 1
90	CPNP PALACIO VIEJO	CALLE PALACIO VIEJO # 112 (A UNA CUADRA DE LA PLAZA DE ARMA)	AREQUIPA	AREQUIPA	AREQUIPA	16.400853	-71.536472	150M		0	1	1	0	1	URBANO	A	TIPO 1
91	COMISARIA DE TURISMO PNP AREQUIPA	PREDIO 24 PUENTE CHILINA (CALLE LAS AZULENAS N° 116) CAYMA	CAYMA	AREQUIPA	AREQUIPA	16.381048	-71.538371	100M		0	0	1	0	1	URBANO	TURISMO	TIPO 1
92	CPNP ACEQUIA ALTA	AV. GRAU # 903	CAYMA	AREQUIPA	AREQUIPA	16.356071 06	-71.54149989	100M		0	1	1	0	1	URBANO	C	TIPO 1
93	CPNP CASIMIRO CUADROS	JR. JUSTINIANO VELARDE SN MZ.N LT.1	CAYMA	AREQUIPA	AREQUIPA	16.349235	-71.55241833	100M		0	1	1	0	1	URBANO	D	TIPO 1
94	CPNP CAYMA	CALLE PLAZA PRINCIPAL DE CAYMA # 412	CAYMA	AREQUIPA	AREQUIPA	16.381603 33	-71.54495833	100M		0	1	1	0	1	URBANO	B	TIPO 1
95	CPNP DEAN VALDIVIA	PI. SIN NOMBRE SECTOR 9 SN MZ.P LT.1	CAYMA	AREQUIPA	AREQUIPA	16.331728 5	-71.54391624	100M		0	1	1	0	1	URBANO	C	TIPO 1
96	HOSPITAL REGIONAL PNP AREQUIPA	AV. BOLOGNESI 602	CAYMA	AREQUIPA	AREQUIPA	16.375592	-71.544811	100M		0	1	1	0	1	URBANO	HOSPITAL	TIPO 1



14	DEPICA/COMPLEJO POLICIAL CAMANA/INSPECTORIA CAMANA	CAMANA	CAMANA	AV. MARISCAL CASTILLA 735 MZ LOTE 9 KM.	AREQUIPA	16.629744	-72.711941	200M	1	1	0	1	0	1	0	3	URBANO	UNIDAD PNP	TIPO 2
98	CPNP SANTA MARTA	AREQUIPA	CERCADO	CALLE SANTA MARTHA # 212	AREQUIPA	16.397696 67	-71.532495	100M		0	1	1	0	1	0	2	URBANO	A	TIPO 1
99	INSPECTORIA DESCENTRALIZADA AREQUIPA	AREQUIPA	CERCADO	AV. JORGE CHAVEZ 304	AREQUIPA	16.404371	-71.53154	100M		0	1	1	0	1	0	1	URBANO	DIVINCRI	TIPO 1
100	OFICINA DE RQ AREQUIPA	AREQUIPA	CERCADO	SIGLO XX S/N	AREQUIPA	16.399837	-71.530253	100M		0	1	1	0	1	0	1	URBANO	RQ	TIPO 1
101	CPNP AEROPUERTO AREQUIPA	AREQUIPA	CERRO COLORADO	AV. AVIACION # SN	AREQUIPA	16.344706 67	-71.56842333	100M		0	1	1	0	1	0	0	URBANO	A	TIPO 1
102	CPNP CERRO COLORADO	AREQUIPA	CERRO COLORADO	AV. ALFONSO UGARTE # SN	AREQUIPA	16.378338 33	-71.55961333	100M		0	1	1	0	1	0	1	URBANO	B	TIPO 1
103	CPNP CIUDAD MUNICIPAL	AREQUIPA	CERRO COLORADO	AV. ANTIGUA CARRETERA YURA SN MZ B LT.5	AREQUIPA	16.327645	-71.5929731	150M		0	1	1	0	1	0	1	URBANO	D	TIPO 1
104	CPNP MARISCAL CASTILLA	AREQUIPA	CERRO COLORADO	AV. 28 DE JULIO # SN	AREQUIPA	16.392800 17	-71.56754918	100M		0	1	1	0	1	0	1	URBANO	B	TIPO 1
105	CPNP ZAMACOLA	AREQUIPA	CERRO COLORADO	AV. MARAÑON # 502	AREQUIPA	16.351688 06	-71.563318	100M		0	1	1	0	1	0	2	URBANO	B	TIPO 1
106	CPNP CHARACATO	AREQUIPA	CHARACATO	CALLE SOCABAYA # SN	AREQUIPA	16.468491 67	-71.48487167	100M		0	1	1	0	1	0	1	URBANO	D	TIPO 1
107	CPNP ANDRES AVELINO CACERES	AREQUIPA	JACOBO HUNTER	AV. JUAN VELASCO ALVARADO SN MZN LT.11	AREQUIPA	16.452636 67	-71.553245	100M		0	1	1	0	1	0	1	URBANO	C	TIPO 1
108	CPNP HUNTER	AREQUIPA	JACOBO HUNTER	AV. BRASILIA # 305	AREQUIPA	-16.44152	-71.55491667	100M		0	1	1	0	1	0	1	URBANO	B	TIPO 1
109	DESPCAR AREQUIPA	AREQUIPA	JACOBO HUNTER	AV. ANDRES AVELINO CACERES # SN	AREQUIPA	16.423540 76	-71.54348642	100M		0	0	1	0	1	0	0	URBANO	CARRETERAS	TIPO 1
110	CPNP JOSE LUIS BUSTAMANTE Y RIVERO	AREQUIPA	JOSE LUIS BUSTAMANTE Y RIVERO	URB. QUINTA TRISTÁN MZY LT. 2	AREQUIPA	-16.42431	-71.529565	100M		0	1	1	0	1	0	1	URBANO	B	TIPO 1
111	CPNP SIMÓN BOLIVAR	AREQUIPA	JOSE LUIS BUSTAMANTE Y RIVERO	AV. CARACAS # 629	AREQUIPA	16.443431 67	-71.513685	100M		0	1	1	0	1	0	1	URBANO	B	TIPO 1
112	CPNP EL TRIUNFO	AREQUIPA	LA JOYA	CLL. MIGUEL GRAU SN MZD LT.4	AREQUIPA	16.496433 33	-71.83764	100M		0	1	1	0	1	0	1	URBANO	C	TIPO 1
113	CPNP Rural LA JOYA	AREQUIPA	LA JOYA	JIRÓN MILLER # 100	AREQUIPA	16.424541 56	-71.8182224	100M		0	1	1	0	1	0	2	URBANO	B	TIPO 1
114	CPNP JERUSALEN	AREQUIPA	MARIANO MELGAR	CALLE DOS DE MAYO # SN	AREQUIPA	16.400925	-71.490645	100M		0	1	1	0	1	0	1	URBANO	C	TIPO 1
115	CPNP MARIANO MELGAR	AREQUIPA	MARIANO MELGAR	OTRO PLAZA UMACHIRI # SN	AREQUIPA	16.399391 25	-71.50661945	100M		0	1	1	0	1	0	2	URBANO	B	TIPO 1
116	CPNP ALTO MISTI	AREQUIPA	MIRAFLORES	CALLE ARTURO VILLEGAS # 300	AREQUIPA	16.389225	-71.51476	100M		0	1	1	0	1	0	1	URBANO	B	TIPO 1
117	CPNP EL PORVENIR	AREQUIPA	MIRAFLORES	AV. SAN MARTIN # 4103	AREQUIPA	16.377135	-71.50864667	100M		0	1	1	0	1	0	2	URBANO	B	TIPO 1
118	CPNP MIRAFLORES	AREQUIPA	MIRAFLORES	AV. SAN MARTIN # 417	AREQUIPA	16.395055	-71.52392	100M		0	1	1	0	1	0	2	URBANO	B	TIPO 1
119	MEDIO AMBIENTE	AREQUIPA	MIRAFLORES	CALLE PUNO 782-862	AREQUIPA	16.398665	-71.516998	100M		0	0	1	0	1	0	1	URBANO	MEDIO AMBIENTE	TIPO 1

Handwritten signatures and initials at the top left of the page.



Handwritten signatures and initials on the left side of the page.

12	CPNP CAMPO MARTE	CALLE ALFONSO UGARTE S/N	PAUCARPATA	AREQUIPA	AREQUIPA	16.427105	-71.49646	100M			0	1	1	0	1	URBANO	C	TIPO 1
12	CPNP FAMILIA PAUCARPATA	AV. REVOLUCION # 1200	PAUCARPATA	AREQUIPA	AREQUIPA	16.417654	-71.491595	100M			0	1	1	0	1	URBANO	B	TIPO 1
12	CPNP ISRAEL	AV. LOS ANGELES SN MZ Y LT. 6	PAUCARPATA	AREQUIPA	AREQUIPA	16.418885	-71.48503167	100M			0	0	1	0	1	URBANO		TIPO 1
12	CPNP JESUS MARIA	CALLE PARQUE CABALLERO # 121	PAUCARPATA	AREQUIPA	AREQUIPA	16.42091333	-71.50925833	100M			0	1	1	0	1	URBANO	C	TIPO 1
12	CPNP JUAN DE DIOS COLCA APAZA	AV. JORGE CHAVEZ S/N	PAUCARPATA	AREQUIPA	AREQUIPA	16.41155643	-71.49675429	100M			0	1	1	0	1	URBANO	B	TIPO 1
12	CPNP MIGUEL GRAU	AV. MIGUEL GRAU # SN	PAUCARPATA	AREQUIPA	AREQUIPA	16.40863	-71.48383167	100M			0	1	1	0	1	URBANO	B	TIPO 1
12	DPTO. INV. ROBO DE VEHICULOS	CALLE MICHAELA BASTIDAS N° 105 PUEBLO JOVEN CIUDAD BLANCA ZONA A	PAUCARPATA	AREQUIPA	AREQUIPA	16.412866	-71.493484	100M			0	1	1	0	1	URBANO	DIPROVE	TIPO 1
12	CPNP SABANDIA	CALLE LAS PISCINAS # SN	SABANDIA	AREQUIPA	AREQUIPA	16.45001275	-71.4955312	100M			0	1	1	0	1	URBANO	C	TIPO 1
12	CPNP PAMPA DE CAMARONES	AV. BRASIL # 517	SACHACA	AREQUIPA	AREQUIPA	16.41130333	-71.571905	100M			0	1	1	0	1	URBANO	C	TIPO 1
12	CPNP SACHACA	AV. ROBERTO PONCE # SN	SACHACA	AREQUIPA	AREQUIPA	16.42314833	-71.564975	100M			0	1	1	0	1	URBANO	C	TIPO 1
13	CPNP SANTA RITA DE SIGUAS	AV. CESAR AUGUSTO GILARDI # 400 REF PLAZA DE ARMAS SANTA RITA DE SIGUAS	SANTA RITA DE SIGUAS	AREQUIPA	AREQUIPA	16.4933817	-72.09464333	100M			0	1	1	0	1	URBANO	D	TIPO 1
13	CPNP CIUDAD MI TRABAJO	AV. INDEPENDENCIA # SN	SOCABAYA	AREQUIPA	AREQUIPA	16.44831833	-71.53257	100M			0	1	1	0	2	URBANO	A	TIPO 1
13	CPNP SOCABAYA	AV. SALAVERRY # 150	SOCABAYA	AREQUIPA	AREQUIPA	16.47217	-71.52854667	100M			0	1	1	0	1	URBANO	B	TIPO 1
13	CPNP TIABAYA	AV. AREQUIPA # 108	TIABAYA	AREQUIPA	AREQUIPA	16.44970663	-71.58686432	100M			0	1	1	0	1	URBANO	B	TIPO 1
13	CPNP CONGATA	AV. RAMÓN CASTILLA ZONA "A" MZ B LOTE 2 Y 3 - CONGATA	UCHUMAYO	AREQUIPA	AREQUIPA	16.44623333	-71.61906667	100M			0	1	1	0	1	URBANO	C	TIPO 1
13	CPNP UCHUMAYO	CALLE SALAVERRY # 103	UCHUMAYO	AREQUIPA	AREQUIPA	16.42580167	-71.67318	100M			0	1	1	0	1	URBANO	B	TIPO 1
48	AEROPUERTO INTERNACIONAL JORGE CHAVEZ	AV. ELMER FAUCETT S/N	CALLAO	CALLAO	LIMA	-12.02405	-77.1122	400M			0	1	1	0	0	URBANO	RQ	TIPO 1
13	DPTO. TRANSITO	URB. JUAN XXIII MZ A LOTE 6	YANAHUARA	AREQUIPA	AREQUIPA	16.397293	-71.54981	100M			0	1	1	0	1	URBANO	TRANSITO	TIPO 1
13	REGPOL AREQUIPA - UNITIC	AV. EMMEL 106	YANAHUARA	AREQUIPA	AREQUIPA	16.391651	-71.543559	150M			0	1	1	0	1	URBANO	MACRE UNITIC	TIPO 1
13	CPNP YARABAMBA	CALLE AMERICA # 105	YARABAMBA	AREQUIPA	AREQUIPA	16.54670961	-71.47513703	100M			0	1	1	0	1	URBANO	C	TIPO 1
14	CPNP YURA	AV. PRINCIPAL BAÑOS DE YURA # SN	YURA	AREQUIPA	AREQUIPA	16.246638	-71.69213	100M			0	1	1	0	1	URBANO	D	TIPO 1
14	CPNP CIUDAD DE DIOS	ASOCIACIÓN URBANIZADORA CIUDAD DE DIOS MZ. T, LOTE 2, SECTOR B, ZONA 3, COMITE 22 DEL DISTRITO DE YURA	YURA	AREQUIPA	AREQUIPA	16.301288	-71.626084	100M			0	1	1	0	1	URBANO	B	TIPO 1
17	DIVINCHI AYACUCHO/COMPLEJO WALTER ROSALLES LEON	JR. LIMA 330	AYACUCHO	HUAMANGA	AYACUCHO	13.160207	-74.22924	200M		1	2	0	1	0	3	URBANO	UNIDAD PNP	TIPO 2



14 3	POL PNP CAMANA	MZ D LOTE 9	CERCADO	CAMANA	AREQUIPA	16.625455	-72.714031	100M			0	1	1	0	1	URBANO	POLICLINICO	TIPO 1
14 4	CPNP RURAL SAN GREGORIO	CALLE PROGRESO # 437	NICOLAS DE PIÉROLA	CAMANA	AREQUIPA	16.573190 46	-72.71662094	100M			0	1	1	0	1	URBANO	C	TIPO 1
14 5	CPNP OCOÑA	AV. JULIO RONALD SALAZAR MONROE # SN	OCOÑA	CAMANA	AREQUIPA	16.494936 67	-73.1066	100M			0	1	1	0	1	URBANO	C	TIPO 1
14 6	CPNP RURAL PNP LA PAMPA	AV. SAMUEL PASTOR # 407	SAMUEL PASTOR	CAMANA	AREQUIPA	16.613553 33	-72.69871833	100M			0	1	1	0	1	URBANO	B	TIPO 1
14 7	CPNP RURAL ACARI	CLL SANTA ROSA Y CAL ENRIQUE BRILKA SN	ACARI	CARAVELI	AREQUIPA	15.436895	-74.617405	100M			0	1	1	0	1	RURAL	C	TIPO 1
14 8	CPNP RURAL ATICO/COM CAR ATICO	AV. AREQUIPA S/N	ATICO	CARAVELI	AREQUIPA	16.228085	-73.60959833	100M			0	1	1	0	1	RURAL	C	TIPO 1
14 9	CPNP RURAL BELLA UNION	AV. FRANCISCO FLORES BERRUESO S/N	BELLA UNION	CARAVELI	AREQUIPA	15.450376 67	-74.65606333	100M			0	1	1	0	1	RURAL	C	TIPO 1
15 0	CPNP RURAL SECTORIAL CARAVELI	AV. 2 DE MAYO # 809	CARAVELI	CARAVELI	AREQUIPA	15.773955	-73.36789667	100M			0	1	1	0	2	RURAL	B	TIPO 1
15 1	CPNP RURAL CHALA	CALLE GRAU # 216	CHALA	CARAVELI	AREQUIPA	-15.86624	-74.24685333	100M			0	1	1	0	1	RURAL	B	TIPO 1
15 2	DESPRCAR CHALA	AV. EMANCIPACION SN	CHALA	CARAVELI	AREQUIPA	15.851641 67	-74.25262833	100M			0	0	1	0	0	RURAL	CARRETERAS	TIPO 1
15 3	CPNP RURAL APLAO	CLL. PARDO SN MZ J1 LT.14	APLAO	CASTILLA	AREQUIPA	16.079521 67	-72.49398333	100M			0	1	1	0	1	RURAL	B	TIPO 1
15 4	DESPRCAR APLAO	CLL. PARDO SN MZ K1 LT.04	APLAO	CASTILLA	AREQUIPA	16.078349	-72.493369	100M			0	0	1	0	0	RURAL	CARRETERAS	TIPO 1
15 5	CPNP RURAL ORCOPAMPA	AV. BUENAVENTURA # SN	ORCOPAMPA	CASTILLA	AREQUIPA	15.267998 33	-72.344395	100M			0	1	1	0	1	RURAL	C	TIPO 1
15 6	CPNP RURAL PAMPACOLCA	CALLE SALAVERRY # SN	PAMPACOLCA	CASTILLA	AREQUIPA	15.714658 33	-72.57313	100M			0	1	1	0	1	RURAL	C	TIPO 1
15 7	CPNP RURAL CHIVAY -CAYLOMA	OTRO PLAZA DE ARMAS # SN	CHIVAY	CAYLOMA	AREQUIPA	15.635900 58	-71.60158843	100M			0	1	1	0	1	RURAL	B	TIPO 1
15 8	DESPRCAR CHIVAY	KM. 82.0 VIA PENETRACION AREQUIPA	CHIVAY	CAYLOMA	AREQUIPA	15.649102	-71.601363	100M			0	0	1	0	1	URBANO	CARRETERAS	TIPO 1
15 9	CPNP DE LA FAMILIA MAJES (PEDREGAL)	EL PEDREGAL MAJES ESPALDA MUNICIPALIDAD PLZ EL PIONERO	MAJES	CAYLOMA	AREQUIPA	16.362121 67	-72.190805	100M			0	1	1	0	1	URBANO	FAMILIA	TIPO 1
16 0	CPNP MODELO EL PEDREGAL	AV. LOS COLONIZADORES S/N MZ O LT. 62	MAJES	CAYLOMA	AREQUIPA	16.348775	-72.18795667	100M			0	1	1	0	1	URBANO	B	TIPO 1
16 1	CPNP RURAL CHUQUIBAMBA	AV. NICOLAS DE PIÉROLA # 100	CHUQUIBAMBA	CONDESUVOS	AREQUIPA	15.840918	-72.65116667	100M			0	1	1	0	1	URBANO	D	TIPO 1
16 2	CPNP COCACHACRA	AV. LIBERTAD # 824	COCACHACRA	ISLAY	AREQUIPA	17.092298 33	-71.76431167	100M			0	1	1	0	1	URBANO	B	TIPO 1
16 3	CPNP LA CURVA	AV. DEAN VALDIVIA # SN	DEAN VALDIVIA	ISLAY	AREQUIPA	17.144042 91	-71.82141691	100M			0	1	1	0	1	URBANO	C	TIPO 1
16 4	CPNP EL ARENAL	CLL ISLAY SN	DEAN VALDIVIA	ISLAY	AREQUIPA	17.121048 33	-71.796055	100M			0	1	1	0	1	URBANO	C	TIPO 1
16 5	CPNP MATARANI	AV. AREQUIPA # SN	ISLAY	ISLAY	AREQUIPA	17.000667	-72.096165	100M			0	1	1	0	1	URBANO	D	TIPO 1

[Handwritten signature]



[Handwritten signature]

16	CPNP MEJIA	AV. TAMBO # SN	MEJIA	ISLAY	AREQUIPA	-17.40222	-71.905055	100M			0	1	1	0	1	URBANO	C	TIPO 1
16	CPNP SECTORIAL MOLLEND	PI ALTO INCLAN MANZANA "Q"	MOLLEND	ISLAY	AREQUIPA	17.019604	-72.003927	100M			0	1	1	0	2	URBANO	A	TIPO 1
16	POSTA PNP ISLAY MOLLEND	CALLE FRANCISCO BOLOGNESI 503	MOLLEND	ISLAY	AREQUIPA	17.019069	-72.006963	100M			0	1	1	0	1	URBANO	POSTA MEDICA	TIPO 1
16	CPNP PUNTA DE BOMBON	CALLE PLAZA 28 DE JULIO # SN	PUNTA DE BOMBON	ISLAY	AREQUIPA	17.171883 01	-71.7904079	100M			0	1	1	0	1	URBANO	C	TIPO 1
17	CPNP RURAL ZONAL COTAHUASI TIPO C	CALLE CABILDO # 107	COTAHUASI	LA UNION	AREQUIPA	15.211875	-72.89061667	100M			0	1	1	0	1	RURAL	C	TIPO 1
17	CPNP SECTORIAL CANGALLO	JR MARISCAL CACERES 152	CANGALLO	CANGALLO	AYACUCHO	13.628941	-74.143551	100M			0	1	1	0	1	URBANO	C	TIPO 1
17	COMISARIA DE TURISMO AYACUCHO	ASOC. EL ARCO MZ D LT. 10 CALLE LOS LAURELES ENACE	AYACUCHO	HUAMANGA	AYACUCHO	-13.13999	-74.22993	100M			0	0	1	0	1	URBANO	TURISMO	TIPO 1
17	CPNP AYACUCHO/OFCRI	JIRÓN 28 DE JULIO # 325	AYACUCHO	HUAMANGA	AYACUCHO	13.163941	-74.227155	150M			0	1	1	0	3	URBANO	A	TIPO 1
17	CPNP DE LA FAMILIA AYACUCHO	JR. LIBERTAD 1200. REFERENCIA EDIFICIO MUNICIPAL JUZGADO FAMILIA 2DO PISO	AYACUCHO	HUAMANGA	AYACUCHO	13.150295	-74.227763	100M			0	1	1	0	1	URBANO	FAMILIA	TIPO 1
17	DIRCOCOR AYACUCHO	AV. CARMEN ALTO N° 378, (REF. ALAMEDA BOLOGNESI) JR. LAS CARDENIAS MZ E LT. 37 (URB. MARISCAL CACERES)	AYACUCHO	HUAMANGA	AYACUCHO	-13.16165	-74.225515	100M			0	1	1	0	1	URBANO	DIRCOCOR	TIPO 1
20	DIVINCI/DIRTURMA/DEPROVE CAJAMARCA	JR. DEL COMERCIO 1021	CAJAMARCA	CAJAMARCA	CAJAMARCA	-7.158129	-78.517082	200M	1		3	0	1	0	3	URBANO	UNIDAD PNP	TIPO 2
17	CPNP CARMEN ALTO	AV. AV. LIBERTADORES SN MZ X LT. 12	CARMEN ALTO	HUAMANGA	AYACUCHO	13.176898 33	-74.221285	100M			0	1	1	0	1	URBANO	C	TIPO 1
17	DIVIDAD CARMEN ALTO (DEPOTAD HUAMANGA)	AV. QUICAPATA S/N	CARMEN ALTO	HUAMANGA	AYACUCHO	13.191027	-74.230065	100M			0	1	1	0	1	URBANO	DIRANDRO	TIPO 1
17	105 EMERGENCIA AYACUCHO	CIRIO ALEGRIA 430	JESUS NAZARENO	HUAMANGA	AYACUCHO	13.157467	-74.216706	100M			0	1	1	0	1	URBANO	EMERGENCIA	TIPO 1
18	DIPROVE AYACUCHO	JR. MANUEL ALARCON 221	JESUS NAZARENO	HUAMANGA	AYACUCHO	13.151762	-74.213247	100M			0	1	1	0	1	URBANO	DIPROVE	TIPO 1
18	CPNP OCROS	JR. PROLG CACERES JR PROCERES SN MZ F LT. 4	OCROS	HUAMANGA	AYACUCHO	13.390963 33	-73.31479333	100M			0	1	1	0	1	RURAL	C	TIPO 1
18	CPNP QUINUA	CALLE SUCRE # 104	QUINUA	HUAMANGA	AYACUCHO	13.048788 48	-74.3927734	100M			0	1	1	0	1	URBANO	C	TIPO 1
18	REGPOL AYACUCHO	AV. AGUSTIN ZEA S/N	SANTA ELEVA	HUAMANGA	AYACUCHO	-13.166211	-74.198431	100M			0	1	1	0	1	URBANO	REGPOL	TIPO 1
18	CPNP HUANTA/COM CAR HUANTA	AV. SAN MARTIN # 372	HUANTA	HUANTA	AYACUCHO	12.941593 33	-74.247085	100M			0	1	1	0	2	URBANO	A	TIPO 1
18	POSTA PNP HUANTA	JR. AYACUCHO 271	HUANTA	HUANTA	AYACUCHO	12.940352	-74.246947	100M			0	1	1	0	1	URBANO	POSTA MEDICA	TIPO 1
18	CPNP PALMAPAMPA	JIRÓN JORGE BASADRE # SN	SAN MIGUEL	LA MAR	AYACUCHO	12.766848 33	-73.65522333	100M			0	1	1	0	1	RURAL	C	TIPO 1
18	CPNP SECTORIAL SAN MIGUEL LA MAR	JIRÓN MARISCAL CACERES # SN	SAN MIGUEL	LA MAR	AYACUCHO	-13.01356	-73.98046	100M			0	1	1	0	1	RURAL	A	TIPO 1
18	DEPOTAD PALMAPAMPA (GOATJ) + POSTA MEDICA PALMAPAMPA	CALLE LOS LAURELES S/N S/N	SAN MIGUEL	LA MAR	AYACUCHO	12.765802	-73.655055	100M			0	1	1	0	1	RURAL	DIRANDRO	TIPO 1
18	CPNP LUCANAS - PUQUIO	JIRÓN TACNA # 657	PUQUIO	LUCANAS	AYACUCHO	14.693858 33	-74.12818833	100M			0	1	1	0	1	RURAL	D	TIPO 1

19	0	CPNP SECTORIAL PARINACOCCHAS	JIRÓN DOS DE MAYO # 820	CORACORA	PARINACOCCHAS	AYACUCHO	15.016859 33	-73.781765	100M			0	1	1	0	1	RURAL	B	TIPO 1
19	1	CPNP SECTORIAL PAUCAR DEL SARA	AV. MIGUEL CERVANTES SAAVEDRA # 519	PAUSA	PAUCAR DEL SARA	AYACUCHO	15.278693 33	-73.34426167	100M			0	1	1	0	1	RURAL	C	TIPO 1
19	2	CPNP TACA	OTRO PLAZA PRINCIPAL # SN	CANARIA	VICTOR FAJARDO	AYACUCHO	13.958801 67	-73.91770667	100M			0	1	1	0	1	RURAL	D	TIPO 1
19	3	CPNP VILLA CANARIA	AV. LIBERTAD # SN	CANARIA	VICTOR FAJARDO	AYACUCHO	13.923641 67	-73.90473667	100M			0	1	1	0	1	RURAL	C	TIPO 1
19	4	CPNP HUANCAPÍ	JIRÓN VICTOR FAJARDO # 745	HUANCAPÍ	VICTOR FAJARDO	AYACUCHO	-13.7516	-74.06583167	100M			0	1	1	0	1	RURAL	C	TIPO 1
19	5	CPNP SECTORIAL VILCASHUAMAN	AV. VILCAS RAYMI B. HUANCAPUQUIO	VILCAS HUAMAN	VILCAS HUAMAN	AYACUCHO	13.657699	-73.953199	100M			0	1	1	0	1	URBANO	D	TIPO 1
19	6	CPNP SECTORIAL CAJABAMBA	AV. LEONCIO MARTINEZ VERAU # 341	CAJABAMBA	CAJABAMBA	CAJAMARCA	7.6278733 33	-78.04395	100M			0	1	1	0	1	URBANO	B	TIPO 1
19	7	CPNP SECTORIAL BAÑOS DEL INCA/DIRCOCOR CAJAMARCA	JIRÓN YAHUAR HUACA # 207	BAÑOS DEL INCA	CAJAMARCA	CAJAMARCA	7.1641933	-78.4629683	100M			0	1	1	0	2	URBANO	B	TIPO 1
19	8	CPNP CAJAMARCA I/COMPLEJO PNP 30 de agosto/CPNP FAMILIA	JR. AMALLA PUGA # 1111	CAJAMARCA	CAJAMARCA	CAJAMARCA	7.1603910 24	-78.51294369	200M			1	0	1	0	1	URBANO	FRENTE B	TIPO 1
19	9	CPNP CAJAMARCA II	JIRÓN CHEPEN # 511	CAJAMARCA	CAJAMARCA	CAJAMARCA	-7.1502	-78.519685	200M			0	1	1	0	3	URBANO	B	TIPO 1
20	1	CPNP DE LA FAMILIA/DEPNICR/DIVCOTER/DIPOLIS (AHORA SEGURIDAD DE ESTADO)	CALLE JORGE OCHOA # 945	SANTIAGO	CUSCO	CUSCO	13.524311 71	-71.98421158	200M	1		2	0	1	0	3	URBANO	UNIDAD PNP	TIPO 2
20	2	CPNP MAGDALENA CAJAMARCA	VIA DE EVITAMIENTO 1083	CAJAMARCA	CAJAMARCA	CAJAMARCA	-7.145627	-78.516962	100M			0	1	1	0	1	URBANO	OFICRI	TIPO 1
20	3	CPNP SECTORIAL CELENDIN	AV. JORGE CHAVEZ # 970	MAGDALENA	CAJAMARCA	CAJAMARCA	7.2517016 67	-78.65664333	100M			0	1	1	0	1	RURAL	C	TIPO 1
20	4	CPNP SECTORIAL CHOTA/DIVPO/POLICINICO	AV. INCA GARCILAZO DE LA VEGA # 724	CHOTA	CELENDIN	CAJAMARCA	-6.872035	-78.142825	100M			0	1	1	0	1	URBANO	B	TIPO 1
20	5	CPNP CHILETE	JIRÓN FERROCARRIL # SN	CHILETE	CONTUMAZA	CAJAMARCA	7.2217316 67	-78.83890333	100M			0	1	1	0	1	URBANO	D	TIPO 1
20	6	DESPRCAR CHILETE	JIRÓN INDEPENDENCIA # 115	CHILETE	CONTUMAZA	CAJAMARCA	7.2219316 67	-78.838895	100M			0	0	1	0	0	URBANO	CARRITERAS	TIPO 1
20	7	CPNP SECTORIAL CONTUMAZA	JIRÓN MELGAR # 195	CONTUMAZA	CONTUMAZA	CAJAMARCA	7.3667266 67	-78.806998	100M			0	1	1	0	2	RURAL	B	TIPO 1
20	8	CPNP SECTORIAL TEMPLADERA	CALLE PLAZA DE ARMAS # SN	YONAN	CONTUMAZA	CAJAMARCA	7.255216 67	-79.13042	100M			0	1	1	0	1	RURAL	C	TIPO 1
20	9	CPNP SECTORIAL CUTERVO	AV. SALOMON VILCHEZ MURGA # SN	CUTERVO	CUTERVO	CAJAMARCA	-6.38312	-78.81660833	100M			0	1	1	0	2	URBANO	B	TIPO 1
21	0	CPNP SECTORIAL BAMBAMARCA	JIRÓN JAIME MARTINEZ # 132	BAMBAMARCA	HUALGAYOC	CAJAMARCA	6.6780916 67	-78.517655	100M			0	1	1	0	1	URBANO	D	TIPO 1
21	1	CPNP JAEN	AV. MESONES MURO # 109	JAEN	JAEN	CAJAMARCA	5.7101133 33	-78.806635	100M			0	1	1	0	3	URBANO	B	TIPO 1



21	CPNP RURAL JAEN/DIVISION POLICIAL JAEN	JR. CAJAMARCA 498-JAEN/JAV MESONES MURO 109	JAEN	JAEN	CAJAMARCA	-5.709992	-78.806317	100M			0	1	1	0	1	URBANO	D	TIPO 1
2	POSTA PNP MEDICA JAEN	CALLE CAJAMARCA 340	JAEN	JAEN	CAJAMARCA	-5.70781	-78.806731	100M			0	1	1	0	1	URBANO	POSTA MEDICA	TIPO 1
3	CPNP SECTORIAL SAN IGNACIO	AV. SAN IGNACIO # SN	SAN IGNACIO	SAN IGNACIO	CAJAMARCA	5.1459666 67	-78.999695	100M			0	1	1	0	2	URBANO	B	TIPO 1
21	CPNP SECTORIAL SAN MARCOS	JIRON INCLAN Y LAVALLE # 141	PEDRO GALVEZ	SAN MARCOS	CAJAMARCA	-7.3348	-78.16963167	100M			0	1	1	0	2	RURAL	B	TIPO 1
21	CPNP SECTORIAL SAN MIGUEL	JIRON BOLOGNESE # 465	SAN MIGUEL	SAN MIGUEL	CAJAMARCA	-7.00025	-78.85136167	100M			0	1	1	0	1	RURAL	C	TIPO 1
21	CPNP SAN PABLO	AV. 13 DE JULIO # 306	SAN PABLO	SAN PABLO	CAJAMARCA	-7.11739	-78.824345	100M			0	1	1	0	1	RURAL	C	TIPO 1
21	CPNP SECTORIAL SANTA CRUZ DE SUCCHABAMBA	CALLE ALFONSO UGARTE # 230	SANTA CRUZ	SANTA CRUZ	CAJAMARCA	6.6246933 33	-78.94401333	100M			0	1	1	0	1	RURAL	B	TIPO 1
21	CPNP ANCAHUASI	KM 45 VIA NACIONAL DISTRITO DE ANCAHUASI	ANCAHUASI	ANTA	CUSCO	-13.45642	-72.301511	100M			0	1	1	0	0	RURAL	E	TIPO 1
22	CPNP IZCUCHACA/COM SECTORIAL ANTA	CALLE JAQUAHUANA # SN	ANTA	ANTA	CUSCO	-13.46401	-72.14420167	100M			0	1	1	0	1	URBANO	D	TIPO 1
22	CPNP RURAL CACHIMAYO	AV. LEONIDAS RODRIGUEZ FIGUEROA # SN	CACHIMAYO	ANTA	CUSCO	-13.47951	-72.06615667	100M			0	1	1	0	0	URBANO	E	TIPO 1
22	CPNP RURAL CALCA	JIRON ESPINAR # 498	CALCA	CALCA	CUSCO	13.320495	-71.95564667	100M			0	1	1	0	1	URBANO	B	TIPO 1
22	CPNP SAN SALVADOR	CALLE CUSCO S/N.	SAN SALVADOR	CALCA	CUSCO	13.490590 55	-71.7990662	100M			0	1	1	0	1	URBANO	C	TIPO 1
22	CPNP RURAL LAYO	AV. MIGUEL GRAU # SN	LAYO	CANAS	CUSCO	14.492094	-71.157504	100M			0	1	1	0	0	RURAL	E	TIPO 1
22	CPNP YANAOC	AV. TUPAC AMARU # 340	YANAOC	CANAS	CUSCO	14.214745	-71.43222167	100M			0	1	1	0	1	URBANO	C	TIPO 1
22	CPNP CHECACUPE	AV. TUPAC AMARU S/N	CHECACUPE	CANCHIS	CUSCO	14.026079	-71.452701	100M			0	1	1	0	0	RURAL	E	TIPO 1
22	CPNP RURAL COMBAPATA E	FRENTE A LA PLAZA DE ARMAS DE COMBAPATA	COMBAPATA	CANCHIS	CUSCO	14.101307	-71.429295	100M			0	1	1	0	0	RURAL	E	TIPO 1
22	CPNP MARANGANI	FRENTE A LA PLAZA DE ARMAS DE MARANGANI	MARANGANI	CANCHIS	CUSCO	14.356728	-71.168544	100M			0	1	1	0	1	RURAL	D	TIPO 1
22	CPNP RURAL PITUMARCA	CALLE SIN NOMBRE # 133 (PLAZA DE ARMAS)	PITUMARCA	CANCHIS	CUSCO	-13.97991	-71.41748167	100M			0	1	1	0	1	URBANO	C	TIPO 1
23	CPNP RURAL DE TORCOMA	AV. CONFEDERACION # SN	SICUANI	CANCHIS	CUSCO	14.255068 33	-71.22999	100M			0	1	1	0	1	URBANO	B	TIPO 1
23	CPNP RURAL SICUANI	AV. GRAU # SN	SICUANI	CANCHIS	CUSCO	14.279436 67	-71.22442833	100M			0	1	1	0	2	URBANO	B	TIPO 1
23	POSTA PNP SICUANI	AV. REPUBLICA DEL PERU CON JR. LAS RETAMAS 117-119	SICUANI	CANCHIS	CUSCO	14.260380	-71.226484	100M			0	1	1	0	1	URBANO	POSTA MEDICA	TIPO 1
23	CPNP RURAL TINTA	AV. TUPAC AMARU # SN	TINTA	CANCHIS	CUSCO	14.142975	-71.40252833	100M			0	1	1	0	0	URBANO	E	TIPO 1
23	CPNP RURAL SANTO TOMAS	CALLE JEREMIAS PASHBY COLLINS # SN	SANTO TOMAS	CHUMBIVILCAS	CUSCO	14.448088 33	-72.08439833	100M			0	1	1	0	1	RURAL	D	TIPO 1
23	CPNP SECTORIAL CUSCO/DIRTEPOL	AV. REGIONAL 902 (ANTES CALLE SAPHY # 510)	CUSCO	CUSCO	CUSCO	13.514638	-71.981428	100M			0	1	1	0	3	URBANO	A	TIPO 1
23	CPNP SIPASPUCCYO	CALLE CESAR VALLEJO # SN	CUSCO	CUSCO	CUSCO	-13.52149	-71.98782	100M			0	1	1	0	1	URBANO	C	TIPO 1
23	CPNP TAHUANTINSUYO CUSCO	PASAJE LAS AMERICAS # SN	CUSCO	CUSCO	CUSCO	13.519068 6	-71.95926905	100M			0	1	1	0	2	URBANO	B	TIPO 1

Handwritten signatures and marks at the top left of the page.



23	8	CPNP POROY	OTRO PISTA ASFALTICA CUSCO - LIMA # SN	POROY	CUSCO	CUSCO	13.485445	-72.04178333	100M		0	1	1	0	1	URBANO	C	TIPO 1
23	9	CPNP SAN JERONIMO	AV. MANCO CAPAC # SN	SAN JERONIMO	CUSCO	CUSCO	13.546151 67	-71.89961333	100M		0	1	1	0	1	URBANO	C	TIPO 1
24	0	CPNP SAN SEBASTIAN	AV. LA CULTURA # SN	SAN SEBASTIAN	CUSCO	CUSCO	13.532281 67	-71.926475	100M		0	1	1	0	1	URBANO	C	TIPO 1
31	5	DIVINCRI ICA/COM FAMILIA ICA	CALLE LIBERTAD 384	ICA	ICA	ICA	14.065925	-75.73204	200M	1	2	0	1	0	3	URBANO	UNIDAD PNP	TIPO 2
24	2	CPNP SANTIAGO	CALLE JORGE OCHOA N° 355	SANTIAGO	CUSCO	CUSCO	13.524125	-71.984302	100M		0	1	1	0	3	URBANO	C	TIPO 1
24	3	CPNP VIVA EL PERU	JR SEÑOR HUANCA SN MZA LT. 4	SANTIAGO	CUSCO	CUSCO	13.538720 86	-71.95853949	100M		0	1	1	0	2	URBANO	C	TIPO 1
24	4	CPNP SAYLLA	AV. CUSCO # SN	SAYLLA	CUSCO	CUSCO	13.572553 69	-71.82559311	100M		0	1	1	0	1	URBANO	C	TIPO 1
24	5	COMISARIA DE TURISMO CUSCO	AV. PLAZA TUPAC AMARU S/N	WANCHAQ	CUSCO	CUSCO	13.522824	-71.967096	100M		0	0	1	0	1	URBANO	TURISMO	TIPO 1
24	6	CPNP AEROPUERTO ALEJANDRO VELAZCO ASTETE	AV. VELASCO ASTETE # SN	WANCHAQ	CUSCO	CUSCO	13.538581 67	-71.94312167	100M		0	1	1	0	0	URBANO	A	TIPO 1
24	7	CPNP SECTORIAL WANCHAQ/COMPLEJO POLICIAL 6 DICIEMBRE	AV. 28 DE JULIO CDRA. 3 URB. TTIO WANCHAQ	WANCHAQ	CUSCO	CUSCO	13.532116 67	-71.959705	100M		0	1	1	0	3	URBANO	B	TIPO 1
24	8	DIVPOLUD - CUSCO	AV. EL SOL CUADRA 2	WANCHAQ	CUSCO	CUSCO	13.522901	-71.974883	100M		0	1	1	0	1	URBANO	POLUIS	TIPO 1
24	9	OFICRI CUZCO	CALLE ALCIDES VIGO S/N REF. COSTADO DEL MINISTERIO DE TRABAJO	WANCHAQ	CUSCO	CUSCO	13.523941	-71.965596	100M		0	1	1	0	1	URBANO	OFICRI	TIPO 1
25	0	REGPOL CUSCO / UNITIC CUSCO	PLAZA TUPAC AMARU S/N - WANCHAQ	WANCHAQ	CUSCO	CUSCO	-13.52306	-71.96602	200M		1	1	1	0	1	RURAL	REGPOL	TIPO 1
25	1	CPNP ESPINAR	CALLE 9 DE DICIEMBRE S/N CON JR. SOL	ESPINAR	ESPINAR	CUSCO	14.790961	-71.412126	100M		0	1	1	0	1	URBANO	B	TIPO 1
25	2	DESPCAR ESPINAR	CALLE HECTOR TELADA # 102	ESPINAR	ESPINAR	CUSCO	14.792291	-71.413633	100M		0	0	1	0	1	RURAL	CARRETERAS	TIPO 1
25	3	DESPCAR QUILLABAMBA	PASAJE PUERTO MALAGA # SN	HUAYOPATA	LA CONVENCIÓN	CUSCO	13.006253 33	-72.55314833	100M		0	0	1	0	0	RURAL	CARRETERAS	TIPO 1
25	4	CPNP DE LA MUJER QUILLABAMBA (TAMBIEN SE IMPLEMENTO EN LA CPNP QUILLABAMBA MISMA UBICACIÓN)	PROLONGACIÓN RICARDO PALMA # SN	SANTA ANA	LA CONVENCIÓN	CUSCO	12.857433 33	-72.69672167	200M		0	1	1	0	1	RURAL	FAMILIA	TIPO 1
25	5	CPNP PAVAYOC	AV. VIRGEN DEL CARMEN S/N - SECTOR PINTOBAMBA GRANDE	SANTA ANA	LA CONVENCIÓN	CUSCO	-12.84731	-72.70705	100M		0	1	1	0	1	URBANO	C	TIPO 1
25	6	CPNP QUILLABAMBA/DIVINCRI/SEANDRO/OFINTE (IMPLEMENTADO EN LA DIVPOLA CONCEPCIÓN)	JIRÓN LIBERTAD # 429	SANTA ANA	LA CONVENCIÓN	CUSCO	12.864063 99	-72.69269161	100M		0	1	1	0	2	RURAL	B	TIPO 1
25	7	CPNP RURAL PARURO	CALLE GRAU # SN	PARURO	PARURO	CUSCO	-13.76064	-71.849625	100M		0	1	1	0	1	RURAL	C	TIPO 1
25	8	CPNP ZONAL RURAL PAUCARTAMBO	CALLE PLAZOLETA MANCO CCAPAC # SN	PAUCARTAMBO	PAUCARTAMBO	CUSCO	13.317995	-71.597485	100M		0	1	1	0	1	URBANO	C	TIPO 1
25	9	CPNP RURAL ANDAHUAYILLAS	CALLE ESPINAR S/N ANDAHUAYILLA (ANTES CALLE GARCILAZO DE LA VEGA N° 800)	ANDAHUAYILLAS	QUISICANCHI	CUSCO	13.673107	-71.677682	100M		0	1	1	0	0	RURAL	E	TIPO 1
26	0	CPNP RURAL KCAURI	CARRETERA INTEROCEANICA # SN	CCATCA	QUISICANCHI	CUSCO	13.694655	-71.52801	100M		0	1	1	0	0	URBANO	E	TIPO 1

[Handwritten signature]



[Handwritten signature]

26 1	CNP RURAL HUAMBUTO	AV. PRINCIPAL DE HUAMBUTO # SN	LUCRE	QUISPICANCHI	CUSCO	13.581868 76	-71.7143029	100M		0	1	1	0	0	URBANO	E	TIPO 1
26 2	CNP RURAL OROPESA	CARRETERA CUSCO - URCOS # SN	OROPESA	QUISPICANCHI	CUSCO	13.600746 67	-71.75607333	100M		0	1	1	0	1	RURAL	C	TIPO 1
26 3	CNP RURAL DE URCOS	OTRO PLAZA DE ARMAS # SN	URCOS	QUISPICANCHI	CUSCO	13.688625	-71.62517157	100M		0	1	1	0	1	URBANO	C	TIPO 1
26 4	DIVISION POLICIAL CUJANI- CANCHIS	AV. CONFEDERACION S/N	CANCHIS	SICUANI	CUSCO	14.254899	-71.229553	100M		0	1	1	0	1	URBANO	DIVPOL	TIPO 1
26 5	CNP RURAL CHINCHERO	OTRO PLAZA CHINCHERO # SN	Callamarca	URUBAMBA	CUSCO	13.391995	-72.04895	100M		0	1	1	0	1	URBANO	C	TIPO 1
26 6	CNP MACHUPICCHU	AV. IMPERIO LOS INCAS # 401	MACHUPICCHU	URUBAMBA	CUSCO	13.154680 33	-72.52544314	100M		0	1	1	0	1	RURAL	C	TIPO 1
26 7	CNP RURAL OLLANTAYTAMBO	OTRO PLAZA DE ARMAS # SN	OLLANTAYTAMBO	URUBAMBA	CUSCO	13.258761 67	-72.26394333	100M		0	1	1	0	1	URBANO	C	TIPO 1
26 8	CNP SECTORIAL URUBAMBA	AA.HH. PRIMERO DE MAYO MZ. B LOTE 2	URUBAMBA	URUBAMBA	CUSCO	13.305948 29	-71.11469501	100M		0	1	1	0	2	URBANO	B	TIPO 1
26 9	CNP SECTORIAL ACOBAMBA	AV. SAN MARTIN # 505	ACOBAMBA	ACOBAMBA	HUANCVELI CA	12.840653 11	-74.57052827	100M		0	1	1	0	1	RURAL	C	TIPO 1
27 0	CNP RURAL CONGALLA "E"	AV. CHAUPIRANRA S/N - PLAZA PRINCIPAL	CONGALLA	ANGARAES	HUANCVELI CA	12.956145	-74.49254333	100M		0	1	1	0	1	RURAL	D	TIPO 1
27 1	CNP ANGARAES - LIRCAY	PROLONGACIÓN OLIMPICO # 104	LIRCAY	ANGARAES	HUANCVELI CA	12.90558 35	-74.72616667	100M		0	1	1	0	1	RURAL	D	TIPO 1
27 2	CNP CASTROVIRREYNA	AV. SAN MARTIN # 179	CASTROVIRREYNA	CASTROVIRREYNA	HUANCVELI CA	13.282348 33	-75.31897667	100M		0	1	1	0	1	RURAL	C	TIPO 1
27 3	CNP CHURCAMP	JR. LA MERCED S/N MZ. Y1 LT. 13A	CHUECAMP	CHURCAMP	HUANCVELI CA	12.738564	-74.38989	100M		0	1	1	0	1	RURAL	B	TIPO 1
27 4	COMISARIA DE TURISMO HUANCVELICA/ DIPROVE / TRANSITO / MEDIO AMBIENTE / INSPECTORIA / TEBNA Y OTROS	MALECON VIRGEN DE LA CADELARIA S/N - BARRIO SAN CRISTOBAL	HUANCVELICA	HUANCVELICA	HUANCVELI CA	12.784570	-74.972645	200M		0	0	1	0	1	URBANO	TURISMO	TIPO 1
27 5	CNP DE LA FAMILIA HUANCVELICA (IMPLEMENTADO EN LA DIVINCHI HUANCVELICA)	JIRÓN CARABAYA # SN	HUANCVELICA	HUANCVELICA	HUANCVELI CA	12.786644 84	-74.97233391	100M		0	1	1	0	2	RURAL	FAMILIA	TIPO 1
27 6	CNP SECTORIAL HUANCVELICA/DIVINCHI/OFCRI	JIRÓN GRAU # 125	HUANCVELICA	HUANCVELICA	HUANCVELI CA	12.785928 33	-74.96892333	100M		0	1	1	0	3	RURAL	B	TIPO 1
27 7	POL PNP HUANCVELICA	JR. MANCO CAPAC 102	HUANCVELICA	HUANCVELICA	HUANCVELI CA	12.78617	-74.973096	100M		0	1	1	0	1	RURAL	POLICLINICO	TIPO 1
27 8	REGPOL HUANCVELICA	JIRÓN GRAU 126 PLAZA SANTA ANA	HUANCVELICA	HUANCVELICA	HUANCVELI CA	12.785867	-74.968951	100M		0	1	1	0	1	RURAL	DIRTEPOL	TIPO 1
27 9	CNP HUANDO	AV. ATAHUALPA # SN	HUANDO	HUANCVELICA	HUANCVELI CA	12.563833 33	-74.94752667	100M		0	1	1	0	1	RURAL	D	TIPO 1
28 0	DESPCAR PAMPAS VRAEM	AV. PROGRESO # SN	PAMPAS	TAYACAJA	HUANCVELI CA	12.393183 33	-74.86978667	100M		0	0	1	0	0	RURAL	CARRETERAS	TIPO 1
28 1	POSTA PNP PAMPAS	JR. SAN SEBASTIAN S/N CRUCE CON JR. ALFONSO UGARTE	PAMPAS	TAYACAJA	HUANCVELI CA	12.398837	-74.865102	100M		0	1	1	0	1	RURAL	POSTA MEDICA	TIPO 1
28 2	CNP SECTORIAL PAMPAS - TAYACAJA	JIRÓN MILLER Y LIMA # 100	PAMPAS	TAYACAJA	HUANCVELI CA	12.397886 67	-74.86904167	100M		0	1	1	0	1	RURAL	B	TIPO 1



28	3	CPNP AMBO	JIRÓN BOLOGNESI # 154	AMBO	AMBO	HUANUCO	10.127405	-76.20424333	100M		0	1	1	0	2	URBANO	C	TIPO 1
28	4	CPNP SECTORIAL DOS DE MAYO/COMCAR LA UNION	JIRÓN LOURDES # 119	LA UNION	DOS DE MAYO	HUANUCO	-9.827985	-76.801775	100M		0	1	1	0	1	RURAL	B	TIPO 1
28	5	CPNP LLATA	JIRÓN 28 DE JULIO # SN	LLATA	HUAMALIES	HUANUCO	-9.550135	-76.818275	100M		0	1	1	0	1	RURAL	C	TIPO 1
63	8	DIRECCION DE BIENESTAR Y APOYO AL POLICIA - DIRBAP	JR. MIELLO FRANCO N° 155	JESUS MARIA	LIMA	LIMA	-12.07447	-77.052338	200M	1	3	0	1	0	3	URBANO	UNIDAD PNP	TIPO 2
28	7	CPNP AMARILIS	AV. LOS GIRASOLES # SN	AMARILIS	HUANUCO	HUANUCO	9.9427616 67	-76.24728167	100M		0	1	1	0	1	URBANO	B	TIPO 1
28	8	CPNP ACOMAYO	CALLE INCAPATA N° 412 CENTRO POBLADO ACOMAYO	CHINCHAO	HUANUCO	HUANUCO	9.8017166 67	-76.07139667	100M		0	1	1	0	1	RURAL	C	TIPO 1
29	9	CPNP RANCHO	CARRETERA CENTRAL HUANUCO/TINGO MARIA # SN	CHURUBAMBA	HUANUCO	HUANUCO	-9.830.984	-76.094.232	100M		0	1	1	0	1	RURAL	D	TIPO 1
29	0	COMISARIA DE TURISMO HUANUCO	JR. PROLONGACIÓN ABTAO N° 479	HUANUCO	HUANUCO	HUANUCO	99.367.224	762.467.656	100M		0	0	1	0	1	URBANO	TURISMO	TIPO 1
29	1	CPNP HUANUCO/REG POL HUANUCO	JIRÓN CONSTITUCION # 501	HUANUCO	HUANUCO	HUANUCO	9.9263030 47	-76.23923779	200M		1	1	1	0	1	URBANO	REGPOL	TIPO 1
29	2	CPNP CAYHUAYNA	CALLE LOS SAUCES N° 237 - MZ. A LOTE 6	PILCO MARCA	HUANUCO	HUANUCO	-9.96268	-76.24330	100M		0	1	1	0	2	URBANO	B	TIPO 1
29	3	ETS PNP HUANUCO	CARRETERA CENTRAL HUANUCO TINGO MARIA KM12.5	SANTA MARIA DEL VALLE	HUANUCO	HUANUCO	-9.860565	-76.167008	100M		0	1	1	0	5	URBANO	ETS	TIPO 1
29	4	CPNP DE JESUS	JIRÓN LEONCIO PRADO # SN	JESUS	LAURICOCHA	HUANUCO	-10.07829	-76.6319	100M		0	1	1	0	1	RURAL	C	TIPO 1
29	5	CPNP AUCAYACU	AV. INDEPENDENCIA # 507 - FRENTE AL COLEGIO INTEGRADO #038	JOSE CRESPO Y CASTILLO	LEONCIO PRADO	HUANUCO	-8.933404	-76.115184	100M		0	1	1	0	2	URBANO	C	TIPO 1
29	6	CPNP DE LA FAMILIA - TINGO MARIA	AV. AREQUIPA 1121	RUPA-RUPA	RUPA-RUPA	HUANUCO	9.2916666	-75.96944	100M		0	1	1	0	1	URBANO	FAMILIA	TIPO 1
29	7	CPNP TINGO MARIA/DIVPOL TINGO MARIA	JIRÓN ANTONIO RAYMONDI # 413	RUPA-RUPA	LEONCIO PRADO	HUANUCO	-9.297975	-76.90281167	100M		0	1	1	0	2	URBANO	B	TIPO 1
29	8	DEINCRI TINGO MARIA/COMCAR TINGO MARIA	AV. LAS BANDERAS TINGO MARIA 210	RUPA-RUPA	LEONCIO PRADO	HUANUCO	9.3033243	-76.0033708	100M		0	1	1	0	2	URBANO	DIVINCRI	TIPO 1
29	9	DEPOTAD RUPA RUPA	AV. PIMENTEL CDRA 07 TINGO MARIA 711	RUPA-RUPA	LEONCIO PRADO	HUANUCO	-9.308218	-76.000876	100M		0	1	1	0	1	URBANO	DIRANDRO	TIPO 1
30	0	CPNP HUACRACHUCO	JIRÓN MARAÑON # SN	HUACRACHUCO	MARAÑON	HUANUCO	8.6039566 67	-77.14897	100M		0	1	1	0	1	RURAL	C	TIPO 1
30	1	CPNP PANAJO - PACHITEA	JIRÓN BOLOGNESI # 225	PANAJO	PACHITEA	HUANUCO	-9.896994	-75.994859	100M		0	1	1	0	1	RURAL	B	TIPO 1
30	2	CPNP PUERTO INCA	AV. FERNANDO BELAUDE TERRY #5/N	PUERTO INCA	PUERTO INCA	HUANUCO	-9.380307	-74.964759	100M		0	1	1	0	1	RURAL	B	TIPO 1
30	3	FRENTE POLICIAL PUERTO INCA	JR. LORETO S/N MZ 1 LOTE 27	PUERTO INCA	PUERTO INCA	HUANUCO	-9.376946	-74.957027	100M		0	0	1	0	1	URBANO	FRENTE	TIPO 1
30	4	CPNP CHAVINILLO	JIRÓN VIRGEN DE FATIMA # SN	CHAVINILLO	YAROWILCA	HUANUCO	9.8592955 83	-76.60876572	100M		0	1	1	0	1	RURAL	C	TIPO 1
30	5	CPNP CHINCHA ALTA/EMERGENCIA 105/HALCONES	CALLE PLAZA DE ARMAS # 400	CHINCHA ALTA	CHINCHA	ICA	13.417133 33	-76.13287167	100M		0	1	1	0	3	URBANO	A	TIPO 1
30	6	DEPINCRI CHINCHA/GIR/TRANSITO	AV. JOSE GALVEZ CHIPOCO 230	CHINCHA ALTA	CHINCHA	ICA	13.413123	-76.131799	100M		0	1	1	0	2	URBANO	DIVINCRI	TIPO 1
30	7	CPNP CHINCHA BAJA	CALLE JUAN C. DE MORA # 150	CHINCHA BAJA	CHINCHA	ICA	13.458711 67	-76.16161883	100M		0	1	1	0	1	URBANO	C	TIPO 1

[Handwritten signatures and marks]



[Handwritten signatures and initials]

308	CPNP EL CARMEN	CALLE PLAZA DE ARMAS # SN	EL CARMEN	CHINCHA	ICA	13.499498 33	-76.057485	100M			0	1	1	0	1	URBANO	C	TIPO 1
309	CPNP GROCIO PRADO	AV. SAN MARTIN # 202	GROCIO PRADO	CHINCHA	ICA	13.397198 33	-76.15537833	100M			0	1	1	0	1	URBANO	B	TIPO 1
310	CPNP PUEBLO NUEVO	AV. SIMON BOLIVAR # 1152	PUEBLO NUEVO	CHINCHA	ICA	-13.39557	-76.13424167	100M			0	1	1	0	1	URBANO	A	TIPO 1
311	POL PNP CHINCHA	AV. OSCAR R. BENAVIDES 601	PUEBLO NUEVO	CHINCHA	ICA	13.405024	-76.127781	100M			0	1	1	0	1	URBANO	POLICLINICO	TIPO 1
312	CPNP SUNAMPE	AV. PLAZA DE ARMAS # SN	SUNAMPE	CHINCHA	ICA	-13.42582	-76.164015	100M			0	1	1	0	1	URBANO	B	TIPO 1
313	CPNP TAMBO DE MORA	AV. SIMON BOLIVAR # 119	TAMBO DE MORA	CHINCHA	ICA	13.460618 33	-76.18360333	100M			0	1	1	0	1	URBANO	C	TIPO 1
314	CPNP ICA	AV. JUAN JOSE ELIAS # SN	ICA	ICA	ICA	-14.06981	-75.732515	100M			0	1	1	0	2	URBANO	A	TIPO 1
321	DIVINCI + SEANDRO JUANUI+DIVPOL	CALLE LA MERCED 428 SE TRASLADÓ A LA COMISARIA DE JUANUI	JUANUI	MARISCAL CACERES	SAN MARTIN	-7.179839	-76.726496	200M	1		3	0	1	0	3	URBANO	UNIDAD PNP	TIPO 2
322	POL PNP ICA	JR. HUÁNUCO 480	ICA	ICA	ICA	14.066069	-75.731672	100M			0	1	1	0	1	URBANO	POLICLINICO	TIPO 1
323	TRANSITO DEPROVE DEPIAT	AV. ARIAS Y ARAGÓES 1115	TACNA	TACNA	TACNA	18.02456	-70.259372	200M	1		2	0	1	0	4	URBANO	UNIDAD PNP	TIPO 2
324	COMISARIA DE TURISMO ICA	CALLE LIMA N° 367 PREFECTURA	ICA	ICA	ICA	14.066144	-75.7277474	100M			0	0	1	0	1	URBANO	TURISMO	TIPO 1
325	CPNP LA TINGUIÑA	AV. VICTORIO GOTUZZO BIANCHI # 432	LA TINGUIÑA	ICA	ICA	14.036496 53	-75.71059987	100M			0	1	1	0	1	URBANO	C	TIPO 1
326	CPNP LOS AQUIES	AV. PRINCIPAL # SN	LOS AQUIES	ICA	ICA	14.097006 67	-75.69105333	100M			0	1	1	0	1	URBANO	C	TIPO 1
327	CPNP PACHACUTEC ICA	CLL HUAYNA CAPAC SN	PACHACUTEC	ICA	ICA	14.152996 67	-75.69128167	100M			0	1	1	0	1	URBANO	D	TIPO 1
328	CPNP PARCONA	CALLE RAUL PORRAS BARRENECHEA # SN	PARCONA	ICA	ICA	-14.04783	-75.70576	100M			0	1	1	0	1	URBANO	B	TIPO 1
329	CPNP PUEBLO NUEVO - ICA	CALLE LIBERTAD # 119	PUEBLO NUEVO	ICA	ICA	14.126708 33	-75.705735	100M			0	1	1	0	1	URBANO	D	TIPO 1
330	CPNP RURAL GUADALUPE (EX SALAS)	AV. MUNICIPALIDAD # SN	SALAS	ICA	ICA	13.985958 33	-75.77224333	100M			0	1	1	0	1	URBANO	C	TIPO 1
331	CPNP LOS MOLINOS	CALLE 9 DE OCTUBRE # SN	SAN JOSE DE LOS MOLINOS	ICA	ICA	13.932486 67	-75.67110167	100M			0	1	1	0	1	URBANO	C	TIPO 1
332	CPNP SAN JUAN BAUTISTA	CALLE MARISCAL CASTILLA # 142	SAN JUAN BAUTISTA	ICA	ICA	14.011348 33	-75.73443	100M			0	1	1	0	1	URBANO	C	TIPO 1
333	CPNP SANTIAGO	CARRETERA PANAMERICANA SUR # SN	SANTIAGO	ICA	ICA	14.184288 25	-75.71470231	100M			0	1	1	0	1	URBANO	C	TIPO 1
334	CPNP SUBTANIALLA	CLL INDEPENDENCIA 396	SUBTANIALLA	ICA	ICA	14.018966 67	-75.75662833	100M			0	1	1	0	1	URBANO	C	TIPO 1
335	CPNP SAN JUAN DE MARCONA	AV. ANDRES AVELINO CACERES # SN	MARCONA	NAZCA	ICA	15.361626 67	-75.164925	100M			0	1	1	0	2	URBANO	B	TIPO 1



33 0	CPNP NAZCA/DIVPOL NAZCA/TURISMO	AV. LOS INCAS # 101	NAZCA	NAZCA	ICA	14.828183 33	-74.944455	100M		0	1	1	0	2	URBANO	A	TIPO 1
33 1	DESPCAR NAZCA	CARRERA PANAMERICANA SUR # SN	NAZCA	NAZCA	ICA	-14.84769	-74.94934	100M		0	0	1	0	0	URBANO	CARRETERAS	TIPO 1
33 2	POSTA PNP NAZCA	PASAJE MONROY S/N PUEBLO SAN CARLOS	NAZCA	NAZCA	ICA	14.830778	-74.95604	100M		0	1	1	0	1	URBANO	POSTA MEDICA	TIPO 1
33 3	CPNP VISTA ALEGRE	CALLE PACHACUTEC # SN	VISTA ALEGRE	NAZCA	ICA	14.844953 33	-74.9403167	100M		0	1	1	0	2	URBANO	B	TIPO 1
33 4	CPNP PALPA/DIVPOL PALPA	AV. GRAU # SN	SAN PEDRO	PALPA	ICA	14.534346 17	-75.18819773	100M		0	1	1	0	2	RURAL	B	TIPO 1
33 5	CPNP INDEPENDENCIA PISCO	AV. FEDERICO URANGA # 100	INDEPENDENCIA	PISCO	ICA	13.693356 67	-76.030235	100M		0	1	1	0	1	URBANO	C	TIPO 1
33 6	CPNP PARACAS	AV. PARACAS # SN	PARACAS	PISCO	ICA	13.82916 67	-76.24679	100M		0	1	1	0	1	URBANO	C	TIPO 1
33 7	CPNP PISCO/DEPROC/SEANDRO/SEINCR/DIVPOL	CALLE SAN FRANCISCO # 139	PISCO	PISCO	ICA	13.709196 67	-76.20259333	100M		0	1	1	0	3	URBANO	A	TIPO 1
33 8	CPNP SAN MIGUEL PISCO	CALLE SAN MARTIN DE PORRAS # SN	PISCO	PISCO	ICA	13.702735	-76.15344833	100M		0	1	1	0	1	URBANO	C	TIPO 1
33 9	POSTA PNP PISCO	CALLE BEATITA DE HUMAY 200	PISCO	PISCO	ICA	13.711819	-76.205705	100M		0	1	1	0	1	URBANO	POSTA MEDICA	TIPO 1
34 0	CPNP SAN ANDRES PISCO	CALLE GRECIA # 501	SAN ANDRES	PISCO	ICA	13.732455	-76.221128	100M		0	1	1	0	1	URBANO	C	TIPO 1
34 1	CPNP HUAMANI	CARR. PANAMERICANA SUR SN KM.226	SAN CLEMENTE	PISCO	ICA	13.683075	-76.15951167	100M		0	1	1	0	1	URBANO	C	TIPO 1
34 2	CPNP TUPAC AMARU INCA	AV. TUPAC AMARU SN MZ.36 LT.10	TUPAC AMARU INCA	PISCO	ICA	-13.7142	-76.1487	100M		0	1	1	0	1	URBANO	D	TIPO 1
34 3	DESPCAR LA MERCEDES	CARRERA CENTRAL TARMA LA MERCEDES # SN	CHANCHAMAYO	CHANCHAMAYO	JUNIN	11.079015 61	-75.32897383	100M		0	0	1	0	0	RURAL	CARRETERAS	TIPO 1
34 4	CPNP LA MERCEDES/DIVPOL CHANCHAMAYO	JIRON TARMA 694	CHANCHAMAYO	CHANCHAMAYO	JUNIN	11.056067 01	-75.33087015	100M		0	1	1	0	2	RURAL	A	TIPO 1
34 5	POSTA PNP LA MERCEDES	JR. TARMA 694	CHANCHAMAYO	CHANCHAMAYO	JUNIN	11.054215	-75.326.614	100M		0	1	1	0	1	RURAL	POSTA MEDICA	TIPO 1
34 6	CPNP VILLA PERENE	JR. ISAIAS ALDORADIN S/N	PERENE	CHANCHAMAYO	JUNIN	10.952126 67	-75.22560833	100M		0	1	1	0	1	RURAL	B	TIPO 1
34 7	CPNP PICHANAQUI	AV. MARGINAL # 509	PICHANAQUI	CHANCHAMAYO	JUNIN	10.927189 39	-74.87345159	100M		0	1	1	0	1	RURAL	B	TIPO 1
34 8	CPNP SAN RAMON	JIRON PACHITEA # 467	SAN RAMON	CHANCHAMAYO	JUNIN	11.120878 33	-75.35469167	100M		0	1	1	0	1	URBANO	B	TIPO 1
34 9	CPNP SECTORIAL CHUPACA/COM CAR CHUPACA	JIRON GRAU # 1	CHUPACA	CHUPACA	JUNIN	12.05916 67	-75.28800167	100M		0	1	1	0	2	URBANO	B	TIPO 1
35 0	CPNP SECTORIAL CONCEPCION	JIRON BOLIVAR # 527	CONCEPCION	CONCEPCION	JUNIN	11.919088 33	-75.314325	100M		0	1	1	0	2	URBANO	A	TIPO 1
35 1	CPNP CHILCA HUANCAYO	PASAJE SAN ANDRES # 189	CHILCA	HUANCAYO	JUNIN	12.080601 51	-75.2080223	100M		0	1	1	0	2	URBANO	A	TIPO 1

Handwritten signatures and marks at the top left of the page.



Handwritten initials and marks on the left side of the page.

35 2	CPNP EL TAMBO	JIRÓN GONZALES PRADA # SN / A MEDIA CUADRA DE LA PLAZA PRINCIPAL	EL TAMBO	HUANCAYO	JUNIN	12.057603 33	-75.21737167	100M			0	1	1	0	1	URBANO	A	TIPO 1
35 3	DIVICAJ PNP HUANCAYO	AV. 13 DE NOVIEMBRE 1280 URB. MITOTINGO	EL TAMBO	HUANCAYO	JUNIN	12.066813	-75.220404	100M			0	1	1	0	1	URBANO	DIVINCRI	TIPO 1
35 4	CPNP FAMILIA HUANCAYO	AV. GIRALDEZ 574	HUANCAYO	HUANCAYO	JUNIN	12.065432	-75.204522	100M			0	1	1	0	1	URBANO	FAMILIA	TIPO 1
35 5	CPNP HUANCAYO/REG POL HUANCAYO ZDO PISO/TRANSITO/DIRTUNA/DIVPOL	AV. FERROCARRIL # 555	HUANCAYO	HUANCAYO	JUNIN	12.064477 3	-75.20747915	150M			0	1	1	0	3	URBANO	A	TIPO 1
35 6	DIRCOTE HUANCAYO	JR. ATALAYA S/N CONDOMINIO LAS CASUARINAS DISTRITO EL TAMBO	HUANCAYO	HUANCAYO	JUNIN	12.039635	-75.2157471	100M			0	1	1	0	1	URBANO	DIRCOTE	TIPO 1
35 7	HOSPITAL HUANCAYO ENRIQUE TORRES/ SANTA ROSA/POLICLINICO	JR. CUZCO 120	HUANCAYO	HUANCAYO	JUNIN	12.065103	-75.207721	100M			0	1	1	0	1	URBANO	HOSPITAL	TIPO 1
99 6	OFICRI (AFIS) TUMBES	AV. PANAMERICANA NORTE KM 1322- TUMBES (COMPLEJO Tnte JORGE TAYPE TABAZONA)	TUMBES	TUMBES	TUMBES	-3.55564	-80.43813	200M			0	1	1	0	1	URBANO	UNIDAD PNP	TIPO 1
35 9	ETS PNP HUANCAYO	JR. NECOCHEA S/N. A LA ALTURA DEL KM. 04 DE LA CARRETERA CENTRAL HUANCAYO - JAUJA	PILCOMAYO	HUANCAYO	JUNIN	12.046452	-75.246502	100M			0	1	1	0	5	URBANO	ETS	TIPO 1
36 0	CPNP SAN AGUSTIN DE CAJAS	AV. LEONCIO PRADO # SN	SAN AGUSTIN	HUANCAYO	JUNIN	11.991498 33	-75.24658167	100M			0	1	1	0	1	URBANO	C	TIPO 1
36 1	CPNP SAN JERONIMO DE TUNAN	AV. AREQUIPA # SN	SAN JERONIMO DE TUNAN	HUANCAYO	JUNIN	11.949605	-75.28255667	100M			0	1	1	0	1	URBANO	C	TIPO 1
36 2	CPNP SAPALLANGA	AV. FIDEL MIRANDA # 1300	SAPALLANGA	HUANCAYO	JUNIN	-12.14367	-75.16218833	100M			0	1	1	0	1	URBANO	C	TIPO 1
36 3	CPNP CMDE FERRE PELAYO ALIAGA MIRANDA	JIRÓN CONSTITUCION # 300	SICAYA	HUANCAYO	JUNIN	12.015425	-75.279605	100M			0	1	1	0	1	URBANO	C	TIPO 1
36 4	CPNP SECTORIAL JAUJA	JIRÓN FRANCISCO PIZARRO # 150	JAUJA	JAUJA	JUNIN	11.78031 67	-75.49719333	100M			0	1	1	0	2	URBANO	A	TIPO 1
36 5	POSTA PNP JAUJA	JR. GALVEZ 335	JAUJA	JAUJA	JUNIN	11.774265	-75.501403	100M			0	1	1	0	1	URBANO	POSTA MEDICA	TIPO 1
36 6	CPNP CARHUAMAYO	AV. LA UNION # SN	CARHUAMAYO	JUNIN	JUNIN	10.934253 33	-76.05399667	100M			0	1	1	0	1	RURAL	C	TIPO 1
36 7	DEINCRI CHANCHAMAYO	JR. ARICA 166	CHANCHAMAYO	JUNIN	JUNIN	11.056343	-75.330573	100M			0	1	1	0	2	RURAL	DIVINCRI	TIPO 1
36 8	CPNP SECTORIAL JUNIN	JIRÓN BERNARDO ALCEDO # SN	JUNIN	JUNIN	JUNIN	11.162553 33	-75.99343833	100M			0	1	1	0	2	URBANO	B	TIPO 1
36 9	DESPICAR JUNIN	JIRÓN YAULI # SN	JUNIN	JUNIN	JUNIN	11.165891 67	-76.000008	100M			0	0	1	0	0	URBANO	CARRETERAS	TIPO 1
37 0	CPNP MAZAMARI	AV. SAN JUAN # SN	MAZAMARI	SATIPO	JUNIN	11.328235 24	-74.52870458	100M			0	1	1	0	1	RURAL	C	TIPO 1
37 1	CPNP RURAL SAN MARTIN DE PANGO	CALLE UCAYALI # SN	PANGO	SATIPO	JUNIN	-11.42882	-74.48844	100M			0	1	1	0	1	RURAL	C	TIPO 1
37 2	CPNP RIO NEGRO / DESPICAR RIO NEGRO	CARRETERA ALAMEDA MARGINAL # SN	RIO NEGRO	SATIPO	JUNIN	11.209535	-74.65966667	100M			0	1	1	0	0	RURAL	C	TIPO 1
37 3	CPNP SATIPO	JIRÓN FRANCISCO IRAZOLA # 493	SATIPO	SATIPO	JUNIN	11.255681 4	-74.63838011	100M			0	1	1	0	2	RURAL	B	TIPO 1
37 4	POSTA PNP SATIPO	JR. JUNIN 580	SATIPO	SATIPO	JUNIN	11.253424 17	-74.6403562	100M			0	1	1	0	1	RURAL	POSTA MEDICA	TIPO 1

Handwritten signature and initials at the top left of the page.



Handwritten signature and initials in the middle left of the page.

37 5	CPNP ACOBAMBA	JIRÓN CALLAO # SN	ACOBAMBA	TARMA	JUNIN	11.953195	-75.65868333	100M			0	1	1	0	1	RURAL	C	TIPO 1
37 6	CPNP HUASAHUASI	JIRÓN SAN JUAN # SN	HUASAHUASI	TARMA	JUNIN	11.265621 67	-75.64917167	100M			0	1	1	0	1	RURAL	C	TIPO 1
37 7	CPNP SECTORIAL TARMA/POSTA MÉDICA TARMA	JIRÓN CALLAO # 118	TARMA	TARMA	JUNIN	11.418909 53	-75.68693876	100M			0	1	1	0	2	URBANO	B	TIPO 1
37 8	CPNP SECTORIAL LA OROVA/COMCAR LA OROVA	AV. HORACIO ZEVALLOS GAMES # 209	LA OROVA	YAUJU	JUNIN	11.522498 33	-75.909135	100M			0	1	1	0	2	URBANO	A	TIPO 1
37 9	CPNP MOROCOCHA	CLL. P. FLUQUER SN	MOROCOCHA	YAUJU	JUNIN	11.587551 67	-76.06252667	100M			0	1	1	0	1	URBANO	C	TIPO 1
38 0	CPNP LA NORIA	AV. AMERICA SUR # 405 URB LA NORIA	TRUJILLO	TRUJILLO	LA LIBERTAD	-8.10350	-79.01049	100M			0	1	1	0	3	URBANO	A	TIPO 1
38 1	CPNP SECTORIAL RURAL ASCOPE	CALLE MANCO CAPAC # 16	ASCOPE	ASCOPE	LA LIBERTAD	7.7138616 67	-79.10762	100M			0	1	1	0	1	URBANO	A	TIPO 1
38 2	CPNP RURAL CASA GRANDE	AV. INDEPENDENCIA # 224	CASA GRANDE	ASCOPE	LA LIBERTAD	7.7452133 33	-79.188485	100M			0	1	1	0	1	URBANO	B	TIPO 1
38 3	CPNP RURAL ROMA	CALLE EDBERTO TORRES # SN	CASA GRANDE	ASCOPE	LA LIBERTAD	-7.764905	-79.14658833	100M			0	1	1	0	1	URBANO	D	TIPO 1
38 4	CPNP RURAL CHICAMA	AV. PROGRESO # 396	CHICAMA	ASCOPE	LA LIBERTAD	7.8449216 67	-79.14708833	100M			0	1	1	0	1	URBANO	C	TIPO 1
38 5	CPNP RURAL SAUSAL	CALLE CASA GRANDE # SN	CHICAMA	ASCOPE	LA LIBERTAD	-7.73606	-79.00716833	100M			0	1	1	0	1	URBANO	D	TIPO 1
38 6	CPNP RURAL CHOCOPE	JIRÓN BOLOGNESI # 196	CHOCOPE	ASCOPE	LA LIBERTAD	7.7912266 67	-79.22331167	100M			0	1	1	0	1	URBANO	B	TIPO 1
38 7	CPNP SECTORIAL RURAL PAIJAN	PANAMERICANA NORTE MZ. 16 LT. 1A - SECTOR JORGE CHAVEZ	PAIJAN	ASCOPE	LA LIBERTAD	7.7193762	-79.3094247	100M			0	1	1	0	2	URBANO	A	TIPO 1
38 8	DIVEME PAIJAN/DIVPOL/DEPINCRI	CARRETERA PANAMERICANA NORTE # SN	PAIJAN	ASCOPE	LA LIBERTAD	-7.718849	-79.309494	100M			0	1	1	0	2	URBANO	DIVINCRI	TIPO 1
38 9	CPNP RURAL RAZURI	CALLE TARAPACA # 203	RAZURI	ASCOPE	LA LIBERTAD	7.7009833 33	-79.43774167	100M			0	1	1	0	1	URBANO	D	TIPO 1
39 0	CPNP RURAL CARTAVIO	CALLE REAL # SN	SANTIAGO DE CAO	ASCOPE	LA LIBERTAD	7.8865566 67	-79.22048667	100M			0	1	1	0	1	URBANO	C	TIPO 1
39 1	CPNP RURAL SANTIAGO DE CAO	CALLE LIBERTAD # 455	SANTIAGO DE CAO	ASCOPE	LA LIBERTAD	-7.959965	-79.239115	100M			0	1	1	0	1	URBANO	C	TIPO 1
39 2	CPNP RURAL TALAMBO	AV. MIRAFLORES # SN	CHEPEN	CHEPEN	LA LIBERTAD	-7.241655	-79.398555	100M			0	1	1	0	1	URBANO	C	TIPO 1
39 3	CPNP SECTORIAL RURAL CHEPEN	JIRÓN PACASMAYO # 471	CHEPEN	CHEPEN	LA LIBERTAD	-7.231765	-79.42438333	100M			0	1	1	0	1	URBANO	A	TIPO 1
39 4	DIVINCRI CHEPEN	PANAMERICANA NORTE S/N	CHEPEN	CHEPEN	LA LIBERTAD	-7.220083	-79.434736	100M			0	1	1	0	2	URBANO	DIVINCRI	TIPO 1
39 5	CPNP RURAL PACANGA	CALLE AYACUCHO # 798	PACANGA	CHEPEN	LA LIBERTAD	-7.170905	-79.48570833	100M			0	1	1	0	1	URBANO	B	TIPO 1
39 6	CPNP RURAL PACANGUILLA	JIRÓN EL MILAGRO # 396	PACANGA	CHEPEN	LA LIBERTAD	7.1590683 33	-79.44394833	100M			0	1	1	0	1	URBANO	C	TIPO 1
39 7	CPNP RURAL PUEBLO NUEVO	JIRÓN INDEPENDENCIA # 312	PUEBLO NUEVO	CHEPEN	LA LIBERTAD	-7.188135	-79.51499833	100M			0	1	1	0	1	URBANO	C	TIPO 1



39	8	CPNP SECTORIAL RURAL CASCAS	JIRÓN 28 DE JULIO # SN	CASCAS	GRAN CHIMU	LA LIBERTAD	7.4806633 33	-78.81823167	100M			0	1	1	0	1	RURAL	B	TIPO 1
39	9	CPNP SECTORIAL RURAL JULCAN	AV. LUIS FELIPE DE LA PUENTE UCEDA # SN	JULCAN	JULCAN	LA LIBERTAD	8.0427416 67	-78.48705833	100M			0	1	1	0	1	RURAL	B	TIPO 1
40	0	DIRCOCOR TRUJILLO	PREDIO UBICADO EN LA CALLE RICARDO SANCHEZ 407	TRUJILLO	LA LIBERTAD	LA LIBERTAD	8.1101934	-79.0082068	100M			0	1	1	0	1	URBANO	DIRCOCOR	TIPO 1
58	3	CARCELETA JUDICIAL LIMA/OFICRI	AV. ABANCAY CUADRA 5 SN CERCADO / JR. AYACUCHO C-6	CERCADO	LIMA	LIMA	-12.05143	-77.02766	100M			0	1	1	0	1	URBANO	POLJUS	TIPO 1
40	2	CPNP SECTORIAL RURAL OTUZCO	CALLE PROGRESO # 388	OTUZCO	OTUZCO	LA LIBERTAD	7.9050931 33	-78.56506437	100M			0	1	1	0	1	URBANO	A	TIPO 1
40	3	CPNP RURAL CIUDAD DE DIOS	AV. REPUBLICA DE ALEMANIA # 303	GUADALUPE	PACASMAYO	LA LIBERTAD	7.3035566 67	-79.48027833	100M			0	1	1	0	1	URBANO	C	TIPO 1
40	4	CPNP RURAL GUADALUPE	AV. NILA CERRUTI # SN	GUADALUPE	PACASMAYO	LA LIBERTAD	7.2482733 33	-79.47657833	100M			0	1	1	0	2	URBANO	B	TIPO 1
40	5	DESPPCAR GUADALUPE	AV. NILA CERRUTI # SN	GUADALUPE	PACASMAYO	LA LIBERTAD	7.2481583 33	-79.47589833	100M			0	0	1	0	0	URBANO	CARRETERAS	TIPO 1
40	6	CPNP RURAL JEQUETEPEQUE	CALLE SAN JOSE # 451	JEQUETEPEQUE	PACASMAYO	LA LIBERTAD	7.3375316 67	-79.56387833	100M			0	1	1	0	1	URBANO	D	TIPO 1
40	7	CPNP RURAL PACASMAYO	CALLE DOS DE MAYO # 105	PACASMAYO	PACASMAYO	LA LIBERTAD	7.3994416 67	-79.57123833	100M			0	1	1	0	2	URBANO	A	TIPO 1
40	8	DEPINRI PACASMAYO/ INSPECTORIA	JR. LEONCIO PRADO Nº 457	PACASMAYO	PACASMAYO	LA LIBERTAD	7.3989493	-79.5579516	100M			0	1	1	0	2	URBANO	DIVINCI	TIPO 1
40	9	CPNP RURAL SAN JOSE	CALLE LIMA # 601	SAN JOSE	PACASMAYO	LA LIBERTAD	7.3499136 99	-79.45659041	100M			0	1	1	0	1	URBANO	C	TIPO 1
41	0	CPNP RURAL SAN PEDRO DE LLOC	AV. 2 DE MAYO # SN	SAN PEDRO DE LLOC	PACASMAYO	LA LIBERTAD	7.4246233 33	-79.50288333	100M			0	1	1	0	2	URBANO	B	TIPO 1
41	1	CPNP SECTORIAL PATAZ - TAYABAMBA	JIRÓN 2 DE MAYO # SN	TAYABAMBA	PATAZ	LA LIBERTAD	8.2725333 33	-77.29928667	100M			0	1	1	0	2	RURAL	A	TIPO 1
41	2	CPNP RURAL HUAMACHUCO/DEINCRI	AV. SANCHEZ CARRION # 1189	HUAMACHUCO	SANCHEZ CARRION	LA LIBERTAD	7.8169416 95	-78.04235078	100M			0	1	1	0	2	URBANO	A	TIPO 1
41	3	DESPPCAR HUAMACHUCO	AV. SANCHEZ CARRION # 1246	HUAMACHUCO	SANCHEZ CARRION	LA LIBERTAD	-7.817078	-78.042783	100M			0	0	1	0	0	URBANO	CARRETERAS	TIPO 1
41	4	CPNP RURAL QUIRUVILCA	CALLE MOROCOCHA # 111	QUIRUVILCA	SANTIAGO DE CHUCO	LA LIBERTAD	8.0007516 67	-78.30986	100M			0	1	1	0	1	RURAL	C	TIPO 1
41	5	CPNP SECTORIAL RURAL SANTIAGO DE CHUCO	AV. MIGUEL GRAU # 1270	SANTIAGO DE CHUCO	SANTIAGO DE CHUCO	LA LIBERTAD	8.1448913 54	-78.17347527	100M			0	1	1	0	1	RURAL	A	TIPO 1
41	6	CPNP ALTO TRUJILLO	AV. 12 DE NOVIEMBRE MZ. P LOTE 1A	EL PORVENIR	TRUJILLO	LA LIBERTAD	-8.06824	-79.02207333	100M			0	1	1	0	1	URBANO	C	TIPO 1
41	7	CPNP NICOLAS ALCAZAR	PASAJE NICOLAS ALCAZAR # 1077	EL PORVENIR	TRUJILLO	LA LIBERTAD	8.0852316 67	-79.00463167	100M			0	1	1	0	2	URBANO	B	TIPO 1
41	8	CPNP SANCHEZ CARRION	AV. SANCHEZ CARRION # 1010	EL PORVENIR	TRUJILLO	LA LIBERTAD	8.0787460 32	-78.99568952	100M			0	1	1	0	2	URBANO	A	TIPO 1

Handwritten signatures and marks at the top left of the page.



41	DIVINCI NORTE TRUJILLO	ANDRES RAZURI S/N III AV CONDORCANQUI CDR 21 (FRENTE A LA IGLESIA CRISTO REY)	TRUJILLO	LA LIBERTAD	-8.070026	-78997815	100M		0	1	1	0	2	URBANO	DIVINCI	TIPO 1
42	CNP FLORENCIA DE MORA	CALLE 28 DE JULIO # 1100	TRUJILLO	FLORENCIA DE MORA	-8.085155	-79.024015	100M		0	1	1	0	1	URBANO	B	TIPO 1
42	CNP HUANCHACO	JIRON COLON # 481	TRUJILLO	HUANCHACO	-8.079575	-79.12158333	100M		0	1	1	0	2	URBANO	C	TIPO 1
42	CNP RURAL EL MILAGRO	AV. TUPAC AMARU MZ. LL LOTE 01 - EL MILAGRO	TRUJILLO	HUANCHACO	8.023784 96	-79.06441215	100M		0	1	1	0	2	URBANO	B	TIPO 1
42	CNP BELLA VISTA TRUJILLO	CALLE 22 DE FEBRERO # 803	TRUJILLO	LA ESPERANZA	-8.084672	-79.039737	100M		0	1	1	0	2	URBANO	B	TIPO 1
42	CNP SECTORIAL JERUSALEN/WICHANZAO	AV. PANAMERICANA NORTE SN MZ 34 LT.1	TRUJILLO	LA ESPERANZA	8.058666 67	-79.053925	100M		0	1	1	0	2	URBANO	A	TIPO 1
42	CNP SECTORIAL RURAL LAREDO	PASAJE LA FORTUNA # SN	TRUJILLO	LAREDO	8.0919042 68	-78.96026105	100M		0	1	1	0	2	URBANO	B	TIPO 1
42	CNP MIRAMAR	AV. SANTA MARIA SN MZ 30 LT.1A	TRUJILLO	MOCHE	8.1808566 67	-78.99415167	100M		0	1	1	0	1	URBANO	C	TIPO 1
42	CNP MOCHE	AV. LA MARINA SN MZ.10 LT.42	TRUJILLO	MOCHE	8.1706136 54	-79.01090384	100M		0	1	1	0	1	URBANO	B	TIPO 1
42	DESPRICAR MOCHE	CARRETERA PANAMERICANA NORTE # SN	TRUJILLO	MOCHE	8.1388959 73	-79.01622802	100M		0	0	1	0	0	URBANO	CARRETERAS	TIPO 1
42	CNP SALAVERRY	CALLE LIBERTAD # 229	TRUJILLO	SALAVERRY	-8.22362	-78.976495	100M		0	1	1	0	1	URBANO	C	TIPO 1
43	DESPRICAR SIMBAL	CARRETERA PENETRACION A LA SIERRA NORTEÑA # SN	TRUJILLO	SIMBAL	8.0643564 6	-78.86052176	100M		0	0	1	0	0	RURAL	CARRETERAS	TIPO 1
43	COMISARIA DE TURISMO LA LIBERTAD	CALLE FEDERICO GERDES MZ LL LOTE 02 URB. MOCHICA	TRUJILLO	TRUJILLO	-8.093442	-79.039126	100M		0	0	1	0	1	URBANO	TURISMO	TIPO 1
43	REGPOLICA/OFCRI	JR. J. ELIAS S/N (CUADRA 06)	ICA	ICA	14.072966	-75.732273	200M	1	3	0	1	0	5	URBANO	COMPLEJO FRENTE	TIPO 2
43	CNP EL ALAMBRE	CALLE PORTO ALEGRE # 100	TRUJILLO	TRUJILLO	8.1071996 79	-79.03950691	100M		0	1	1	0	2	URBANO	A	TIPO 1
43	DIVICAL-SECARI -LA LIBERTAD	SECTOR NATASHA ALTA AV. AMERICA NOR OESTE S/N CUADRA 7 URB COVICORTI SOTANO DE LA CORTE SUPERIOR DE JUSTICIA LA LIBERTAD	TRUJILLO	TRUJILLO	-8.113471	-79.048251	100M		0	1	1	0	1	URBANO	DIVINCI	TIPO 1
43	REGPOL LA LIBERTAD	JR. DIEGO DE ALMAGRO N° 327	TRUJILLO	TRUJILLO	-8.111251	-79.030128	150M		0	1	1	0	1	URBANO	REGPOL	TIPO 1
43	POL PNP TRUJILLO	AV. STA TERESITA DE JESUS S/N	Trujillo	Trujillo	-8.123257	-79.031604	100M		0	1	1	0	1	URBANO	POLICINICO	TIPO 1
43	CNP BUENOS AIRES	AV. LARCO HERRERA # 598	VICTOR LARCO HERRERA	TRUJILLO	8.1406866 67	-79.05229833	100M		0	1	1	0	2	URBANO	B	TIPO 1
43	CNP RURAL CHAO	AV. VICTOR RAUL HAYA DE LA TORRE SN MZ.3 LT.11 KM.500	CHAO	LA LIBERTAD	8.5373566 67	-78.67920833	100M		0	1	1	0	1	RURAL	C	TIPO 1
43	CNP RURAL VICTOR RAUL HAYA DE LA TORRE	CALLE CESAR VALLEJO # SN	VIRU	LA LIBERTAD	-8.404665	-78.82218667	100M		0	1	1	0	1	URBANO	C	TIPO 1
44	CNP RURAL VIRU/TRANSITO UUEE	AV. VIRU # 125	VIRU	LA LIBERTAD	8.4152575 9	-78.75504591	100M		0	1	1	0	2	URBANO	B	TIPO 1

Handwritten signatures and marks at the top left of the page.



Handwritten initials 'M' and 'W' in the middle left margin.

44	1	DESPRCAR VIRU	CARRTERA PANAMERICANA NORTE # SN	VIRU	VIRU	LA LIBERTAD	8.4238366 67	-78.78235167	100M			0	0	1	0	0	URBANO	CARRETERAS	TIPO 1
44	2	CPNP SECTORIAL CAYALTI	AV. 9 DE OCTUBRE # 110	CAVALTI	CHICLAYO	LAMBAYEQU E	-6.89141	-79.56132	100M			0	1	1	0	1	URBANO	B	TIPO 1
44	3	CP PNP JUAN ARAGON VENTE / DEPUNEME CHICLAYO / AGUILAS NEGRAS / UDEX / RESCATE	CALLE CADIZ N° 154 URB SAN JUAN	CHICLAYO	CHICLAYO	LAMBAYEQU E	-6.767580	-79.833460	100M			0	0	1	0	1	URBANO	COMPLEJO MACRE	TIPO 1
35	8	REGPOL JUNIN - HUANCAYO / OFICRI / INSPECTORIA	JR. CUSCO 666, ESQUINA DE JR. CUSCO CON JR. LIBERTAD	HUANCAYO	HUANCAYO	JUNIN	12.066796	-75.220477	200M	1		2	0	1	0	5	URBANO		TIPO 2
29	6	CP SAN MARTIN DIVINCRI/DIRTUMA/OFCRI	JR. SAN MARTIN COA 7	RESTAURACION	HUARAZ	ANCASH	-9.529525	-77.530045	200M	1		1	0	1	0	3	RURAL	COMPLEJO 1	TIPO 2
44	6	CPNP CAMPONONICO	AV. JORGE CHAVEZ # 801	CHICLAYO	CHICLAYO	LAMBAYEQU E	-6.76828	-79.82985	100M			0	1	1	0	1	URBANO	B	TIPO 1
44	7	CPNP CESAR LLATAS CASTRO	CALLE VICENTE DE LA VEGA # 1182	CHICLAYO	CHICLAYO	LAMBAYEQU E	6.7707366 67	-79.83541667	100M			0	1	1	0	2	URBANO	A	TIPO 1
44	8	CPNP DEL NORTE	CALLE FRANCISCO CUNEO # 1119	CHICLAYO	CHICLAYO	LAMBAYEQU E	-6.76913	-79.85572	100M			0	1	1	0	1	URBANO	B	TIPO 1
44	9	CPNP EL PORVENIR	CALLE ARICA # 499	CHICLAYO	CHICLAYO	LAMBAYEQU E	6.7660316 67	-79.84469833	100M			0	1	1	0	1	URBANO	C	TIPO 1
45	0	ETS PNP CHICLAYO	KM.18.5 CARR. CHICLAYO	CHICLAYO	CHICLAYO	LAMBAYEQU E	-6.885145	-79.823772	100M			0	1	1	0	5	URBANO	ETS	TIPO 1
45	1	REGPOL LAMBAYEQUE	MANCO CAPAC N°205 ESQUINA CON CALLE SAN JOSE	CHICLAYO	CHICLAYO	LAMBAYEQU E	-6.77138	-79.83541	150M			0	1	1	0	1	URBANO	REGPOL	TIPO 1
45	2	CPNP PAMPA GRANDE	AV. TUPAC AMARU # SN	CHONGOYAPE	CHICLAYO	LAMBAYEQU E	6.7461616 67	-79.47912667	100M			0	1	1	0	1	URBANO	D	TIPO 1
45	3	CPNP SECTORIAL CHONGOYAPE	CALLE SIMON BOLIVAR # 2520	CHONGOYAPE	CHICLAYO	LAMBAYEQU E	-6.63645	-79.3945333	100M			0	1	1	0	1	URBANO	C	TIPO 1
45	4	CPNP CIUDAD ETEN	CALLE PEDRO RUIZ GALLO # 692	ETEN	CHICLAYO	LAMBAYEQU E	-6.9072	-79.86165	100M			0	1	1	0	1	URBANO	D	TIPO 1
45	5	CPNP PUERTO ETEN	CALLE DIEGO FERRE # SN	ETEN PUERTO	CHICLAYO	LAMBAYEQU E	-6.927315	-79.86366	100M			0	1	1	0	1	URBANO	D	TIPO 1
45	6	CPNP ATUSPARIA	AV. VIRREY TOLEDO # 1098	JOSE LEONARDO ORTIZ	CHICLAYO	LAMBAYEQU E	-6.75917	-79.82561	100M			0	1	1	0	2	URBANO	B	TIPO 1
45	7	CPNP JOSE LEONARDO ORTIZ	AV. ARGENTINA # 2252	JOSE LEONARDO ORTIZ	CHICLAYO	LAMBAYEQU E	6.7526633 33	-79.84270167	100M			0	1	1	0	1	URBANO	B	TIPO 1
45	8	CPNP LA VICTORIA CHICLAYO	AV. PACHACUTEC # 1510	LA VICTORIA	CHICLAYO	LAMBAYEQU E	6.7986751 24	-79.83548462	100M			0	1	1	0	2	URBANO	B	TIPO 1
45	9	CPNP SECTORIAL MONSEFU	CALLE 7 DE JUNIO # 519	MONSEFU	CHICLAYO	LAMBAYEQU E	-6.87793	-79.87246	100M			0	1	1	0	1	URBANO	B	TIPO 1
46	0	CPNP PATAPO	CALLE SALAZAR # 13	PATAPO	CHICLAYO	LAMBAYEQU E	-6.73767	-79.64052657	100M			0	1	1	0	1	URBANO	D	TIPO 1
46	1	CPNP POSOPE ALTO	CALLE SANTA ROSA # 398	PATAPO	CHICLAYO	LAMBAYEQU E	-6.73519	-79.63466	100M			0	1	1	0	1	URBANO	C	TIPO 1
46	2	CPNP PICSI	JR. SAN MARTIN S/N	PICSI	CHICLAYO	LAMBAYEQU E	-6.71795	-79.76999	100M			0	1	1	0	1	URBANO	C	TIPO 1
46	3	CPNP PIMENTEL	CALLE GRAU # SN	PIMENTEL	CHICLAYO	LAMBAYEQU E	-6.83491	-79.93585	100M			0	1	1	0	1	URBANO	C	TIPO 1
46	4	CPNP POMALCA	CALLE LOS PROFESIONALES - CHALE NRO. 5 - URB. MIRAFLORES	POMALCA	CHICLAYO	LAMBAYEQU E	-6.77034	-79.77272	100M			0	1	1	0	1	URBANO	C	TIPO 1
46	5	CPNP REQUE	CALLE DIEGO FERRE # 100	REQUE	CHICLAYO	LAMBAYEQU E	6.8631983 33	-79.81846167	100M			0	1	1	0	1	URBANO	C	TIPO 1
46	6	CPNP SANTA ROSA LAMBAYEQUE	AV. MARISCAL CASTILLA # 901	SANTA ROSA	CHICLAYO	LAMBAYEQU E	-6.87972	-79.92344	100M			0	1	1	0	1	URBANO	D	TIPO 1



46	7	CPNP JAIME ANTONIO LI CHUNG	AV. POMALCA SN	SARA	CHICLAYO	LAMBAYEQUE	6.8117533 33	-79.64037167	100M			0	1	1	0	1	URBANO	D	TIPO 1
46	8	CPNP SECTORIAL TUMAN	AV. RAMON CASTILLA # 418	TUMAN	CHICLAYO	LAMBAYEQUE	-6.74996	-79.70300167	100M			0	1	1	0	1	URBANO	B	TIPO 1
46	9	CPNP SECTORIAL FERRENAFE	AV. TACNA # 620	FERRENAFE	FERRENAFE	LAMBAYEQUE	6.6352283 33	-79.79128167	100M			0	1	1	0	2	URBANO	A	TIPO 1
47	0	CPNP BATANGRADE	CALLE CALPON # 15	PITITO	FERRENAFE	LAMBAYEQUE	-6.4833	-79.65425167	100M			0	1	1	0	1	URBANO	C	TIPO 1
47	1	CPNP JAVANCA	CALLE ELIAS AGUIRRE # 405	JAVANCA	LAMBAYEQUE	6.3914633 33	-79.82297667	100M				0	1	1	0	1	URBANO	C	TIPO 1
47	2	CPNP SAN MARTIN DE PORRAS	CALLE CAPITAN ORBEGOSO # SN	LAMBAYEQUE	LAMBAYEQUE	6.7083683 33	-79.91427833	100M				0	1	1	0	4	URBANO	B	TIPO 1
47	3	CPNP SECTORIAL LAMBAYEQUE	CALLE DOS DE MAYO # 316	LAMBAYEQUE	LAMBAYEQUE	-6.70113	-79.90669	100M				0	1	1	0	2	URBANO	A	TIPO 1
47	4	CPNP MOCHUMI	AV. JOSE DE SAN MARTIN # 461	MOCHUMI	LAMBAYEQUE	6.5511166 67	-79.86653667	100M				0	1	1	0	1	URBANO	C	TIPO 1
47	5	CPNP INTE VICTOR HERNAN COSTA SAABER	AV. PRIMAVERA # 477	MOTUPE	LAMBAYEQUE	-6.153845	-79.71215833	100M				0	1	1	0	1	URBANO	C	TIPO 1
47	6	CPNP TUCUME	AV. FEDERICO VILLARREAL # 266	TUCUME	LAMBAYEQUE	-6.50636	-79.85943667	100M				0	1	1	0	1	URBANO	D	TIPO 1
56	8	CENTRO DE PROTECCION N° 1 SALAMANCA - DIVINA-DISECU PNP	CALLE LAS AZUCENAS 260 SALAMANCA	ATE	LIMA	12.074962	-76.990691	100M				0	0	1	0	1	URBANO	UNIDAD	TIPO 1
70	7	CPNP JO DE OCTUBRE	JIRON MARCELO # SN	SAN JUAN DE LURIGANCHO	LIMA	-11.94451	-76.98846833	100M				5	1	1	0	3	URBANO	B	TIPO 1
47	9	DIVPOL BARRANCA JEFATURA	JR JOSE GALVEZ N° 490	BARRANCA	BARRANCA	10.753863	-77.758897	150M				0	1	1	0	1	URBANO	DIVPOL	TIPO 1
49	0	CPNP AEROPUERTO INTERNACIONAL JORGE CHAVEZ	AV. ELMER FAUCETT REF. CUADRA 30 COSTADO DEL AEROPUERTO INTERNACIONAL JORGE CHAVEZ	CALLAO	CALLAO	12.026165 67	-77.10455444	400M				0	1	1	0	0	URBANO	B	TIPO 1
58	6	CPNP ALFONSO UGARTE	AV. ALFONSO UGARTE # 1325	CERCADO	LIMA	12.057042 4	-77.04130411	100M				0	1	1	0	3	URBANO	A	TIPO 1
55	7	DIROPE	AV. CRNEL MARCO PUENTE LLANOS	ATE	LIMA	12.039006	-76.914048	100M				0	1	1	0	1	URBANO	COMISARIA	TIPO 1
56	7	CPNP ANCON	AV. JOSE CARLOS MARIATEGUI # SN	ANCON	LIMA	11.775947 8	-77.16932058	100M				0	1	1	0	2	URBANO	B	TIPO 1
52	4	CPNP ASIA	AV. LA MAR # SN	ASIA	CAÑETE	12.779074 98	-76.55660734	100M				0	1	1	0	1	URBANO	COMISARIA	TIPO 1
54	2	CPNP AUALLAMA	JIRON PROGRESO # SN	AUALLAMA	HUARAL	11.558623 33	-77.17915	100M				0	1	1	0	1	RURAL	C	TIPO 1
72	8	CPNP BARBONCITOS	JIRON EL SALVADOR # SN	SAN MARTIN DE PORRES	LIMA	12.030886 67	-77.070025	100M				0	1	1	0	3	URBANO	B	TIPO 1
47	7	CPNP BARRANCA	AV. INDEPENDENCIA # SN	BARRANCA	BARRANCA	-10.75077	-77.76506	100M				0	1	1	0	2	URBANO	A	TIPO 1
70	8	CPNP BAYOVAR	AV. 1 DE MAYO # SN	SAN JUAN DE LURIGANCHO	LIMA	11.952412 61	-76.9917798	100M				0	1	1	0	3	URBANO	B	TIPO 1
28	6	CP ALDES VIGO HURTADO/DIRCOCOR/DEINCRI/CARRERTRAS/ OFICRI	JR. CALICANTO 19 CUADRA S/N	AMARILIS	HUANUCO	-9.993396	-76.235644	200M			1	2	0	1	0	3	URBANO	COMPLEJO 1	TIPO 2

[Handwritten signature]



[Handwritten signature]

48	CPNP BELLAVISTA CALLAO	AV. GUARDIA CHALACA # SN	BELLAVISTA	CALLAO	LIMA	12.061621 67	-77.12518167	100M			0	1	1	0	3	URBANO B	TIPO 1
49	CPNP BOCANegra	CALLE GAMMA # SN	CALLAO	CALLAO	LIMA	12.024315	-77.09550667	100M			0	1	1	0	2	URBANO B	TIPO 1
70	CPNP CAJA DE AGUA	JR. MOQUEGUA Y JR. TRUJILLO S/N	SAN JUAN DE LURIGANCHO	LIMA	LIMA	1.202.723. 00000	7.701.509.000 00	100M			0	1	1	0	3	URBANO A	TIPO 1
52	CPNP CALANGO	AV. GRANADO # 350	CALANGO	CAÑETE	LIMA	12.526581 65	-76.54374038	100M			0	1	1	0	1	URBANO	TIPO 1
49	CPNP CALLAO	JIRÓN SUPE # SN	CALLAO	CALLAO	LIMA	12.054933 33	-77.12884833	100M			0	1	1	0	3	URBANO A	TIPO 1
52	CPNP CANTA	AV. 26 DE JUNIO # SN	CANTA	CANTA	LIMA	11.469083 33	-76.62419	100M			0	1	1	0	1	URBANO B	TIPO 1
71	CPNP CANTO REY	JIRÓN RIO UCAYALI # 3550	SAN JUAN DE LURIGANCHO	LIMA	LIMA	11.975373 33	-76.59600833	100M			0	1	1	0	3	URBANO B	TIPO 1
57	CPNP CARABAYLO	JIRÓN MIGUEL GRAU # 285	CARABAYLO	LIMA	LIMA	-11.854	-77.03787667	100M			0	1	1	0	2	URBANO B	TIPO 1
50	CPNP CARMEN DE LA LEGUA REYNOSO	AV. 1 DE MAYO # 1106	CARMEN DE LA LEGUA REYNOSO	CALLAO	LIMA	12.039228 33	-77.08735667	100M			0	1	1	0	2	URBANO B	TIPO 1
54	CPNP CASAPALCA	CARRETERA CENTRAL # SN	CHICLA	HUAROCHIRI	LIMA	11.652247	-76.235607	100M			0	1	1	0	1	RURAL B	TIPO 1
76	CPNP CATAHUASI	AV. GONZALES PRADA N. 165	CATAHUASI	YAUYES	LIMA	12.799892 9	-75.89156165	100M			0	1	1	0	1	URBANO	TIPO 1
52	CPNP CERRO AZUL	JIRÓN ALFONSO UGARTE # SN	CERRO AZUL	CAÑETE	LIMA	13.024893 33	-76.47857333	100M			0	1	1	0	1	URBANO B	TIPO 1
69	CPNP CHACARILLA DEL ESTANQUE	JIRÓN ALFREDO GALEON MAYORAZGO # SN	SAN BORJA	LIMA	LIMA	12.108558 33	-76.98350667	100M			0	1	1	0	2	URBANO B	TIPO 1
43	CP ALCIDES VIGO HURTADO (DEPINCRI SEG. ESTADO, DIVICOTE, DIVANDRO, OFICRI) - LA LIBERTAD	CALLE SANTO TORIBIO DE MOGROVEJO 387 URB. SAN ANDRES	TRUJILLO	TRUJILLO	LA LIBERTAD	8.1178512	-79.0351151	200M	1		2	0	1	0	5	URBANO COMPLEJO 1	TIPO 2
60	CPNP CHACACAYO/POLICLINICO	AV. EL ROSARIO # 591	CHACACAYO	LIMA	LIMA	11.977128 33	-76.76541667	100M			0	1	1	0	2	URBANO B	TIPO 1
57	CPNP CHACRA COLORADA	JIRÓN CARHUAZ # 479	BREÑA	LIMA	LIMA	-12.05412	-77.05092833	100M			0	1	1	0	4	URBANO B	TIPO 1
50	AEROPUERTO JORGE CHAVEZ	AV. ELMER FAUCETT S/N - SALIDA INTERNACIONAL	CALLAO	CALLAO	LIMA	-12.02405	-77.1122	200M			0	1	1	0	1	URBANO RQ	TIPO 1
54	CPNP CHANCAY	AV. BOLIVAR # 150	CHANCAY	HUARAL	LIMA	11.562593 01	-77.26937167	100M			0	1	1	0	2	URBANO B	TIPO 1
52	CPNP CHILCA	AV. SAN MARCELO # 412	CHILCA	CAÑETE	LIMA	12.517925	-76.73706833	100M			0	1	1	0	1	URBANO B	TIPO 1
44	CP 7 DE AGOSTO (DIVOPUS/DIVISION POLICIA COMUNITARIA, SEGURIDAD ESTADO, UNITIC)	AV. JOSE BALTA 80	CHICLAYO	CHICLAYO	LAMBAYEQUE	-6.777582	-79.838858	200M	1		2	0	1	0	5	URBANO COMPLEJO 1	TIPO 2
60	CPNP CHORRILLOS	AV. DEFENSORES DEL MORRO # 656	CHORRILLOS	LIMA	LIMA	12.170308 33	-77.02331333	100M			0	1	1	0	3	URBANO A	TIPO 1
66	CPNP CHOSICA	AV. 28 DE JULIO # 576	LURIGANCHO	LIMA	LIMA	11.938795	-76.696531	100M			0	1	1	0	2	URBANO A	TIPO 1

76	5	CPNP CHURIN	AV. LARCO HERRERA N° 280	PACHANGARA	OYON	LIMA	10.811057	-76.874955	100M			0	1	1	0	1	URBANO	COMISARIA	TIPO 1
51	3	CPNP LA PUNTA/ CPNP ESPECIAL DE TURISMO	AV. MIGUEL GRAU # 1002	LA PUNTA	CALLAO	LIMA	12.068276 67	-77.15785	150M			1	1	1	0	3	URBANO	B	TIPO 1
61	5	CPNP CIENEGUILLA/DESPICAR CIENEGUILLA	AV. NUEVA TOLEDO # 104	CIENEGUILLA	LIMA	LIMA	12.115665	-76.81292833	100M			1	1	1	0	2	URBANO	B	TIPO 1
48	7	CPNP CIUDAD DEL PESCADOR	AV. JUAN VELASCO ALVARADO # 1299	BELAVISTA	CALLAO	LIMA	-12.05897	-77.104905	100M			0	1	1	0	4	URBANO	B	TIPO 1
68	7	CPNP CIUDAD Y CAMPO	CALLE JACINTO BENAVENTE # 258	RIMAC	LIMA	LIMA	12.024368	-77.02795	100M			0	1	1	0	2	URBANO	B	TIPO 1
49	3	CPNP CIUDADELA CHALACA	CLL. 12 DE MAYO MZ. J LT 13	CALLAO	CALLAO	LIMA	12.050253 89	-77.131598	100M			0	1	1	0	3	URBANO	B	TIPO 1
61	6	CPNP COLLIQUE	AV. REVOLUCION # SN	COMAS	LIMA	LIMA	11.913295	-77.01616	100M			0	1	1	0	3	URBANO	B	TIPO 1
58	7	CPNP CONDE DE LA VEGA	JIRÓN CONDESUYOS # 659	CERCADO	LIMA	LIMA	12.038528 33	-77.05324667	100M			0	1	1	0	2	URBANO	A	TIPO 1
72	9	CPNP CONDEVILLA	JIRÓN PABLO BERMUDEZ Y BILLINGHURST # SN	SAN MARTIN DE PORRES	LIMA	LIMA	12.020489 16	-77.08542109	100M			0	1	1	0	3	URBANO	B	TIPO 1
58	8	CPNP COTABAMBAS	JIRÓN BUENAVENTURA # SN	CERCADO	LIMA	LIMA	12.058045 05	-77.03417413	100M			0	1	1	0	2	URBANO	A	TIPO 1
56	1	CPNP CRUZ BLANCA	CARRETERA ANTIGUA PANAMERICANA NORTE # SN	HUALMAY	HUALMAY	LIMA	-11.09729	-77.59568333	100M			0	1	1	0	1	URBANO	B	TIPO 1
75	3	CPNP DE LA FAMILIA - VILLA EL SALVADOR	OTRO SECTOR 2 GRUPO 15 # SN	VILLA EL SALVADOR	LIMA	LIMA	12.212518 33	-76.938495	100M			0	1	1	0	1	URBANO	FAMILIA	TIPO 1
58	9	CPNP DE LA FAMILIA BERTHA GONZALES POSADA ETZAGUIRE	PASAJE BUENAVENTURA # SN	CERCADO	LIMA	LIMA	12.057931 67	-77.034525	100M			0	1	1	0	1	URBANO	FAMILIA	TIPO 1
71	1	CPNP DE LA FAMILIA CANTO REY	CLL. RIO CHIRA SN	SAN JUAN DE LURIGANCHO	LIMA	LIMA	11.975901 67	-76.95548167	100M			0	1	1	0	1	URBANO	FAMILIA	TIPO 1
61	7	CPNP DE LA FAMILIA COMAS COLLIQUE	CALLE LOS OLIVOS # SN	COMAS	LIMA	LIMA	11.912983 33	-77.01021	100M			0	1	1	0	1	URBANO	FAMILIA	TIPO 1
63	1	CPNP DE LA FAMILIA INDEPENDENCIA	JIRÓN 1 DE MAYO # 337	INDEPENDENCIA	LIMA	LIMA	-11.99228	-77.05040833	100M			0	1	1	0	1	URBANO	FAMILIA	TIPO 1
72	0	CPNP DE LA FAMILIA SAN JUAN MIRAFLORES	AV. TOMAS GUZMAN # 320	SAN JUAN DE MIRAFLORES	LIMA	LIMA	12.166498 33	-76.96638833	100M			0	1	1	0	1	URBANO	FAMILIA	TIPO 1
67	5	CPNP DISTRITO PACHACAMAC	JIRÓN CASTILLA # 521	PACHACAMAC	LIMA	LIMA	12.227761 67	-76.85851333	100M			0	1	1	0	2	URBANO	B	TIPO 1
49	4	CPNP DULANTO	JIRÓN HUANCAYO # SN	CALLAO	CALLAO	LIMA	12.044185	-77.10468167	100M			0	1	1	0	2	URBANO	B	TIPO 1
62	4	CPNP EL AGUSTINO	JIRÓN JUAN HOYLE PALACIOS # 440	EL AGUSTINO	LIMA	LIMA	-12.04936	-76.997755	100M			0	1	1	0	2	URBANO	A	TIPO 1
68	8	CPNP EL MANZANO	PASAJE CASSINELLI # 140	RIMAC	LIMA	LIMA	-12.0283	-77.03003333	100M			0	1	1	0	2	URBANO	B	TIPO 1
57	9	CPNP EL PROGRESO	AV. TUPAC AMARU # 3300	CARABAYLLO	LIMA	LIMA	11.874608 61	-77.01572992	100M			0	1	1	0	3	URBANO	B	TIPO 1
65	2	CPNP ESPECIAL DE TURISMO LIMA NORTE	JR. ALMIRANTE MARTIN GUISE Nº 1715	LINCE	LIMA	LIMA	12.082069 79	-77.03919278	100M			0	0	1	0	1	URBANO	TURISMO	TIPO 1

Handwritten signature and initials at the top left of the page.



Handwritten signature and initials in the middle left of the page.

62	CPNP FAMILIA EL AGUSTINO	JR ALFREDO TEADA DIAZ 237 EL AGUSTINO	LIMA	LIMA	-12.05041	-76.99804	100M				0	1	1	0	1	0	1	URBANO	COMISARIA	TIPO 1
68	CPNP FLOR DE AMANCAES	COMITÉ 13 AAHH FLOR DE AMANCAES	LIMA	LIMA	-12.01004	-77.03348	100M				0	1	1	0	1	0	2	URBANO	C	TIPO 1
48	CPNP GORGOR	PLAZA DE PRINCIPAL S/N	BARRANCA	LIMA	-10.46589	-70.46698	100M				0	1	1	0	1	0	1	URBANO	COMISARIA	TIPO 1
66	CPNP HUACHIPA	AV. LAS GARZAS # SN	LIMA	LIMA	12.014598 33	-76.937425	100M				0	1	1	0	1	0	2	URBANO	B	TIPO 1
55	CPNP HUACHO	JIRÓN SALAVERRY # 279	HUACHO	LIMA	11.09733 33	-77.60778833	100M				0	1	1	0	1	0	3	URBANO	A	TIPO 1
76	SECPV PNP	AV. 13 DE JULIO N° 205	CAJAMARCA	CAJAMARCA	-7.452401	-78.523000	100M				0	1	1	0	1	0	1	URBANO	COMISARIA	TIPO 1
54	CPNP HUARAL	AV. EL SOLAR # 454	HUARAL	LIMA	11.494393 33	-77.20673657	100M				0	1	1	0	1	0	1	URBANO	A	TIPO 1
54	CPNP HUARACHIRI	PROLONG. GRAU S/N MAZ. 76 LT. 36 KM. 150	HUARACHIRI	LIMA	12.135137	-76.234567	100M				0	1	1	0	1	0	1	URBANO	COMISARIA	TIPO 1
56	CPNP HUAURA	OTRO PLAZUELA SAN FRANCISCO # SN	HUAURA	LIMA	11.068058 33	-77.59945167	100M				0	1	1	0	1	0	2	URBANO	A	TIPO 1
56	CPNP HUAYCAN	AV. JOSE CARLOS MARIATEGUI # SN	LIMA	LIMA	12.012383 33	-76.827405	100M				0	1	1	0	1	0	2	URBANO	B	TIPO 1
52	CPNP IMPERIAL	JIRÓN DOS DE MAYO # 350	CAÑETE	LIMA	13.061371 67	-76.35300333	100M				0	1	1	0	1	0	2	URBANO	A	TIPO 1
63	CPNP JESUS MARIA	AV. ARNALDO MARQUEZ N° 1044	LIMA	LIMA	12.071032 46	-77.04754344	100M				0	1	1	0	1	0	3	URBANO	A	TIPO 1
66	CPNP JICAMARCA	OVALO CENTRAL S/N JICAMARCA ANEXO-08	LIMA	LIMA	11.980922 43	-76.94387302	100M				0	1	1	0	1	0	1	URBANO	COMISARIA	TIPO 1
75	CPNP JOSE CARLOS MARIATEGUI	JIRÓN JORGE CHAVEZ # 181	LIMA	LIMA	12.149666	-76.950367	100M				0	1	1	0	1	0	2	URBANO	B	TIPO 1
75	CPNP JOSE GALVEZ	AV. LIMA # 500	LIMA	LIMA	12.207816 67	-76.90640167	100M				0	1	1	0	1	0	2	URBANO	B	TIPO 1
49	CPNP JUAN INGUNZA VALDIVIA	AV. TOMAS VALLE # SN	CALLAO	LIMA	12.014306 67	-77.09654833	100M				0	1	1	0	1	0	3	URBANO	B	TIPO 1
68	CPNP LA ENSENADA	JIRÓN JACARANDA # SN	LIMA	LIMA	11.996258 33	-77.09414167	100M				0	1	1	0	1	0	3	URBANO	B	TIPO 1
71	CPNP LA HUAYRONA	JIRÓN LAS GENAS # SN	LIMA	LIMA	11.984241 67	-77.00683167	100M				0	1	1	0	1	0	3	URBANO	B	TIPO 1
50	CPNP LA LEGUA	CALLE MANUEL VIDAURRE # 100	CALLAO	LIMA	12.052855	-77.09692	100M				0	1	1	0	1	0	2	URBANO	B	TIPO 1
64	CPNP LA MOLINA	AV. ELIAS APARICIO # SN	LIMA	LIMA	12.077321 67	-76.916685	100M				0	1	1	0	1	0	2	URBANO	A	TIPO 1
61	CPNP LA PASCANA	JIRÓN JOSE CARLOS MARIATEGUI # SN	LIMA	LIMA	11.935536 76	-77.04673827	100M				0	1	1	0	1	0	3	URBANO	B	TIPO 1
51	CPNP LA PERLA	JIRÓN BRASIL # 664	CALLAO	LIMA	12.070133 33	-77.12629	100M				0	1	1	0	1	0	3	URBANO	A	TIPO 1

63	CPNP LA UNIFICADA	AV. 2 DE MARZO N° 229 (AA.HH EL VOLANTE)	LIMA	LIMA	12.005906	-77.047787	100M		0	1	1	0	2	URBANO	C	TIPO 1
64	CPNP LA VICTORIA	AV. 28 DE JULIO # 1600	LIMA	LIMA	12.063096	-77.0261	100M	1	3	0	1	0	3	URBANO	A	TIPO 2
65	DIVICAJ / OFICINA HUACHO	AV. PANAMERICA NORTE URB. SANTA MARIA 1360	HUALAURA	LIMA	11.105669	-77.595426	150M		0	1	1	0	1	URBANO	DIVINCRI	TIPO 1
75	CPNP LADERAS DE VILLA	CALLE SIN NOMBRE # SN	LIMA	LIMA	12.190716	-76.95762333	100M		0	1	1	0	2	URBANO	B	TIPO 1
64	CPNP LAS PRADERAS	AV. ALAMEDA DEL CORREGIDOR # SN	LIMA	LIMA	12.114718	-76.93712	100M		0	1	1	0	2	URBANO	B	TIPO 1
65	CPNP LAURA CALLER IBERICO	AV. RIO MARAÑON # SN	LIMA	LIMA	11.970631	-77.07812833	100M		0	1	1	0	3	URBANO	B	TIPO 1
65	CPNP LINCE	JIRÓN JOSE BERNANDO ALCEDO # 865	LIMA	LIMA	12.083368	-77.02702167	100M		0	1	1	0	3	URBANO	A	TIPO 1
52	CPNP LUNAHUANA	JIRÓN SIMON BOLIVAR # SN	CAÑETE	LIMA	12.963563	-76.14018833	100M		0	1	1	0	2	URBANO	B	TIPO 1
66	CPNP LURIN	JIRÓN UNION # 160	LIMA	LIMA	12.273685	-76.869174	100M		0	1	1	0	3	URBANO	B	TIPO 1
66	CPNP LURIN VILLA ALEJANDRO	MZ. O LT. 1 AA. HH VILLA ALEJANDRO	LIMA	LIMA	12.294075	-76.90772	100M		0	1	1	0	1	URBANO	B	TIPO 1
67	CPNP MAGDALENA DEL MAR	JIRÓN CUZCO # 756	LIMA	LIMA	12.088168	-77.0737167	100M		0	1	1	0	3	URBANO	A	TIPO 1
53	CPNP MALA	CALLE CORONEL CASTILLA MZ B LT 5-6 URB CASUARINAS	CAÑETE	LIMA	12.660.823	-76.632.053	100M		0	1	1	0	3	URBANO	A	TIPO 1
67	CPNP MANCHAY	AV. MANCHAY # SN	LIMA	LIMA	12.116138	-76.87007167	100M		0	1	1	0	1	URBANO	B	TIPO 1
73	CPNP MARANGA	AV. LOS PRECURSORES # SN	LIMA	LIMA	-12.06987	-77.093015	100M		0	1	1	0	3	URBANO	B	TIPO 1
71	CPNP MARISCAL CACERES	CALLE MZ. R8 LT. 1. CNEL. ALTHAUS	LIMA	LIMA	11.949195	-76.98109833	100M		0	1	1	0	3	URBANO	B	TIPO 1
49	CPNP MARQUEZ	AV. VENCEDOR # SN	CALLAO	LIMA	11.944738	-77.13421333	100M		0	1	1	0	2	URBANO	B	TIPO 1
60	CPNP MATEO PUMACAHUA	AV. SANTA ROSA DE LIMA # SN	LIMA	LIMA	12.192046	-76.98017667	100M		0	1	1	0	2	URBANO	B	TIPO 1
57	CPNP BARRANCO/CPNP TURISMO LIMA SUR	PROLONGACIÓN SAN MARTIN # 250	LIMA	LIMA	12.170258	-77.0232515	150M		0	1	1	0	3	URBANO	A	TIPO 1
57	CPNP BREÑA/DIVINCRI	JIRÓN GENERAL FELIPE VARELA # 1978	BREÑA	LIMA	12.067196	-77.05289833	150M	1	3	0	1	0	3	URBANO	A	TIPO 2
54	CPNP MATUCANA	AV. FERROCARRIL # SN	HUARACHIRI	LIMA	11.843716	-76.38565	100M		0	1	1	0	2	URBANO	A	TIPO 1
51	CPNP MI PERU	CALLE MI PERU S/N MZ G LOTE 1	CALLAO	LIMA	11.854455	-77.12346667	100M		0	1	1	0	2	URBANO	B	TIPO 1
59	CPNP MIRONES ALTO	AV. LUIS BRAYLE # SN	LIMA	LIMA	12.051335	-77.06745	100M		0	1	1	0	3	URBANO	B	TIPO 1
59	CPNP MIRONES BAJO	JIRÓN MANUEL PEREZ DE TUDELA # 3344	LIMA	LIMA	-12038004	-77082207	100M		0	1	1	0	2	URBANO	B	TIPO 1

Handwritten signatures and marks at the top left of the page.



59	CPNP MONSERRATE	JIRÓN CALLAO # 891	LIMA	LIMA	12.041238 12	-77.09937694	100M			0	1	1	0	3	URBANO	A	TIPO 1
74	CPNP MONTERICO	AV. MANUEL OLGUIN CUADRA 6	LIMA	LIMA	12.094702	-76.973602	100M			0	1	1	0	3	URBANO	B	TIPO 1
75	CPNP NUEVA ESPERANZA	AV. 26 DE NOVIEMBRE 1391	LIMA	LIMA	12.169484 54	-76.92875322	100M			0	1	1	0	3	URBANO	B	TIPO 1
53	CPNP NUEVO IMPERIAL	AV. AUGUSTO B. LEGUIA # 501	CAÑETE	LIMA	13.075973 33	-76.31964167	100M			0	1	1	0	2	URBANO	B	TIPO 1
58	CENTRAL EMERGENCIA 105	AV. ESPAÑA 400-3ER. PISO (COSTADO PREFECTURA LIMA)	Lima	Lima	-12.05773	-77.0412	400M			0	0	1	0	0	URBANO	105	TIPO 1
44	CP MV. PNP FELIX TELLO ROJAS (DIVINCRI. DEPROVE. OFICRI CHICLAYO)	AV. SALAVERRY CON P.I. JOSE OLAYA 929	CHICLAYO	LAMBAYEQUE	-6.770414	-79.85462	200M		1	2	0	1	0	5	URBANO	COMPLEJO 1	TIPO 2
13	CPNP NUEVO PROGRESO	Av. 2 Mz C-1 AAHH NUEVO PROGRESO/ 7MA ZONA NUEVO MILENIO	LIMA	LIMA	12.219249	-76.917878	100M			0	1	1	0	2	URBANO	D	TIPO 1
49	CPNP OQUEENDO	CALLE BUENOS AIRES Y BOLIVIA Y PARQUE N° 02 - EX FUNDO OQUEENDO CALLAO	CALLAO	LIMA	11.978481 43	-77.12322381	100M			0	1	1	0	1	URBANO	COMISARIA	TIPO 1
70	CPNP ORRANTIA DEL MAR	AV. AUGUSTO PEREZ ARANIBAR # 2075	LIMÁ	LIMA	12.104488 33	-77.05753	100M			0	1	1	0	3	URBANO	B	TIPO 1
53	CPNP PACARAN	IR. MIRAFLORES 155	cañete	Lima	12.865846	-76.054236	100M			0	1	1	0	1	URBANO	COMISARIA	TIPO 1
51	CPNP PACHACUTEC	AV. DOSCIENTOS VEINTICINCO SN MZ.W LT.13	CALLAO	LIMA	11.833791 67	-77.142075	100M			0	1	1	0	2	URBANO	C	TIPO 1
59	CPNP PALOMINO	CALLE SANTA JUSTINA # SN	LIMA	LIMA	12.060253 33	-77.07249833	100M			0	1	1	0	2	URBANO	B	TIPO 1
72	CPNP PAMPLONA 1	CALLE SECTOR NUEVO HORIZONTE # SN	LIMA	LIMA	12.148005	-76.96603	100M			0	1	1	0	2	URBANO	B	TIPO 1
72	CPNP PAMPLONA II	AV. EDILBERTO RAMOS # SN	LIMA	LIMA	12.131136 67	-76.95800333	100M			0	1	1	0	2	URBANO	B	TIPO 1
48	CPNP PARAMONGA	AV. CENTRAL # 275	BARRANCA	LIMA	-10.67324	-77.81323157	100M			fx	1	1	0	2	URBANO	B	TIPO 1
48	CPNP PATIVILCA	AV. SIMON BOLIVAR # 117	BARRANCA	LIMA	-10.69596	-77.778336	100M			0	1	1	0	1	URBANO	B	TIPO 1
63	CPNP PAYET	JIRÓN PALLCAMARCA # SN	LIMA	LIMA	11.971951 67	-77.04370657	100M			0	1	1	0	3	URBANO	B	TIPO 1
48	CP SANTA MARINA OFICRI	JR. SUPE 3 AV. FERNANDINI	CALLAO	LIMA	12.054672	-77.129257	200M		1	2	0	1	0	5	URBANO	COMPLEJO 1	TIPO 2
59	CP PETIT THOUARS	AV. PETIT THOUARS # 455	LIMA	LIMA	12.068863 33	-77.03521167	100M			0	1	1	0	3	URBANO	A	TIPO 1
69	CPNP PIEDRA LIZA	PASAJE NUMERO UNO # SN	LIMA	LIMA	12.039746 83	-77.01772481	100M			0	1	1	0	2	URBANO	B	TIPO 1
49	CPNP PLAYA RIMAC	JIRÓN MIGUEL GRAU # 200	CALLAO	LIMA	-12.03751	-77.09698833	100M			0	1	1	0	2	URBANO	B	TIPO 1
65	CPNP PRO	CALLE CONFRATERNIDAD # SN	LIMA	LIMA	-11.99454	-77.07575333	100M			0	1	1	0	3	URBANO	A	TIPO 1
50	DIRECCION DE AVIACION POLICIAL - DIRAVPOL	AV. ELMER FAUCCETT S/N. AL COSTADO DEL AUCH	CALLAO	LIMA	12.027179	-77.103601	200M		1	3	0	0	2	3	URBANO	COMPLEJO 1	TIPO 2
67	CPNP PUCUSANA	JIRÓN UNION # SN	LIMA	LIMA	-12.48267	-76.796365	100M			0	1	1	0	1	URBANO	B	TIPO 1

Handwritten signatures and marks on the left side of the page.

Handwritten signatures and marks at the top left of the page.



67	1	CNP PUEBLO LIBRE	PASAJE VIVANCO # 101	LIMA	LIMA	12.077046 67	-77.06560833	100M		0	1	1	0	3	URBANO	A	TIPO 1
53	3	CNP PUEBLO NUEVO DE CONTA	AV. LOSTAJUNAU SN MZ L IT. 2	CAÑETE	CAÑETE	13.038175	-76.339938	100M		0	1	1	0	1	URBANO	C	TIPO 1
58	1	CNP PUENTE PIEDRA	AV. REP. DE VENEZUELA CON AV. BUENOS AIRES (REF. PLAZA DE ARMAS)	LIMA	LIMA	11.866.288	-77.077.672	100M		0	1	1	0	3	URBANO	A	TIPO 1
58	4	CNP PUNTA HERMOSA	URB. EL CARMEN MZ "A-1" IT. "12-13"	LIMA	LIMA	12.312523 33	-76.83720833	100M		0	1	1	0	1	URBANO	B	TIPO 1
68	5	CNP PUNTA NEGRA	AV. GUANAY NORTE # SN	LIMA	LIMA	12.364161 67	-76.79570167	100M		0	1	1	0	1	URBANO	B	TIPO 1
53	5	CNP QUILMANA	AV. LIMA # SN	CAÑETE	CAÑETE	12.949713 33	-76.38269333	100M		0	1	1	0	1	URBANO	C	TIPO 1
61	0	DEPINCRI CHORRILLOS- BARBANCO/TRANQUITO/HALCONES	AV. SOL S/N CUADRA 16	LIMA	LIMA	12.181129	-76.992562	300M		0	1	1	0	3	URBANO	DIVINCI	TIPO 1
49	9	CNP RAMON CASTILLA	JIRÓN TALARA # 200	CALLAO	CALLAO	12.044078 33	-77.12400867	100M		0	1	1	0	2	URBANO	B	TIPO 1
50	9	CP ALIPIO PONCE VASQUEZ	JR. APURIMAC 647	CALLAO	CALLAO	12.063313	-77.137148	400M	1	4	0	0	2	5	URBANO	COMPLEJO 1	TIPO 2
55	0	CNP RICARDO PALMA	CALLE ANGEL BARACCO # SN	HUAROCHIRI	HUAROCHIRI	11.923276 12	-76.66508138	100M		0	1	1	0	1	RURAL	B	TIPO 1
69	1	CNP RIMAC	JIRÓN CHICLAYO # 450	LIMA	LIMA	12.039483 33	-77.027905	100M		0	1	1	0	3	URBANO	A	TIPO 1
74	3	CNP SAGITARIO	AV. LAS GAVIOTA # SN	LIMA	LIMA	12.164779	-76.596769	100M		0	1	1	0	3	URBANO	B	TIPO 1
57	0	CNP SALAMANCA	PASAJE LOS AYMARAS # 264	LIMA	LIMA	-12.0757	-76.98863	100M		0	1	1	0	4	URBANO	B	TIPO 1
59	5	CNP SAN ANDRES	JIRÓN HUALLAGA # 862	LIMA	LIMA	12.051516 67	-77.02353333	100M		0	1	1	0	3	URBANO	A	TIPO 1
67	4	CNP SAN ANTONIO	AV. TOMAS MARZANO # 1180	LIMA	LIMA	-12.11489	-77.010743	100M		0	1	1	0	2	URBANO	B	TIPO 1
53	6	CNP SAN ANTONIO CAÑETE	AV. LIBERTAD # 433	CAÑETE	CAÑETE	12.642163 33	-76.650745	100M		0	1	1	0	1	URBANO	C	TIPO 1
55	1	CNP SAN ANTONIO DE JICAMARCA	AV. INCA YUPANQUI MZ AO / INTERSECCIÓN CON LA AV. LOS ANDES - ANEXO 22	HUAROCHIRI	HUAROCHIRI	11.925783	-76.966853	100M		0	1	1	0	1	URBANO	COMISARIA	TIPO 1
69	6	CNP SAN BARTOLO	AV. SAN BARTOLO # SN	LIMA	LIMA	12.387463 33	-76.77730667	100M		0	1	1	0	2	URBANO	B	TIPO 1
70	0	CNP SAN BORJA	JR. FEDOROVICH STRANVINSKY CD 2 SN	LIMA	LIMA	12.105668 33	-76.999985	100M		0	1	1	0	3	URBANO	A	TIPO 1
62	6	CNP SAN CAYETANO	JIRÓN SUCRE # 100	LIMA	LIMA	-12.05681	-77.00803833	100M		0	1	1	0	2	URBANO	B	TIPO 1
64	9	CNP SAN COSME	PASAJE ENRIQUE MEIGGS # 2125	LIMA	LIMA	12.064578 33	-77.00778	100M		0	1	1	0	2	URBANO	B	TIPO 1
55	2	CNP SAN DAMIAN	JR. MANCO CAPAC # 199	HUAROCHIRI	HUAROCHIRI	12.017116 2	-76.39168042	100M		0	1	1	0	1	URBANO	COMISARIA	TIPO 1

Handwritten signatures and initials at the top left of the page.



Handwritten signatures and initials in the middle left of the page.

76	0	CPNP SAN FRANCISCO TABLADA LURIN	AV. SAN MARTIN # 170	LIMA	LIMA	12.200036 67	-76.52815833	100M			0	1	1	0	2	URBANO	B	TIPO 1
60	8	CPNP SAN GENARO	AV. PRINCIPAL # SN	LIMA	CHORRILLOS	12.195998	-77.020556	100M			0	1	1	0	2	URBANO	B	TIPO 1
70	4	CPNP SAN ISIDRO	CALLE ANTEQUERA # 116	LIMA	SAN ISIDRO	12.095094 76	-77.0323348	100M			0	1	1	0	3	URBANO	A	TIPO 1
72	6	CPNP SAN LUIS	JIRÓN JOSE ORENGO # 903	LIMA	SAN LUIS	12.075025	-76.599540667	100M			0	1	1	0	3	URBANO	A	TIPO 1
53	7	CPNP SAN LUIS CAÑETE	CALLE PLAZA DE ARMAS # 131	CAÑETE	SAN LUIS	13.050758 33	-76.430455	100M			0	1	1	0	1	URBANO	B	TIPO 1
55	4	CPNP SAN MATEO	JIRÓN LIMA # SN		SAN MATEO	11.759306 67	-76.39935667	100M			0	1	1	0	1	URBANO	B	TIPO 1
63	2	CPNP INDEPENDENCIA/DIVINCRI/DIVPOL	AV. TUPAC AMARU KM. 4.5	LIMA	INDEPENDENCIA	11.995285 93	-77.05482781	150M		1	3	0	1	0	3	URBANO	A	TIPO 2
73	4	CPNP SAN MIGUEL	CALLE UNO # SN	LIMA	SAN MIGUEL	12.089586 67	-77.087785	100M			0	1	1	0	3	URBANO	B	TIPO 1
62	7	CPNP SAN PEDRO	AV. 15 DE ABRIL CDR. 3	LIMA	EL AGUSTINO	12.059683 33	-77.00317167	100M			0	1	1	0	2	URBANO	B	TIPO 1
76	7	CPNP SAN PEDRO DE CAPILLUCAS	CARRETERA CAÑETE AYUYOS KM 109	YAUYES	ALLAUCA	12.707477	-75.969145	100M			0	1	1	0	1	URBANO	COMISARIA	TIPO 1
53	9	CPNP SAN VICENTE DE CAÑETE	JIRÓN SANTA RITA # SN	CAÑETE	SAN VICENTE DE CAÑETE	13.078295	-76.38896333	100M			0	1	1	0	2	URBANO	A	TIPO 1
73	6	CPNP SANTA ANITA	JIRÓN CIRO ALEGRIA # 555	LIMA	SANTA ANITA	12.044845	-76.97673833	100M			0	1	1	0	3	URBANO	A	TIPO 1
58	5	CP ALCIDES VIGO HURTADO DIRINCRI / OFICRI	AV. ESPAÑA CDR. 03 PISO 4		CERCADO	12.058296	-77.040046	400M		1	2	0	0	2	5	URBANO	COMPLEJO 1	TIPO 2
63	9	AREANDRO PNP MOQUEGUA	SECTOR MONTALVO CALALUNA WFLIB-B VALLE	MOQUEGUA	SAN ANTONIO	17.212073	-70.968232	100M			0	1	1	0	1		DIRANDRO	TIPO 1
59	7	DIPROVE / OFICRI	JR. CONCHUCOS 666 BARRIOS ALTOS PISO 2	LIMA	CERCADO	12.048661	-77.011628	400M		1	2	0	0	2	3	URBANO	COMPLEJO 1	TIPO 2
57	1	CPNP SANTA CLARA	CARRETERA CENTRAL # 1	LIMA	ATE	12.016836 06	-76.88417226	100M			0	1	1	0	2	URBANO	B	TIPO 1
71	4	CPNP SANTA ELIZABETH	JR. NEVADO HUANDROY SN MZ.F LT.18	LIMA	SAN JUAN DE LURIGANCHO	11.983885	-77.015015	100M			0	1	1	0	3	URBANO	B	TIPO 1
55	6	CPNP SANTA EULALIA	AV. JOSE BERNARDO ALCEDO # SN		SANTA EULALIA	11.900926 67	-76.66405167	100M			0	1	1	0	2	RURAL	B	TIPO 1
64	4	CPNP SANTA FELICIA	LOS CANARIOS. LA MOLINA 15024	LIMA	LA MOLINA	12.07221	-76.55523333	100M			0	1	1	0	2	URBANO	B	TIPO 1
58	0	CPNP SANTA ISABEL	AV. MARIA PARADO DE BELIDO # SN	LIMA	CARABAYLLO	11.968542 21	-77.05675364	100M			0	1	1	0	3	URBANO	B	TIPO 1
61	9	CPNP SANTA LUZMILA	AV. GERARDO UNGER # 6500	LIMA	COMAS	11.94467	-77.06635333	100M			0	1	1	0	3	URBANO	B	TIPO 1
64	7	CPNP APOLO/DIVINCRI	JIRÓN 3 DE FEBRERO # 1050	LIMA	LA VICTORIA	12.071352 01	-77.00980291	150M		1	3	0	1	0	3	URBANO	A	TIPO 2
73	9	CPNP SANTA MARIA DEL MAR	AV. TERRAMAR # SN	LIMA	SANTA MARIA DEL MAR	12.999675	-76.773	100M			0	1	1	0	1	URBANO	B	TIPO 1
74	0	CPNP SANTA ROSA	AV. ALEJANDRO BERTELLO # SN	LIMA	SANTA ROSA	11.79655	-77.17104833	100M			0	1	1	0	2	URBANO	C	TIPO 1

[Handwritten signature]



[Handwritten signature]

60	REGPOL LIMA - (105)/DIRCOTE	AV. ESPAÑA CDRA 45/N	CERCADO	LIMA	LIMA	12.057998	-77.040982	400M	1	4	0	0	2	5	URBANO	COMPLEJO 1	TIPO 2
65	UNIDAD DE EMERGENCIA CENTRO	AV. 28 DE JULIO 1650 // BAUSATE Y MESA	LA VICTORIA	LIMA	LIMA	12.064016	-77.025725	150M		0	1	1	0	1	URBANO	EMERGENCIA	TIPO 1
66	CPNP SANTA ROSA IRRIGACION	AV. PRINCIPAL LA VILLA # SN - IRRIGACION SANTA ROSA	SAYAN	HUALURA	LIMA	11.235186	-77.381099	100M		0	1	1	0	1	URBANO	COMISARIA	TIPO 1
74	CPNP SANTIAGO DE SURCO	JIRON ARICA # 388	SURCO	LIMA	LIMA	-12.14538	-77.00303	100M		0	1	1	0	3	URBANO	A	TIPO 1
62	CPNP SANTOYO	JIRON CHIMBOTE # 2110	EL AGUSTINO	LIMA	LIMA	12.051353 33	-77.0085333	100M		0	1	1	0	2	URBANO	B	TIPO 1
50	CPNP SARITA COLONIA	AV. VICTOR A. BELAUDE # SN	CALLAO	CALLAO	LIMA	12.023691 67	-77.13439	100M		0	1	1	0	2	URBANO	B	TIPO 1
61	ESCUELA DE OFICIALES	AV. GUARDIA CIVIL S/N	CHORRILLOS	LIMA	LIMA	12.175243	-76.993587	200M	1	4	0	0	2	2	URBANO	COMPLEJO 1	TIPO 2
56	CPNP SAYAN	OTRO PLAZA DE ARMAS # SN	SAYAN	HUALURA	LIMA	11.134968 33	-77.19262	100M		0	1	1	0	1	URBANO	B	TIPO 1
76	CPNP SECTORIAL OYON	CALLE COMERCIO # 481	OYON	OYON	LIMA	10.669535	-76.76970833	100M		0	1	1	0	1	RURAL	A	TIPO 1
65	CPNP SOL DE ORO	AV. BUEN PASTOR # SN	LOS OLIVOS	LIMA	LIMA	11.997563 33	-77.063925	100M		0	1	1	0	3	URBANO	A	TIPO 1
48	CPNP SUPE PUEBLO	JIRON SUCRE # 350	SUPE	BARRANCA	LIMA	10.795248 33	-77.71631333	100M		0	1	1	0	1	URBANO	B	TIPO 1
48	CPNP SUPE PUERTO	CALLE CALLAO # 501	SUPE PUERTO	BARRANCA	LIMA	10.796988 33	-77.7417	100M		0	1	1	0	1	URBANO	B	TIPO 1
74	CPNP SURQUILLO	JIRON SAN DIEGO # 401	SURQUILLO	LIMA	LIMA	12.118732	-77.022453	100M		0	1	1	0	3	URBANO	A	TIPO 1
63	CPNP TAHUANTINSUYO	JIRON OLLANTAYTAMBO # SN	INDEPENDENCIA	LIMA	LIMA	11.960585	-77.04887	100M		0	1	1	0	2	URBANO	B	TIPO 1
62	CPNP TUPAC AMARU	AV. TUPAC AMARU # 1121	COMAS	LIMA	LIMA	11.955216 67	-77.05255167	100M		0	1	1	0	3	URBANO	A	TIPO 1
59	CPNP UNIDAD VECINAL NIRO 3	AV. OSCAR BENAVIDES # SN	CERCADO	LIMA	LIMA	12.051371 67	-77.08204333	100M		0	1	1	0	3	URBANO	B	TIPO 1
62	CPNP UNIVERSITARIA	AV. UNIVERSITARIA # SN	COMAS	LIMA	LIMA	11.947443 33	-77.06020657	100M		0	1	1	0	2	URBANO	B	TIPO 1
75	CPNP URB. PACHACAMAC	JR. JORGE CHAVEZ 181	VILLA EL SALVADOR	LIMA	LIMA	12.230055	-76.92325333	100M		0	1	1	0	2	URBANO	B	TIPO 1
56	CPNP VEGUETA	AV. GRAU # 133	VEGUETA	HUALURA	LIMA	11.023390 19	-77.64370143	100M		0	1	1	0	1	URBANO	B	TIPO 1
51	CPNP VENTANILLA	AV. PEDRO BELTRAN # 138	VENTANILLA	CALLAO	LIMA	11.872876 67	-77.126185	100M		0	1	1	0	4	URBANO	A	TIPO 1
62	CPNP VILLA HERMOSA	JIRON RIO NANAY # SN	EL AGUSTINO	LIMA	LIMA	12.041471 67	-76.98885657	100M		0	1	1	0	2	URBANO	B	TIPO 1
51	CPNP VILLA LOS REYES	MZ. C.L.T. 3 AA. HH. VILLA LOS REYES	VENTANILLA	CALLAO	LIMA	-11.83087	-77.121875	100M		0	1	1	0	3	URBANO	B	TIPO 1
76	CPNP VILLA MARIA DEL TRIUNFO	AV. EL TRIUNFO # 374	VILLA MARIA DEL TRIUNFO	LIMA	LIMA	12.165745	-76.94780833	100M		0	1	1	0	3	URBANO	A	TIPO 1

Handwritten signatures and marks at the top left of the page.



Handwritten signatures and initials on the left side of the page.

67	3	CPNP MIRAFLORES/DIVINCRI	CALLE GENERAL VIDAL # 230	MIRAFLORES	LIMA	LIMA	12.114423 33	-77.02813	150M		0	1	1	0	1	0	4	URBANO	A	TIPO 1
60	9	CPNP VILLA-CHORRILLOS	PROLONGACIÓN HUAYLAS CDR. 1. DISTRITO DE CHORRILLOS	CHORRILLOS	LIMA	LIMA	12.185788 33	-77.00787833	100M		0	1	1	0	1	0	3	URBANO	B	TIPO 1
57	2	CPNP VITARTE	CARRETERA CENTRAL # SN	ATE	LIMA	LIMA	-12.02611	-76.91959	100M		0	1	1	0	1	0	2	URBANO	A	TIPO 1
52	2	CPNP YANGAS	KM 56 CARRETERA LIMA A CANTA	SANTA ROSA DE QUIVES	CANTA	LIMA	11.694886 59	-76.84566417	100M		0	1	1	0	1	0	1	URBANO	COMISARIA	TIPO 1
77	0	CPNP YAUJOS	JR. TRUJILLO S/N	YAUJOS	YAUJOS	LIMA	12.460053 8	-75.9167047	100M		0	1	1	0	1	0	1	URBANO	COMISARIA	TIPO 1
72	7	CPNP YERBATEROS	JIRÓN PABLO RISSO # 190	SAN LUIS	LIMA	LIMA	12.064718 33	-76.99734	100M		0	1	1	0	1	0	2	URBANO	B	TIPO 1
68	2	CPNP ZAPALLAL	JIRÓN GALILEA # SN	PUENTE PIEDRA	LIMA	LIMA	11.828025	-77.11752833	100M		0	1	1	0	1	0	3	URBANO	B	TIPO 1
71	5	CPNP ZARATE	AV. PIRAMIDE DEL SOL # 200	SAN JUAN DE LURIGANCHO	LIMA	LIMA	12.027083 33	-77.00126333	100M		0	1	1	0	1	0	3	URBANO	A	TIPO 1
54	0	CPNP ZUÑIGA	AV. BERNARDO ALCEDO # 214	ZUÑIGA	CAÑETE	LIMA	12.860295 54	-76.0224031	100M		0	1	1	0	1	0	1	URBANO	COMISARIA	TIPO 1
53	8	DEPICA/DIVPOL CAÑETE	PLAZA SAN MARTIN 236 CERCADO CAÑETE	SAN VICENTE	CAÑETE	LIMA	13.076558	-76.385877	100M		0	1	1	0	1	0	2	URBANO	DIVINCRI	TIPO 1
64	0	HOSPITAL NACIONAL PNP "LUIS N. SAENZ"	AV. DE LA POLICIA N° 335	JESUS MARIA	LIMA	LIMA	12.085627 85	-77.05989198	400M	1	4	0	0	2	0	2	0	URBANO	COMPLEJO 1	TIPO 2
47	8	DEPINCRI BARRANCA	URB LAS PALMERAS MZ. M.I.T.1	BARRANCA	BARRANCA	LIMA	10.741327	-77.765152	100M		0	1	1	0	1	0	1	URBANO	DEPINCRI	TIPO 1
50	1	DEPINCRI CALLAO	JR. CONSTITUCIÓN CDA 2 S/N	CALLAO	CALLAO	LIMA	12.059776	-77.147082	100M		0	1	1	0	1	0	3	URBANO	DIVINCRI	TIPO 1
65	0	DIRSEVI - DIVPOLTRAN	AV. 28 DE JULIO Y LA MAR 2090	LA VICTORIA	LIMA	LIMA	12.061949	-77.019961	400M	1	4	0	0	2	3	3	0	URBANO	COMPLEJO 1	TIPO 2
58	1	DEPINCRI CARABAYLLO	AV. COLECTORA MZ H8 LOT 1.2.3.4 / URB SANTA MARIA. 1 ETAPA / CARABAYLLO	CARABAYLLO	LIMA	LIMA	11.841079	-77.045862	100M		0	1	1	0	1	0	2	URBANO	DIVINCRI	TIPO 1
59	9	DEPINCRI CERCADO	JR. HUALLAGA N° 876(310)	CERCADO	LIMA	LIMA	12.051235	-77.023317	100M		0	1	1	0	1	0	3	URBANO	DIVINCRI	TIPO 1
66	4	DEPINCRI CHOSICA	AV. SANTA INÉS 316	LURIGANCHO	LIMA	LIMA	11.972389	-76.755672	100M		0	1	1	0	1	0	2	URBANO	DIVINCRI	TIPO 1
62	2	DEPINCRI COMAS	AV. GUILLERMO DE LA FUENTE N°1058	COMAS	LIMA	LIMA	-11.94755	-77.0518	100M		0	1	1	0	1	0	2	URBANO	DIVINCRI	TIPO 1
63	0	DEPINCRI EL AGUSTINO	BOULEVARD REPUBLICA 661 - EL AGUSTINO	EL AGUSTINO	LIMA	LIMA	-12.04979	-77.01014	100M		0	1	1	0	1	0	2	URBANO	DEPINCRI	TIPO 1
64	5	DEPINCRI LA MOLINA - CIENEGUILLA	AV. MOLINA ESTE 2350 URB. MUSA	LA MOLINA	LIMA	LIMA	12.986544 3	-76.8938654	100M		0	1	1	0	1	0	2	URBANO	DEPINCRI	TIPO 1
66	0	DEPINCRI LOS OLIVOS	JR. MARCARÁ CON CHASQUITAMBO URB. NARANJAL	LOS OLIVOS	LIMA	LIMA	11.976516 2	-77.0692785	100M		0	1	1	0	1	0	3	URBANO	DIVINCRI	TIPO 1
69	4	DIRLOG TELEMATICA	PSJE. SAN GERMAN CDA 2 COSTADO HOSPITAL BLEGUJA S/N	RIMAC	LIMA	LIMA	12.033437	-77.032566	200M		0	1	1	0	1	0	1	URBANO	DIVLOG	TIPO 1
69	5	HOSPITAL POLICIAL "AUGUSTO B. LEGUIA"	PSJE. SAN GERMAN CDA. 2	RIMAC	LIMA	LIMA	12.035265	-77.033962	200M		0	1	1	0	1	0	1	URBANO	HOSPITAL	TIPO 1
66	8	DEPINCRI LURIN-PACHACAMAC Y BALNERIOS	ASOC. LOS CLAVES MZA Ñ LOTE 15	LURIN	LIMA	LIMA	12.295489	-76.855269	100M		0	1	1	0	1	0	3	URBANO	DIVINCRI	TIPO 1



73	DEPINCRI NORTE SAN MARTIN DE PORRES	JR. JOAQUÍN CAPELLA 672 URB. INGENIERIA	SAN MARTIN DE PORRES	LIMA	LIMA	12.029508 4	-77.0567105	100M			0	1	1	0	2	URBANO	DIVINCRI	TIPO 1
69	DEPINCRI RIMAC	AV. EVITAMIENTO S/N. JR. GARCIA RIBEYRO S/N	RIMAC	LIMA	LIMA	12.036907	-77.041318	100M			0	1	1	0	1	URBANO	DIVINCRI	TIPO 1
70	DEPINCRI SAN BORJA/JEFATURA AREA INVESTIGACION CRIMINAL- SUR	CALLE 2 N° 568	SAN BORJA	LIMA	LIMA	12.089549	-76.984382	100M			0	1	1	0	2	URBANO	DIVINCRI	TIPO 1
72	DEPINCRI SAN JUAN DE MIRAFLORES	AV. JOSE R. ECHENIQUE 420-PAMPLONA MIRAFLORES	SAN JUAN DE MIRAFLORES	LIMA	LIMA	12.148437	-76.975692	100M			0	1	1	0	2	URBANO	DIVINCRI	TIPO 1
75	DEPINCRI SAN MIGUEL	CALLE MANUELA MARTICORENA N° 163	SAN MIGUEL	LIMA	LIMA	-12.08254	-77.079573	100M			0	1	1	0	2	URBANO	DIVINCRI	TIPO 1
71	DEPINCRI SIL 1	INTERSECCION DE LA CALLE RIO UCAVALI CON RIO APURIMAC MZ. O LITE 20	SAN JUAN DE LURIGANCHO	LIMA	LIMA	11.974718 74	-76.99548379	100M			0	1	1	0	0	URBANO	DIVINCRI	TIPO 1
71	DEPINCRI SIL 2	SAN HILARION ESTE, SAN JUAN DE LURIGANCHO 15434	SAN JUAN DE LURIGANCHO	LIMA	LIMA	11.992401	-77.00857	100M			0	1	1	0	2	URBANO	DIVINCRI	TIPO 1
51	DEPINCRI VENTANILLA	CALLE TROMPETEROS 136 (ESPALDA DE LA CPNP VENTANILLA)	VENTANILLA	CALLAO	LIMA	11.872098	-77.126318	100M			0	1	1	0	2	URBANO	DIVINCRI	TIPO 1
65	CP DIVPOL NORTE 1 / UNEME NORTE-SOES NORTE 1/ TRANSITO NORTE / DITROVENORTE)	JR. LOS SILICIOS 5534 PAN. NORTE PARADERO NISSAN PASANDO OVALO NARANJAL	LOS OLIVOS	LIMA	LIMA	11.967957	-77.063192	400M	1		3	0	1	0	1	URBANO	COMPLEJO 1	TIPO 2
68	ETS PNP PUENTE PIEDRA	AV. PANAMERICANA NORTE KM. 26.5	PUENTE PIEDRA	LIMA	LIMA	-11.89582	-77.06846	400M	1		5	0	0	2	8	URBANO	COMPLEJO 1	TIPO 2
76	DEPINCRI VILLA MARIA DEL TRIUNFO	AV. GENERAL VIDAL 300 MZ. 1-B, LOTE 17 PJ SAN FRANCISCO TABLADA DE LURIN	VILLA MARIA DEL TRIUNFO	LIMA	LIMA	12.201076	-76.928479	100M			0	1	1	0	2	URBANO	DEPINCRI	TIPO 1
50	DEPROVE CALLAO/ORIPACIU	OVALO CANADA S/N	CALLAO	CALLAO	LIMA	-12.06849	-77.133575	100M			0	1	1	0	1	URBANO	FAMILIA	TIPO 1
53	DESPRCAR BUJAMA	CLL. PROGRESO SN MZ.D LT.6	MAIA	CAÑETE	LIMA	12.719366 67	-76.62937	100M			0	0	1	0	0	URBANO	CARRETERAS	TIPO 1
54	DESPRCAR CHICLA	CARR. CENTRAL KM 106 S/N PLAZA DE ARMAS - CHICLA	CHICLA	HUAROCHIRI	LIMA	11.704883	-76.268785	100M			0	0	1	0	0	RURAL	CARRETERAS	TIPO 1
69	DESPRCAR SAN BARTOLO	AV. EL GOLF S/N	SAN BARTOLO	LIMA	LIMA	12.387248	-76.77745	100M			0	0	1	0	0	URBANO	CARRETERAS	TIPO 1
55	DESPRCAR SAN JERONIMO SURCO	JIRON BOLOGNESI S/N SAN JERONIMO DE SURCO	SAN JERONIMO DE SURCO	HUAROCHIRI	LIMA	11.884191 7	-76.4400617	100M			0	0	1	0	0	URBANO	CARRETERAS	TIPO 1
55	DESPRCAR SANTA CRUZ DE COCACHACRA	CARRETERA CENTRAL # SN	SANTA CRUZ DE COCACHACRA	HUAROCHIRI	LIMA	11.911178 29	-76.58751726	100M			0	0	1	0	0	RURAL	CARRETERAS	TIPO 1
56	DESPRCAR SAYAN	CARRETERA PENETRACION A SAYAN 45.6	SAYAN	HUAURA	LIMA	-11.13467	-77.198538	100M			0	0	1	0	0	URBANO	CARRETERAS	TIPO 1
74	DESPRCAR STA ROSA	CARRETERA PANAMERICANA NORTE KM.42 DESTACAMENTO POLICIAL DE CARRETERA.	SANTA ROSA	LIMA	LIMA	11.792279	-77.1477796	100M			0	0	1	0	0	URBANO	CARRETERAS	TIPO 1
52	DESPRCAR YANGAS	MZ C LOTE 11- CENTRO POBLADO BUENA VISTA- CARRETERA LIMA-CANTA	SANTA ROSA DE QUIVES	CANTA	LIMA	11.728954	-76.968231	100M			0	0	1	0	0	URBANO	CARRETERAS	TIPO 1
59	DIRANDRO - DIVISION DE INVESTIGACION CONTRA EL DESVÍO DE INSUMOS QUIMICOS	AV. RESTAURACIÓN 600 PISO 3	CERCADO	LIMA	LIMA	12.061814	-77.051589	100M			0	1	1	0	1	URBANO	DIRANDRO	TIPO 1
63	DIRANDRO - UN DE LOGISTICA - OFAD	AV. ARENALES 855	JESUS MARIA	LIMA	LIMA	12.073168	-77.037185	100M			0	1	1	0	1	URBANO	DIRANDRO	TIPO 1
71	DEPARTAMENTO DE REQUISITORIAS	JR. LOS TORDOS N°1042	SAN JUAN DE LURIGANCHO	LIMA	LIMA	12.016042	-76.997805	150M	1		1	0	1	0	2	URBANO	RQ/OFCRI	TIPO 2
81	DIRECCION CONTRA LA CORRUPCION - 0	AV. SAEZ PEÑA N° 116	BARRANCO	LIMA	LIMA	12.142931	-77.022374	100M			0	1	1	0	3	URBANO	DIRECCOR	TIPO 1
65	DIRECCION DE POLICIA FISCAL	AV. BELISARIO FLORES 565	LINCE	LIMA	LIMA	12.082504	-77.040622	100M			0	1	1	0	1	URBANO	DIREPOLFIS	TIPO 1



66	9	DIRECCION DE TURISMO PNP -DIRTUR PNP	JIRON MOORE 268	MAGDALENA	LIMA	LIMA	12.095489 5	-77.06879294	100M			0	0	1	0	1	0	1	TURISMO	TIPO 1
72	3	CPNP SAN JUAN DE MIRAFLORES	PASAJE SAN JUAN # SN	SAN JUAN DE MIRAFLORES	LIMA	LIMA	12.157933 02	-76.97529227	150M			0	1	1	0	3		URBANO	A	TIPO 1
68	6	CP JUAN BENITEZ LIMA CIBELES	CALLE LOS CIBELES 150	RIMAC	LIMA	LIMA	12.033548	-77.032547	400M	1		5	0	0	2	12		URBANO	COMPLEJO 1	TIPO 2
75	0	DIRECCION NACIONAL DE ORDEN Y SEGURIDAD DIRNOS	AV. GRAL. RECAVAREN 1378	SURQUILLO	LIMA	LIMA	12.106663 5	-77.0238846	100M			0	1	1	1	1		URBANO	ENTIDAD DEL ESTADO	TIPO 1
74	5	DIRPACIU	AV. V. ASTETE 1131 URB. CH. DEL ESTANQUE	SURCO	LIMA	LIMA	12.113925	-76.984107	100M			0	1	1	0	1		URBANO	DIRPACIU	TIPO 1
74	6	DIRPOLFIS (POLICIA FISCAL)	AV. INGENIEROS 574	SURCO	LIMA	LIMA	12.127852	-76.972709	100M			0	1	1	0	1		URBANO	DIRPOLFIS	TIPO 1
67	2	DIRSAPOL PNP	AV. AREQUIPA N° 4898	MIRAFLORES	LIMA	LIMA	-12.11478	-77.02984	100M			0	1	1	0	1		URBANO	SANIDAD	TIPO 1
51	9	DIVCMIPA - DIVCTIPRN	AV. DEL BIERZO KM 1.5	VENTANILLA	CALLAO	LIMA	-11942471	-77117822	100M			0	1	1	0	1		URBANO	DIRMEAMB	TIPO 1
73	0	CPNP SAN MARTIN DE PORRES	JIRON MANUEL VILLAR # 1	SAN MARTIN DE PORRES	LIMA	LIMA	12.025688	-77.055866	150M			1	1	1	0	3		URBANO	A	TIPO 1
69	2	DIVISION DE ASUNTOS SOCIALES /DEPARTAMENTO DE PROTECCION DE OBRAS CIVILES	JIRON LORETO 278	RIMAC	LIMA	LIMA	12.042781	-77.028281	100M			0	0	1	0	1		URBANO	DIPROC (DEPARTAMENT O DE PROTECCION DE OBRAS CIVILES)	TIPO 1
61	1	DIVISION DE INVESTIGACION CONTRA EL CRIMEN ORGANIZADO - DIRECCION DE MEDIO AMBIENTE PNP	ALAMEDA DEL PREMIO REAL MZ J LT 16 URB LA ENCANTADA DE VILLA CHORRILLOS	CHORRILLOS	LIMA	LIMA	12.209203	-77.006881	100M			0	0	1	0	1		URBANO		TIPO 1
65	5	DIVISION DE INVESTIGACIÓN DE DELITOS CONTRA LOS DERECHOS INTELECTUALES	JR. JOSE PEZAT Y MONEL ANTES JR. TUPAC AMARU 1894	LINCE	LIMA	LIMA	12.084551	-77.042691	100M			0	1	1	0	1		URBANO	DIRPOLFIS	TIPO 1
82	3	DIVISION DE PROTECCION CONTRA LA VIOLENCIA FAMILIAR PNP - DIVPCVF	JR. CHOTA N°1434	LIMA	LIMA	LIMA	12.058792	-77.040324	100M			0	1	1	0	2		URBANO	DIVPCVF	TIPO 1
73	7	DIVISION DE PROTECCION DE BANCOS	AV. BOLOGNESI 282	SANTA ANITA	LIMA	LIMA	12.054533	-76.969801	100M			0	0	1	0	1		URBANO	AGUILAS NEGRAS	TIPO 1
67	7	DIVISION INVESTIGACION DE DELITOS CONTRA EL ESTADO - DIVIDCE	JR. ANTONIO ARRIETA 278	PUEBLO LIBRE	LIMA	LIMA	12.074907	-77.055543	100M			0	1	1	0	1		URBANO	DIRSEG	TIPO 1
76	6	DIVISION POLICIAL ESTE 1	JR. CELEDONIAS CODA 6 URB LAS FLORES DE PRIMAVERA PARADERO 13 DE LA AV. LAS FLORES SUL	SAN JUAN DE LURIGANCHO	LIMA	LIMA	14.067848 33	-70.43133333	100M			0	1	1	0	3		RURAL	B	TIPO 1
54	1	DIVISION POLICIAL HUACHO	AV. 28 DE JULIO N° 210- ESQUINA DE 28 DE JULIO CON DOMINGO COLOMA	HUACHO	LIMA	LIMA	-11.10713	-77.60638	100M			0	1	1	0	1		URBANO	DIVPOL	TIPO 1
66	5	DIVPOL CHOSICA	PSJE. SOLEA 198 KM 32 CAT CENTRAL CHACLAAYO	LURIGANCHO	LIMA	LIMA	11.945102	-76.710469	100M			0	1	1	0	0		URBANO	E	TIPO 1
54	5	DIVPOL HUARAL DEPICAJ HUARAL	CALLE MANCO CAPAC S/N EL MILAGRO	HUARAL	LIMA	LIMA	-11.49438	-77.216379	100M			0	1	1	0	2		URBANO	DIVINCRI	TIPO 1
61	3	ESCUELA POSGRADO PNP	AV. GUARDIA CIVIL 800	CHORRILLOS	LIMA	LIMA	12.177083	-76.995105	100M			0	1	1	0	1		URBANO	ENF	TIPO 1
74	7	INTERPOL - SURCO	AV. MANUEL OLGUIN CUADRA 6 - PISO 2	SURCO	LIMA	LIMA	12.094793 33	-76.97326333	100M			0	1	1	0	1		URBANO	INTERPOL	TIPO 1
60	0	JEPOLTRAN - FENIX	AV. ALFONSO UGARTE CDA. 1	CERCADO	LIMA	LIMA	12.039994	-77.043545	100M			0	1	1	0	1		URBANO	TRANSITO	TIPO 1
73	8	JEPOLTRAN LIMA ESTE/POLICIA FISCAL	AV. 7 DE JUNIO - LOS FICUS	SANTA ANITA	LIMA	LIMA	12.050294	-76.975754	100M			0	1	1	0	1		URBANO	TRANSITO	TIPO 1
62	3	MAESTRANZA	CA 13 S/N URB CARABAYLLO 5 METROPOLITANA MERCADO HYPER ESPALDA	COMAS	LIMA	LIMA	11.967624	-77.06003	100M			0	1	1	0	1		URBANO	DIVLOG	TIPO 1



60	3	MAESTRANZA 1	JR CHOTA 1322	LIMA	LIMA	12.056685 4	-77.0408121	100M			0	1	1	0	1	URBANO	DIVLOG	TIPO 1
60	4	MAESTRANZA 2 Y 3	AV ARGENTINA CDA 15	LIMA	LIMA	-12.04513	-77.05931	100M			0	1	1	0	1	URBANO	DIVLOG	TIPO 1
70	5	DIRANDRO	CALLE LOS CISNES 594 PISO 10 ARAMBURU	LIMA	LIMA	12.102281	-77.023562	400M	1		4	0	0	2	5	URBANO	COMPLEJO 1	TIPO 2
60	6	MINISTERIO PUBLICO	AV. ABANCAY CDRA. 5 S/N PISO 11 - LIMA	LIMA	LIMA	-12.05166	-77.02842	100M			0	1	0	0	1	URBANO	ENTIDAD DEL ESTADO	TIPO 1
64	1	OFICRI DIRANDRO LIMA	CALLE RAMON DAGUINO N°442 - RESIDENCIAL PIO XII - 2DO BLOCK PRIMER PISO	LIMA	LIMA	12.071542	-77.038015	100M			0	1	1	0	1	URBANO	OFICRI	TIPO 1
50	4	POUCIA JUDICIAL CALLAO	AV. 2 DE MAYO S/N CDA 5	CALLAO	LIMA	12.056804	-77.142677	100M			0	1	1	0	1	URBANO	POLIS	TIPO 1
69	8	POUCINICO POLICIAL - SEDE ESCUELA DE SAN BARTOLO	AV. EL GOLF S/N SAN BARTOLO	LIMA	LIMA	12.384413	-76.7799	100M			0	1	1	0	1	URBANO	POSTA MEDICA	TIPO 1
57	7	POUCINICO POLICIAL CAÑETE	AV. PROLONG. AUGUSTO B LEGUIA S/N	LIMA	LIMA	13.076097	-76.316168	100M			0	1	1	0	1	URBANO	POSTA MEDICA	TIPO 1
58	2	POUCINICO POLICIAL CARABAYLO	MZ G1 L35 S/N MZ G1 LOTE KM.	LIMA	LIMA	11.888395	-77.038235	100M			0	1	1	0	1	URBANO	POSTA MEDICA	TIPO 1
73	2	POUCINICO POLICIAL SAN DIEGO	CALLE SANTO TOMAS DE AQUINO CDA 3 S/N	LIMA	LIMA	11.941602	-77.086059	100M			0	1	1	0	1	URBANO	POLICLINICO	TIPO 1
75	6	CPNP VILLA EL SALVADOR/DIVINCR/CONTRA INVASIONES	AV. CESAR VALLEJO # SN	LIMA	LIMA	12.212957 58	-76.9366765	150M			0	1	1	0	3	URBANO	A	TIPO 1
50	5	POUCINICO POLICIAL VIPOL	CALLE LOS NENUFAR S/N	CALLAO	CALLAO	12.012214	-77.097921	100M			0	1	1	0	1	URBANO	POLICLINICO	TIPO 1
51	2	POUCINIO POLICIAL CALLAO	AV. LA PAZ S/N	CALLAO	CALLAO	12.072372	-77.124381	100M			0	1	1	0	1	URBANO	POLICLINICO	TIPO 1
56	0	POSTA MEDICA POLICIAL HUACHO	CALLE 28 DE JULIO 103	HUACHO	HUACHO	-11.10793	-77.585091	100M			0	1	1	0	1	URBANO	POSTA MEDICA	TIPO 1
52	0	POSTA MEDICA POLICIAL VENTANILLA	AV. PEDRO BELTRAN CDA 10 S/N	CALLAO	CALLAO	-11.87153	-77.122556	100M			0	1	1	0	1	URBANO	POSTA MEDICA	TIPO 1
70	2	SEDE RENIEC CONEXIÓN SEDE PRINCIPAL PNP	JR. TIZIANO VECELLIO 245, SAN BORJA	LIMA	LIMA	12.088450 65	-77.00122831	100M			0	1	0	0	1	URBANO	ENTIDAD DEL ESTADO	TIPO 1
75	1	SOPORTE TECNICO - DIRTIC PNP	AV. ANDRÉS ARAMBURU N° 550 (CP WALTER ROSALES LEON, PISO 7)	LIMA	LIMA	12.102790	-77.02502	100M			0	1	1	0	1	URBANO	DIRTIC	TIPO 1
51	1	UNIDAD DE EMERGENCIA CALLAO - UNEME CALLAO	AV. LA PAZ N° 2685	CALLAO	CALLAO	-12.07715	-77.110172	100M			0	1	1	0	1	URBANO	EMERGENCIA	TIPO 1
71	8	UNIDAD DE EMERGENCIA ESTE 1	AV. FERNANDO WIESE 313	LIMA	LIMA	11.980552	-77.005478	100M			0	1	1	0	1	URBANO	EMERGENCIA	TIPO 1
57	3	UNIDAD DE EMERGENCIA ESTE 2	AV. JOSÉ C. MARIATEGUI 68	LIMA	LIMA	12.011854	-76.827383	100M			0	1	1	0	1	URBANO	EMERGENCIA	TIPO 1
75	1	UNIDAD DE EMERGENCIA SUR 1	AV. REPÚBLICA DE PANAMÁ 4450	LIMA	LIMA	12.109228	-77.018509	100M			0	1	1	0	1	URBANO	EMERGENCIA	TIPO 1
76	3	UNIDAD DE EMERGENCIA SUR 2 - UNEME SUR	AV. PACHACUTEC 2220 URB VILLA JARDIN	LIMA	LIMA	12.167383 976	76.951909853	100M			0	0	1	0	1	URBANO	UNEME	TIPO 1
40	1	UNIDAD FUNCIONAL DE CRIMINALISTICA ESTE 1 - UNIFUCRI ESTE 1	CALLE LOS NARANJOS 126 (5 to piso)	LIMA	LIMA	11.981027	-77.011369	150M			0	1	1	0	1	URBANO	DIRCRI	TIPO 1
48	0	UNIDAD PREVENCIÓN E INVESTIGACIÓN DE ROBO DE VEHÍCULOS - UNIPRV BARRANCA	JIRON STA. ZORAIDA # SN	BARRANCA	BARRANCA	10.750620	-77.764824	100M			0	1	1	0	2	RURAL	B	TIPO 1
64	6	UNINST - DIRTIC PNP	JR. CRISANTEMOS 164 MZ PJLT-9	LIMA	LIMA	12.086208	-76.958033	100M			0	1	1	0	0	URBANO	ETS	TIPO 1
77	1	CPNP ALTO AMAZONAS - YURIMAGUAS/DIVPOL	CALLE CONDOMINE # SN	LORETO	ALTO AMAZONAS	5.8974083 33	-76.11445167	100M			0	1	1	0	2	URBANO	B	TIPO 1

77	2	CPNP SECTORIAL LORETO - NAUTA	CALLE MANUEL PACAYA # 345	NAUTA	LORETO	LORETO	4.5068383 33	-73.57502167	100M		0	1	1	0	1	URBANO	B	TIPO 1
77	3	CPNP 9 DE OCTUBRE	CALLE TAHUANTINSUYO # SN	BELEN	MAYNAS	LORETO	3.7665756 21	-73.26095336	100M		0	1	1	0	1	URBANO	B	TIPO 1
77	4	CPNP BELEN	CALLE SEIS # SN	BELEN	MAYNAS	LORETO	3.7608016 67	-73.24907	100M		0	1	1	0	1	URBANO	B	TIPO 1
77	5	CPNP TASHIYACU	CALLE ALANZA PAZ SOLDAN # 107	FERNANDO LORES	MAYNAS	LORETO	4.0022316 67	-73.15991833	100M		0	1	1	0	1	RURAL	C	TIPO 1
77	6	CPNP AEROPUERTO INTERNACIONAL FRANCISCO SECADA VIGNETTA	OTRO INSTALACIONES DEL AEROPUERTO INTERNACIONAL # 1	IQUITOS	MAYNAS	LORETO	3.7843416 67	-73.30262167	100M		0	1	1	0	0	URBANO	C	TIPO 1
77	7	CPNP IQUITOS	CALLE MORONA # 120	IQUITOS	MAYNAS	LORETO	3.7522667 66	-73.24464664	100M		0	1	1	0	1	URBANO	A	TIPO 1
77	8	CPNP MORONACOCHA/CPNP FAMILIA/DIRCOCOR MAYNAS	AV. MARISCAL CACERES 2200	IQUITOS	MAYNAS	LORETO	-3.745247	-73.264983	100M		0	1	1	0	2	URBANO	A	TIPO 1
77	9	DIVTURMA IQUITOS	PROLONGACIÓN PUTUMAYO Nº 1658	IQUITOS	MAYNAS	LORETO	-3.739301	-73.256882	100M		0	0	1	0	1	URBANO	TURISMO	TIPO 1
78	0	ETS PNP IQUITOS	ALTURA DEL KM. 5.100. DE LA CARRETERA IQUITOS-NAUTA. CASERIO DE QUISTOCOCCHA.	IQUITOS	MAYNAS	LORETO	-3.81905	-73.323346	100M		0	1	1	0	5	URBANO	ETS	TIPO 1
78	1	OFICRI IQUITOS	JR. PROSPERO N°565 - IQUITOS	IQUITOS	MAYNAS	LORETO	-3.75354	-73.24635	100M		0	1	1	0	1	URBANO	OFICRI	TIPO 1
78	2	RQ AEROPUERTO GRNL. FAP FRANCISCO SECADA VIGETA	AV. A. QUIÑONES KM 6-AEROPUERTO	IQUITOS	MAYNAS	LORETO	-3.785033	-73.303278	100M		0	1	1	0	1	URBANO	RQ	TIPO 1
78	3	UNIPRCAR IQUITOS	CALLE PUTUMAYO 762	IQUITOS	MAYNAS	LORETO	-3.74613	-73.248669	100M		0	0	1	0	0	URBANO	CARRETERAS	TIPO 1
78	4	REGPOL LORETO	AV. BRASIL 147 IQUITOS	IQUITOS	MAYNAS	LORETO	-3.753337	-73.245438	150M		0	1	1	0	1	URBANO	REGPOL	TIPO 1
78	5	CPNP PUNCHANA	AV. LA MARINA # 1101	PUNCHANA	MAYNAS	LORETO	3.7291633 33	-73.24078667	100M		0	1	1	0	1	URBANO	A	TIPO 1
78	6	DIVINCI IQUITOS	CALLE 28 DE JULIO 103	PUNCHANA	MAYNAS	LORETO	3.7287735	-73.2409193	100M		0	1	1	0	2	URBANO	DIVINCI	TIPO 1
78	7	POLICLINICO POLICIAL IQUITOS	CALLE ABELARDO QUIÑONEZ KM 2.5	SAN JUAN BAUTISTA	MAYNAS	LORETO	-3.769623	-73.277574	100M		0	1	1	0	1	URBANO	POLICLINICO	TIPO 1
78	8	DIVTURMA MADRE DE DIOS	JR. DANIEL ALCIDES CARRION 440	TAMBOPATA	MADRE DE DIOS	MADRE DE DIOS	12.593326	-69.178204	100M		0	0	1	0	1	URBANO	TURISMO	TIPO 1
78	9	CPNP RURAL IBERIA	AV. JORGE CHAVEZ # 986	IBERIA	TAHUAMANU	MADRE DE DIOS	11.405351 67	-69.489645	100M		0	1	1	0	1	RURAL	D	TIPO 1
79	0	FRONTERIZO INAPARI	AV. HAYA DE LA TORRE CON A. BOLIVIA	INAPARI	TAHUAMANU	MADRE DE DIOS	10.944700	-69.57594	100M		0	0	1	0	1	RURAL	CEBAF	TIPO 1
79	1	CPNP MAZUKO	AV. INAMBARI SN MZLL LT.1	INAMBARI	TAMBOPATA	MADRE DE DIOS	13.100475	-70.36712667	100M		0	1	1	0	1	RURAL	D	TIPO 1
79	2	CPNP PLANCHON	CARR. CARRET INTEROCEANICA SN	LAS PIEDRAS	TAMBOPATA	MADRE DE DIOS	12.275726 67	-69.15207833	100M		0	1	1	0	1	URBANO	C	TIPO 1
70	6	DIRINT	AV. PASEO DE LA REPUBLICA 3681 PISO 7	SAN ISIDRO	LIMA	LIMA	12.100656	-77.026466	400M	1	1	0	0	1	0	URBANO	COMPLEJO 1	TIPO 2
79	4	CPNP DE LA FAMILIA MALDONADO	AV. APURIMAC S/N CRUCE CON AV. ERNESTO RIVERO	TAMBOPATA	TAMBOPATA	MADRE DE DIOS	12.601541 67	-69.18892833	100M		0	1	1	0	1	RURAL	FAMILIA	TIPO 1
79	5	CPNP PUERTO MALDONADO - TAMBOPATA	JIRÓN DANIEL ALCIDES CARRION # 410	TAMBOPATA	TAMBOPATA	MADRE DE DIOS	-12.59345	-69.17810333	100M		0	1	1	0	2	RURAL	A	TIPO 1



Handwritten signatures and initials in the top left corner of the page.

Handwritten signature and initials at the top left of the page.



Handwritten signature and initials on the left side of the page.

79	CPNP TAMBOPATA	AV. 2 DE MAYO S/N - ÓVALO CARRETERA INTEROCÉANICA	TAMBOPATA	TAMBOPATA	MADRE DE DIOS	12.583286 67	-69.19316333	100M		0	1	1	0	1	RURAL	B	TIPO 1
79	DIRCOCOR TAMBOPATA	JR. CUSCO CON JR. MARCO RUIZ	TAMBOPATA	TAMBOPATA	MADRE DE DIOS	12.582917	-69.19138	100M		0	1	1	0	1	RURAL	DIRCOCOR	TIPO 1
79	DIVINCRI MADRE DE DIOS/DEPOTAD MADRE DE DIOS	JR. BILLINGHURST 387	TAMBOPATA	TAMBOPATA	MADRE DE DIOS	12.592228	-69.176611	100M		0	1	1	0	2	RURAL	DIVINCRI	TIPO 1
79	REGPOL MADRE DE DIOS	AV. ELMER FAUCETT S/N - URB. LA JOYA	TAMBOPATA	TAMBOPATA	MADRE DE DIOS	12.596938	-69.220247	100M		0	1	1	0	1	RURAL	DIRCOCOR	TIPO 1
80	DIVIDA Y DIVIDCOEFM	AV. GUARDIA CIVIL N° 377-B LA CAMPINA	CHORRILLOS	CHORRILLOS	LIMA	12.183471	-77.001334	100M		0	1	1	0	1	RURAL	C	TIPO 1
80	CPNP SECTORIAL OMATE / COMISARIA RURAL OMATE	CALLE IGNACIO JOVE # S/N	OMATE	OMATE	MOQUEGUA	16.674941 4	-70.9699805	100M		0	1	1	0	1	RURAL	B	TIPO 1
80	CPNP ILO/POSTA MÉDICA (IMPLEMENTADO EN LA CPNP ILO SOLAMENTE)	CALLE PICHINCHA # 327	ILO	ILO	MOQUEGUA	-17.64465	-71.343747	100M		0	1	1	0	2	URBANO	A	TIPO 1
80	CPNP PAMPA INALAMBICA	AV. BOULEVAR # SN	ILO	ILO	MOQUEGUA	-17.65242	-71.32462	100M		0	1	1	0	1	URBANO	B	TIPO 1
80	CPNP SECTORIAL ILO/OFCRI	AV. MARIANO LINO URQUIETA # 301	ILO	ILO	MOQUEGUA	-17.64211	-71.34083833	100M		0	1	1	0	2	URBANO	A	TIPO 1
80	DIVINCRI ILO/DIVANDRO ILO	AV. MARIANO LINO URQUIETA # 319	ILO	ILO	MOQUEGUA	17.641502	-71.340665	100M		0	1	1	0	2	URBANO	DIVINCRI	TIPO 1
80	DIVTURMA ILO (IMPLEMENTO TAMBIEN EN LA POSTA MEDICA ILO)	JR. ZEPITA 602	ILO	ILO	MOQUEGUA	17.644377	-71.34389	100M		0	0	1	0	1	URBANO	TURISMO	TIPO 1
80	CPNP DE LA FAMILIA MOQUEGUA	CALLE AYACUCHO # SN	MOQUEGUA	MOQUEGUA	MOQUEGUA	-17.19175	-70.929683	100M		0	1	1	0	1	URBANO	FAMILIA	TIPO 1
80	CPNP LOS ANGELES	CALLE 2 DE MAYO # 302	MOQUEGUA	MOQUEGUA	MOQUEGUA	17.169587 51	-70.90696067	100M		0	1	1	0	1	URBANO	C	TIPO 1
80	CPNP MOQUEGUA	CALLE AYACUCHO # 308	MOQUEGUA	MOQUEGUA	MOQUEGUA	17.193003	-70.9254833	100M		0	1	1	0	3	URBANO	B	TIPO 1
81	UNIPOMON TACALA / DIVSESP	MZ. V.I.T. 19 CALLE LOS SAUCES - AA.HH. VILLA TACALA	CHORRILLOS	CHORRILLOS	LIMA	12.186807	-76.988297	100M		0	1	1	0	1	URBANO	B	TIPO 1
81	DIVINCRI MOQUEGUA/REGION POLICIAL/OFCRI (AFIS)	CALLE AMAZONAS S/N	MOQUEGUA	MOQUEGUA	MOQUEGUA	17.188970 9	-70.9332212	100M		0	1	1	0	3	URBANO	DIVINCRI	TIPO 1
81	CPNP SAMEGUA	AV. EMANCIPACION SN MZ.2 LT.12	SAMEGUA	SAMEGUA	MOQUEGUA	17.182531 78	-70.89945316	100M		0	1	1	0	2	URBANO	B	TIPO 1
81	POL PNP MOQUEGUA	AV. ANDRES AVELINO CACERES S/N	SAMEGUA	SAMEGUA	MOQUEGUA	17.186757	-70.907793	100M		0	1	1	0	1	URBANO	POLICINICO	TIPO 1
81	CPNP TORATA	CALLE GRAU # 5	TORATA	TORATA	MOQUEGUA	17.077068 33	-70.84528	100M		0	1	1	0	1	RURAL	D	TIPO 1
81	CPNP SECTORIAL DANIEL CARRION YANAHUANCA	JIRÓN 28 DE JULIO # SN	YANAHUANCA	YANAHUANCA	PASCO	10.491336 67	-76.51449333	100M		0	1	1	0	1	RURAL	B	TIPO 1
81	CPNP COMANDANCIA RURAL OXAPAMPA	JIRÓN ENRIQUE BOTTGGER # 338	OXAPAMPA	OXAPAMPA	PASCO	10.576101 67	-75.40269833	100M		0	1	1	0	2	RURAL	A	TIPO 1
81	CPNP VILLA RICA/DESPROCAR SAN LUIS DE SHUARO	AV. PADRE SALAS # SN	VILLA RICA	OXAPAMPA	PASCO	10.737766 67	-75.26921	100M		0	1	1	0	1	RURAL	B	TIPO 1
81	CPNP CHAUPIMARCA	JIRÓN YAULI # 180	CHAUPIMARCA	CHAUPIMARCA	PASCO	10.685131 67	-76.25437833	100M		0	1	1	0	1	RURAL	B	TIPO 1
81	CPNP LA ESPERANZA	AV. PROGRESO SN	SIMON BOLIVAR	PASCO	PASCO	10.703602	-76.291688	100M		0	1	1	0	1		C	TIPO 1

[Handwritten signature]



[Handwritten signature]

CPNP HUARIACA	PASAJE HEROES DE LA GUERRA DEL PASIFICO # SN	HUARIACA	PASCO	PASCO	10.444926 67	-76.18642	100M			0	1	1	0	1	0	1	RURAL	C	TIPO 1
82 0	CPNP HUATLAY		PASCO	PASCO			100M			0	1	1	0	1	0	1	RURAL	C	TIPO 1
82 1	POSTA MEDICA POLICIAL CERRO DE PASCO	JIRÓN PASCO # SN	PASCO	PASCO	11.000105	-76.36158167	100M			0	1	1	0	1	0	1	RURAL	POLICLINICO	TIPO 1
82 2	UNIPROCAR LIMA SUR	AV. LOS PROCERES Y LOPEZ ALBUJAR S/N	PASCO	PASCO	10.662493	-76.251784	100M			0	1	1	0	1	0	1	URBANO	CARRETERAS	TIPO 1
67 8	UNIPROCAR LIMA SUR	KM 56 PANAMERICANA SUR	LIMA	LIMA	12.455439	-76.753394	100M			0	0	1	0	1	0	0	URBANO	CARRETERAS	TIPO 1
82 4	DIVINCRI PASCO/OFICRI (AFIS)	AV. LOS INCAS CUADRA 1	PASCO	PASCO	10.667373	-76.252363	100M			0	1	1	0	1	0	2	RURAL	DIVINCRI	TIPO 1
82 5	CPNP SAN FRANCISCO DE ASIS DE YARUJAYAN	JIRÓN LIBERTAD # SN	PASCO	PASCO	-10.49098	-76.197259	100M			0	1	1	0	1	0	0	RURAL	E	TIPO 1
82 6	CPNP SECTORIAL TINAHUARCO COLQUIJRCA	AV. 28 DE JULIO # SN	PASCO	PASCO	10.754995	-76.26485667	100M			0	1	1	0	1	0	1	RURAL	C	TIPO 1
82 7	CPNP LA QUINUA / DESPRCAR LA QUINUA	CARRETERA CENTRAL VIA OROYA - HUANUCO # SN / FRENTE A PLAZA LA MONEDA	PASCO	PASCO	10.614818	-76.179603	100M			0	1	1	0	1	0	1	URBANO	COMISARIA	TIPO 1
82 8	CPNP YANACANCHA	AV. LOS PROCERES # 203	PASCO	PASCO	10.666060 29	-76.253196	100M			0	1	1	0	1	0	2	RURAL	B	TIPO 1
82 9	REGPOL PASCO/ DIVTURMA PASCO YANACANCHA	AV. LOS PROCERES 906	PASCO	PASCO	10.662712	-76.252213	100M			0	0	1	0	1	0	1	RURAL	TURISMO	TIPO 1
83 0	CPNP SECTORIAL AYABACA	CALLE CACERES S/N AYABACA	AYABACA	AYABACA	-4.641835	-79.715373	100M			0	1	1	0	1	0	1	URBANO	B	TIPO 1
83 1	CPNP HUANCABAMBA	AV. CENTENARIO # 390	HUANCABAMBA	HUANCABAMBA	-5.23636	-79.45303333	100M			0	1	1	0	1	0	1	RURAL	B	TIPO 1
83 2	CPNP KILOMETRO 50	CARR. CARRETERA CHULUCANAS KM50 SN MZ C LT. 277	MORROPON	MORROPON	-5.169395	-80.18613167	100M			0	1	1	0	1	0	1	URBANO	D	TIPO 1
83 3	CPNP PACCHA	AV. CALLE PRINCIPAL # SN	MORROPON	MORROPON	-5.01628	-80.22088667	100M			0	1	1	0	1	0	1	URBANO	D	TIPO 1
83 4	CPNP SECTORIAL CHULUCANAS	AV. RAMON CASTILLA # 1300	MORROPON	MORROPON	5.1008718 68	-80.1671277	100M			0	1	1	0	1	0	2	URBANO	A	TIPO 1
83 5	CPNP RURAL MATANZA	AV. 27 DE NOVIEMBRE # 236	MORROPON	MORROPON	5.2149016 67	-80.090435	100M			0	1	1	0	1	0	1	RURAL	D	TIPO 1
83 6	CPNP SECTORIAL MORROPON	JIRÓN LOPEZ # 201	MORROPON	MORROPON	-5.188795	-79.97140167	100M			0	1	1	0	1	0	2	URBANO	B	TIPO 1
83 7	CPNP SAN JUAN DE BIGOTE	AV. VICTOR RAUL HAYA DE LA TORRE # SN	MORROPON	MORROPON	5.3187466 67	-79.78662167	100M			0	1	1	0	1	0	1	RURAL	D	TIPO 1
83 8	CPNP SAN LUCAS DE COLAN	CARRETERA SULLANA A PAITA - SAN LUCAS DE COLAN # SN	PAITA	PAITA	5.0070666 67	-81.05663333	100M			0	1	1	0	1	0	1	RURAL	D	TIPO 1
83 9	CPNP CIUDAD DEL PESCADOR PIURA	AV. VICTOR RAUL HAYA DE LA TORRE SN MZ F1 LT. 1	PAITA	PAITA	-5.09461	-81.10010333	100M			0	1	1	0	1	0	1	URBANO	C	TIPO 1
84 0	CPNP SECTORIAL PAITA	JIRÓN INDEPENDENCIA # 427	PAITA	PAITA	5.0663816 67	-81.110685	100M			0	1	1	0	1	0	1	URBANO	B	TIPO 1
84 1	CPNP AEROPUERTO PIURA	AV. CORPAC # SN	PIURA	PIURA	5.2099380 76	-80.61630249	100M			0	1	1	0	1	0	0	URBANO	A	TIPO 1
84 2	CPNP CASTILLA	AV. CORPAC # 100	PIURA	PIURA	5.20559566	-80.6206591	100M			0	1	1	0	1	0	1	URBANO	B	TIPO 1
84 3	CPNP EL INDIO	CALLE D # 261	PIURA	PIURA	5.2246083 33	-80.61843833	100M			0	1	1	0	1	0	1	URBANO	C	TIPO 1



84	4	CPNP LOS ALGARROBOS	AV. AV. 289 DE JULIO SN SN MZ.6 LT.1	CASTILLA	PIURA	PIURA	5.1725151 31	-80.64975567	100M			0	1	1	0	2	URBANO	B	TIPO 1
84	5	CPNP TACALA	AV. LOS BRILLANTES # SN	CASTILLA	PIURA	PIURA	5.1870883 33	-80.59857	100M			0	1	1	0	1	URBANO	C	TIPO 1
84	6	POL. PNP ALMIRANTE MIGUEL GRAU (PIURA)	AV. CAYETANO HEREDIA S/N	CASTILLA	PIURA	PIURA	-5.195287	-80.62088	100M			0	1	1	0	1	URBANO	POLICLINICO	TIPO 1
84	7	CPNP SECTORIAL CATAOAS	AV. FRANCISCO BOLOGNESI # SN	CATAOAS	PIURA	PIURA	5.2661916 67	-80.67180167	100M			0	1	1	0	1	URBANO	B	TIPO 1
84	8	CPNP CUCUNGARA	AV. GRAU # 715	CURA MORI	PIURA	PIURA	5.3246483 33	-80.66487333	100M			0	1	1	0	1	URBANO	D	TIPO 1
84	9	CPNP LA ARENA	JIRÓN COMERCIO # 930	LA ARENA	PIURA	PIURA	-5.347885	-80.71320833	100M			0	1	1	0	1	URBANO	C	TIPO 1
85	0	CPNP LAS LOMAS	JIRÓN MIGUEL GRAU # 599	LAS LOMAS	PIURA	PIURA	4.6566966 67	-80.24405167	100M			0	1	1	0	1	URBANO	D	TIPO 1
72	4	DIVISION DE PROTECCION DE CARRETERAS - DIVPRCAR	AV. VARGAS MACHUCA CDA. 4 - JUNTO A LA CT	SAN JUAN DE MIRAFLORES	LIMA	LIMA	12.165632	-76.97361	400M	1		3	0	0	2	3	URBANO	COMPLEJO 1	TIPO 2
74	8	CP WALTER ROSALES LEON ARAMBURU	AV. ARAMBURU 550 - PISO 4	SURQUILLO	LIMA	LIMA	12.102718	-77.025027	400M	1		5	0	0	2	8	URBANO	COMPLEJO 1	TIPO 2
85	3	CPNP PIURA	AV. SANCHEZ CERRO # 1381	PIURA	PIURA	PIURA	-5.190595	-80.63419	100M			0	1	1	0	2	URBANO	A	TIPO 1
85	4	CPNP SAN MARTIN	AV. JOSE CARLOS MARIATEGUI # 304	PIURA	PIURA	PIURA	5.1854600 52	-80.66849224	100M			0	1	1	0	1	URBANO	B	TIPO 1
85	5	DEPEME PIURA	CALLE 5 URB. SAN JOSE	PIURA	PIURA	PIURA	-5.193431	-80.644795	100M			0	1	1	0	1	URBANO	EMERGENCIA	TIPO 1
85	6	COMTUR PIURA / DIVMA PIURA	AV. LOS COCOS 250 URBANIZACION CLUB GRAU	PIURA	PIURA	PIURA	-5.190867	-80.634356	100M			0	0	1	0	1	URBANO	TURISMO	TIPO 1
85	7	REGPOL PIURA	CARRETERA PIURA-SULLANA KM. 3.5 ZONA INDUSTRIAL	PIURA	PIURA	PIURA	-5.182270	-80.654212	150M			0	1	1	0	1	URBANO	REGPOL	TIPO 1
85	8	POSTA PNP SULLANA	CALLE UGARTECHE 416	SULLANA	PIURA	PIURA	-4.88877	-80.684876	100M			0	1	1	0	1	URBANO	POSTA MEDICA	TIPO 1
85	9	CPNP CRUCETA	AV. JESUS MARIA # SN	TAMBO GRANDE	PIURA	PIURA	4.8370789 33	-80.270185	100M			0	1	1	0	1	URBANO	D	TIPO 1
86	0	CPNP TAMBOGRANDE	JIRÓN PAITA # 759	TAMBO GRANDE	PIURA	PIURA	4.9322133 33	-80.34211333	100M			0	1	1	0	1	URBANO	B	TIPO 1
86	1	CPNP LA UNION	CALLE UNION # 501	LA UNION	PIURA	PIURA	5.4023469 89	-80.74340366	100M			0	1	1	0	1	URBANO	C	TIPO 1
86	2	CPNP SECTORIAL SECHURA	CALLE SUCRE # 221	SECHURA	SECHURA	PIURA	5.5545878 96	-80.82269311	100M			0	1	1	0	2	URBANO	B	TIPO 1
86	3	CPNP BELLAVISTA PIURA	CALLE PUÑO # 251	BELLAVISTA	SULLANA	PIURA	-4.891266	-80.68181	100M			0	1	1	0	2	RURAL	B	TIPO 1
86	4	CPNP SAN JACINTO	CALLE LOS LAURELES # SN	IGNACIO ESCUDERO	SULLANA	PIURA	4.8474416 67	-80.873556	100M			0	1	1	0	1	URBANO	D	TIPO 1
86	5	CPNP MARCAVELICA	CARRETERA PANAMERICANA NORTE # SN	MARCAVELICA	SULLANA	PIURA	4.8819433 33	-80.70671667	100M			0	1	1	0	1	URBANO	C	TIPO 1
86	6	DESPPCAR MARCAVELICA	CARRETERA PANAMERICANA NORTE # SN	MARCAVELICA	SULLANA	PIURA	4.8858483 33	-80.69810833	100M			0	0	1	0	0	URBANO	CARRETERAS	TIPO 1

[Handwritten signature]



[Handwritten signature]

86 7	CPNP SECTORIAL QUERECOTILLO	CALLE RODRIGUEZ # 485	QUERECOTILLO	SULLANA	PIURA	4.8414683 33	-80.65206667	100M			0	1	1	0	1	URBANO	C	TIPO 1
86 8	CPNP EL OBRERO	CALLE 13 DE DICIEMBRE # SN	SULLANA	SULLANA	PIURA	4.9105016 67	-80.68264833	100M			0	1	1	0	0	URBANO	E	TIPO 1
86 9	CPNP SULLANA	PASAJE LAS CAPULLANAS # 107	SULLANA	SULLANA	PIURA	4.8990653 33	-80.69023833	100M			0	1	1	0	2	URBANO	B	TIPO 1
87 0	SEINCRI SULLANA	AV. JOSE DE LAMA C/8 AA-HI SANCHEZ CERRO	SULLANA	SULLANA	PIURA	4.8997971	-80.6935268	100M			0	1	1	0	1	URBANO	DIVINCRI	TIPO 1
87 1	CPNP EL ALTO	AV. BOLOGNESI # SN	EL ALTO	TALARA	PIURA	4.2667166 67	-81.21316833	100M			0	1	1	0	1	URBANO	D	TIPO 1
87 2	CPNP NEGRITOS	AV. MIGUEL GRAU # 349	LA BREA	TALARA	PIURA	-4.654365	-81.30501167	100M			0	1	1	0	1	RURAL	D	TIPO 1
87 3	CPNP LOS ORGANOS	AV. TUPAC AMARU # 519	LOS ORGANOS	TALARA	PIURA	4.1793466 67	-81.129755	100M			0	1	1	0	1	URBANO	D	TIPO 1
87 4	CPNP MANCORA	AV. PIURA # 625	MANCORA	TALARA	PIURA	-4.106935	-81.05293667	100M			0	1	1	0	1	URBANO	D	TIPO 1
87 5	DINTURMA SULLANA CAMBIADO SECTOR MANCORA	AV. PIURA N°330	MANCORA	TALARA	PIURA	4.1073638 83	-81.05694334	100M			0	0	1	0	1	URBANO	TURISMO	TIPO 1
87 6	CPNP SECTORIAL TALARA	AV. BOLOGNESI # SN	PARINAS	TALARA	PIURA	-4.576145	-81.27648833	100M			0	1	1	0	2	URBANO	B	TIPO 1
87 7	CPNP TALARA ALTA	AV. A # 55	PARINAS	TALARA	PIURA	-4.589485	-81.25667167	100M			0	1	1	0	1	URBANO	C	TIPO 1
87 8	CPNP RURAL ASILLO (E)	JIRÓN BOLOGNESI # SN	ASILLO	AZANGARO	PUNO	14.786361 67	-70.35442833	100M			0	1	1	0	1	RURAL	C	TIPO 1
87 9	CPNP SECTORIAL AZANGARO	JIRÓN TACNA # 313	AZANGARO	AZANGARO	PUNO	14.909836 67	-70.196465	100M			0	1	1	0	1	RURAL	B	TIPO 1
88 0	CPNP RURAL JOSE DOMINGO CHOQUEHUANCA	JR. CUSCO N° 710	JOSE DOMINGO CHOQUEHUANCA	AZANGARO	PUNO	15.090921	-70.340838	100M			0	1	1	0	1	RURAL	B	TIPO 1
88 1	CPNP MACUSANI	COPACABANA N° 242 - COSTADO DE TERMINAL	MACUSANI	CARABAYA	PUNO	14.064695	-70.434991	100M			0	1	1	0	1	RURAL	B	TIPO 1
88 2	CPNP SECTORIAL DESAGUADERO/CARRETERA DESAGUADERO/CEM	AV. 28 DE JULIO # 325	DESAGUADERO	CHUCUITO	PUNO	16.564245	-69.03947833	100M			0	1	1	0	2	RURAL	B	TIPO 1
88 3	CPNP POMATA	JIRÓN LIMA NORTE # SN	POMATA	CHUCUITO	PUNO	16.271908 33	-69.29286833	100M			0	1	1	0	1	RURAL	C	TIPO 1
88 4	CPNP SECTORIAL ILAVE/DIVPOL ILAVE	JIRÓN ANDINO # 412	ILAVE	EL COLLAO	PUNO	16.085753 33	-69.63805833	100M			0	1	1	0	2	RURAL	A	TIPO 1
88 5	CPNP SECTORIAL HUANCANE	JIRÓN PECOSANI # 109	HUANCANE	HUANCANE	PUNO	15.701351 67	-69.7656	100M			0	1	1	0	1	RURAL	B	TIPO 1
88 6	CPNP SECTORIAL LAMPA	JIRÓN JOSE MANUEL RIOS # 232	LAMPA	LAMPA	PUNO	15.363606 67	-70.36710833	100M			0	1	1	0	1	RURAL	B	TIPO 1
88 7	CPNP SANTA LUCIA	JR. MANUEL CERVANTES N° 520	SANTA LUCIA	LAMPA	PUNO	15.701796	-70.609044	100M			0	1	1	0	1	RURAL	D	TIPO 1
88 8	CPNP SECTORIAL AYAVIRI	JIRÓN 2 DE MAYO # 581	AYAVIRI	MELGAR	PUNO	14.881883 33	-70.59221667	100M			0	1	1	0	2	RURAL	A	TIPO 1

[Handwritten signature]



[Handwritten signature]

[Handwritten signature]

88	DESPCAR AYAVIRI	CALLE UMACHIRI # SN	AYAVIRI	MELGAR	PUNO	14.884663 33	-70.59669657	100M			0	0	1	0	0	0	RURAL	CARRETERAS	TIPO 1
89	CPNP ORURILLO	JIRÓN PIMENTEL # SN	ORURILLO	MELGAR	PUNO	14.727410 68	-70.51095128	100M			0	1	1	0	1	0	RURAL	C	TIPO 1
89	CPNP RURAL SANTA ROSA	AV. MANCO CAPAC # 104	SANTA ROSA	MELGAR	PUNO	14.608096 67	-70.79126667	100M			0	1	1	0	1	0	RURAL	C	TIPO 1
89	CPNP RURAL MOHO	AV. AREQUIPA # 105	MOHO	MOHO	PUNO	15.359111 67	-69.49870167	100M			0	1	1	0	1	0	RURAL	C	TIPO 1
89	CPNP ACORA	AV. RAMON CASTILLA # 480	ACORA	PUNO	PUNO	15.976265	-69.796665	100M			0	1	1	0	1	0	RURAL	B	TIPO 1
89	CPNP CAPACHICA	JIRÓN AREQUIPA # SN	CAPACHICA	PUNO	PUNO	15.641866 86	-69.83118832	100M			0	1	1	0	1	0	RURAL	C	TIPO 1
89	CPNP CHUCUITO	JR. PASTOR Nº 611	CHUCUITO	PUNO	PUNO	15.894796	-69.889785	100M			0	1	1	0	1	0	RURAL	C	TIPO 1
89	CPNP ALTO PUNO	JR. MILLER FULLER MZA. N. LOTE 8	PUNO	PUNO	PUNO	15.820018	-70.029527	100M			0	1	1	0	1	0	URBANO	D	TIPO 1
89	CPNP DE LA FAMILIA PUNO	JR. DEUSTUA Nº 536	PUNO	PUNO	PUNO	15.840424	-70.02852	100M			0	1	1	0	1	0	URBANO	FAMILIA	TIPO 1
89	CPNP HUASCAR TIPO D / POLICINICO	AV. JULIACA # SN	PUNO	PUNO	PUNO	15.827763 33	-70.03424	100M			0	1	1	0	2	0	URBANO	C	TIPO 1
89	CPNP ICHU / DESPCAR PUNO	PANAMERICANA SUR Nº 1372 PUNO- CHUCUITO	PUNO	PUNO	PUNO	15.875469	-69.9278321	100M			0	1	1	0	2	0	RURAL	B	TIPO 1
90	CPNP SECTORIAL PUNO/DECODE/ESC VERDE/DIVPOL/MEDIO AMBIENTE	JIRÓN DEUSTUA # 536 - 538	PUNO	PUNO	PUNO	15.840445	-70.028503	100M			0	1	1	0	3	0	URBANO	A	TIPO 1
90	DEPINCRI - PUNO	JR. RICARDO PALMA 225	PUNO	PUNO	PUNO	15.841426 2	-70.0209345	100M			0	1	1	0	2	0	URBANO	DIVINCI	TIPO 1
90	OFITIC PUNO	JR. TACNA SN ESQUINA CON JR. RICARDO PALMA	PUNO	PUNO	PUNO	15.842977	-70.023324	100M			0	1	1	0	2	0	RURAL	OFITIC	TIPO 1
90	REGPOL PUNO	AV. EL SOL 450	PUNO	PUNO	PUNO	15.835892	-70.023276	200M			0	1	1	0	1	0	URBANO	REGPOL	TIPO 1
90	CPNP LA RINCONADA	CALLE COLOMBIA # SN	ANANEA	SAN ANTONIO DE PUTINA	PUNO	-14.63425	-69.44711167	100M			0	1	1	0	1	0	RURAL	C	TIPO 1
90	CPNP SECTORIAL SAN ANTONIO DE PUTINA	AV. LIBERTAD # SN	PUTINA	SAN ANTONIO DE PUTINA	PUNO	14.916226 67	-69.86633167	100M			0	1	1	0	1	0	RURAL	A	TIPO 1
90	CPNP CABANILLAS	JIRÓN SAN MARTIN # 221	CABANILLAS	SAN ROMAN	PUNO	15.643775	-70.35106833	100M			0	1	1	0	1	0	RURAL	C	TIPO 1
90	CPNP CARACOTO	AV. LIMA # SN	CARACOTO	SAN ROMAN	PUNO	15.566458 33	-70.10168167	100M			0	1	1	0	1	0	RURAL	D	TIPO 1
90	CPNP AEROPUERTO INCA MANCO CAPAC	AV. AEROPUERTO # SN	JULIACA	SAN ROMAN	PUNO	15.470203 33	-70.15710333	100M			0	1	1	0	0	0	URBANO	A	TIPO 1
90	CPNP JULIACA/DIVPOL JULIACA/ OFICRI/ FAMILIA JULIACA/ OFICINA DISCIPLINA/ USE	JIRÓN RAMON CASTILLA Nº 725 CON JR. SAN MARTIN	JULIACA	SAN ROMAN	PUNO	15.492834	-70.128058	200M			1	1	1	0	3	0	URBANO	A	TIPO 1
91	CPNP SANTA BARBARA/105, ESCUADRON DE EMERGENCIA	JIRÓN LOS OLIVOS # SN	JULIACA	SAN ROMAN	PUNO	15.505381 67	-70.12800167	150M			1	1	1	0	1	0	URBANO	B	TIPO 1
91	DEPINCRI PNP JULIACA	JIRON ARICA 100 URB. LA RINCONADA	JULIACA	SAN ROMAN	PUNO	15.499631	-70.132408	150M			0	1	1	0	2	0	URBANO	DIVINCI	TIPO 1
91	DESPCAR JULIACA	AV. CIRCUNVALACION ESTE Nº 924	JULIACA	SAN ROMAN	PUNO	-15.49205	-70.12199	100M			0	0	1	0	0	0	URBANO	CARRETERAS	TIPO 1

Handwritten marks and signatures at the top left of the page.



91	TRANSITO / DEPROVE	JULIACA	SAN ROMAN	PUNO	-70.13289	200M		0	1	1	0	1	URBANO	DIPROVE	TIPO 1
91 3	AV. C. TELLO CUADRA 8 - LA CAPILLA (JIRON CAHUIDE 347)			PUNO	15.487185	100M			1	1	0	1	RURAL	B	TIPO 1
91 4	CPNP SECTORIAL PNP YUNGUYO	YUNGUYO	YUNGUYO	PUNO	16.243776 67	100M			1	1	0	1	RURAL	B	TIPO 1
91 5	CPNP SANDIA	SANDIA	SANDIA	PUNO	14.322222	100M			1	1	0	2	URBANO	A	TIPO 1
91 6	CPNP BELLAVISTA	BELLAVISTA	BELLAVISTA	SAN MARTIN	7.0652266 67	100M			1	1	0	1	URBANO	B	TIPO 1
91 7	CPNP SAPOSOA	SAPOSOA	HUALLAGA	SAN MARTIN	6.9363210 9	100M			1	1	0	1	URBANO	B	TIPO 1
91 8	CPNP LAMAS	LAMAS	LAMAS	SAN MARTIN	6.423028	100M			1	1	0	1	URBANO	B	TIPO 1
91 9	CPNP SORITOR	SORITOR	LAMAS	SAN MARTIN	6.3876033 33	100M			1	1	0	1	URBANO	B	TIPO 1
92 0	CPNP Sectorial JUANUI	JUANUI	MARISCAL CACERES	SAN MARTIN	7.1798366 67	100M			1	1	0	1	URBANO	B	TIPO 1
92 1	CP USE PNP/SEGURIDAD DEL ESTADO/DIPOLCAR/OPICRI	TAMBOPATA	TAMBOPATA	MADRE DE DIOS	12.587636	200M	1	2	0	1	0	5	RURAL	COMPLEJO 1	TIPO 2
92 2	CPNP CALZADA	CALZADA	MOYOBAMBA	SAN MARTIN	6.0304966 67	100M			1	1	0	1	RURAL	D	TIPO 1
92 3	CPNP JEPOLACIO	JEPOLACIO	MOYOBAMBA	SAN MARTIN	6.1082139 45	100M			1	1	0	1	RURAL	D	TIPO 1
92 4	CP JUAN BENITEZ LUNA DEPOTAD DIVSEG PIURA SSEE	PIURA	PIURA	PIURA	-5.185474	200M	1	5	0	1	0	4	URBANO	COMPLEJO 1	TIPO 2
92 5	CPNP MOYOBAMBA	MOYOBAMBA	MOYOBAMBA	SAN MARTIN	6.0344821 91	100M			1	1	0	2	URBANO	A	TIPO 1
92 6	CPNP UCHUGLLA	MOYOBAMBA	MOYOBAMBA	SAN MARTIN	-6.04775	100M			1	1	0	1	URBANO	C	TIPO 1
92 7	CPNP TABALOSOS	SORITOR	MOYOBAMBA	SAN MARTIN	6.1350304 37	100M			1	1	0	1	URBANO	C	TIPO 1
92 8	CPNP PICOTA	PICOTA	PICOTA	SAN MARTIN	-6.91891	100M			1	1	0	1	URBANO	C	TIPO 1
92 9	CPNP SAN HILARION	SAN HILARION	PICOTA	SAN MARTIN	6.9598216 67	100M			1	1	0	1	RURAL	D	TIPO 1
93 0	CPNP SEGUNDA JERUSALEN	ELIAS SOPLIN VARGAS	RIOJA	SAN MARTIN	5.9880133 33	100M			1	1	0	1	RURAL	D	TIPO 1
93 1	CPNP NUEVA CAJAMARCA	NUEVA CAJAMARCA	RIOJA	SAN MARTIN	-5.943097	100M			1	1	0	1	URBANO	B	TIPO 1
93 2	CPNP NARANJOS	PARDO MIGUEL	RIOJA	SAN MARTIN	5.7404922 13	100M			1	1	0	1	RURAL	C	TIPO 1
93 3	CPNP RIOJA	RIOJA	RIOJA	SAN MARTIN	-6.0638	100M			1	1	0	1	URBANO	B	TIPO 1
93 4	CPNP YURACYACU	YURACYACU	RIOJA	SAN MARTIN	5.9282821 22	100M			1	1	0	1	RURAL	D	TIPO 1
93 5	DIVMA TARAPOTO	BANDA DE SHILCAYO	SAN MARTIN	SAN MARTIN	-6.482214	100M			0	1	0	1	URBANO	TURISMO	TIPO 1

Handwritten signature and initials at the top left of the page.



Handwritten signature and initials in the middle left margin.

93 6	CPNP LA BANDA DE SHILCAYO	JIRÓN SANTA MARIA # 180	LA BANDA DE SHILCAYO	SAN MARTIN	SAN MARTIN	-6.4907	-76.354037	100M		0	1	1	0	1	URBANO	C	TIPO 1
93 7	CPNP MORALES/COM CAR TARAPOTO	AV. SALAVERRY # 213 # 225	MORALES	SAN MARTIN	SAN MARTIN	6.4794233 33	-76.38299167	100M		0	1	1	0	2	URBANO	B	TIPO 1
93 8	DEPOTAD MORALES	JR. SEVILLA 351	MORALES	SAN MARTIN	SAN MARTIN	-6.473491	-76.388949	100M		0	1	1	0	1	URBANO	DIRANDRO	TIPO 1
93 9	POL PNP MOYOBAMBA	AV. GRAU BARRIO CALVARIO 451	MOYOBAMBA	SAN MARTIN	SAN MARTIN	-6.044314	-76.370821	100M		0	1	1	0	1	URBANO	POLCLINICO	TIPO 1
94 0	CPNP AEROPUERTO TARAPOTO	JIRÓN JORGE CHAVEZ # SN	TARAPOTO	SAN MARTIN	SAN MARTIN	6.5110533 33	-76.36914333	100M		0	1	1	0	0	URBANO	A	TIPO 1
94 1	CPNP DE LA FAMILIA TARAPOTO	JIRÓN MATEO PUMACAHUA # SN	TARAPOTO	SAN MARTIN	SAN MARTIN	6.4863283 33	-76.37376333	100M		0	1	1	0	1	URBANO	FAMILIA	TIPO 1
94 2	CPNP TARAPOTO/DEPANDRO/REG POL SAN MARTIN	JIRÓN RAMIREZ HURTADO # 298	TARAPOTO	SAN MARTIN	SAN MARTIN	-6.48673	-76.35915	300M		3	1	1	0	3	URBANO	A	TIPO 1
94 3	DIVINCR-APLT OFICRI TARAPOTO	JR. LEONCIO PRADO 349	TARAPOTO	SAN MARTIN	SAN MARTIN	-6.484855	-76.360652	150M		3	1	1	0	2	URBANO	DIVINCR/OFCRI	TIPO 1
94 4	DIVISIÓN DE EMERGENCIA - TARAPOTO	C12 ALFONSO UGARTE	TARAPOTO	SAN MARTIN	SAN MARTIN	-6.492159	-76.371773	100M		0	1	1	0	1	URBANO	EMERGENCIA	TIPO 1
94 5	OFICINA DE INTELIGENCIA TERRITORIAL	AV. SAN MARTIN N° 614	TARAPOTO	SAN MARTIN	SAN MARTIN	-6.493590	-76.353700	100M		0	0	1	0	1	URBANO	ORI	TIPO 1
94 6	POL PNP TARAPOTO	JR. LOS GIRASOLES 300	TARAPOTO	SAN MARTIN	SAN MARTIN	-6.493199	-76.372249	100M		0	1	1	0	1	URBANO	POLCLINICO	TIPO 1
94 7	CPNP NUEVO PROGRESO	CARRETERA FERNANDO BELAUNDE TERRY # SN	NUEVO PROGRESO	TOCACHE	TOCACHE	8.4533216 67	-76.32424833	100M		0	1	1	0	1	RURAL	C	TIPO 1
94 8	DEPOTAD SANTA LUCIA (Antes DEPOTAD UCHIZA)	AV. LAS PALMAS 04 S/N-INTERIOR DE LA UCHIZA	SANTA LUCIA (Antes Uchiza)	TOCACHE	TOCACHE	-8.340909	-76.387207	100M		0	1	1	0	1	RURAL	DIRANDRO	TIPO 1
94 9	CPNP SECTORIAL TOCACHE	JIRÓN FREDY ALIAGA # SN	TOCACHE	TOCACHE	TOCACHE	8.1883166 67	-76.51220167	100M		0	1	1	0	1	RURAL	B	TIPO 1
95 0	DESPICAR TOCACHE	JIRÓN SAN MARTIN # SN	TOCACHE	TOCACHE	TOCACHE	8.1911583 33	-76.51072333	100M		0	0	1	0	0	RURAL	CARRETERAS	TIPO 1
95 1	CPNP UCHIZA	AV. MARCELINO ALVAREZ # SN	UCHIZA	TOCACHE	TOCACHE	8.4505216 67	-76.46213167	100M		0	1	1	0	1	RURAL	C	TIPO 1
95 2	POSTA PNP SANTA LUCIA	AV. LAS PALMAS S/N	UCHIZA	TOCACHE	TOCACHE	-8.340989	-76.387246	100M		0	1	1	0	1	RURAL	POSTA MEDICA	TIPO 1
95 3	COMISARIA DE TURISMO SAN MARTIN	JR. TOMAS MEZA Nº 134	TARAPOTO	SAN MARTIN	SAN MARTIN	6.4841222 05	-76.36340723	100M		0	0	1	0	1	URBANO	AMBIENTE	TIPO 1
95 4	CPNP RURAL CANDARAVE	CALLE ARICA # 407	CANDARAVE	CANDARAVE	TACNA	17.271926	-70.25253667	100M		0	1	1	0	1	RURAL	B	TIPO 1
95 5	CPNP TOQUEPALA	OTRO SIN NOMBRE # SN	ILABAYA	JORGE BASADRE	TACNA	17.279301 66	-70.630985	100M		0	1	1	0	1	RURAL	B	TIPO 1
95 6	CPNP ITE	AV. PRINCIPAL # SN	ITE	JORGE BASADRE	TACNA	17.862473 33	-70.96418333	100M		0	1	1	0	1	RURAL	D	TIPO 1
95 7	CPNP LOCUMBA	CALLE SUCRE # SN	LOCUMBA	JORGE BASADRE	TACNA	17.611836 67	-70.76209667	100M		0	1	1	0	1	RURAL	C	TIPO 1
95 8	COMISARIA PNP ESPECIAL CAMIARA	CARRETERA PANAMERICANA SUR SN. KM 1204	LUCUMBA	JORGE BASADRE	TACNA	17.647509	-70.900123	100M		0	1	1	0	1	RURAL	COMISARIA	TIPO 1
95 9	CPNP ALTO DE LA ALIANZA	CALLE MARIANO SANTOS S/N	ALTO DE LA ALIANZA	TACNA	TACNA	17.987995	-70.24142667	100M		0	1	1	0	1	URBANO	C	TIPO 1

Handwritten signature and initials at the top left of the page.



Handwritten signature and initials in the middle left of the page.

96 0	CPNP CALANA	AV. GENERAL VARELA # SN	CALANA	TACNA	TACNA	17.940615	-70.1869567	100M			0	1	1	0	1	URBANO	D	TIPO 1
96 1	REGPOL TACNA	PASAJE CALDERON DE LA BARCA 353	CERCADO	TACNA	TACNA	18.010183	-70.249024	200M			0	1	1	0	1	URBANO	REGPOL	TIPO 1
96 2	CPNP CIUDAD NUEVA	CLL CASIMIRO ESPEJO SN	CIUDAD NUEVA	TACNA	TACNA	17.978906	-70.236505	100M			0	1	1	0	1	URBANO	B	TIPO 1
96 3	CPNP AEROPUERTO TACNA	OTRO PANAMERICANA SUR # SN	CORONEL GREGORIO ALBARRACIN LANCHIPA	TACNA	TACNA	18.049135	-70.27765	100M			0	1	1	0	0	RURAL	A	TIPO 1
96 4	CPNP CORONEL GREGORIO ALBARRACIN LANCHIPA	AV. MUNICIPAL # SN	CORONEL GREGORIO ALBARRACIN LANCHIPA	TACNA	TACNA	18.041941	-70.25118833	100M			0	1	1	0	2	RURAL	B	TIPO 1
96 5	DEPINCRI TACNA	ASOCIACION VIV 24 DE JUNIO MZ 4 LITE 02	CORONEL GREGORIO ALBARRACIN LANCHIPA	TACNA	TACNA	18.056467	-70.25492907	100M			0	1	1	0	2	URBANO	DIVINCRI	TIPO 1
96 6	CPNP SAMA INCLAN	AV. LAS VILCAS # SN	INCLAN	TACNA	TACNA	17.79488	-70.49471	100M			0	1	1	0	1	RURAL	C	TIPO 1
96 7	COMISARIA DE TURISMO PNP TACNA	AV. GRAU NRO. 57 CERCADO DE TACNA	TACNA	TACNA	TACNA	18.016811	-70.253939	100M			0	0	1	0	1	URBANO	TURISMO	TIPO 1
96 8	CPNP POCOLLAY	AV. CELESTINO VARGAS # 1145	POCOLLAY	TACNA	TACNA	17.99519	-70.22024333	100M			0	1	1	0	1	URBANO	C	TIPO 1
96 9	CPNP BOCCA DEL RIO	AV. GRAU SN	SAMA	TACNA	TACNA	18.158001	-70.67884	100M			0	1	1	0	1	RURAL	D	TIPO 1
97 0	CPNP SAMA LAS YARAS	AV. HEROES DE LA GUERRA DEL PACIFICO, CRUCE CA. SIMON BOLIVAR # SN	SAMA	TACNA	TACNA	17.862837	-70.560151	100M			0	1	1	0	1	RURAL	C	TIPO 1
97 1	DESPRAR BOCA DEL RIO	CARRETERA COSTANERA SUR # SN	SAMA	TACNA	TACNA	17.89716	-70.9693	100M			0	0	1	0	0	RURAL	CARRETERAS	TIPO 1
97 2	CPNP AUGUSTO B. LEGUIA	AV. 200 MILLAS CON CALLE JOSE GALVEZ SN	TACNA	TACNA	TACNA	18.03444	-70.27667	100M			0	1	1	0	1	URBANO	C	TIPO 1
97 3	CPNP CENTRAL TACNA	CALLE CALLAO # 121	TACNA	TACNA	TACNA	18.014794	-70.251762	100M			0	1	1	0	2	URBANO	A	TIPO 1
97 4	CPNP DE LA FAMILIA TACNA	AV. HIPOLITO UNANUE # 970	TACNA	TACNA	TACNA	18.007580	-70.25539041	100M			0	1	1	0	1	URBANO	FAMILIA	TIPO 1
97 5	CPNP GONZALES VIGIL	AV. INDUSTRIAL # SN	TACNA	TACNA	TACNA	17.997405	-70.24562985	100M			0	1	1	0	2	URBANO	A	TIPO 1
97 6	CPNP LA NATIVIDAD	CALLE 8 DE SEPTIEMBRE # 1937	TACNA	TACNA	TACNA	18.011672	-70.233148	100M			0	1	1	0	1	URBANO	B	TIPO 1
97 7	CPNP RURAL LA CONCORDIA	OTRO PANAMERICANA SUR # SN	TACNA	TACNA	TACNA	18.307723	-70.313745	100M			0	1	1	0	1	URBANO	A	TIPO 1
97 8	CPNP TERMINAL TERRESTRE MANUEL A. ODRIA	AV. HIPOLITO UNANUE # SN	TACNA	TACNA	TACNA	18.005458	-70.25773167	100M			0	1	1	0	1	URBANO	C	TIPO 1
97 9	DESPRAR TACNA	AV. MANUEL A. ODRIA S/N	TACNA	TACNA	TACNA	18.026376	-70.261768	100M			0	0	1	0	0	URBANO	CARRETERAS	TIPO 1
98 0	DIRECOR TACNA	URB VILLA DEL SOL MZ CI LOTE 11 CENTRO POBLADO LA NATIVIDAD	TACNA	TACNA	TACNA	18.016749	-70.236578	100M			0	1	1	0	1	URBANO	DIRECOR	TIPO 1
98 1	DIVINCRI TACNA	AV. TOMAS MARZANO S/N CON INTERSECCION AV. LIBERTADORA	TACNA	TACNA	TACNA	18.056493	-70.254795	100M			0	1	1	0	2	URBANO	DIVINCRI	TIPO 1
98 2	OFICRI TACNA	AV. ARIAS Y ARAGONES S/N	TACNA	TACNA	TACNA	18.002836	-70.257759	100M			0	1	1	0	1	URBANO	OFICRI	TIPO 1
98 3	POL PNP TACNA	CALLE BLONDELL 110	TACNA	TACNA	TACNA	18.015675	-70.254338	100M			0	1	1	0	1	URBANO	POLICINICO	TIPO 1
85 2	CP MAY ROBERTO MORALES ROJAS /DIVINCRI/OFICRI/DIVANDRO/DEPROVE	AV. PROLONGACION SANCHEZ CERRO S/N CARRETERA PIURA SULLANA. S/N	PIURA	PIURA	PIURA	-5.185024	-80.647686	400M		1	1	0	1	0	3	URBANO	COMPLEJO 1	TIPO 2



98 5	CPNP RURAL TARATA	CALLE PRIMERO DE SETIEMBRE # SN	TARATA	TARATA	TACNA	17.472548 33	-70.03111833	100M			0	1	1	1	0	1	RURAL	B	TIPO 1
98 6	CPNP SECTORIAL ZORRITOS	AV. REPUBLICA DEL PERU # SN	ZORRITOS	CONTRALMIRANTE VILLAR	TUMBES	-3.68048	-80.675705	100M			0	1	1	1	0	1	URBANO	B	TIPO 1
98 7	CPNP CORRALES	CALLE SAN PEDRO # 600	CORRALES	TUMBES	TUMBES	3.6018166 67	-80.48098833	100M			0	1	1	1	0	1	URBANO	B	TIPO 1
98 8	CPNP LA CRUZ	AV. PIURA # 422	LA CRUZ	TUMBES	TUMBES	-3.637655	-80.59257167	100M			0	1	1	1	0	1	URBANO	C	TIPO 1
98 9	COMISARIA DE TURISMO TUMBES	CARRETERA PANAMERICANA NORTE KM. 4.5 (INTERIOR DE LA EX-ESTPP- TUMBES)	TUMBES	TUMBES	TUMBES	3.5536244 66	-80.42995158	100M			0	0	1	1	0	1	URBANO	TURISMO	TIPO 1
92 4	CP PNP WALTER JIMENEZ/ COM CAR MOYOBAMBA /DIRCOCOR /DIVINCRI	JR. CRNL. SECADA 113	MOYOBAMBA	MOYOBAMBA	SAN MARTIN	-6.038881	-76.97029	200M		1	1	0	1	1	0	3	URBANO	COMPLEJO 1	TIPO 2
99 1	CPNP ANDRES ARAUJO MORAN	CLL. MAXIMILIANO MORAN SN MZ.18 LT. SN	TUMBES	TUMBES	TUMBES	3.5600516 67	-80.42805833	100M			0	1	1	1	0	1	URBANO	C	TIPO 1
99 2	CPNP DE LA FAMILIA TUMBES	AV. TUPAC AMARU # SN	TUMBES	TUMBES	TUMBES	3.5726066 67	-80.45198333	100M			0	1	1	1	0	1	URBANO	FAMILIA	TIPO 1
99 3	CPNP EL TABLAZO	CALLE HILARIO CARRASCO # 515	TUMBES	TUMBES	TUMBES	3.5682816 67	-80.450175	100M			0	1	1	1	0	1	URBANO	C	TIPO 1
99 4	CPNP PUERTO PIZARRO	CALLE JOSE OLAYA # 202	TUMBES	TUMBES	TUMBES	3.5030216 67	-80.39119833	100M			0	1	1	1	0	1	URBANO	C	TIPO 1
99 5	CPNP SAN JOSE - TUMBES	CALLE ZARUMILLA # 301	TUMBES	TUMBES	TUMBES	3.5629883 33	-80.460245	100M			0	1	1	1	0	2	URBANO	A	TIPO 1
99 6	CP Tnte JORGE TAPE TARAZONA (DIVTRAN DIVINCRI DIVANDRO	AV. PANAMERICANA NORTE KM 1322	TUMBES	TUMBES	TUMBES	-3.555376	-80.437942	200M			2	0	1	1	0	3	URBANO	COMPLEJO 1	TIPO 1
99 7	REGPOL TUMBES	AV. PANAMERICANA NORTE S/N 1033	TUMBES	TUMBES	TUMBES	-3.557394	-80.451689	200M			1	0	1	1	0	1	URBANO	FRENTE	TIPO 1
99 8	POL PNP TUMBES	AV. TUMBES 706 (AV. TUMBES CON AV. JOSE OLAYA)	TUMBES	TUMBES	TUMBES	-3.565518	-80.457418	100M			0	1	1	1	0	1	URBANO	POLICLINICO	TIPO 1
99 9	CPNP AGUAS VERDES	AV. REPUBLICA DEL PERU # 254	AGUAS VERDES	ZARUMILLA	TUMBES	3.4816318 16	-80.24548441	100M			0	1	1	1	0	1	URBANO	C	TIPO 1
10 0	CEBAF - CONTROL POLICIAL ZARUMILLA	PAN.NORT KM 1268 (4KM DE FRONT ECUADOR)	ZARUMILLA	ZARUMILLA	TUMBES	-3.510765	-80.2750539	100M			0	0	1	1	0	1	URBANO	CEBAF	TIPO 1
10 01	CPNP ZARUMILLA	CALLE TUMBES # 304	ZARUMILLA	ZARUMILLA	TUMBES	-3.50163	-80.27586167	100M			0	1	1	1	0	2	URBANO	A	TIPO 1
10 02	BRECC-LIMA NORTE	JR. ANDRÉS TORRES PAZ N° 116 - URBANIZACIÓN CONDEVILLA SEÑOR	SAN MARTIN DE PORRES	LIMA	LIMA	12.018940	-77.088923	100M			0	1	1	1	0	0	RURAL	E	TIPO 1
10 03	CP SOTL PNP ARTEMIO SANCHEZ PAREDES DIVINCRI/OFCRI PUCALLPA	AV. 9 DE OCTUBRE N°167	CALLERIA	CORONEL PORTILLO	UCAYALI	8.3877901	-74.5444298	200M	1		2	0	1	1	0	3	URBANO	COMPLEJO 1	TIPO 2
10 04	CPNP PUCALLPA	JIRÓN INDEPENDENCIA # 360	CALLERIA	CORONEL PORTILLO	UCAYALI	8.3821193 9	-74.53240871	100M			0	1	1	1	0	2	URBANO	A	TIPO 1
10 05	POL PNP PUCALLPA	JR. SUCRE CDA 4 S/N	CALLERIA	CORONEL PORTILLO	UCAYALI	-8.383793	-74.531983	100M			0	1	1	1	0	1	URBANO	POLICLINICO	TIPO 1
10 06	REGPOL UCAYALI	AV. SAN MARTIN 466	CALLERIA	CORONEL PORTILLO	UCAYALI	-8.384316	-74.531174	150M			0	1	1	1	0	1	URBANO	REGPOL	TIPO 1
10 07	CPNP CAMPO VERDE/COM CAR CAMPO VERDE	AV. 1 DE JUNIO # SN	CAMPOVERDE	CORONEL PORTILLO	UCAYALI	8.4757438 49	-74.80449468	100M			0	1	1	1	0	1	URBANO	C	TIPO 1
10 08	CPNP SAN FERNANDO (MANANTAY)	JIRÓN LOS MANGOS # 572	MANANTAY	CORONEL PORTILLO	UCAYALI	-8.39809	-74.536905	100M			0	1	1	1	0	1	RURAL	B	TIPO 1

[Handwritten signature]



[Handwritten signature]

[Handwritten signature]

10 09	COMISARIA DE TURISMO UCAYALI	AA. HH. FAUSTINO MALDONADO MZ. D LT. 7 - YARINACCOCHA	YARINACCOCHA	CORONEL PORTILLO	UCAYALI	-8.378077	-74.558173	100M				0	0	1	0	1	0	1	URBANO	TURISMO	TIPO 1
10 10	CPNP YARINACCOCHA	AV. YARINACCOCHA # 376	YARINACCOCHA	CORONEL PORTILLO	UCAYALI	8.3550349 15	-74.57652166	100M				0	1	1	0	1	0	1	URBANO	B	TIPO 1
10 11	DEP. UNIDAD DESCONCENTRADO DE PROTECCION DEL MEDIO AMBIENTE	CARRETERA FEDERICO BASADRE 10.5	YARINACCOCHA	CORONEL PORTILLO	UCAYALI	-8.401911	-74.619968	100M				0	0	1	0	1	0	1	URBANO	MEDIO AMBIENTE	TIPO 1
10 12	RQ. AEROPUERTO CAP. FAP DAVID ABENSUR RENGIFO	CARRETERA FEDERICO BASADRE	YARINACCOCHA	CORONEL PORTILLO	UCAYALI	-8.384974	-74.573885	100M				0	1	1	0	1	0	1	URBANO	RQ	TIPO 1
10 13	CPNP ALEXANDER VON HUMBOLDT	CARRETERA REGIONAL FEDERICO BASADRE # SN	IRAZOLA	PADRE ABAD	UCAYALI	-8.82504	-75.05160833	100M				0	1	1	0	1	0	1	RURAL	B	TIPO 1
10 14	CPNP NESHUYA HUALLAGA	CARRETERA FEDERICO BASADRE # SN	IRAZOLA	PADRE ABAD	UCAYALI	8.6422016 67	-74.96223167	100M				0	1	1	0	1	0	1	RURAL	C	TIPO 1
10 15	CPNP SAN ALEJANDRO	CALLE REGIONAL FEDERICO BASADRE # SN	IRAZOLA	PADRE ABAD	UCAYALI	-8.82949	-75.21611667	100M				0	1	1	0	1	0	1	RURAL	C	TIPO 1
10 16	DESPRACAR VON HUMBOLT	AV. 1 DE JUNIO # SN	IRAZOLA	PADRE ABAD	UCAYALI	8.8251259 05	-75.05201966	100M				0	0	1	0	1	0	0	RURAL	CARRETERAS	TIPO 1
10 17	CPNP SECTORIAL PADRE ABAD - AGUAYTIA/COM CAR AGUAYTIA	CARRETERA FEDERICO BASADRE KM 162 - AGUAYTIA	PADRE ABAD	PADRE ABAD	UCAYALI	-9.037733	-75.5069754	100M				0	1	1	0	1	0	1	RURAL	B	TIPO 1
10 18	CPNP SECTORIAL UCAYALI CONTAMANA	CALLE MANUEL E. ROJAS # 315	CONTAMANA	UCAYALI	UCAYALI	7.3497916 67	-75.00849833	100M				0	1	1	0	1	0	2	RURAL	B	TIPO 1

13 30 137 891 02 28

ANEXO A1 CIRCUITOS DE DATACENTER

Handwritten signatures and initials at the top left of the page.



Handwritten initials and a large 'D' mark on the left side of the page.

Nº	SEDE	DIRECCION ACTUAL	DISTRITO	PROVINCIA	DEPARTAMENTO	LATITUD	LONGITUD	ANCHO DE BANDA	Zonificación II	TIPO DE UNIDAD
1	DATACENTER MININTER(PRINCIPAL) INTERNET	Av. Canaval y Moreyra S/N cuadra 7 - San Isidro	San Isidro	LIMA	LIMA	- 12.0980545	- 77.0154904	2000M	URBANO	DATACENTER
2	DATACENTER MININTER(PRINCIPAL) IPV/PN INTRANET 5GB	Av. Canaval y Moreyra S/N cuadra 7 - San Isidro	San Isidro	LIMA	LIMA	- 12.0980545	- 77.0154904	5000M	URBANO	DATACENTER
3	DATACENTER MININTER(RESPALDO) INTERNET	Av. Canaval y Moreyra S/N cuadra 7 - San Isidro	San Isidro	LIMA	LIMA	- 12.0980545	- 77.0154904	2000M	URBANO	DATACENTER
4	DATACENTER MININTER(RESPALDO) IPV/PN INTRANET 5GB	Av. Canaval y Moreyra S/N cuadra 7 - San Isidro	San Isidro	LIMA	LIMA	- 12.0980545	- 77.0154904	5000M	URBANO	DATACENTER
5	DATACENTER SAN ISIDRO (PRINCIPAL) INTERNET	Ricardo Angulo s/n SAN ISIDRO (PROPUESTO POR EL CONTRATISTA)	San Isidro	LIMA	LIMA	-12.085231	-76.97244	2000M	URBANO	DATACENTER

6	DATACENTER SAN ISIDRO (PRINCIPAL) IPV/PN INTRANET 5GB	Ricardo Angulo s/n SAN ISIDRO (PROPUESTO POR EL CONTRATISTA)	San Isidro	LIMA	LIMA	-12.085231	-76.97244	5000M	URBANO	DATACENTER
7	DATACENTER SAN ISIDRO (RESPALDO) INTERNET	Ricardo Angulo s/n SAN ISIDRO (PROPUESTO POR EL CONTRATISTA)	San Isidro	LIMA	LIMA	-12.085231	-76.97244	2000M	URBANO	DATACENTER
8	DATACENTER SAN ISIDRO (RESPALDO) IPV/PN INTRANET 5GB	Ricardo Angulo s/n SAN ISIDRO (PROPUESTO POR EL CONTRATISTA)	San Isidro	LIMA	LIMA	-12.085231	-76.97244	5000M	URBANO	DATACENTER

ANEXO B1 975 SEDES TIPO 1

N°	SEDE	DIRECCIÓN ACTUAL	DISTRITO	PROVINCIA	DPTO	LATITUD	LONGITUD	ANCHO BANDA	SWITCH CORE LAN Y GABINETE PRINCIPAL	SWITCH LAN 48 PUERTO S Y GABINETE PRINCIPAL	SWITCH LAN DE 48 PUERTOS Y GABINETE DE DISTRIBUCION	SWITCH LAN DE 24 PUERTOS Y GABINETE PRINCIPAL	FIREWALL	FIREWALL DE PROXIMA GENERACION	N° DE ACCESOS	Zonificación	TIPO DE UNIDAD	TIPO
1	CPNP SECTORIAL BAGUA	AV. HEROES DEL CENEPA # 1000	BAGUA	BAGUA	AMAZONAS	-5.638949	-78.531008	100M			0	1	1	0	2	URBANO	B	TIPO 1
2	CPNP SECTORIAL JAZAN	AV. MARGINAL # 121	JAZAN	BONGARA	AMAZONAS	222291	-77.978215	100M			0	1	1	0	2	URBANO	B	TIPO 1
3	DESPRICAR PEDRO RUIZ GALLO	CARRITERA FERNANDO BELAUDE TERRY # SN	JAZAN	BONGARA	AMAZONAS	-5.941878	-77.976206	100M			0	0	1	0	0	URBANO	CARRITERAS	TIPO 1
4	COMISARIA DE TURISMO AMAZONAS - COMITUR AMAZONAS	JR. PUNO N° 571 - CHACHAPOYAS	CHACHAPOYAS	CHACHAPOYAS	AMAZONAS	-6.22949471	-77.8754326	100M			0	0	1	0	1	URBANO	TURISMO	TIPO 1
5	CPNP SECTORIAL CHACHAPOYAS / OFICRI	JIRÓN AMAZONAS # 1220	CHACHAPOYAS	CHACHAPOYAS	AMAZONAS	-6.229875	-77.874661	100M			0	1	1	0	3	URBANO	A	TIPO 1
6	DIRCOCOR AMAZONAS	JR. LIBERTAD N° 1353-1357	CHACHAPOYAS	CHACHAPOYAS	AMAZONAS	-6.228768	-77.875471	100M			0	1	1	0	1	URBANO	DIRCOCOR	TIPO 1
7	DIV MEDIO AMBIENTE(DIV.UNI.ESP.)	JR. SANTO DOMINGO 876	CHACHAPOYAS	CHACHAPOYAS	AMAZONAS	-6.232306	-77.874628	100M			0	0	1	0	1	URBANO	AMBIENTE	TIPO 1
8	CPNP SECTORIAL LAMUD	JIRÓN GRAU # 451	LAMUD	LUYA	AMAZONAS	6.139210704	-77.95205555	100M			0	1	1	0	1	URBANO	B	TIPO 1
9	CPNP LUYA - CRUZ SANTIAGO VALQUI OROSCO	JIRÓN SAN MARTIN # 910	LUYA	LUYA	AMAZONAS	6.163343333	-77.94431667	100M			0	1	1	0	1	URBANO	C	TIPO 1
10	CPNP SECTORIAL SAN NICOLAS	JIRÓN HUAMBO # 316	SAN NICOLAS	RODRIGUEZ DE MENDOZA	AMAZONAS	6.394868333	-77.4827833	100M			0	1	1	0	1	URBANO	B	TIPO 1
11	CP UTUBAMBABA- CPNP SECTORIAL UTUBAMBABA (o BAGUA GRANDE)/POLICINICO BAGUA GRANDE/DEPINCRI BAGUA GRANDE	AV. CHACHAPOYAS 2318	BAGUA GRANDE	UTCUBAMBABA	AMAZONAS	5.757451667	-78.44050833	400M			2	1	1	1	0	URBANO	UNIDAD PNP	TIPO 1
12	CPNP CAJARURO	JIRÓN EL COMERCIO # 407	CAJARURO	UTCUBAMBABA	AMAZONAS	-5.73741	-78.42963	100M			0	1	1	1	0	URBANO	D	TIPO 1
13	CPNP SECTORIAL AUA	AV. TUPAC AMARU - PEDRO PABLO ATUSPARIA # SN	AUA	AUA	ANCASH	-9.78324	-77.60937667	100M			0	1	1	0	1	RURAL	C	TIPO 1
14	CPNP SECTORIAL ASUNCION - CHACAS	JIRÓN RAYMONDI # SN	CHACAS	ASUNCION	ANCASH	-9.16347	-77.36637833	100M			0	1	1	0	1	RURAL	C	TIPO 1
15	CPNP SECTORIAL BOLOGNESI CHIQUEJAN	JIRÓN COMERCIO # SN	CHIQUEJAN	BOLOGNESI	ANCASH	-10.154715	-77.15747667	100M			0	1	1	0	1	RURAL	B	TIPO 1
16	CPNP SECTORIAL CARHUAZ	JIRÓN RIO BUIN # SN	CARHUAZ	CARHUAZ	ANCASH	-9.282405	-77.64595333	100M			0	1	1	0	1	URBANO	B	TIPO 1
17	CPNP SECTORIAL SAN LUIS	JIRÓN DANIEL ALCIDES CARRION # 310	SAN LUIS	CARLOS FERMIN FITZCARRALD	ANCASH	-9.0946	-77.33010167	100M			0	1	1	0	1	RURAL	C	TIPO 1
18	CPNP SECTORIAL CASMA/DESPRAR CASMA	AV. MAGDALENA SN. CASMA	CASMA	CASMA	ANCASH	9.475601667	-78.30602667	100M			0	1	1	0	2	URBANO	A	TIPO 1
19	CPNP YAUTAN	AV. CASMA S/N MZ 1 LT.1	YAUTAN	CASMA	ANCASH	9.511861667	-77.96693167	100M			0	1	1	0	1	RURAL	C	TIPO 1
20	DIV. POL. CHIMBOTE	JR. LEONCIO PRADO 401 -CERCADO	CERCADO	CHIMBOTE	ANCASH	-9.0739664	-78.5937685	100M			0	1	1	0	1	URBANO	DIVPOL	TIPO 1
21	CPNP SECTORIAL CORONGO	JIRÓN LIMA # SN	CORONGO	CORONGO	ANCASH	8.570581667	-77.89895167	100M			0	1	1	0	1	RURAL	B	TIPO 1
22	CPNP HUARAZ	JIRÓN JOSE DE SUCRE # SN	HUARAZ	HUARAZ	ANCASH	9.52948343	-77.52987184	100M			0	1	1	0	1	URBANO	A	TIPO 1
23	CPNP SAN GERONIMO	AV. FRANCISCO BOLOGNESI # SN	HUARAZ	HUARAZ	ANCASH	9.527095667	-77.535495	100M			0	1	1	0	1	URBANO	C	TIPO 1

Handwritten signature and initials at the top left of the page.



2	CPNP TACLAN	CARRETERA PENETRACION PATIVILCA HUARAZ # SN	HUARAZ	HUARAZ	ANCASH	-9.542485	-77.593225	100M			0	1	1	0	1	URBANO	C	TIPO
4	REGPOL ANCASH	JIRON 28 DE JULIO 755	HUARAZ	HUARAZ	ANCASH	-9.53109	-77.52825	200M			0	1	1	0	1	URBANO	REGPOL	TIPO
5	COMISARIA DE TURISMO HUARAZ	JR. MARIANO MELGAR N° 453-CENTENARIO	INDEPENDENCIA	HUARAZ	ANCASH	-9.519668	-77.527482	100M			0	0	1	0	1	URBANO	TURISMO	TIPO
6	CPNP PARIACOTO	JR. GONZALO SALAZAR MIGUEL A MORAN SN	PARIACOTO	HUARAZ	ANCASH	9.559716667	-77.89026167	100M			0	1	1	0	1	RURAL	C	TIPO
7	CPNP RURAL CHAVIN DE HUANTAR	JIRON 17 DE ENERO # SN	CHAVIN DE HUANTAR	HUARI	ANCASH	9.583558333	-77.17781167	100M			0	1	1	0	1	RURAL	C	TIPO
8	CPNP RURAL CHAVIN DE HUANTAR	JR. ANCASH CDRA.10 Y JR. ELIAZAR	CHAVIN DE HUANTAR	HUARI	ANCASH	-9.348804	-77.173099	100M			0	1	1	0	2	RURAL	B	TIPO
9	CPNP RURAL CHAVIN DE HUANTAR	JR. LAS FLORES S/N CHAVIN DE HUANTAR (COSO TAURINO)	HUARI	HUARI	ANCASH	-9.382573	-77.177715	100M			0	0	1	0	0	RURAL	CARRERE RAS	TIPO
0	CPNP RURAL SAN MARCOS	JIRON GRAU # SN	SAN MARCOS	HUARI	ANCASH	9.52951667	-77.15768167	100M			0	1	1	0	1	RURAL	C	TIPO
1	CPNP RURAL HUARMEY	AV. CABO ALBERTO REYES # 224	HUARMEY	HUARMEY	ANCASH	10.06908947	-78.15456972	100M			0	1	1	0	2	URBANO	A	TIPO
2	CPNP CAÑON DEL PATO HUALLANCA	AV. 14 DE ABRIL # 171	HUALLANCA	HUAYLAS	ANCASH	-8.81843	-77.86193	100M			0	1	1	0	1	RURAL	DIRCOCO R	TIPO
3	CPNP SECTORIAL MARISCAL LUZURIAGA - PISCOBAMBA	JIRON MARISCAL LUZURIAGA # 125	PISCOBAMBA	MARISCAL LUZURIAGA	ANCASH	8.858379662	-77.35507965	100M			0	1	1	0	1	RURAL	C	TIPO
4	CPNP SECTORIAL CABANA	CALLE PLAZA DE ARMAS # SN	CABANA	PALLASCA	ANCASH	-8.3931431	-78.0087637	100M			0	1	1	0	1	RURAL	B	TIPO
5	CPNP SECTORIAL POMABAMBA	OTRO PLAZUELA CONVENTO # SN	POMABAMBA	POMABAMBA	ANCASH	8.819455031	-77.46140309	100M			0	1	1	0	1	RURAL	B	TIPO
6	CPNP CATAC	AV. 31 DE MAYO SN	CATAC	RECUAY	ANCASH	9.797966667	-77.432525	100M			0	1	1	0	1	URBANO	C	TIPO
7	DESPRCAR CATAC	AV. 31 DE MAYO # SN	CATAC	RECUAY	ANCASH	9.801463333	-77.43131333	100M			0	1	1	0	2	URBANO	B	TIPO
8	CPNP SECTORIAL RECUAY	JIRON LA SOLEDAD # SN	RECUAY	RECUAY	ANCASH	9.718889184	-77.45635986	100M			0	0	1	0	0	URBANO	CARRERE RAS	TIPO
9	COMISARIA DE TURISMO CHIMBOTE	JR. TUPAC AMARU MZ 8 LT. 9 (URBANIZACION LA LIBERTAD)	CHIMBOTE	SANTA	ANCASH	-9.09608	-78.56856	100M			0	0	1	0	1	URBANO	TURISMO	TIPO
0	DIVPOL CHIMBOTE	JIRON LEONCIO PRADO N° 401	CHIMBOTE	SANTA	ANCASH	9.073778977	-78.59377898	100M			0	1	1	0	1	URBANO	DIVPOL	TIPO
1	CPNP 21 DE ABRIL	AV. JOSE BALTA CDR 11. UR 21 DE ABRIL ZN :B. CHIMBOTE	CHIMBOTE	SANTA	ANCASH	9.068136667	-78.5892833	100M			0	1	1	0	2	URBANO	A	TIPO
2	CPNP ALTO PERU	JR. MOQUEGUA S/N CDR-9 AH :ALTO PERU. CHIMBOTE	CHIMBOTE	SANTA	ANCASH	-9.07828	-78.57349	100M			0	1	1	0	1	URBANO	B	TIPO
3	CPNP CHIMBOTE	AV. VICTOR RAUL HAYA DE LA TORRE # 296	CHIMBOTE	SANTA	ANCASH	9.073206448	-78.59978288	100M			0	1	1	0	2	URBANO	A	TIPO
4	CPNP LA LIBERTAD	AV. ENRIQUE MEIGES # 1535	CHIMBOTE	SANTA	ANCASH	9.088788333	-78.57503833	100M			0	1	1	0	2	URBANO	A	TIPO
5	CPNP RINCONADA	AV. VICTOR RAUL HAYA DE LA TORRE SN MZ. LT.3	CHIMBOTE	SANTA	ANCASH	-8.8932039	-78.562873	100M			0	0	1	0	1	URBANO		TIPO
6	CPNP SAN PEDRO CHIMBOTE	CLL LOS ALAMOS SN MZ Y1 LT.9	CHIMBOTE	SANTA	ANCASH	-9.0490582	-78.586830	100M			0	1	1	0	2	URBANO	COMISARI A	TIPO
7	CPNP TAMBO REAL	AV. AMERICAS S/N CASERIO TAMBO REAL NUEVO	CHIMBOTE	SANTA	ANCASH	-8.9649342	-78.55519	100M			0	1	1	0	0	URBANO	E	TIPO
8	CP SANTA ROSA DE LIMA /OFICRI AREQUIPA	AV. GOYENECHE 317	CERCADO	AREQUIPA	AREQUIPA	-16.400265	-71.526808	150M			0	1	1	0	4	URBANO	UNIDAD PNP	TIPO
9	DEPINCRI CHIMBOTE	JR. LADISLAO ESPINAR 181	CHIMBOTE	SANTA	ANCASH	-9.0722173	-78.5958651	100M			0	1	1	0	1	URBANO	DIVINCRI	TIPO
0	POL PNP CHIMBOTE	AV. PARDO 292	CHIMBOTE	SANTA	ANCASH	-8.073091	-78.599419	100M			0	1	1	0	1	URBANO	POLICINI CO	TIPO

[Handwritten signatures and marks]



[Handwritten initials and marks]

5	CPNP COISHCO	AV. PANAMERICANA ANTIGUA # 410	COISHCO	SANTA	ANCASH	-9.0207799	-78.6152822	100M			0	1	1	0	1	1	0	1	URBANO	C	TIPO 1
2																			RURAL	C	TIPO 1
3	CPNP NEPEÑA	CLL HIPOLITO UNANUE SN MZA LT.8	NEPEÑA	SANTA	ANCASH	-9.172025	-78.361235	100M			0	1	1	0	1	1	0	1	RURAL	C	TIPO 1
5	CPNP SAN JACINTO ANCASH	AV. PROGRESO SN	NEPEÑA	SANTA	ANCASH	-9.15164	-78.27908167	100M			0	1	1	0	1	1	0	1	RURAL	C	TIPO 1
4																			URBANO	FAMILIA	TIPO 1
5	CPNP DE LA FAMILIA CHIMBOTE	CENTRO CIVICO SECTOR 74-75 MZ.-D. LOTE 02 - NVO. CHIMBOTE-SANTA	NEPEÑA	SANTA	ANCASH	9.127328333	-78.52199167	100M			0	1	1	0	1	1	0	2	URBANO	A	TIPO 1
5	CPNP SECTORIAL BUENOS AIRES	AV. PACIFICO SN MZ.E LT.45	NEPEÑA	SANTA	ANCASH	9.128121667	-78.52114	100M			0	1	1	0	1	1	0	2	URBANO	B	TIPO 1
7	CPNP VILLA MARIA / OFICRI	JR. LOS ANGELES CRUCE CON CALLE INDEPENDENCIA	NEPEÑA	SANTA	ANCASH	9.117028333	-78.54481667	150M			0	1	1	0	1	1	0	2	URBANO	CARRETE RAS	TIPO 1
5	DESPRCAR CHIMBOTE	JIRÓN NEPEÑA # 100	NEPEÑA	SANTA	ANCASH	9.126596667	-78.52760333	100M			0	1	1	0	1	1	0	0	URBANO	C	TIPO 1
8											0	1	1	0	1	1	0	1	URBANO	C	TIPO 1
5	CPNP SAMANCO	JIRÓN PASCUAL CORCINO CUETO # 237	SAMANCO	SANTA	ANCASH	9.261633333	-78.49572167	100M			0	1	1	0	1	1	0	1	URBANO	B	TIPO 1
9											0	1	1	0	1	1	0	1	URBANO	C	TIPO 1
0	CPNP SECTORIAL SANTA	JIRÓN UCAVALI # 142	SANTA	SANTA	ANCASH	8.997081667	-78.61310667	100M			0	1	1	0	1	1	0	1	URBANO	B	TIPO 1
6	CPNP SECTORIAL SIHUAS	JIRÓN SAN MARTIN # 130	SIHUAS	SIHUAS	ANCASH	8.554286261	-77.63150007	100M			0	1	1	0	1	1	0	1	RURAL	C	TIPO 1
1											0	1	1	0	1	1	0	1	RURAL	C	TIPO 1
6	DESPRCAR SIHUAS	JIRÓN LAS PONCIANAS # 240	SIHUAS	SIHUAS	ANCASH	-8.553275	-77.63134	100M			0	1	1	0	1	1	0	0	RURAL	CARRETE RAS	TIPO 1
2											0	1	1	0	1	1	0	2	URBANO	B	TIPO 1
6	CPNP SECTORIAL YUNGAY	AV. 28 DE JULIO Y ARIAS GRACIANI # SN	YUNGAY	YUNGAY	ANCASH	-9.14086	-77.74472333	100M			0	1	1	0	1	1	0	3	URBANO	C	TIPO 1
3											0	1	1	0	1	1	0	1	URBANO	C	TIPO 1
4	CPNP ABANCAY/DEPINCRI/OFICRI	JIRÓN HUANCABAMBA # 215	ABANCAY	ABANCAY	APURIMAC	13.63663333	-72.87791167	150M			0	1	1	0	1	1	0	1	URBANO	C	TIPO 1
5	CPNP BELLA VISTA ABANCAY	AV. PANAMERICANA # 1600	ABANCAY	ABANCAY	APURIMAC	-13.63669	-72.8771667	100M			0	1	1	0	1	1	0	1	URBANO	C	TIPO 1
6	CPNP FAMILIA DE ABANCAY	JIRÓN LIMA # 1000	ABANCAY	ABANCAY	APURIMAC	13.63595167	-72.88465833	200M			0	1	1	0	1	1	0	1	URBANO	FRENTE Y FAMILIA	TIPO 1
6											0	1	1	0	1	1	0	1	URBANO	D	TIPO 1
7	CPNP VILLA ANIPAY	AV. MAGISTERIAL S/N, CENTRO POBLADO PUEBLO JOVEN, AV PERU REF. PARQUE PIQUICHA	ABANCAY	ABANCAY	APURIMAC	-13.631715	-72.88478333	100M			0	1	1	0	1	1	0	1	RURAL	D	TIPO 1
6	INSPECTORIA / OFICINA DE DISCIPLINA ABANCAY	AV. BELLA ABANCAY # 409	ABANCAY	ABANCAY	APURIMAC	-13.633577	-72.867265	100M			0	1	1	0	1	1	0	1	URBANO	UNIDAD	TIPO 1
8											0	1	1	0	1	1	0	1	URBANO	MEDIO AMBIENT E	TIPO 1
9	MEDIO AMBIENTE	PROLONGACION CUSCO A-12	ABANCAY	ABANCAY	APURIMAC	-13.627745	-72.878455	100M			0	1	1	0	1	1	0	1	URBANO	REGPOL	TIPO 1
7	REGPOL APURIMAC / OFITIC ABANCAY	JR LIMA N° 1000	ABANCAY	ABANCAY	APURIMAC	-13.63587	-72.88447	150M			0	1	1	0	1	1	0	1	URBANO	D	TIPO 1
7	CPNP TAMBURCO	AV. 14 DE SETIEMBRE / SN	TAMBURCO	ABANCAY	APURIMAC	13.62245941	72°52'34.0	100M			0	1	1	0	1	1	0	1	URBANO	A	TIPO 1
1											0	1	1	0	1	1	0	2	RURAL	E	TIPO 1
2	CPNP ANDAHUAYLAS	AV. PERU # 198	ANDAHUAYLAS	ANDAHUAYLAS	APURIMAC	-13.656515	-73.384836	100M			0	1	1	0	1	1	0	0	RURAL	E	TIPO 1
7	CPNP HUANCABAMBA ANDAHUAYLAS	AV. HUANCABAMBA # SN	ANDAHUAYLAS	ANDAHUAYLAS	APURIMAC	13.72987333	-73.35364167	100M			0	1	1	0	1	1	0	0	RURAL	CARRETE RAS	TIPO 1
3											0	1	1	0	1	1	0	0	RURAL	FAMILIA	TIPO 1
7	DESPRCAR ANDAHUAYLAS	AV. SEQUICENTENARIO # 1845	ANDAHUAYLAS	ANDAHUAYLAS	APURIMAC	-13.655235	-73.41374833	100M			0	1	1	0	1	1	0	1	URBANO	C	TIPO 1
4											0	1	1	0	1	1	0	1	RURAL	D	TIPO 1
7	CPNP FAMILIA ANDAHUAYLAS	JR. CARMEN N° 542	SAN JERONIMO	ANDAHUAYLAS	APURIMAC	-13.653143	-73.370081	100M			0	1	1	0	1	1	0	1	URBANO	E	TIPO 1
5											0	1	1	0	1	1	0	1	RURAL	C	TIPO 1
7	CPNP SAN JERONIMO ANDAHUAYLAS	AV. ALFONSO UGARTE # 112	SAN JERONIMO	ANDAHUAYLAS	APURIMAC	13.65179167	-73.36528167	100M			0	1	1	0	1	1	0	1	URBANO	D	TIPO 1
6											0	1	1	0	1	1	0	1	URBANO	E	TIPO 1
7	CPNP TALAVERA	AV. MANCO CAPAC # 505	TALAVERA	ANDAHUAYLAS	APURIMAC	-13.656250	-73.43043667	100M			0	1	1	0	1	1	0	0	URBANO	E	TIPO 1
7	CPNP ANTABAMBA	JIRÓN APURIMAC # SN	ANTABAMBA	ANTABAMBA	APURIMAC	-14.366306	-72.876796	100M			0	1	1	0	1	1	0	0	URBANO	E	TIPO 1

A handwritten signature 'D. H. H.' in dark ink, with a circular stamp or seal to its left. The signature is written in a cursive style. The stamp is a simple circle with some internal texture, possibly a wax seal or a printed mark.

[Handwritten signature]



[Handwritten signature]

1	CPNP HUNTER	AV. BRASILIA # 305	JACOBO HUNTER	AREQUIPA	AREQUIPA	-16.44152	-71.55491667	100M			0	1	1	0	1	URBANO	B	TIPO 1
5	DESPECAR AREQUIPA	AV. ANDRES AVELINO CACERES # SN	JACOBO HUNTER	AREQUIPA	AREQUIPA	16.42354076	-71.54548642	100M			0	0	1	0	0	URBANO	CARRETE RAS	TIPO 1
6	CPNP JOSE LUIS BUSTAMANTE Y RIVERO	URB. QUINTA TRISTÁN MZ Y LT. 2	JOSE LUIS BUSTAMANTE Y RIVERO	AREQUIPA	AREQUIPA	-16.42431	-71.529565	100M			0	1	1	0	1	URBANO	B	TIPO 1
7	CPNP SIMÓN BOLÍVAR	AV. CARACAS # 629	JOSE LUIS BUSTAMANTE Y RIVERO	AREQUIPA	AREQUIPA	16.44343167	-71.513685	100M			0	1	1	0	1	URBANO	B	TIPO 1
8	CPNP EL TRIUNFO	CLL. MIGUEL GRAU SN MZ D LT. 4	LA JOYA	AREQUIPA	AREQUIPA	16.49643333	-71.83764	100M			0	1	1	0	1	URBANO	C	TIPO 1
9	CPNP RURAL LA JOYA	JIRÓN MILLER # 100	LA JOYA	AREQUIPA	AREQUIPA	16.42454156	-71.8182224	100M			0	1	1	0	2	URBANO	B	TIPO 1
1	CPNP JERUSALEN	CALLE DOS DE MAYO # SN	MARIANO MELGAR	AREQUIPA	AREQUIPA	-16.400925	-71.490645	100M			0	1	1	0	1	URBANO	C	TIPO 1
1	CPNP MARIANO MELGAR	OTRO PLAZA UMACHIRI # SN	MARIANO MELGAR	AREQUIPA	AREQUIPA	16.39939125	-71.50661945	100M			0	1	1	0	2	URBANO	B	TIPO 1
2	CPNP ALTO MISTI	CALLE ARTURO VILLEGAS # 300	MIRAFLORES	AREQUIPA	AREQUIPA	-16.389225	-71.51476	100M			0	1	1	0	1	URBANO	B	TIPO 1
1	CPNP EL PORVENIR	AV. SAN MARTÍN # 4103	MIRAFLORES	AREQUIPA	AREQUIPA	-16.377135	-71.50864667	100M			0	1	1	0	2	URBANO	B	TIPO 1
1	CPNP MIRAFLORES	AV. SAN MARTÍN # 417	MIRAFLORES	AREQUIPA	AREQUIPA	-16.395055	-71.52392	100M			0	1	1	0	2	URBANO	B	TIPO 1
5	MEDIO AMBIENTE	CALLE PUNO 782-862	MIRAFLORES	AREQUIPA	AREQUIPA	-16.398665	-71.516998	100M			0	0	1	0	1	URBANO	MEDIO AMBIENTE	TIPO 1
1	CPNP CAMPO MARTE	CALLE ALFONSO UGARTE S/N	PAUCARPATA	AREQUIPA	AREQUIPA	-16.427105	-71.49646	100M			0	1	1	0	1	URBANO	C	TIPO 1
1	CPNP FAMILIA PAUCARPATA	AV. REVOLUCION # 1200	PAUCARPATA	AREQUIPA	AREQUIPA	-16.417654	-71.491595	100M			0	1	1	0	1	URBANO	B	TIPO 1
8	CPNP ISRAEL	AV. LOS ANGELES SN MZ Y LT. 6	PAUCARPATA	AREQUIPA	AREQUIPA	-16.418885	-71.48503167	100M			0	0	1	0	1	URBANO		TIPO 1
1	CPNP JESUS MARIA	CALLE PARQUE CABALLERO # 121	PAUCARPATA	AREQUIPA	AREQUIPA	16.42091333	-71.50925833	100M			0	1	1	0	1	URBANO	C	TIPO 1
2	CPNP JUAN DE DIOS COLCA APAZA	AV. JORGE CHAVEZ S/N	PAUCARPATA	AREQUIPA	AREQUIPA	16.41155643	-71.49675429	100M			0	1	1	0	1	URBANO	B	TIPO 1
1	CPNP MIGUEL GRAU	AV. MIGUEL GRAU # SN	PAUCARPATA	AREQUIPA	AREQUIPA	-16.40863	-71.48383167	100M			0	1	1	0	1	URBANO	B	TIPO 1
2	DPTO. INV. ROBO DE VEHICULOS	CALLE MICHAELA BASTIDAS N° 105 PUEBLO JOVEN CIUDAD BLANCA ZONA A	PAUCARPATA	AREQUIPA	AREQUIPA	-16.419266	-71.493484	100M			0	1	1	0	1	URBANO	DIPROVE	TIPO 1

Handwritten signatures and initials at the top left of the page.



Handwritten signatures and initials in the middle left of the page.

1	2	CPNP SABANDIA	CALLE LAS PISCINAS # SN	SABANDIA	AREQUIPA	AREQUIPA	16.45001275	-71.4955312	100M				0	1	1	0	1	URBANO	C	TIPO 1
4	1	CPNP PAMPA DE CAMARONES	AV. BRASIL # 517	SACHACA	AREQUIPA	AREQUIPA	16.41130333	-71.571905	100M				0	1	1	0	1	URBANO	C	TIPO 1
5	2	CPNP SACHACA	AV. ROBERTO PONCE # SN	SACHACA	AREQUIPA	AREQUIPA	16.42314833	-71.564975	100M				0	1	1	0	1	URBANO	C	TIPO 1
6	1	CPNP SANTA RITA DE SIGUAS	AV. CESAR AUGUSTO GILARDI # 400 REF PLAZA DE ARMAS SANTA RITA DE SIGUAS	SANTA RITA DE SIGUAS	AREQUIPA	AREQUIPA	-16.4933817	-72.09464333	100M				0	1	1	0	1	URBANO	D	TIPO 1
7	2	CPNP CIUDAD MI TRABAJO	AV. INDEPENDENCIA # SN	SOCABAYA	AREQUIPA	AREQUIPA	16.44831833	-71.53257	100M				0	1	1	0	2	URBANO	A	TIPO 1
8	1	CPNP SOCABAYA	AV. SALAVERRY # 150	SOCABAYA	AREQUIPA	AREQUIPA	-16.47217	-71.52854667	100M				0	1	1	0	1	URBANO	B	TIPO 1
9	2	CPNP TIABAYA	AV. AREQUIPA # 108	TIABAYA	AREQUIPA	AREQUIPA	16.44970663	-71.58868432	100M				0	1	1	0	1	URBANO	B	TIPO 1
0	3	CPNP CONGATA	AV. RAMÓN CASTILLA ZONA "A" MZ B LOTE 2 Y 3 - CONGATA	UCHUMAYO	AREQUIPA	AREQUIPA	16.44623333	-71.61906657	100M				0	1	1	0	1	URBANO	C	TIPO 1
1	1	CPNP UCHUMAYO	CALLE SALAVERRY # 103	UCHUMAYO	AREQUIPA	AREQUIPA	16.42580167	-71.67318	100M				0	1	1	0	1	URBANO	B	TIPO 1
2	3	AEROPUERTO INTERNACIONAL JORGE CHAVEZ	AV. ELMER FAUCETT S/N	CALLAO	AREQUIPA	LIMA	-12.02405	-77.1122	400M				0	1	1	0	0	URBANO	RQ	TIPO 1
3	1	DPTO. TRANSITO	URB. JUAN XXIII MZ A LOTE 6	YANAHUARA	AREQUIPA	AREQUIPA	-16.397293	-71.54981	100M				0	1	1	0	1	URBANO	TRANSITO	TIPO 1
4	3	REGPOL AREQUIPA - UNITIC	AV. EMMEL 106	YANAHUARA	AREQUIPA	AREQUIPA	-16.391651	-71.543559	150M				0	1	1	0	1	URBANO	MACRE UNITIC	TIPO 1
5	3	CPNP YARABAMBA	CALLE AMERICA # 105	YARABAMBA	AREQUIPA	AREQUIPA	16.54670961	-71.47513703	100M				0	1	1	0	1	URBANO	C	TIPO 1
6	1	CPNP YURA	AV. PRINCIPAL BAÑOS DE YURA # SN	YURA	AREQUIPA	AREQUIPA	-16.246638	-71.69213	100M				0	1	1	0	1	URBANO	D	TIPO 1
7	3	CPNP CIUDAD DE DIOS	ASOCIACIÓN URBANIZADORA CIUDAD DE DIOS MZ. T, LOTE 2, SECTOR B, ZONA 3, COMITE 22 DEL DISTRITO DE YURA	YURA	AREQUIPA	AREQUIPA	-16.301288	-71.626084	100M				0	1	1	0	1	URBANO	B	TIPO 1
8	3	POL PNP CAMANA	MZ D LOTE 9	CERCADO	AREQUIPA	CAMANA	-16.625455	-72.714031	100M				0	1	1	0	1	URBANO	POLICIA CO	TIPO 1
9	1	CPNP RURAL SAN GREGORIO	CALLE PROGRESO # 437	NICOLAS DE PIEROLA	AREQUIPA	CAMANA	16.57319046	-72.71662094	100M				0	1	1	0	1	URBANO	C	TIPO 1
0	4	CPNP OCOÑA	AV. JULIO RONALD SALAZAR MONROE # SN	OCOÑA	AREQUIPA	CAMANA	-16.43493567	-73.1066	100M				0	1	1	0	1	URBANO	C	TIPO 1
1	4	CPNP RURAL PNP LA PAMPA	AV. SAMUEL PASTOR # 407	SAMUEL PASTOR	AREQUIPA	CAMANA	16.61355333	-72.69871833	100M				0	1	1	0	1	URBANO	B	TIPO 1
2	1																			

[Handwritten signature]



[Handwritten signature]

1	CPNP RURAL ACARI	CLL SANTA ROSA Y CAL ENRIQUE BRILKA SN	ACARI	CARAVELI	AREQUIPA	-15.436895	-74.617405	100M			0	1	1	0	1	RURAL	C	TIPO 1
4	CPNP RURAL ATICO/COM CAR ATICO	AV. AREQUIPA S/N	ATICO	CARAVELI	AREQUIPA	-16.228085	-73.60959833	100M			0	1	1	0	1	RURAL	C	TIPO 1
3	CPNP RURAL BELLA UNION	AV. FRANCISCO FLORES BERRUESO S/N	BELLA UNION	CARAVELI	AREQUIPA	15.45037667	-74.65606333	100M			0	1	1	0	1	RURAL	C	TIPO 1
4	CPNP RURAL SECTORIAL CARAVELI	AV. 2 DE MAYO # 809	CARAVELI	CARAVELI	AREQUIPA	-15.773955	-73.36789667	100M			0	1	1	0	2	RURAL	B	TIPO 1
5	CPNP RURAL CHALA	CALLE GRAU # 216	CHALA	CARAVELI	AREQUIPA	-15.86624	-74.24685333	100M			0	1	1	0	1	RURAL	B	TIPO 1
1	DESPRCAR CHALA	AV. EMANCIPACION SN	CHALA	CARAVELI	AREQUIPA	15.85164167	-74.25262833	100M			0	0	1	0	0	RURAL	CARRETE RAS	TIPO 1
4	CPNP RURAL APLAO	CLL PARDO SN MZ J1 LT.14	APLAO	CASTILLA	AREQUIPA	16.07952167	-72.49398333	100M			0	1	1	0	1	RURAL	B	TIPO 1
8	DESPRCAR APLAO	CLL PARDO SN MZ K1 LT.04	APLAO	CASTILLA	AREQUIPA	-16.078349	-72.493369	100M			0	0	1	0	0	RURAL	CARRETE RAS	TIPO 1
1	CPNP RURAL ORCOPAMPA	AV. BUENAVENTURA # SN	ORCOPAMPA	CASTILLA	AREQUIPA	15.26799833	-72.344395	100M			0	1	1	0	1	RURAL	C	TIPO 1
5	CPNP RURAL PAMPACOLCA	CALLE SALAVERRY # SN	PAMPACOLCA	CASTILLA	AREQUIPA	15.71465833	-72.57313	100M			0	1	1	0	1	RURAL	C	TIPO 1
1	CPNP RURAL CHIVAY -CAYLLOMA	OTRO PLAZA DE ARMAS # SN	CHIVAY	CAYLLOMA	AREQUIPA	15.63690058	-71.60158843	100M			0	1	1	0	1	RURAL	B	TIPO 1
3	DESPRCAR CHIVAY	KM. 82.0 VIA PENETRACION AREQUIPA	CHIVAY	CAYLLOMA	AREQUIPA	-15.649102	-71.601363	100M			0	0	1	0	1	URBANO	CARRETE RAS	TIPO 1
1	CPNP DE LA FAMILIA MAJES (PEDREGAL)	EL PEDREGAL MAJES ESPALDA MUNICIPALIDAD PIZ EL PIONERO	MAJES	CAYLLOMA	AREQUIPA	16.36212167	-72.190805	100M			0	1	1	0	1	URBANO	FAMILIA	TIPO 1
5	CPNP MODELO EL PEDREGAL	AV. LOS COLONIZADORES S/N MZ O LT. 62	MAJES	CAYLLOMA	AREQUIPA	-16.348775	-72.18795667	100M			0	1	1	0	1	URBANO	B	TIPO 1
6	CPNP RURAL CHUQUIBAMBA	AV. NICOLAS DE PIÉROLA # 100	CHUQUIBAMBA	CONDESUYOS	AREQUIPA	-15.840918	-72.65116667	100M			0	1	1	0	1	URBANO	D	TIPO 1
1	CPNP COCACHACRA	AV. LIBERTAD # 824	COCACHACRA	ISLAY	AREQUIPA	17.09229833	-71.76451167	100M			0	1	1	0	1	URBANO	B	TIPO 1
5	CPNP LA CURVA	AV. DEAN VALDIVIA # SN	DEAN VALDIVIA	ISLAY	AREQUIPA	17.14404291	-71.82141691	100M			0	1	1	0	1	URBANO	C	TIPO 1
9	CPNP EL ARENAL	CLL ISLAY SN	DEAN VALDIVIA	ISLAY	AREQUIPA	17.12104833	-71.796055	100M			0	1	1	0	1	URBANO	C	TIPO 1
1	CPNP MATARANI	AV. AREQUIPA # SN	ISLAY	ISLAY	AREQUIPA	-17.000667	-72.096165	100M			0	1	1	0	1	URBANO	D	TIPO 1

Handwritten signatures and initials at the top left of the page.



Handwritten signatures and initials in the middle left of the page.

1	CPNP MEJIA	AV. TAMBO # SN	MEJIA	ISLAY	AREQUIPA	-17.10222	-71.905055	100M			0	1	1	0	1	URBANO	C	TIPO 1
2																		
3	CPNP SECTORIAL MOLLEND	PJ ALTO INCLAN MANIZANA "Q"	MOLLEND	ISLAY	AREQUIPA	-17.019604	-72.003927	100M			0	1	1	0	2	URBANO	A	TIPO 1
4																		
5	POSTA PNP ISLAY MOLLEND	CALLE FRANCISCO BOLOGNESI 503	MOLLEND	ISLAY	AREQUIPA	-17.019069	-72.006963	100M			0	1	1	0	1	URBANO	POSTA MEDICA	TIPO 1
6																		
7	CPNP PUNTA DE BOMBON	CALLE PLAZA 28 DE JULIO # SN	PUNTA DE BOMBON	ISLAY	AREQUIPA	17.17188301	-71.7904079	100M			0	1	1	0	1	URBANO	C	TIPO 1
8																		
9	CPNP RURAL ZONAL COTAHUASI TIPO C	CALLE CABILDO # 107	COTAHUASI	LA UNION	AREQUIPA	-15.211875	-71.89061667	100M			0	1	1	0	1	RURAL	C	TIPO 1
10																		
11	CPNP SECTORIAL CANGALLO	JR MARISCAL CACERES 152	CANGALLO	CANGALLO	AYACUCHO	-13.628941	-74.143551	100M			0	1	1	0	1	URBANO	C	TIPO 1
12																		
13	COMISARIA DE TURISMO AYACUCHO	ASOC. EL ARCO MZ. D. LT. 10 CALLE LOS LAURELES ENACE	AYACUCHO	HUAMANGA	AYACUCHO	-13.13999	-74.22993	100M			0	0	1	0	1	URBANO	TURISMO	TIPO 1
14																		
15	CPNP AYACUCHO/OFCRI	JIRON 28 DE JULIO # 325	AYACUCHO	HUAMANGA	AYACUCHO	-13.163941	-74.227155	150M			0	1	1	0	3	URBANO	A	TIPO 1
16																		
17	CPNP DE LA FAMILIA AYACUCHO	JR. LIBERTAD 1200. REFERENCIA EDIFICIO MUNICIPAL JUZGADO FAMILIA 2DO PISO	AYACUCHO	HUAMANGA	AYACUCHO	-13.150295	-74.227763	100M			0	1	1	0	1	URBANO	FAMILIA	TIPO 1
18																		
19	DIRECCOR AYACUCHO	AV. CARMEN ALTO N° 378. (REF. ALAMEDA BOLOGNESI)JR. LAS CARDENAS MZ LT. 37 (URB. MARISCAL CACERES)	AYACUCHO	HUAMANGA	AYACUCHO	-13.16165	-74.225515	100M			0	1	1	0	1	URBANO	DIRECCOR	TIPO 1
20																		
21	CPNP CARMEN ALTO	AV. AV. LIBERTADORES SN MZ X LT. 12	CARMEN ALTO	HUAMANGA	AYACUCHO	13.17689833	-74.221285	100M			0	1	1	0	1	URBANO	C	TIPO 1
22																		
23	DIVIDEAD CARMEN ALTO (DEPOTAD HUAMANGA)	AV. QUICAPATA S/N	CARMEN ALTO	HUAMANGA	AYACUCHO	-13.191027	-74.230065	100M			0	1	1	0	1	URBANO	DIVANDR	TIPO 1
24																		
25	305 EMERGENCIA AYACUCHO	CIRO ALEGRIA 430	JESUS NARAZERO	HUAMANGA	AYACUCHO	-13.157467	-74.216706	100M			0	1	1	0	1	URBANO	EMERGENCIA	TIPO 1
26																		
27	DIPROVE AYACUCHO	JR. MANUEL ALARCON 221	JESUS NAZARENO	HUAMANGA	AYACUCHO	-13.151762	-74.213247	100M			0	1	1	0	1	URBANO	DIPROVE	TIPO 1
28																		
29	CPNP OCROS	JR. PROLG CACERES JR PROCERES SN MZF LT. 4	OCROS	HUAMANGA	AYACUCHO	13.39096333	-73.91479333	100M			0	1	1	0	1	RURAL	C	TIPO 1
30																		
31	CPNP QUINUA	CALLE SUCRE # 104	QUINUA	HUAMANGA	AYACUCHO	13.04678848	-74.13927734	100M			0	1	1	0	1	URBANO	C	TIPO 1
32																		
33	REGPOL AYACUCHO	AV. AGUSTIN ZEAS/N	SANTA ELENA	HUAMANGA	AYACUCHO	-13166211	-74198431	100M			0	1	1	0	1	URBANO	REGPOL	TIPO 1
34																		
35	CPNP HUANTA/COM CAR HUANTA	AV. SAN MARTIN # 372	HUANTA	HUANTA	AYACUCHO	12.94159333	-74.247085	100M			0	1	1	0	2	URBANO	A	TIPO 1
36																		
37	POSTA PNP HUANTA	JR. AYACUCHO 271	HUANTA	HUANTA	AYACUCHO	-12.940352	-74.246847	100M			0	1	1	0	1	URBANO	POSTA MEDICA	TIPO 1

Handwritten signature and initials at the top left of the page.



Handwritten signature and initials in the middle left of the page.

1	1	CPNP PALMAMPAMPA	JIRÓN JORGE BASADRE # SN	SAN MIGUEL	LA MAR	AYACUCHO	12.7664833	-73.6552233	100M			0	1	1	0	1	RURAL	C	TIPO 1
8	1	CPNP PALMAMPAMPA	JIRÓN JORGE BASADRE # SN	SAN MIGUEL	LA MAR	AYACUCHO	12.7664833	-73.6552233	100M			0	1	1	0	1	RURAL	A	TIPO 1
8	2	CPNP SECTORIAL SAN MIGUEL LA MAR	JIRÓN MARISCAL CACERES # SN	SAN MIGUEL	LA MAR	AYACUCHO	-13.01356	-73.98046	100M			0	1	1	0	1	RURAL	A	TIPO 1
8	3	DEPOTAD PALMAMPAMPA (GOAT) + POSTA MEDICA PALMAMPAMPA	CALLE LOS LAURELES S/ N/S/N	SAN MIGUEL	LA MAR	AYACUCHO	-12.765802	-73.655055	100M			0	1	1	0	1	RURAL	DIRANDR O	TIPO 1
8	4	CPNP LUCANAS - PUQUIO	JIRÓN TACNA # 657	PUQUIO	LUCANAS	AYACUCHO	14.69985833	-74.12818833	100M			0	1	1	0	1	RURAL	D	TIPO 1
8	5	CPNP SECTORIAL PARINACOCCHAS	JIRÓN DOS DE MAYO # 820	CORACORA	PARINACOCCHAS	AYACUCHO	15.01685333	-73.781765	100M			0	1	1	0	1	RURAL	B	TIPO 1
8	6	CPNP SECTORIAL PAUCAR DEL SARA	AV. MIGUEL CERVANTES SAAVEDRA # 519	PAUSA	PAUCAR DEL SARA	AYACUCHO	15.27869333	-73.34426167	100M			0	1	1	0	1	RURAL	C	TIPO 1
8	7	CPNP TACA	OTRO PLAZA PRINCIPAL # SN	CANARIA	VICTOR FAJARDO	AYACUCHO	13.95880167	-73.91770667	100M			0	1	1	0	1	RURAL	D	TIPO 1
8	8	CPNP VILLA CANARIA	AV. LIBERTAD # SN	CANARIA	VICTOR FAJARDO	AYACUCHO	13.92364167	-73.90473667	100M			0	1	1	0	1	RURAL	C	TIPO 1
8	9	CPNP HUANCAPÍ	JIRÓN VICTOR FAJARDO # 745	HUANCAPÍ	VILCAS HUAMAN	AYACUCHO	-13.7516	-74.06583167	100M			0	1	1	0	1	RURAL	C	TIPO 1
8	10	CPNP SECTORIAL VILCASHUAMAN	AV. VILCAS RAYMI B. HUANCAPUQUIO	VILCAS HUAMAN	VILCAS HUAMAN	AYACUCHO	-13.657699	-73.955199	100M			0	1	1	0	1	URBANO	D	TIPO 1
8	11	CPNP SECTORIAL CAJABAMBA	AV. LEONCIO MARTINEZ VERAU # 341	CAJABAMBA	CAJABAMBA	CAJAMARCA	7.62787333	-78.04396	100M			0	1	1	0	1	URBANO	B	TIPO 1
8	12	CPNP SECTORIAL BAÑOS DEL INCA/DIRCOCOR CAJAMARCA	JIRÓN YAHUAR HUACA # 207	BAÑOS DEL INCA	CAJAMARCA	CAJAMARCA	-7.1641933	-78.4629683	100M			0	1	1	0	2	URBANO	B	TIPO 1
8	13	CPNP CAJAMARCA II	JR. AMALIA PUGA # 1111	CAJAMARCA	CAJAMARCA	CAJAMARCA	7.160391024	-78.51294369	200M			1	0	1	0	1	URBANO	PRENTE 8	TIPO 1
8	14	CPNP CAJAMARCA II	JIRÓN CHEPEN # 511	CAJAMARCA	CAJAMARCA	CAJAMARCA	-7.1502	-78.519685	200M			0	1	1	0	3	URBANO	B	TIPO 1
8	15	OFICRI / ESTA EN TRANSITO - CAJAMARCA	VIA DE EVITAMIENTO 1083	CAJAMARCA	CAJAMARCA	CAJAMARCA	-7.145627	-78.516962	100M			0	1	1	0	1	URBANO	OFICRI	TIPO 1
8	16	CPNP MAGDALENA CAJAMARCA	AV. JORGE CHAVEZ # 970	MAGDALENA	CAJAMARCA	CAJAMARCA	7.251701667	-78.6564333	100M			0	1	1	0	1	RURAL	C	TIPO 1
8	17	CPNP SECTORIAL CELENDIN	AV. CAJAMARCA # SN	CELENDIN	CELENDIN	CAJAMARCA	-6.872035	-78.142825	100M			0	1	1	0	1	URBANO	B	TIPO 1
8	18	CPNP SECTORIAL CHOTA/DIVPOL/POLICLINICO	AV. INCA GARCILAZO DE LA VEGA # 724	CHOTA	CHOTA	CAJAMARCA	6.560011667	-78.65583333	100M			0	1	1	0	3	URBANO	B	TIPO 1
8	19	CPNP CHILETE	JIRÓN FERROCARRIL # SN	CHILETE	CONTUMAZA	CAJAMARCA	7.221731667	-78.88890333	100M			0	1	1	0	1	URBANO	D	TIPO 1

Handwritten signatures and initials at the top left of the page.



Handwritten signatures and initials in the middle left of the page.

2	0	DESPIRCHAR CHILETE	JIRÓN INDEPENDENCIA # 115	CHILETE	CONTUMAZA	CAJAMARCA	7.221931667	-78.838895	100M				0	1	0	0	URBANO	CARRETE RAS	TIPO 1
2	0	CPNP SECTORIAL CONTUMAZA	JIRÓN MELGAR # 195	CONTUMAZA	CONTUMAZA	CAJAMARCA	7.366726667	-78.80608	100M				0	1	0	2	RURAL	B	TIPO 1
2	0	CPNP SECTORIAL TEMBLADERA	CALLE PLAZA DE ARMAS # SN	YONAN	CONTUMAZA	CAJAMARCA	7.253521667	-79.13042	100M				0	1	0	1	RURAL	C	TIPO 1
2	0	CPNP SECTORIAL CUTERVO	AV. SALOMON VILCHEZ MURGA # SN	CUTERVO	CUTERVO	CAJAMARCA	-6.38312	-78.81660833	100M				0	1	0	2	URBANO	B	TIPO 1
2	0	CPNP SECTORIAL BAMBAMARCA	JIRÓN JAIME MARTINEZ # 132	BAMBAMARCA	HUALGAYOC	CAJAMARCA	6.678091667	-78.517655	100M				0	1	0	1	URBANO	D	TIPO 1
2	0	CPNP JAEN	AV. MESONES MURO # 109	JAEN	JAEN	CAJAMARCA	5.710113333	-78.806635	100M				0	1	0	3	URBANO	B	TIPO 1
2	0	CPNP RURAL JAEN/DIVISION POLICIAL JAEN	JR. CAJAMARCA 498-JAEN//JAV MESONES MURO 109	JAEN	JAEN	CAJAMARCA	-5.709992	-78.806317	100M				0	1	0	1	URBANO	D	TIPO 1
2	0	POSTA PNP MEDICA JAEN	CALLE CAJAMARCA 340	JAEN	JAEN	CAJAMARCA	-5.70781	-78.806731	100M				0	1	0	1	URBANO	POSTA MEDICA	TIPO 1
2	0	CPNP SECTORIAL SAN IGNACIO	AV. SAN IGNACIO # SN	SAN IGNACIO	SAN IGNACIO	CAJAMARCA	5.145966667	-78.999695	100M				0	1	0	2	URBANO	B	TIPO 1
2	0	CPNP SECTORIAL SAN MARCOS	JIRÓN INCLAN Y LAVALLE # 141	PEDRO GALVEZ	SAN MARCOS	CAJAMARCA	-7.3348	-78.16965167	100M				0	1	0	2	RURAL	B	TIPO 1
2	0	CPNP SECTORIAL SAN MIGUEL	JIRÓN BOLOGNESI # 465	SAN MIGUEL	SAN MIGUEL	CAJAMARCA	-7.00025	-78.85136167	100M				0	1	0	1	RURAL	C	TIPO 1
2	0	CPNP SAN PABLO	AV. 13 DE JULIO # 306	SAN PABLO	SAN PABLO	CAJAMARCA	-7.11739	-78.824345	100M				0	1	0	1	RURAL	C	TIPO 1
2	0	CPNP SECTORIAL SANTA CRUZ DE SUCCABAMBA	CALLE ALFONSO UGARTE # 230	SANTA CRUZ	SANTA CRUZ	CAJAMARCA	6.624693333	-78.94401333	100M				0	1	0	1	RURAL	B	TIPO 1
2	0	CPNP ANCAHUASI	KM 45 VIA NACIONAL DISTRITO DE ANCAHUASI	ANCAHUASI	ANTA	CUSCO	-13.45642	-72.301511	100M				0	1	0	0	RURAL	E	TIPO 1
2	0	CPNP IZCUCHACA/COM SECTORIAL ANTA	CALLE JAQUIHUANA # SN	ANTA	ANTA	CUSCO	-13.46401	-72.14420167	100M				0	1	0	1	URBANO	D	TIPO 1
2	0	CPNP RURAL CACHIMAYO	AV. LEONIDAS RODRIGUEZ FIGUEROA # SN	CACHIMAYO	ANTA	CUSCO	-13.47951	-72.06615667	100M				0	1	0	0	URBANO	E	TIPO 1
2	0	CPNP RURAL CALCA	JIRÓN ESPINAR # 498	CALCA	CALCA	CUSCO	-13.320495	-71.95564667	100M				0	1	0	1	URBANO	B	TIPO 1
2	0	CPNP SAN SALVADOR	CALLE CUSCO S/N.	SAN SALVADOR	CALCA	CUSCO	13.49059055	-71.77990662	100M				0	1	0	1	URBANO	C	TIPO 1
2	0	CPNP RURAL LAYO	AV. MIGUEL GRAU # SN	LAYO	CANAS	CUSCO	-14.492094	-71.157504	100M				0	1	0	0	RURAL	E	TIPO 1

Handwritten signature and initials at the top left of the page.



2	1	CPNP YANAOCA	AV. TUPAC AMARU # 340	YANAOCA	CANAS	CUSCO	-14.214745	-71.43222167	100M				0	1	1	0	1	URBANO	C	TIPO 1
2	2	CPNP CHECACUPE	AV. TUPAC AMARU S/N	CHECACUPE	CANCHIS	CUSCO	-14.026079	-71.452701	100M				0	1	1	0	0	RURAL	E	TIPO 1
2	2	CPNP RURAL COMBAPATA E	FRENTE A LA PLAZA DE ARMAS DE COMBAPATA	COMBAPATA	CANCHIS	CUSCO	-14.101307	-71.429295	100M				0	1	1	0	0	RURAL	E	TIPO 1
2	2	CPNP MARANGANI	FRENTE A LA PLAZA DE ARMAS DE MARANGANI	MARANGANI	CANCHIS	CUSCO	-14.356728	-71.168544	100M				0	1	1	0	1	RURAL	D	TIPO 1
2	2	CPNP RURAL PITUMARCA	CALLE SIN NOMBRE # 135 (PLAZA DE ARMAS)	PITUMARCA	CANCHIS	CUSCO	-13.97991	-71.41748167	100M				0	1	1	0	1	URBANO	C	TIPO 1
2	2	CPNP RURAL DE TORCOMA	AV. CONFEDERACION # SN	SICUANI	CANCHIS	CUSCO	14.25506833	-71.22939	100M				0	1	1	0	1	URBANO	B	TIPO 1
2	2	CPNP RURAL SICUANI	AV. GRAU # SN	SICUANI	CANCHIS	CUSCO	14.27943667	-71.22442833	100M				0	1	1	0	2	URBANO	B	TIPO 1
2	2	POSTA PNP SICUANI	AV. REPUBLICA DEL PERU CON JUR. LAS RETAMAS 117-119	SICUANI	CANCHIS	CUSCO	-14.260380	-71.226484	100M				0	1	1	0	1	URBANO	POSTA MEDICA	TIPO 1
2	2	CPNP RURAL TINTA	AV. TUPAC AMARU # SN	TINTA	CANCHIS	CUSCO	-14.142975	-71.40252833	100M				0	1	1	0	0	URBANO	E	TIPO 1
2	2	CPNP RURAL SANTO TOMAS	CALLE JEREMIAS PASHBY COLLINS # SN	SANTO TOMAS	CHUMBIVILCA	CUSCO	14.44808833	-72.08439833	100M				0	1	1	0	1	RURAL	D	TIPO 1
2	2	CPNP SECTORIAL CUSCO/DIRTEPOL	AV. REGIONAL 902 (ANTES, CALLE SAPHY # 510)	CUSCO	CUSCO	CUSCO	-13.514638	-71.981428	100M				0	1	1	0	3	URBANO	A	TIPO 1
2	3	CPNP SIPASPUYCO	CALLE CESAR VALLEJO # SN	CUSCO	CUSCO	CUSCO	-13.52149	-71.98782	100M				0	1	1	0	1	URBANO	C	TIPO 1
2	3	CPNP TAHUANTINSUYO CUSCO	PASAJE LAS AMERICAS # SN	CUSCO	CUSCO	CUSCO	-13.5190686	-71.95926905	100M				0	1	1	0	2	URBANO	B	TIPO 1
2	3	CPNP POROY	OTRO PISTA ASFALTICA CUSCO - LIMA # SN	POROY	CUSCO	CUSCO	-13.495445	-72.04178333	100M				0	1	1	0	1	URBANO	C	TIPO 1
2	3	CPNP SAN JERONIMO	AV. MANCO CAPAC # SN	SAN JERONIMO	CUSCO	CUSCO	13.54615167	-71.88961333	100M				0	1	1	0	1	URBANO	C	TIPO 1
2	3	CPNP SAN SEBASTIAN	AV. LA CULTURA # SN	SAN SEBASTIAN	CUSCO	CUSCO	13.53228167	-71.926475	100M				0	1	1	0	1	URBANO	C	TIPO 1
2	3	CPNP SANTIAGO	CALLE JORGE OCHOA N° 355	SANTIAGO	CUSCO	CUSCO	-13.524125	-71.984302	100M				0	1	1	0	3	URBANO	C	TIPO 1
2	3	CPNP VIVA EL PERU	JR SEÑOR HUANCA SN MZA LT.4	SANTIAGO	CUSCO	CUSCO	13.53872086	-71.95853949	100M				0	1	1	0	2	URBANO	C	TIPO 1
2	3	CPNP SAYLLA	AV. CUSCO # SN	SAYLLA	CUSCO	CUSCO	13.5755369	-71.82559311	100M				0	1	1	0	1	URBANO	C	TIPO 1

[Handwritten signature]

[Handwritten signature]



[Handwritten signature]

[Handwritten signature]

2	COMISARIA DE TURISMO CUSCO	AV. PLAZA TUPAC AMARU S/N	WANCHAQ	CUSCO	CUSCO	-13.522824	-71.967096	100M			0	1	0	1	0	1	URBANO	TURISMO	TIPO 1
3																			
8																			
2	CPNP AEROPUERTO ALEJANDRO VELAZCO ASTETE	AV. VELASCO ASTETE # SN	WANCHAQ	CUSCO	CUSCO	13.53858167	-71.94312167	100M			0	1	0	1	0	1	URBANO	A	TIPO 1
3																			
9																			
2	CPNP SECTORIAL WANCHAQ/COMPLEJO POLICIAL 6 DICIEMBRE	AV. 28 DE JULIO CDRA. 3 URB. TTIO WANCHAQ	WANCHAQ	CUSCO	CUSCO	13.53211667	-71.959705	100M			0	1	0	1	0	1	URBANO	B	TIPO 1
4																			
0																			
2	DIVPOLIUD - CUSCO	AV. EL SOL CUADRA 2	WANCHAQ	CUSCO	CUSCO	-13.522301	-71.974883	100M			0	1	0	1	0	1	URBANO	POLJUS	TIPO 1
1																			
2																			
4	OFICRI CUZCO	CALLE ALCIDES VIGO S/N REF. COSTADO DEL MINISTERIO DE TRABAJO	WANCHAQ	CUSCO	CUSCO	-13.523341	-71.963596	100M			0	1	0	1	0	1	URBANO	OFICRI	TIPO 1
2																			
4	REGPOL CUSCO / UNITIC CUSCO	PLAZA TUPAC AMARU S/N - WANCHAQ	WANCHAQ	CUSCO	CUSCO	-13.52306	-71.96602	200M			1	1	0	1	0	1	RURAL	REGPOL	TIPO 1
3																			
2	CPNP ESPINAR	CALLE 9 DE DICIEMBRE S/N CON JR.SOL	ESPINAR	ESPINAR	ESPINAR	-14.790961	-71.412126	100M			0	1	0	1	0	1	URBANO	B	TIPO 1
4																			
4	DESPRCAR ESPINAR	CALLE HECTOR TEJADA # 102	ESPINAR	ESPINAR	ESPINAR	-14.792291	-71.413633	100M			0	0	0	1	0	1	RURAL	CARRETE RAS	TIPO 1
5																			
2	DESPRCAR QUILLABAMBA	PASAJE PUERTO MALAGA # SN	HUAYOPATA	LA CONVENCIÓN	LA CONVENCIÓN	13.00625333	-71.55314833	100M			0	0	0	1	0	0	RURAL	CARRETE RAS	TIPO 1
4																			
6																			
2	CPNP DE LA MUJER QUILLABAMBA (TAMBIEN SE IMPLEMENTA EN LA CPNP QUILLABAMBA MISMA UBICACIÓN)	PROLONGACIÓN RICARDO PALMA # SN	SANTA ANA	LA CONVENCIÓN	LA CONVENCIÓN	12.85743333	-72.69672167	200M			0	1	0	1	0	1	RURAL	FAMILIA	TIPO 1
4																			
7																			
2	CPNP PAVAYOC	AV. VIRGEN DEL CARMEN S/N - SECTOR PINTOBAMBA GRANDE	SANTA ANA	LA CONVENCIÓN	LA CONVENCIÓN	-13.84731	-72.70705	100M			0	1	0	1	0	1	URBANO	C	TIPO 1
4																			
8																			
2	CPNP QUILLABAMBA/DIVINCRI/SEANDRO/ORINTE (IMPLEMENTADO EN LA DNPOLLA CONCEPCIÓN)	JIRÓN LIBERTAD # 429	SANTA ANA	LA CONVENCIÓN	LA CONVENCIÓN	12.86406399	-72.69269161	100M			0	1	0	1	0	2	RURAL	B	TIPO 1
4																			
9																			
2	CPNP RURAL PARURO	CALLE GRAU # SN	PARURO	PARURO	PARURO	-13.76064	-71.849625	100M			0	1	0	1	0	1	RURAL	C	TIPO 1
5																			
0																			
2	CPNP ZONAL RURAL PAUCARTAMBO	CALLE PLAZOLETA MANCO CCAPAC # SN	PAUCARTAMBO	PAUCARTAMBO	PAUCARTAMBO	-13.317995	-71.597485	100M			0	1	0	1	0	1	URBANO	C	TIPO 1
5																			
1																			
2	CPNP RURAL ANDAHUAYLILLAS	CALLE ESPINAR S/N ANDAHUAYLILLA (ANTES CALLE GARCILAZO DE LA VEGA N° 600)	ANDAHUAYLILLAS	QUISPICANCHI	QUISPICANCHI	-13.673107	-71.677682	100M			0	1	0	1	0	0	RURAL	E	TIPO 1
5																			
5	CPNP RURAL KCAURI	CARRETERA INTEROCEANICA # SN	CCATCA	QUISPICANCHI	QUISPICANCHI	-13.694655	-71.52801	100M			0	1	0	1	0	0	URBANO	E	TIPO 1
3																			
2																			
5	CPNP RURAL HUAMBUTIO	AV. PRINCIPAL DE HUAMBUTIO # SN	LUCRE	QUISPICANCHI	QUISPICANCHI	13.58186876	-71.7143029	100M			0	1	0	1	0	0	URBANO	E	TIPO 1
2																			
4																			
5	CPNP RURAL OROPESA	CARRETERA CUSCO - URCOS # SN	OROPESA	QUISPICANCHI	QUISPICANCHI	13.60074667	-71.76607333	100M			0	1	0	1	0	1	RURAL	C	TIPO 1
2																			
5	CPNP RURAL DE URCOS	OTRO PLAZA DE ARMAS # SN	URCOS	QUISPICANCHI	QUISPICANCHI	-13.688625	-71.62517167	100M			0	1	0	1	0	1	URBANO	C	TIPO 1
2																			
6																			

Handwritten signature and initials at the top left of the page.



Handwritten signature and initials on the left side of the page, below the stamp.

2	5	DIVISION POLICIAL CUJANI- CANCHIS	AV. CONFEDERACION S/N	CANCHIS	SICUANI	CUSCO	-14.254899	-71.229553	100M			0	1	1	0	1	URBANO	DIVPOL	TIPO 1
2	5	CPNP RURAL CHINCHERO	OTRO PLAZA CHINCHERO # SN	calamarca	URUBAMBA	CUSCO	-13.391995	-72.04895	100M			0	1	1	0	1	URBANO	C	TIPO 1
2	5	CPNP MACHUPICCHU	AV. IMPERIO LOS INCAS # 401	MACHUPICCHU	URUBAMBA	CUSCO	13.15468033	-72.52544314	100M			0	1	1	0	1	RURAL	C	TIPO 1
2	6	CPNP RURAL OLLANTAYTAMBO	OTRO PLAZA DE ARMAS # SN	OLLANTAYTAMBO	URUBAMBA	CUSCO	13.25876167	-72.26394333	100M			0	1	1	0	1	URBANO	C	TIPO 1
2	6	CPNP SECTORIAL URUBAMBA	AA.HH. PRIMERO DE MAYO MZ. B LOTE 2	URUBAMBA	URUBAMBA	CUSCO	13.30594829	-72.11469501	100M			0	1	1	0	2	URBANO	B	TIPO 1
2	6	CPNP SECTORIAL ACOBAMBA	AV. SAN MARTIN # 505	ACOBAMBA	ACOBAMBA	HUANCAMELICO	12.84065311	-74.57052827	100M			0	1	1	0	1	RURAL	C	TIPO 1
2	6	CPNP RURAL CONGALLA "E"	AV. CHAUPIRANPA S/N - PLAZA PRINCIPAL	CONGALLA	ANGARAES	HUANCAMELICO	-12.956145	-74.49254333	100M			0	1	1	0	1	RURAL	D	TIPO 1
2	6	CPNP ANGARAES - LIRCAY	PROLONGACIÓN OLIMPICO # 104	LIRCAY	ANGARAES	HUANCAMELICO	12.9055833	-74.72616667	100M			0	1	1	0	1	RURAL	D	TIPO 1
2	6	CPNP CASTROVIRREYNA	AV. SAN MARTIN # 179	CASTROVIRREYNA	CASTROVIRREYNA	HUANCAMELICO	13.28234833	-75.31897667	100M			0	1	1	0	1	RURAL	C	TIPO 1
2	6	CPNP CHURCAMP	JR. LA MERCED S/N MZ. Y1 LT. 13A	CHUECAMP	CHURCAMP	HUANCAMELICO	-12.738564	-74.38989	100M			0	1	1	0	1	RURAL	B	TIPO 1
2	6	COMISARIA DE TURISMO HUANCAMELICO / DIPROVE / TRANSITO / MEDIO AMBIENTE / INSPECTORIA / TERNIA Y OTROS	MALECON VIRGEN DE LA CADELARIA S/N - BARRIO SAN CRISTOBAL	HUANCAMELICO	HUANCAMELICO	HUANCAMELICO	-12.784570	-74.9725645	200M			0	0	1	1	0	URBANO	TURISMO	TIPO 1
2	6	CPNP DE LA FAMILIA HUANCAMELICO (IMPLEMENTADO EN LA DIVINCR HUANCAMELICO)	JIRON CARABAYA # SN	HUANCAMELICO	HUANCAMELICO	HUANCAMELICO	12.78664484	-74.97233391	100M			0	1	1	0	2	RURAL	FAMILIA	TIPO 1
2	6	CPNP SECTORIAL HUANCAMELICO/DIVINCR/OFCRI	JIRON GRAU # 126	HUANCAMELICO	HUANCAMELICO	HUANCAMELICO	12.78592833	-74.96892333	100M			0	1	1	0	3	RURAL	B	TIPO 1
2	7	POL PNP HUANCAMELICO	JR. MANCO CAPAC 102	HUANCAMELICO	HUANCAMELICO	HUANCAMELICO	-12.78637	-74.973096	100M			0	1	1	0	1	RURAL	POLICIA	TIPO 1
2	7	REGPOL HUANCAMELICO	JIRON GRAU 126 PLAZA SANTA ANA	HUANCAMELICO	HUANCAMELICO	HUANCAMELICO	-12.785867	-74.968951	100M			0	1	1	0	1	RURAL	DIRTEPOL	TIPO 1
2	7	CPNP HUANDO	AV. ATAHUALPA # SN	HUANDO	HUANCAMELICO	HUANCAMELICO	12.56833333	-74.94752667	100M			0	1	1	0	1	RURAL	D	TIPO 1
2	7	DESPPCAR PAMPAS VRAEM	AV. PROGRESO # SN	PAMPAS	TAYACAJA	HUANCAMELICO	12.39518333	-74.86978667	100M			0	0	1	0	0	RURAL	CARRETE RAS	TIPO 1
2	7	POSTA PNP PAMPAS	JR. SAN SEBASTIAN S/N CRUCE CON JR. ALFONSO UGARTE	PAMPAS	TAYACAJA	HUANCAMELICO	-12.398837	-74.865102	100M			0	1	1	0	1	RURAL	POSTA MEDICA	TIPO 1
2	7	CPNP SECTORIAL PAMPAS - TAYACAJA	JIRON MILLER Y LIMA # 100	PAMPAS	TAYACAJA	HUANCAMELICO	12.39788667	-74.86904167	100M			0	1	1	0	1	RURAL	B	TIPO 1

Handwritten signatures and marks at the top left of the page.



Handwritten signatures and marks in the middle left of the page.

2	7	CPNP AMBO	JIRÓN BOLOGNESI # 154	AMBO	AMBO	HUANUCO	-10.127405	-76.20424333	100M					0	1	1	0	2	URBANO	C	TIPO 1
6	7	CPNP SECTORIAL DOS DE MAYO/COMCAR LA UNION	JIRÓN LOURDES # 119	LA UNION	DOS DE MAYO	HUANUCO	-9.827985	-76.801775	100M					0	1	1	0	1	RURAL	B	TIPO 1
7	7	CPNP LLATA	JIRÓN 28 DE JULIO # SN	LLATA	HUAMALIES	HUANUCO	-9.550135	-76.818275	100M					0	1	1	0	1	RURAL	C	TIPO 1
2	7	CPNP AMARILIS	AV. LOS GIRASOLES # SN	AMARILIS	HUANUCO	HUANUCO	9.942761667	-76.24728167	100M					0	1	1	0	1	URBANO	B	TIPO 1
9	2	CPNP ACOMAYO	CALLE INCAPATA N° 412 CENTRO POBLADO ACOMAYO	CHINCHAO	HUANUCO	HUANUCO	9.801716667	-76.07139667	100M					0	1	1	0	1	RURAL	C	TIPO 1
0	8	CPNP RANCHO	CARRETERA CENTRAL HUANUCO/TINGO MARIA # SN	CHURUBAMBA	HUANUCO	HUANUCO	-9.830.984	-76.094.232	100M					0	1	1	0	1	RURAL	D	TIPO 1
2	8	COMISARIA DE TURISMO HUANUCO	JR. PROLONGACIÓN ABTAO N° 479	HUANUCO	HUANUCO	HUANUCO	-99.367.224	762.467.656	100M					0	1	1	0	1	URBANO	TURISMO	TIPO 1
2	8	CPNP HUANUCO/REG POL HUANUCO	JIRÓN CONSTITUCIÓN # 501	HUANUCO	HUANUCO	HUANUCO	9.926303047	-76.23923779	200M					1	1	1	0	1	URBANO	RESPOL	TIPO 1
3	2	CPNP CAYHUAYNA	CALLE LOS SAUCES N° 237 - MZ. A LOTE 6	PILCO MARCA	HUANUCO	HUANUCO	-9.96268	-76.24330	100M					0	1	1	0	2	URBANO	B	TIPO 1
4	2	ETS PNP HUANUCO	CARRETERA CENTRAL HUANUCO TINGO MARIA KM12.5	SANTA MARIA DEL VALLE	HUANUCO	HUANUCO	-9.860565	-76.167008	100M					0	1	1	0	5	URBANO	ETS	TIPO 1
5	2	CPNP DE JESUS	JIRÓN LEONCIO PRADO # SN	JESUS	LAURICOCHA	HUANUCO	-10.07829	-76.6319	100M					0	1	1	0	1	RURAL	C	TIPO 1
6	2	CPNP AUCAVACU	AV. INDEPENDENCIA # 507 - FRENTE AL COLEGIO INTEGRADO #038	JOSE CRESPO Y CASTILLO	LEONCIO PRADO	HUANUCO	-8.93404	-76.115184	100M					0	1	1	0	2	URBANO	C	TIPO 1
7	8	CPNP DE LA FAMILIA - TINGO MARIA	AV. AREQUIPA 1121	RUPA-RUPA	LEONCIO PRADO	HUANUCO	-9.2916666	-75.996944	100M					0	1	1	0	1	URBANO	FAMILIA	TIPO 1
8	2	CPNP TINGO MARIA/DIVPOL TINGO MARIA	JIRÓN ANTONIO RAYMONDI # 413	RUPA-RUPA	LEONCIO PRADO	HUANUCO	-9.297975	-76.00281167	100M					0	1	1	0	2	URBANO	B	TIPO 1
9	2	DEINCR TINGO MARIA/COMCAR TINGO MARIA	AV. LAS BANDERAS TINGO MARIA 210	RUPA-RUPA	LEONCIO PRADO	HUANUCO	-9.3033243	-76.0033708	100M					0	1	1	0	2	URBANO	DIVINCR	TIPO 1
0	2	DEPOTAT RUPA RUPA	AV. PIMENTEL CDRA 07 TINGO MARIA 711	RUPA-RUPA	LEONCIO PRADO	HUANUCO	-9.308218	-76.000976	100M					0	1	1	0	1	URBANO	DIVANDR	TIPO 1
1	2	CPNP HUACRACHUCO	JIRÓN MARAÑON # SN	HUACRACHUCO	MARAÑON	HUANUCO	8.603956667	-77.14897	100M					0	1	1	0	1	RURAL	C	TIPO 1
2	9	CPNP PANAO - PACHITEA	JIRÓN BOLOGNESI # 225	PANAO	PACHITEA	HUANUCO	-9.896994	-75.994859	100M					0	1	1	0	1	RURAL	B	TIPO 1
3	9	CPNP PUERTO INCA	AV. FERNANDO BELAUDE TERRY #5/N	PUERTO INCA	PUERTO INCA	HUANUCO	-9.380307	-74.964759	100M					0	1	1	0	1	RURAL	B	TIPO 1
4	9																				

Handwritten signatures and initials at the top left of the page.



Handwritten signatures and initials in the middle left of the page.

2	FRONTE POLICIAL PUERTO INCA	JR. LORETO S/N MZ 1 LOTE 27	PUERTO INCA	PUERTO INCA	HUANUCO	-9.376946	-74.967027	100M			0	0	1	0	1	URBANO	FRONTE	TIPO 1
5	CPNP CHAVINILLO	JIRÓN VIRGEN DE FATIMA # SN	CHAVINILLO	YAROWILCA	HUANUCO	9.859295583	-76.60876572	100M			0	1	1	0	1	RURAL	C	TIPO 1
6	CPNP CHINCHA ALTA/EMERGENCIA 105/HALCONES	CALLE PLAZA DE ARMAS # 400	CHINCHA ALTA	CHINCHA	ICA	13.41713333	-76.13287167	100M			0	1	1	0	3	URBANO	A	TIPO 1
2	DEPINCR CHINCHA/GIR/TRANSITO	AV. JOSE GALVEZ CHIPOCO 230	CHINCHA ALTA	CHINCHA	ICA	-13.413123	-76.131799	100M			0	1	1	0	2	URBANO	DIVINCRI	TIPO 1
2	CPNP CHINCHA BAJA	CALLE JUAN C. DE MORA # 150	CHINCHA BAJA	CHINCHA	ICA	13.45871167	-76.16161833	100M			0	1	1	0	1	URBANO	C	TIPO 1
3	CPNP EL CARMEN	CALLE PLAZA DE ARMAS # SN	EL CARMEN	CHINCHA	ICA	13.49549833	-76.057485	100M			0	1	1	0	1	URBANO	C	TIPO 1
0	CPNP GROCIO PRADO	AV. SAN MARTIN # 202	GROCIO PRADO	CHINCHA	ICA	13.39719833	-76.15537833	100M			0	1	1	0	1	URBANO	B	TIPO 1
1	CPNP PUEBLO NUEVO	AV. SIMON BOLIVAR # 1152	PUEBLO NUEVO	CHINCHA	ICA	-13.39557	-76.19424167	100M			0	1	1	0	1	URBANO	A	TIPO 1
3	POL PNP CHINCHA	AV. OSCAR R. BENAVIDES 601	PUEBLO NUEVO	CHINCHA	ICA	-13.405024	-76.127781	100M			0	1	1	0	1	URBANO	POLICLINICO	TIPO 1
3	CPNP SUNAMPE	AV. PLAZA DE ARMAS # SN	SUNAMPE	CHINCHA	ICA	-13.42682	-76.164015	100M			0	1	1	0	1	URBANO	B	TIPO 1
4	CPNP TAMBO DE MORA	AV. SIMON BOLIVAR # 119	TAMBO DE MORA	CHINCHA	ICA	13.46061833	-76.18360333	100M			0	1	1	0	1	URBANO	C	TIPO 1
3	CPNP ICA	AV. JUAN JOSE ELIAS # SN	ICA	ICA	ICA	-14.06981	-75.732515	100M			0	1	1	0	2	URBANO	A	TIPO 1
0	POL PNP ICA	JR. HUÁNUCO 480	ICA	ICA	ICA	-14.066069	-75.731672	100M			0	1	1	0	1	URBANO	POLICLINICO	TIPO 1
3	COMISARIA DE TURISMO ICA	CALLE LIMA N° 367 PREFECTURA	ICA	ICA	ICA	-14.066144	-75.7277474	100M			0	0	1	0	1	URBANO	TURISMO	TIPO 1
8	CPNP LA TINGUIÑA	AV. VICTORIO GOTUZZO BIANCHI # 432	LA TINGUIÑA	ICA	ICA	14.03649653	-75.71059987	100M			0	1	1	0	1	URBANO	C	TIPO 1
9	CPNP LOS AQUJES	AV. PRINCIPAL # SN	LOS AQUJES	ICA	ICA	14.09700667	-75.69105333	100M			0	1	1	0	1	URBANO	C	TIPO 1
3	CPNP PACHACUTECH ICA	CLL. HUAYNA CAPAC SN	PACHACUTECH	ICA	ICA	14.15299667	-75.69128167	100M			0	1	1	0	1	URBANO	D	TIPO 1
1	CPNP PARCONA	CALLE RAUL PORRAS BARRENECHEA # SN	PARCONA	ICA	ICA	-14.04783	-75.70576	100M			0	1	1	0	1	URBANO	B	TIPO 1
2	CPNP PUEBLO NUEVO - ICA	CALLE LIBERTAD # 119	PUEBLO NUEVO	ICA	ICA	14.12670833	-75.705795	100M			0	1	1	0	1	URBANO	D	TIPO 1
3											0	1	1	0	1	URBANO	D	TIPO 1

[Handwritten signatures and marks at the top of the page]

[Handwritten signatures and marks on the left side of the page]



3	CPNP RURAL GUADALUPE (EX SALAS)	AV. MUNICIPALIDAD # SN	SALAS	ICA	ICA	13.98595833	-75.77224333	100M			0	1	1	0	1	URBANO	C	TIPO 1
1																		
4																		
1	CPNP LOS MOLINOS	CALLE 9 DE OCTUBRE # SN	SAN JOSE DE LOS MOLINOS	ICA	ICA	13.93248667	-75.67110167	100M			0	1	1	0	1	URBANO	C	TIPO 1
5																		
1	CPNP SAN JUAN BAUTISTA	CALLE MARISCAL CASTILLA # 42	SAN JUAN BAUTISTA	ICA	ICA	14.01134833	-75.73443	100M			0	1	1	0	1	URBANO	C	TIPO 1
3																		
6																		
1	CPNP SANTIAGO	CARRETERA PANAMERICANA SUR # SN	SANTIAGO	ICA	ICA	14.18428925	-75.71470231	100M			0	1	1	0	1	URBANO	C	TIPO 1
3																		
7																		
1	CPNP SUBTANALLA	CUL. INDEPENDENCIA 396	SUBTANALLA	ICA	ICA	14.01886667	-75.75662833	100M			0	1	1	0	1	URBANO	C	TIPO 1
8																		
3	CPNP SAN JUAN DE MARCONA	AV. ANDRES AVELINO CACERES # SN	MARCONA	NAZCA	NAZCA	15.36162667	-75.164925	100M			0	1	1	0	2	URBANO	B	TIPO 1
1																		
9																		
3	CPNP NAZCA/DIVPOL NAZCA/TURISMO	AV. LOS INCAS # 101	NAZCA	NAZCA	NAZCA	14.82818333	-74.944455	100M			0	1	1	0	2	URBANO	A	TIPO 1
0																		
3	DESPICAR NAZCA	CARRETERA PANAMERICANA SUR # SN	NAZCA	NAZCA	NAZCA	-14.84769	-74.94934	100M			0	0	1	0	0	URBANO	CARRERE RAS	TIPO 1
2																		
1	POSTA PNP NAZCA	PASAJE MONROY S/N PUEBLO SAN CARLOS	NAZCA	NAZCA	NAZCA	-14.830778	-74.93604	100M			0	1	1	0	1	URBANO	POSTA MEDICA	TIPO 1
3																		
2	CPNP VISTA ALEGRE	CALLE PACHACUTEC # SN	VISTA ALEGRE	NAZCA	NAZCA	14.84465333	-74.94033167	100M			0	1	1	0	2	URBANO	B	TIPO 1
3																		
2	CPNP PALPA/DIVPOL PALPA	AV. GRAU # SN	SAN PEDRO	PALPA	PALPA	14.59434617	-75.18819273	100M			0	1	1	0	2	RURAL	B	TIPO 1
4																		
3	CPNP INDEPENDENCIA PISCO	AV. FEDERICO URANGA # 100	INDEPENDENCIA	PISCO	PISCO	13.6935667	-76.030235	100M			0	1	1	0	1	URBANO	C	TIPO 1
5																		
3	CPNP PARACAS	AV. PARACAS # SN	PARACAS	PISCO	PISCO	13.83291667	-76.24679	100M			0	1	1	0	1	URBANO	C	TIPO 1
6																		
3	CPNP PISCO/DEPROC/SEANDRO/SEINCR/DIVPOL	CALLE SAN FRANCISCO # 139	PISCO	PISCO	PISCO	13.70919667	-76.20299333	100M			0	1	1	0	3	URBANO	A	TIPO 1
2																		
2	CPNP SAN MIGUEL PISCO	CALLE SAN MARTIN DE PORRAS # SN	PISCO	PISCO	PISCO	-13.702735	-76.15344833	100M			0	1	1	0	1	URBANO	C	TIPO 1
8																		
3	POSTA PNP PISCO	CALLE BEATTA DE HUMAY 200	PISCO	PISCO	PISCO	-13.711819	-76.205705	100M			0	1	1	0	1	URBANO	POSTA MEDICA	TIPO 1
9																		
3	CPNP SAN ANDRES PISCO	CALLE GRECIA # 501	SAN ANDRES	PISCO	PISCO	-13.732455	-76.221128	100M			0	1	1	0	1	URBANO	C	TIPO 1
0																		
3	CPNP HUAMANI	CARR. PANAMERICANA SUR KM.226	SAN CLEMENTE	PISCO	PISCO	-13.683075	-76.15951167	100M			0	1	1	0	1	URBANO	C	TIPO 1
3																		
3	CPNP TUPAC AMARU INCA	AV. TUPAC AMARU SN MZ.36 I.T.10	TUPAC AMARU INCA	PISCO	PISCO	-13.7142	-76.1487	100M			0	1	1	0	1	URBANO	D	TIPO 1
2																		

Handwritten signatures and initials at the top left of the page.



3	3	DESPRCAR LA MERCED	CARRETERA CENTRAL TARMA LA MERCED # SN	CHANCHAMAYO	CHANCHAMAYO	JUNIN	11.07901561	-75.32897383			0	0	1	0	0	RURAL	CARRETE RAS	TIPO 1
3	3	CPNP LA MERCED/DIVPOL CHANCHAMAYO	JIRON TARMA 694	CHANCHAMAYO	CHANCHAMAYO	JUNIN	11.05606701	-75.33087015	100M		0	1	1	0	2	RURAL	A	TIPO 1
3	3	POSTA PNP LA MERCED	JR. TARMA 694	CHANCHAMAYO	CHANCHAMAYO	JUNIN	-11.054.215	-75.326.614	100M		0	1	1	0	1	RURAL	POSTA MEDICA	TIPO 1
3	3	CPNP VILLA PERENE	JR. ISAJAS ALDORADIN S/N	PERENE	CHANCHAMAYO	JUNIN	10.95212667	-75.22560833	100M		0	1	1	0	1	RURAL	B	TIPO 1
3	3	CPNP PICHANAQUI	AV. MARGINAL # 509	PICHANAQUI	CHANCHAMAYO	JUNIN	10.92718939	-74.87345159	100M		0	1	1	0	1	RURAL	B	TIPO 1
3	3	CPNP SAN RAMON	JIRON PACHITEA # 467	SAN RAMON	CHANCHAMAYO	JUNIN	11.12087833	-75.35469167	100M		0	1	1	0	1	URBANO	B	TIPO 1
3	3	CPNP SECTORIAL CHUPACA/COM CAR CHUPACA	JIRON GRAU # 1	CHUPACA	CHUPACA	JUNIN	12.05991667	-75.28800167	100M		0	1	1	0	2	URBANO	B	TIPO 1
3	3	CPNP SECTORIAL CONCEPCION	JIRON BOLIVAR # 527	CONCEPCION	CONCEPCION	JUNIN	11.91908833	-75.314325	100M		0	1	1	0	2	URBANO	A	TIPO 1
3	3	CPNP CHILCA HUANCAYO	PASAJE SAN ANDRES # 189	CHILCA	HUANCAYO	JUNIN	12.08060151	-75.2080223	100M		0	1	1	0	2	URBANO	A	TIPO 1
3	3	CPNP EL TAMBO	JIRON GONZALES PRADA # SN / A MEDIA CUADRA DE LA PLAZA PRINCIPAL	EL TAMBO	HUANCAYO	JUNIN	12.05760333	-75.21737167	100M		0	1	1	0	1	URBANO	A	TIPO 1
3	3	DIVICAI PNP HUANCAYO	AV. 13 DE NOVIEMBRE 1280 URB. MIYOTINGO	EL TAMBO	HUANCAYO	JUNIN	-12.068813	-75.220404	100M		0	1	1	0	1	URBANO	DIVINCRI	TIPO 1
3	3	CPNP FAMILIA HUANCAYO	AV. GIRALDEZ 574	HUANCAYO	HUANCAYO	JUNIN	-12.065432	-75.204522	100M		0	1	1	0	1	URBANO	FAMILIA	TIPO 1
3	3	CPNP HUANCAYO/REG POL HUANCAYO 2DO PISO/TRANSITO/DIRTUMA/DIVPOL	AV. FERROCARRIL # 555	HUANCAYO	HUANCAYO	JUNIN	-12.0644773	-75.20747915	150M		0	1	1	0	3	URBANO	A	TIPO 1
3	3	DIRCOTE HUANCAYO	JR. ATALAYA S/N CONDOMINIO LAS CASUARINAS DISTRITO EL TAMBO	HUANCAYO	HUANCAYO	JUNIN	-12.0966356	-75.2157471	100M		0	1	1	0	1	URBANO	DIRCOTE	TIPO 1
3	3	HOSPITAL HUANCAYO ENRIQUE TORRES/ SANTA ROSA/POLICLINICO	JR. CUZCO 120	HUANCAYO	HUANCAYO	JUNIN	-12.065103	-75.207721	100M		0	1	1	0	1	URBANO	HOSPITAL	TIPO 1
3	3	OFICRI (AFIS) TUMBES	AV. PANAMERICANA NORTE KM 1322- TUMBES (COMPLEJO INTE JORGE TAYPE TARAZONA)	TUMBES	TUMBES	TUMBES	-3.55564	-80.43813	200M		0	1	1	0	1	URBANO	UNIDAD PNP	TIPO 1
3	3	ETS PNP HUANCAYO	JR. NECOCHEA S/N A LA ALTURA DEL KM. 04 DE LA CARRETERA CENTRAL HUANCAYO - JAJUA	PILCOMAYO	HUANCAYO	JUNIN	-12.046452	-75.245502	100M		0	1	1	0	5	URBANO	ETS	TIPO 1
3	3	CPNP SAN AGUSTIN DE CAJAS	AV. LEONCIO PRADO # SN	SAN AGUSTIN	HUANCAYO	JUNIN	11.99149833	-75.24658167	100M		0	1	1	0	1	URBANO	C	TIPO 1
3	3	CPNP SAN JERONIMO DE TUNAN	AV. AREQUIPA # SN	SAN JERONIMO DE TUNAN	HUANCAYO	JUNIN	-11.949605	-75.28255667	100M		0	1	1	0	1	URBANO	C	TIPO 1

3	CPNP SAPALLANGA	AV. FIDEL MIRANDA # 1300	SAPALLANGA	HUANCAYO	JUNIN	-12.14367	-75.16218833	100M				0	1	1	0	1	URBANO	C	TIPO 1
2																			
3	CPNP CMOTE FERRE PELAYO ALIAGA MIRANDA	JIRÓN CONSTITUCION # 300	SICAYA	HUANCAYO	JUNIN	-12.015425	-75.279505	100M				0	1	1	0	1	URBANO	C	TIPO 1
3																			
3	CPNP SECTORIAL JAUJA	JIRÓN FRANCISCO PIZARRO # 150	JAUJA	JAUJA	JUNIN	11.77803167	-75.49719333	100M				0	1	1	0	2	URBANO	A	TIPO 1
4																			
3	POSTA PNP JAUJA	JR. GALVEZ 335	JAUJA	JAUJA	JUNIN	-11.774265	-75.501403	100M				0	1	1	0	1	URBANO	POSTA MEDICA	TIPO 1
5																			
3	CPNP CARHUAMAYO	AV. LA UNION # SN	CARHUAMAYO	JUNIN	JUNIN	10.99425333	-76.05395667	100M				0	1	1	0	1	RURAL	C	TIPO 1
6																			
3	DEINCHI CHANCHAMAYO	JR. ARICA 166	CHANCHAMAYO	JUNIN	JUNIN	-11.056343	-75.330573	100M				0	1	1	0	2	RURAL	DIVINCRI	TIPO 1
5																			
3	CPNP SECTORIAL JUNIN	JIRÓN BERNARDO ALCEDO # SN	JUNIN	JUNIN	JUNIN	11.16255333	-75.99343833	100M				0	1	1	0	2	URBANO	B	TIPO 1
7																			
3	DESPRCAR JUNIN	JIRÓN YAUJI # SN	JUNIN	JUNIN	JUNIN	11.16589167	-76.00008	100M				0	0	1	0	0	URBANO	CARRERE RAS	TIPO 1
5																			
3	CPNP MAZAMARI	AV. SAN JUAN # SN	MAZAMARI	SATIPO	JUNIN	11.32823524	-74.52870458	100M				0	1	1	0	1	RURAL	C	TIPO 1
6																			
3	CPNP RIO NEGRO / DESPRCAR RIO NEGRO	CALLE UCAYALI # SN	PANGO	SATIPO	JUNIN	-11.421882	-74.48844	100M				0	1	1	0	1	RURAL	C	TIPO 1
1																			
3	CPNP RIO NEGRO / DESPRCAR RIO NEGRO	CARRERA ALAMEDA MARGINAL # SN	RIO NEGRO	SATIPO	JUNIN	-11.209535	-74.65966667	100M				0	1	1	0	0	RURAL	C	TIPO 1
6																			
3	CPNP SATIPO	JIRÓN FRANCISCO IRAZOLA # 493	SATIPO	SATIPO	JUNIN	-11.2556814	-74.63838011	100M				0	1	1	0	2	RURAL	B	TIPO 1
3																			
3	POSTA PNP SATIPO	JR. JUNIN 580	SATIPO	SATIPO	JUNIN	11.25342417	-74.6403562	100M				0	1	1	0	1	RURAL	POSTA MEDICA	TIPO 1
4																			
3	CPNP ACOBAMBA	JIRÓN CALLAO # SN	ACOBAMBA	TARMA	JUNIN	-11.353195	-75.65868333	100M				0	1	1	0	1	RURAL	C	TIPO 1
5																			
3	CPNP HUASAHUASI	JIRÓN SAN JUAN # SN	HUASAHUASI	TARMA	JUNIN	11.26562167	-75.64917167	100M				0	1	1	0	1	RURAL	C	TIPO 1
6																			
3	CPNP SECTORIAL TARMA/POSTA MEDICA TARMA	JIRÓN CALLAO # 118	TARMA	TARMA	JUNIN	11.41890953	-75.68693876	100M				0	1	1	0	2	URBANO	B	TIPO 1
6																			
3	CPNP SECTORIAL LA OROYA/COMICAR LA OROYA	AV. HORACIO ZEVALLOS GAMES # 209	LA OROYA	YAUJI	JUNIN	11.52249833	-75.909135	100M				0	1	1	0	2	URBANO	A	TIPO 1
5																			
3	CPNP MOROCOCHA	CLL. P. FLUQUER SN	MOROCOCHA	YAUJI	JUNIN	11.58755167	-76.06252667	100M				0	1	1	0	1	URBANO	C	TIPO 1
6																			
3	CPNP LA NORIA	AV. AMERICA SUR # 405 URB LA NORIA	TRUJILLO	TRUJILLO	LA LIBERTAD	-8.10950	-79.01049	100M				0	1	1	0	3	URBANO	A	TIPO 1
7																			
0																			

[Handwritten signature]



[Handwritten signature]

[Handwritten signature]

3	7	CPNP SECTORIAL RURAL ASCOPE	CALLE MANCO CAPAC # 16	ASCOPE	ASCOPE	LA LIBERTAD	7.713861667	-79.10762	100M			0	1	1	0	1	URBANO	A	TIPO 1
3	7	CPNP RURAL CASA GRANDE	AV. INDEPENDENCIA # 224	CASA GRANDE	ASCOPE	LA LIBERTAD	7.745213333	-79.188485	100M			0	1	1	0	1	URBANO	B	TIPO 1
3	7	CPNP RURAL ROMA	CALLE EDBERTO TORRES # SN	CASA GRANDE	ASCOPE	LA LIBERTAD	-7.764905	-79.14658833	100M			0	1	1	0	1	URBANO	D	TIPO 1
3	7	CPNP RURAL CHICAMA	AV. PROGRESO # 396	CHICAMA	ASCOPE	LA LIBERTAD	7.844921667	-79.14708833	100M			0	1	1	0	1	URBANO	C	TIPO 1
3	7	CPNP RURAL SAUSAL	CALLE CASA GRANDE # SN	CHICAMA	ASCOPE	LA LIBERTAD	-7.73606	-79.00716833	100M			0	1	1	0	1	URBANO	D	TIPO 1
3	7	CPNP RURAL CHOCOP	JIRÓN BOLOGNESI # 196	CHOCOP	ASCOPE	LA LIBERTAD	7.791226667	-79.22331167	100M			0	1	1	0	1	URBANO	B	TIPO 1
3	7	CPNP SECTORIAL RURAL PAJAN	PANAMERICANA NORTE MZ. 16 LT. 1A - SECTOR JORGE CHAVEZ	PAJAN	ASCOPE	LA LIBERTAD	-7.7193762	-79.3094247	100M			0	1	1	0	2	URBANO	A	TIPO 1
3	7	DIVEME PAJAN/DIVPOL/DEPINCRI	CARRETERA PANAMERICANA NORTE # SN	PAJAN	ASCOPE	LA LIBERTAD	-7.718849	-79.309494	100M			0	1	1	0	2	URBANO	DIVINCRI	TIPO 1
3	7	CPNP RURAL RAZURI	CALLE TARAPACA # 203	RAZURI	ASCOPE	LA LIBERTAD	7.700833333	-79.43774167	100M			0	1	1	0	1	URBANO	D	TIPO 1
3	7	CPNP RURAL CARTAVIO	CALLE REAL # SN	SANTIAGO DE CAO	ASCOPE	LA LIBERTAD	7.886556667	-79.22048667	100M			0	1	1	0	1	URBANO	C	TIPO 1
3	7	CPNP RURAL SANTIAGO DE CAO	CALLE LIBERTAD # 455	SANTIAGO DE CAO	ASCOPE	LA LIBERTAD	-7.959965	-79.239115	100M			0	1	1	0	1	URBANO	C	TIPO 1
3	7	CPNP RURAL TALAMBO	AV. MIRAFLORES # SN	CHEPEN	CHEPEN	LA LIBERTAD	-7.241655	-79.398555	100M			0	1	1	0	1	URBANO	C	TIPO 1
3	7	CPNP SECTORIAL RURAL CHEPEN	JIRÓN PACASMAYO # 471	CHEPEN	CHEPEN	LA LIBERTAD	-7.231765	-79.42438333	100M			0	1	1	0	1	URBANO	A	TIPO 1
3	7	DIVINCRI CHEPEN	PANAMERICANA NORTE S/N	CHEPEN	CHEPEN	LA LIBERTAD	-7.220083	-79.434736	100M			0	1	1	0	2	URBANO	DIVINCRI	TIPO 1
3	7	CPNP RURAL PACANGA	CALLE AYACUCHO # 798	PACANGA	CHEPEN	LA LIBERTAD	-7.170905	-79.48570833	100M			0	1	1	0	1	URBANO	B	TIPO 1
3	7	CPNP RURAL PACANGUILLA	JIRÓN EL MILAGRO # 336	PACANGA	CHEPEN	LA LIBERTAD	7.159668333	-79.44394833	100M			0	1	1	0	1	URBANO	C	TIPO 1
3	7	CPNP RURAL PUEBLO NUEVO	JIRÓN INDEPENDENCIA # 312	PUEBLO NUEVO	CHEPEN	LA LIBERTAD	-7.188135	-79.51499833	100M			0	1	1	0	1	URBANO	C	TIPO 1
3	7	CPNP SECTORIAL RURAL CASCAS	JIRÓN 28 DE JULIO # SN	CASCAS	GRAN CHIMU	LA LIBERTAD	7.480663333	-78.81823167	100M			0	1	1	0	1	RURAL	B	TIPO 1
3	7	CPNP SECTORIAL RURAL JULCAN	AV. LUIS FELIPE DE LA PUENTE UCEDA # SN	JULCAN	JULCAN	LA LIBERTAD	8.042741667	-78.48705833	100M			0	1	1	0	1	RURAL	B	TIPO 1

Handwritten signature and initials.

Handwritten signature and initials.



3	DIRCOCOR TRUJILLO	PREDIO UBICADO EN LA CALLE RICARDO SANCHEZ 407	TRUJILLO	LA LIBERTAD	LA LIBERTAD	-8.1101954	-79.0082068	100M			0	1	1	0	1	URBANO	DIRCOCO R	TIPO 1
0																		
3	CARCELETA JUDICIAL LIMA/OFICRI	AV. ABANCAY CUADRA 5 SN CERCADO / JR. AYACUCHO C-6	CERCADO	LIMA	LIMA	-12.05143	-77.02765	100M			0	1	1	0	1	URBANO	POLJUS	TIPO 1
1																		
3	CNPJ SECTORIAL RURAL OTUZCO	CALLE PROGRESO # 388	OTUZCO	OTUZCO	LA LIBERTAD	7.905083133	-78.56506437	100M			0	1	1	0	1	URBANO	A	TIPO 1
2																		
3	CNPJ RURAL CIUDAD DE DIOS	AV. REPUBLICA DE ALEMANIA # 303	GUADALUPE	PACASMAYO	LA LIBERTAD	7.305556667	-79.48027833	100M			0	1	1	0	1	URBANO	C	TIPO 1
3																		
9	CNPJ RURAL GUADALUPE	AV. NILA CERRUTI # SN	GUADALUPE	PACASMAYO	LA LIBERTAD	7.248273333	-79.47657833	100M			0	1	1	0	2	URBANO	B	TIPO 1
4																		
3	DESPRCAR GUADALUPE	AV. NILA CERRUTI # SN	GUADALUPE	PACASMAYO	LA LIBERTAD	7.248158333	-79.47588333	100M			0	0	1	0	0	URBANO	CARRETE RAS	TIPO 1
5																		
3	CNPJ RURAL JEQUETEPEQUE	CALLE SAN JOSE # 451	JEQUETEPEQUE	PACASMAYO	LA LIBERTAD	7.337551667	-79.56387833	100M			0	1	1	0	1	URBANO	D	TIPO 1
6																		
3	CNPJ RURAL PACASMAYO	CALLE DOS DE MAYO # 105	PACASMAYO	PACASMAYO	LA LIBERTAD	7.399441567	-79.57123833	100M			0	1	1	0	2	URBANO	A	TIPO 1
9																		
3	DEPINCRI PACASMAYO/ INSPECTORIA	JR. LEONCIO PRADO N° 457	PACASMAYO	PACASMAYO	LA LIBERTAD	-7.3989493	-79.5679516	100M			0	1	1	0	2	URBANO	DIVINCI	TIPO 1
8																		
3	CNPJ RURAL SAN JOSE	CALLE LIMA # 601	SAN JOSE	PACASMAYO	LA LIBERTAD	7.349913699	-79.45659041	100M			0	1	1	0	1	URBANO	C	TIPO 1
9																		
4	CNPJ RURAL SAN PEDRO DE LLOC	AV. 2 DE MAYO # SN	SAN PEDRO DE LLOC	PACASMAYO	LA LIBERTAD	7.424623333	-79.50288333	100M			0	1	1	0	2	URBANO	B	TIPO 1
0																		
4	CNPJ SECTORIAL PATAZ - TAYABAMBA	JIRÓN 2 DE MAYO # SN	TAYABAMBA	PATAZ	LA LIBERTAD	8.272533333	-77.29928667	100M			0	1	1	0	2	RURAL	A	TIPO 1
1																		
4	CNPJ RURAL HUAMACHUCO/DEINCI	AV. SANCHEZ CARRION # 1189	HUAMACHUCO	SANCHEZ CARRION	LA LIBERTAD	7.816941695	-78.04235078	100M			0	1	1	0	2	URBANO	A	TIPO 1
0																		
2	DESPRCAR HUAMACHUCO	AV. SANCHEZ CARRION # 1246	HUAMACHUCO	SANCHEZ CARRION	LA LIBERTAD	-7.817078	-78.042783	100M			0	0	1	0	0	URBANO	CARRETE RAS	TIPO 1
4																		
3	CNPJ RURAL QUIRUVILCA	CALLE MOROCOCOA # 111	QUIRUVILCA	SANTIAGO DE CHUCO	LA LIBERTAD	8.000751667	-78.30986	100M			0	1	1	0	1	RURAL	C	TIPO 1
0																		
4	CNPJ SECTORIAL RURAL SANTIAGO DE CHUCO	AV. MIGUEL GRAU # 1270	SANTIAGO DE CHUCO	SANTIAGO DE CHUCO	LA LIBERTAD	8.144891354	-78.17347527	100M			0	1	1	0	1	RURAL	A	TIPO 1
5																		
4	CNPJ ALTO TRUJILLO	AV. 12 DE NOVIEMBRE MZ. P LOTE 1A	EL PORVENIR	TRUJILLO	LA LIBERTAD	-8.06824	-79.02207333	100M			0	1	1	0	1	URBANO	C	TIPO 1
6																		
4	CNPJ NICOLAS ALCAZAR	PASAJE NICOLAS ALCAZAR # 1077	EL PORVENIR	TRUJILLO	LA LIBERTAD	8.085231667	-79.00463167	100M			0	1	1	0	2	URBANO	B	TIPO 1
0																		
4	CNPJ SANCHEZ CARRION	AV. SANCHEZ CARRION # 1010	EL PORVENIR	TRUJILLO	LA LIBERTAD	8.078746032	-78.9968952	100M			0	1	1	0	2	URBANO	A	TIPO 1
8																		

[Handwritten signature]



[Handwritten signature]

4	DIVINCI NORTE TRUJILLO	ANDRES RAZURI S/N III/AV CONDOCANQUI CDR 21 (FRENTE A LA IGLESIA CRISTO REY)	TRUJILLO	LA LIBERTAD	-8.070026	-78987815	100M		0	1	1	0	2	URBANO	DIVINCI	TIPO 1
4	CPNP FLORENCIA DE MORA	CALLE 26 DE JULIO # 1100	TRUJILLO	LA LIBERTAD	-8.085155	-79.024015	100M		0	1	1	0	1	URBANO	B	TIPO 1
4	CPNP HUANCHACO	JIRÓN COLON # 481	TRUJILLO	LA LIBERTAD	-8.079575	-79.12158333	100M		0	1	1	0	2	URBANO	C	TIPO 1
4	CPNP RURAL EL MILAGRO	AV. TUPAC AMARU MZ. LL LOTE 01 - EL MILAGRO	TRUJILLO	LA LIBERTAD	8.023378496	-79.06641215	100M		0	1	1	0	2	URBANO	B	TIPO 1
4	CPNP BELLAVISTA TRUJILLO	CALLE 22 DE FEBRERO # 803	TRUJILLO	LA ESPERANZA	-8.084672	-79.039737	100M		0	1	1	0	2	URBANO	B	TIPO 1
4	CPNP SECTORIAL JERUSALEN/WICHANZAO	AV. PANAMERICANA NORTE SN MZ.34 LT.1	TRUJILLO	LA ESPERANZA	8.056866667	-79.053925	100M		0	1	1	0	2	URBANO	A	TIPO 1
4	CPNP SECTORIAL RURAL LAREDO	PASAJE LA FORTUNA # SN	TRUJILLO	LA LIBERTAD	8.091904268	-78.96026105	100M		0	1	1	0	2	URBANO	B	TIPO 1
4	CPNP MIRAMAR	AV. SANTA MARIA SN MZ.30 LT.1A	TRUJILLO	LA LIBERTAD	8.180856667	-78.95415167	100M		0	1	1	0	1	URBANO	C	TIPO 1
4	CPNP MOCHE	AV. LA MARINA SN MZ.10 LT.42	TRUJILLO	LA LIBERTAD	8.170613654	-79.01090384	100M		0	1	1	0	1	URBANO	B	TIPO 1
4	DESPRCAR MOCHE	CARRETERA PANAMERICANA NORTE # SN	TRUJILLO	LA LIBERTAD	8.138895973	-79.01622802	100M		0	0	1	0	0	URBANO	CARRETE RAS	TIPO 1
4	CPNP SALAVERRY	CALLE LIBERTAD # 229	TRUJILLO	SALAVERRY	-8.22362	-78.576495	100M		0	1	1	0	1	URBANO	C	TIPO 1
4	DESPRCAR SIMBAL	CARRETERA PENETRACION A LA SIERRA NORTEÑA # SN	TRUJILLO	SIMBAL	-8.06435646	-78.86052176	100M		0	0	1	0	0	RURAL	CARRETE RAS	TIPO 1
4	COMISARIA DE TURISMO LA LIBERTAD	CALLE FEDERICO GERDES MZ L LOTE 02 URB. MOCHICA	TRUJILLO	LA LIBERTAD	-8.093442	-79.039126	100M		0	0	1	0	1	URBANO	TURISMO	TIPO 1
4	CPNP EL ALAMBRE	CALLE PORTO ALEGRE # 100	TRUJILLO	LA LIBERTAD	8.107195679	-79.03950691	100M		0	1	1	0	2	URBANO	A	TIPO 1
4	DIVICA-SECAP -LA LIBERTAD	SECTOR NATASHA ALTA AV. AMERICA NOR OESTE S/N CUADRA 7 URB COVICORTI SOTANO DE LA CORTE SUPERIOR DE JUSTICIA LA LIBERTAD	TRUJILLO	LA LIBERTAD	-8.113471	-79.048251	100M		0	1	1	0	1	URBANO	DIVINCI	TIPO 1
4	REGPOL LA LIBERTAD	JR. DIEGO DE ALMAGRO N° 327	TRUJILLO	LA LIBERTAD	-8.111251	-79.030128	150M		0	1	1	0	1	URBANO	REGPOL	TIPO 1
4	POL PNP TRUJILLO	AV. STA TERESITA DE JESÚS S/N	Trujillo	LA LIBERTAD	-8.123257	-79.031604	100M		0	1	1	0	1	URBANO	POLICINI CO	TIPO 1
4	CPNP BUENOS AIRES	AV. LARCO HERRERA # 598	TRUJILLO	VICTOR LARCO HERRERA	8.140866667	-79.05229833	100M		0	1	1	0	2	URBANO	B	TIPO 1
4	CPNP RURAL CHAO	AV. VICTOR BAUL HAYA DE LA TORRE SN MZ.3 LT.11 KM.500	VIRU	CHAO	8.53756667	-78.67920833	100M		0	1	1	0	1	RURAL	C	TIPO 1

[Handwritten signature]



[Handwritten signature]

4	CPNP RURAL VICTOR RAUL HAYA DE LA TORRE	CALLE CESAR VALLEJO # SN	VIRU	VIRU	LA LIBERTAD	-8.404665	-78.82218667	100M			0	1	1	0	1	URBANO	C	TIPO 1
2																		
8																		
4	CPNP RURAL VIRU/TRANSITO UIUEE	AV. VIRU # 125	VIRU	VIRU	LA LIBERTAD	-8.41525759	-78.75504591	100M			0	1	1	0	2	URBANO	B	TIPO 1
2																		
9																		
4	DESPICAR VIRU	CARRITERA PANAMERICANA NORTE # SN	VIRU	VIRU	LA LIBERTAD	8.423836667	-78.78235167	100M			0	0	1	0	0	URBANO	CARRETERAS	TIPO 1
0																		
4	CPNP SECTORIAL CAYALTI	AV. 9 DE OCTUBRE # 110	CAYALTI	CHICLAYO	LAMBAYEQUE	-6.89141	-79.56132	100M			0	1	1	0	1	URBANO	B	TIPO 1
3																		
1																		
4	CP PNP JUAN ARAGON VENTE /DEPLINEME	CALLE CADIZ N° 154 URB SAN JUAN	CHICLAYO	CHICLAYO	LAMBAYEQUE	-6.767580	-79.833460	100M			0	0	1	0	1	URBANO		TIPO 1
3	CHICLAYO /AGUILAS NEGRAS/ UDEB/ RESCATE																	
2																		
4	CPNP CAMPODONICO	AV. JORGE CHAVEZ # 801	CHICLAYO	CHICLAYO	LAMBAYEQUE	-6.76828	-79.82985	100M			0	1	1	0	1	URBANO	B	TIPO 1
3																		
3	CPNP CESAR LLATAS CASTRO	CALLE VICENTE DE LA VEGA # 1182	CHICLAYO	CHICLAYO	LAMBAYEQUE	6.770736667	-79.83541667	100M			0	1	1	0	2	URBANO	A	TIPO 1
4																		
4	CPNP DEL NORTE	CALLE FRANCISCO CUNEO # 1119	CHICLAYO	CHICLAYO	LAMBAYEQUE	-6.76913	-79.85572	100M			0	1	1	0	1	URBANO	B	TIPO 1
5																		
4	CPNP EL PORVENIR	CALLE ARICA # 499	CHICLAYO	CHICLAYO	LAMBAYEQUE	6.766031667	-79.84469833	100M			0	1	1	0	1	URBANO	C	TIPO 1
3																		
6																		
4	ETS PNP CHICLAYO	KM.18.5 CARR. CHICLAYO	CHICLAYO	CHICLAYO	LAMBAYEQUE	-6.885145	-79.823772	100M			0	1	1	0	5	URBANO	ETS	TIPO 1
3																		
7																		
4	REGPOL LAMBAYEQUE	MANCO CAPAC N°205 ESQUINA CON CALLE SAN JOSE	CHICLAYO	CHICLAYO	LAMBAYEQUE	-6.77138	-79.89541	150M			0	1	1	0	1	URBANO	REGPOL	TIPO 1
3																		
8																		
4	CPNP PAMPA GRANDE	AV. TUPAC AMARU # SN	CHONGOYAPE	CHONGOYAPE	LAMBAYEQUE	6.746161667	-79.47912667	100M			0	1	1	0	1	URBANO	D	TIPO 1
3																		
9																		
4	CPNP SECTORIAL CHONGOYAPE	CALLE SIMON BOLIVAR # 2520	CHONGOYAPE	CHONGOYAPE	LAMBAYEQUE	-6.63645	-79.39415333	100M			0	1	1	0	1	URBANO	C	TIPO 1
0																		
4	CPNP CIUDAD ETEN	CALLE PEDRO RUJZ GALLO # 692	ETEN	ETEN	LAMBAYEQUE	-6.9072	-79.86165	100M			0	1	1	0	1	URBANO	D	TIPO 1
1																		
4	CPNP PUERTO ETEN	CALLE DIEGO FERRE # SN	ETEN PUERTO	ETEN PUERTO	LAMBAYEQUE	-6.927315	-79.86366	100M			0	1	1	0	1	URBANO	D	TIPO 1
4																		
2																		
4	CPNP ATUSPARIA	AV. VIRREY TOLEDO # 1098	JOSE LEONARDO ORTIZ	CHICLAYO	LAMBAYEQUE	-6.75917	-79.82561	100M			0	1	1	0	2	URBANO	B	TIPO 1
4																		
3																		
4	CPNP JOSE LEONARDO ORTIZ	AV. ARGENTINA # 2252	JOSE LEONARDO ORTIZ	CHICLAYO	LAMBAYEQUE	6.752663333	-79.84270167	100M			0	1	1	0	1	URBANO	B	TIPO 1
4																		
4																		
4	CPNP LA VICTORIA CHICLAYO	AV. PACHACUTEC # 1510	LA VICTORIA	CHICLAYO	LAMBAYEQUE	6.798675124	-79.83548462	100M			0	1	1	0	2	URBANO	B	TIPO 1
5																		
4	CPNP SECTORIAL MONSEFU	CALLE 7 DE JUNIO # 519	MONSEFU	CHICLAYO	LAMBAYEQUE	-6.87793	-79.87246	100M			0	1	1	0	2	URBANO	B	TIPO 1
6																		

4	4	CPNP PATAPO	CALLE SALAZAR # 13	PATAPO	CHICLAYO	LAMBAYEQUE	-6.73767	-79.64052667	100M			0	1	1	0	1	URBANO	D	TIPO 1
4	4	CPNP POSOPE ALTO	CALLE SANTA ROSA # 398	PATAPO	CHICLAYO	LAMBAYEQUE	-6.73519	-79.63466	100M			0	1	1	0	1	URBANO	C	TIPO 1
4	4	CPNP PICSÍ	JR. SAN MARTÍN S/N	PICSÍ	CHICLAYO	LAMBAYEQUE	-6.71795	-79.76999	100M			0	1	1	0	1	URBANO	C	TIPO 1
4	4	CPNP PIMENTEL	CALLE GRAU # SN	PIMENTEL	CHICLAYO	LAMBAYEQUE	-6.83491	-79.93585	100M			0	1	1	0	1	URBANO	C	TIPO 1
4	4	CPNP POMALCA	CALLE LOS PROFESIONALES - CHALE NRO. 5 - URB. MIRAFLORES	POMALCA	CHICLAYO	LAMBAYEQUE	-6.77034	-79.77272	100M			0	1	1	0	1	URBANO	C	TIPO 1
4	4	CPNP REQUE	CALLE DIEGO FERRE # 100	REQUE	CHICLAYO	LAMBAYEQUE	6.863198333	-79.81846167	100M			0	1	1	0	1	URBANO	C	TIPO 1
4	4	CPNP SANTA ROSA LAMBAYEQUE	AV. MARISCAL CASTILLA # 901	SANTA ROSA	CHICLAYO	LAMBAYEQUE	-6.87972	-79.92344	100M			0	1	1	0	1	URBANO	D	TIPO 1
4	4	CPNP JAIME ANTONIO LI CHUNG	AV. POMALCA SN	SARA	CHICLAYO	LAMBAYEQUE	6.811753333	-79.64037167	100M			0	1	1	0	1	URBANO	D	TIPO 1
4	4	CPNP SECTORIAL TUMAN	AV. RAMON CASTILLA # 418	TUMAN	CHICLAYO	LAMBAYEQUE	-6.74956	-79.70300167	100M			0	1	1	0	1	URBANO	B	TIPO 1
4	4	CPNP SECTORIAL FERREÑAFE	AV. TACNA # 620	FERREÑAFE	FERREÑAFE	LAMBAYEQUE	6.635228333	-79.79128167	100M			0	1	1	0	2	URBANO	A	TIPO 1
4	4	CPNP BATANGRADE	CALLE CALPON # 16	PITPO	FERREÑAFE	LAMBAYEQUE	-6.4833	-79.65425167	100M			0	1	1	0	1	URBANO	C	TIPO 1
4	4	CPNP JAYANCA	CALLE ELIAS AGUIRRE # 405	JAYANCA	LAMBAYEQUE	LAMBAYEQUE	6.391463333	-79.82297667	100M			0	1	1	0	1	URBANO	C	TIPO 1
4	4	CPNP SAN MARTIN DE PORRAS	CALLE CAPITAN ORBEGOSO # SN	LAMBAYEQUE	LAMBAYEQUE	LAMBAYEQUE	6.708368333	-79.91427833	100M			0	1	1	0	4	URBANO	B	TIPO 1
4	4	CPNP SECTORIAL LAMBAYEQUE	CALLE DOS DE MAYO # 316	LAMBAYEQUE	LAMBAYEQUE	LAMBAYEQUE	-6.70113	-79.90669	100M			0	1	1	0	2	URBANO	A	TIPO 1
4	4	CPNP MOCHUMI	AV. JOSE DE SAN MARTIN # 461	MOCHUMI	LAMBAYEQUE	LAMBAYEQUE	6.551116667	-79.86653667	100M			0	1	1	0	1	URBANO	C	TIPO 1
4	4	CPNP TINTÉ VICTOR HERNAN COSTA SAAVEDRA	AV. PRIMAVERA # 477	MOTUPE	LAMBAYEQUE	LAMBAYEQUE	-6.153845	-79.71215833	100M			0	1	1	0	1	URBANO	C	TIPO 1
4	4	CPNP TUCUME	AV. FEDERICO VILLARREAL # 266	TUCUME	LAMBAYEQUE	LAMBAYEQUE	-6.50636	-79.85943667	100M			0	1	1	0	1	URBANO	D	TIPO 1
4	4	CENTRO DE PROTECCION N° 1 SALAMANCA - DIVNA-DIRSECU PNP	CALLE LAS AZULENAS 260 SALAMANCA	ATE	LIMA	LIMA	-12.074962	-76.990691	100M			0	0	1	0	1	URBANO	UNIDAD	TIPO 1
4	4	CPNP 10 DE OCTUBRE	JIRON MARCELO # SN	SAN JUAN DE LURIGANCHO	LIMA	LIMA	-11.94451	-76.98846833	100M			5	1	1	0	3	URBANO	B	TIPO 1



4	6	DIVPOL BARRANCA JEFATURA	JR JOSE GALVEZ N°490	BARRANCA	BARRANCA	LIMA	-10.753863	-77.758897	150M			0	1	1	0	1	URBANO	DIVPOL	TIPO 1
4	6	CPNP AEROPUERTO INTERNACIONAL JORGE CHAVEZ	AV. ELMER FAUCETT REF. CUADRA 30 COSTADO DEL AEROPUERTO INTERNACIONAL JORGE CHAVEZ	CALLAO	CALLAO	LIMA	12.02616567	-77.10455444	100M			0	1	1	0	0	URBANO	B	TIPO 1
4	6	CPNP ALFONSO UGARTE	AV. ALFONSO UGARTE # 1325	CERCADO	LIMA	LIMA	-12.0570424	-77.04130411	100M			0	1	1	0	3	URBANO	A	TIPO 1
4	6	DIROPS	AV. CRNEL MARCO PUENTE LLANOS	ATE	LIMA	LIMA	-12.039006	-76.914048	100M			0	1	1	0	1	URBANO	COMISARI A	TIPO 1
4	6	CPNP ANCON	AV. JOSE CARLOS MARIATEGUI # SN	ANCON	LIMA	LIMA	-11.7759478	-77.16932058	100M			0	1	1	0	2	URBANO	B	TIPO 1
4	6	CPNP ASIA	AV. LA MAR # SN	ASIA	CAÑETE	LIMA	12.77907498	-76.55660734	100M			0	1	1	0	1	URBANO	COMISARI A	TIPO 1
4	6	CPNP AUCALLAMA	JIRÓN PROGRESO # SN	AUCALLAMA	HUARAL	LIMA	11.55862333	-77.17915	100M			0	1	1	0	1	RURAL	C	TIPO 1
4	6	CPNP BARBONCITOS	JIRÓN EL SALVADOR # SN	SAN MARTIN DE PORRES	LIMA	LIMA	12.03089667	-77.070025	100M			0	1	1	0	3	URBANO	B	TIPO 1
4	6	CPNP BARRANCA	AV. INDEPENDENCIA # SN	BARRANCA	BARRANCA	LIMA	-10.75077	-77.76506	100M			0	1	1	0	2	URBANO	A	TIPO 1
4	6	CPNP BAYOVAR	AV. 1 DE MAYO # SN	SAN JUAN DE LURIGANCHO	LIMA	LIMA	11.95241261	-76.9917798	100M			0	1	1	0	3	URBANO	B	TIPO 1
4	6	CPNP BELLAVISTA CALLAO	AV. GUARDIA CHALACA # SN	BELLAVISTA	CALLAO	LIMA	12.06162167	-77.12518157	100M			0	1	1	0	3	URBANO	B	TIPO 1
4	6	CPNP BOCANEGRA	CALLE GAMMA # SN	CALLAO	CALLAO	LIMA	-12.024315	-77.09550667	100M			0	1	1	0	2	URBANO	B	TIPO 1
4	6	CPNP CAJA DE AGUA	JR. MOQUEGUA Y JR. TRUJILLO S/N	SAN JUAN DE LURIGANCHO	LIMA	LIMA	1.202.723.000.000	7.701.509.000.000	100M			0	1	1	0	3	URBANO	A	TIPO 1
4	6	CPNP CALANGO	AV. GRANADO # 350	CALANGO	CAÑETE	LIMA	12.52658165	-76.54374038	100M			0	1	1	0	1	URBANO	COMISARI A	TIPO 1
4	6	CPNP CALLAO	JIRÓN SUPE # SN	CALLAO	CALLAO	LIMA	12.05493333	-77.12884833	100M			0	1	1	0	3	URBANO	A	TIPO 1
4	6	CPNP CANTA	AV. 26 DE JUNIO # SN	CANTA	CANTA	LIMA	11.46908333	-76.62419	100M			0	1	1	0	1	URBANO	B	TIPO 1
4	6	CPNP CANTO REY	JIRÓN RIO UCAYALI # 3550	SAN JUAN DE LURIGANCHO	LIMA	LIMA	11.97557333	-76.99600833	100M			0	1	1	0	3	URBANO	B	TIPO 1
4	6	CPNP CARABAYLLO	JIRÓN MIGUEL GRAU # 285	CARABAYLLO	LIMA	LIMA	-11.854	-77.03787667	100M			0	1	1	0	2	URBANO	B	TIPO 1
4	6	CPNP CARMEN DE LA LEGUA REYNOSO	AV. 1 DE MAYO # 1106	CARMEN DE LA LEGUA REYNOSO	CALLAO	LIMA	12.03922833	-77.08735667	100M			0	1	1	0	2	URBANO	B	TIPO 1

Handwritten signatures and marks at the top left of the page.



Handwritten signatures and initials in the middle left margin.

4	CPNP CASAPALCA	CARRTERA CENTRAL # SN	CHICLA	HUARACHIRI	LIMA	-11.652247	-76.235607	100M			0	1	1	0	1	RURAL	B	TIPO 1
5	CPNP CATAHUASI	AV. GONZALES PRADA N. 165	CATAHUASI	YAUYES	LIMA	-12.798929	-75.89156165	100M			0	1	1	0	1	URBANO	COMISARI A	TIPO 1
6	CPNP CERRO AZUL	JIRÓN ALFONSO UGARTE # SN	CERRO AZUL	CANETE	LIMA	13.02489333	-76.47857333	100M			0	1	1	0	1	URBANO	B	TIPO 1
7	CPNP CHACARILLA DEL ESTANQUE	JIRÓN ALFREDO GALEON MAYORAZGO # SN	SAN BORJA	LIMA	LIMA	12.10855833	-76.98350667	100M			0	1	1	0	2	URBANO	B	TIPO 1
8	CPNP CHACACAYO/POLICLINICO	AV. EL ROSARIO # 591	CHACACAYO	LIMA	LIMA	11.97712833	-76.76541667	100M			0	1	1	0	2	URBANO	B	TIPO 1
9	CPNP CHACRA COLORADA	JIRÓN CARHUAZ # 479	BREÑA	LIMA	LIMA	-12.05412	-77.05092833	100M			0	1	1	0	4	URBANO	B	TIPO 1
0	AEROPUERTO JORGE CHAVEZ	AV. ELMER FAUCETT S/N - SALIDA INTERNACIONAL	CALLAO	CALLAO	LIMA	-12.02405	-77.1122	200M			0	1	1	0	1	URBANO	RQ	TIPO 1
1	CPNP CHANCAY	AV. BOLIVAR # 150	CHANCAY	HUARAL	LIMA	11.56259301	-77.26937167	100M			0	1	1	0	2	URBANO	B	TIPO 1
2	CPNP CHILCA	AV. SAN MARCELO # 412	CHILCA	CANETE	LIMA	-12.517925	-76.73706833	100M			0	1	1	0	1	URBANO	B	TIPO 1
3	CPNP CHORRILLOS	AV. DEFENSORES DEL MORRO # 656	CHORRILLOS	LIMA	LIMA	12.17030833	-77.02331333	100M			0	1	1	0	3	URBANO	A	TIPO 1
4	CPNP CHOSICA	AV. 28 DE JULIO # 576	LURIGANCHIO	LIMA	LIMA	-11.988795	-76.696551	100M			0	1	1	0	2	URBANO	A	TIPO 1
5	CPNP CHURIN	AV. LARCO HERRERA N° 280	PACHANGARA	OYON	LIMA	-10.811067	-76.874955	100M			0	1	1	0	1	URBANO	COMISARI A	TIPO 1
6	CPNP LA PUNTA/ CPNP ESPECIAL DE TURISMO	AV. MIGUEL GRAU # 1002	LA PUNTA	CALLAO	LIMA	12.06827667	-77.15785	150M			1	1	1	0	3	URBANO	B	TIPO 1
7	CPNP CIENEGUILLA/DESPCAR CIENEGUILLA	AV. NUEVA TOLEDO # 104	CIENEGUILLA	LIMA	LIMA	-12.115665	-76.81292833	100M			1	1	1	0	2	URBANO	B	TIPO 1
8	CPNP CIUDAD DEL PESCADOR	AV. JUAN VELASCO ALVARADO # 1299	BELLAVISTA	CALLAO	LIMA	-12.05887	-77.104905	100M			0	1	1	0	4	URBANO	B	TIPO 1
9	CPNP CIUDAD Y CAMPO	CALLE JACINTO BENAVENTE # 258	RIMAC	LIMA	LIMA	-12.024368	-77.02795	100M			0	1	1	0	2	URBANO	B	TIPO 1
0	CPNP CIUDADELA CHALACA	CLL. 12 DE MAYO MZ. I LT 13	CALLAO	CALLAO	LIMA	12.05025389	-77.131598	100M			0	1	1	0	3	URBANO	B	TIPO 1
1	CPNP COLLIQUE	AV. REVOLUCION # SN	COMAS	LIMA	LIMA	-11.913295	-77.01616	100M			0	1	1	0	3	URBANO	B	TIPO 1
2	CPNP CONDE DE LA VEGA	JIRÓN CONDESUYOS # 659	CERCADO	LIMA	LIMA	12.03852833	-77.05324667	100M			0	1	1	0	2	URBANO	A	TIPO 1
3																		

Handwritten signature and initials.



Handwritten signature.

Handwritten signature.

5	0	CPNP CONDEVILLA	JIRÓN PABLO BERMUDEZ Y BILLINGHURST # SN	SAN MARTIN DE PORRES	LIMA	LIMA	12.02048916	-77.08542109	100M			0	1	1	0	3	URBANO	B	TIPO 1
4	0	CPNP COTABAMBAS	JIRÓN BUENAVENTURA # SN	CERCADO	LIMA	LIMA	12.05804505	-77.03417413	100M			0	1	1	0	2	URBANO	A	TIPO 1
5	0	CPNP CRUZ BLANCA	CARRITERA ANTIGUA PANAMERICANA NORTE # SN	HUALWAY	HUALA	LIMA	-11.09729	-77.59568333	100M			0	1	1	0	1	URBANO	B	TIPO 1
6	0	CPNP DE LA FAMILIA - VILLA EL SALVADOR	OTRO SECTOR 2 GRUPO 15 # SN	VILLA EL SALVADOR	LIMA	LIMA	12.21251833	-76.938495	100M			0	1	1	0	1	URBANO	FAMILIA	TIPO 1
7	5	CPNP DE LA FAMILIA BERTHA GONZALES POSADA EYZAGUIRE	PASAJE BUENAVENTURA # SN	CERCADO	LIMA	LIMA	12.05793167	-77.034525	100M			0	1	1	0	1	URBANO	FAMILIA	TIPO 1
8	0	CPNP DE LA FAMILIA CANTO REY	CLL RIO CHIRA SN	SAN JUAN DE LURIGANCHO	LIMA	LIMA	11.97590167	-76.99548167	100M			0	1	1	0	1	URBANO	FAMILIA	TIPO 1
9	5	CPNP DE LA FAMILIA COMAS COLIQUE	CALLE LOS OLIVOS # SN	COMAS	LIMA	LIMA	11.91298333	-77.01021	100M			0	1	1	0	1	URBANO	FAMILIA	TIPO 1
0	5	CPNP DE LA FAMILIA INDEPENDENCIA	JIRÓN 1 DE MAYO # 337	INDEPENDENCIA	LIMA	LIMA	-11.99228	-77.05040833	100M			0	1	1	0	1	URBANO	FAMILIA	TIPO 1
1	5	CPNP DE LA FAMILIA SAN JUAN MIRAFLORES	AV. TOMAS GUZMAN # 320	SAN JUAN DE MIRAFLORES	LIMA	LIMA	12.16649833	-76.96538833	100M			0	1	1	0	1	URBANO	FAMILIA	TIPO 1
2	5	CPNP DISTRITO PACHACAMAC	JIRÓN CASTILLA # 521	PACHACAMAC	LIMA	LIMA	12.22776167	-76.85851333	100M			0	1	1	0	2	URBANO	B	TIPO 1
3	5	CPNP DULANTO	JIRÓN HUANCAYO # SN	CALLAO	CALLAO	LIMA	-12.044185	-77.10468167	100M			0	1	1	0	2	URBANO	B	TIPO 1
4	5	CPNP EL AGUSTINO	JIRÓN JUAN HOYLE PALACIOS # 440	EL AGUSTINO	LIMA	LIMA	-12.04936	-76.997755	100M			0	1	1	0	2	URBANO	A	TIPO 1
5	5	CPNP EL MAIZANO	PASAJE CASSINELLI # 140	RIMAC	LIMA	LIMA	-12.0283	-77.03003333	100M			0	1	1	0	2	URBANO	B	TIPO 1
6	5	CPNP EL PROGRESO	AV. TUPAC AMARU # 3900	CARABAYLLO	LIMA	LIMA	11.87460861	-77.01572992	100M			0	1	1	0	3	URBANO	B	TIPO 1
7	5	CPNP ESPECIAL DE TURISMO LIMA NORTE	JR. ALMIRANTE MARTIN GUISE Nº 1715	LINCE	LIMA	LIMA	12.08206979	-77.03919278	100M			0	0	1	0	1	URBANO	TURISMO	TIPO 1
8	5	CPNP FAMILIA EL AGUSTINO	JR ALFREDO TEJADA DIAZ 237 EL AGUSTINO	EL AGUSTINO	LIMA	LIMA	-12.05041	-76.99804	100M			0	1	1	0	1	URBANO	COMISARI A	TIPO 1
9	5	CPNP FLOR DE AMANCAES	COMITÉ 13 AAHH FLOR DE AMANCAES	RIMAC	LIMA	LIMA	-12.01004	-77.03348	100M			0	1	1	0	2	URBANO	C	TIPO 1
0	5	CPNP GORGOR	PLAZA DE PRINCIPAL S/N	GORGOR	BARREANCA	LIMA	-10.64589	-70.46598	100M			0	1	1	0	1	URBANO	COMISARI A	TIPO 1
1	5	CPNP HUACHIPA	AV. LAS GARZAS # SN	LURIGANCHO	LIMA	LIMA	12.01459833	-76.957425	100M			0	1	1	0	2	URBANO	B	TIPO 1
2	2																		

Handwritten signatures and marks at the top left of the page.



Handwritten signature and initials in the middle left of the page.

5	CPNP HUACHO	JIRÓN SALAVERRY # 279	HUACHO	HUAURA	LIMA	11.10973333	-77.60778933	100M			0	1	1	0	3	URBANO	A	TIPO 1
3																		
5	SECPRY PNP	AV. 19 DE JULIO N° 205	CAJAMARCA	CAJAMARCA	CAJAMARCA	-7.159401	-78.523000	100M			0	1	1	0	1	URBANO	COMISARI A	TIPO 1
2	CPNP HUARAL	AV. EL SOLAR # 454	HUARAL	HUARAL	LIMA	11.49499333	-77.20673667	100M			0	1	1	0	1	URBANO	A	TIPO 1
5																		
5	CPNP HUARACHIRI	PROLONG. GRAU S/N MAZ. 76 LT. 36 KM. 150	HUARACHIRI	HUARACHIRI	LIMA	-12.135137	-76.234567	100M			0	1	1	0	1	URBANO	COMISARI A	TIPO 1
6																		
5	CPNP HUAURA	OTRO PLAZUELA SAN FRANCISCO # SN	HUAURA	HUAURA	LIMA	11.06805833	-77.59945167	100M			0	1	1	0	2	URBANO	A	TIPO 1
7																		
5	CPNP HUAYCAN	AV. JOSE CARLOS MARIATEGUI # SN	ATE	LIMA	LIMA	12.01298333	-76.827405	100M			0	1	1	0	2	URBANO	B	TIPO 1
2																		
5	CPNP IMPERIAL	JIRÓN DOS DE MAYO # 350	IMPERIAL	CAÑETE	LIMA	13.06137167	-76.35300333	100M			0	1	1	0	2	URBANO	A	TIPO 1
9																		
5	CPNP JESUS MARIA	AV. ARNALDO MARQUEZ N° 1044	JESUS MARIA	LIMA	LIMA	12.07103246	-77.04754344	100M			0	1	1	0	3	URBANO	A	TIPO 1
3																		
5	CPNP JICAMARCA	OVALO CENTRAL S/N JICAMARCA ANEXO-08	LURIGANCHO	LIMA	LIMA	11.98092243	-76.94387302	100M			0	1	1	0	1	URBANO	COMISARI A	TIPO 1
1																		
5	CPNP JOSE CARLOS MARIATEGUI	JIRÓN JORGE CHAVEZ # 181	VILLA MARIA DEL TRIUNFO	LIMA	LIMA	-12.149666	-76.950367	100M			0	1	1	0	2	URBANO	B	TIPO 1
3																		
5	CPNP JOSE GALVEZ	AV. LIMA # 500	VILLA MARIA DEL TRIUNFO	LIMA	LIMA	12.20781667	-76.96640167	100M			0	1	1	0	2	URBANO	B	TIPO 1
3																		
5	CPNP JUAN INGUNZA VALDIVIA	AV. TOMAS VALLE # SN	CALLAO	CALLAO	LIMA	12.01430667	-77.09654833	100M			0	1	1	0	3	URBANO	B	TIPO 1
3																		
5	CPNP LA ENSENADA	JIRÓN JACARANDA # SN	PUENTE PIEDRA	LIMA	LIMA	11.93625833	-77.09414167	100M			0	1	1	0	3	URBANO	B	TIPO 1
3																		
5	CPNP LA HUAYRONA	JIRÓN LAS GEMAS # SN	SAN JUAN DE LURIGANCHO	LIMA	LIMA	11.99424167	-77.00683167	100M			0	1	1	0	3	URBANO	B	TIPO 1
3																		
5	CPNP LA LEGUA	CALLE MANUEL VIDAURRE # 100	CARMEN DE LA LEGUA REYNOSO	CALLAO	LIMA	-12.052855	-77.09692	100M			0	1	1	0	2	URBANO	B	TIPO 1
3																		
5	CPNP LA MOLINA	AV. ELIAS APARICIO # SN	LA MOLINA	LIMA	LIMA	12.07732167	-76.916685	100M			0	1	1	0	2	URBANO	A	TIPO 1
3																		
5	CPNP LA PASCANA	JIRÓN JOSE CARLOS MARIATEGUI # SN	COMAS	LIMA	LIMA	11.93553676	-77.04673827	100M			0	1	1	0	3	URBANO	B	TIPO 1
3																		
5	CPNP LA PERLA	JIRÓN BRASIL # 664	LA PERLA	CALLAO	LIMA	12.07013333	-77.12629	100M			0	1	1	0	3	URBANO	A	TIPO 1
3																		
5	CPNP LA UNIFICADA	AV. 2 DE MARZO N° 229 (AA.HH.EL VOLANTE)	INDEPENDENCIA	LIMA	LIMA	-12.055906	-77.047787	100M			0	1	1	0	2	URBANO	C	TIPO 1
3																		



5	AV. PANAMERICA NORTE URB. SANTA MARIA 1360	HUACHO	HUAURA	LIMA	-11.105669	-77.595426	150M				0	1	1	0	1	URBANO	DIVINCI	TIPO 1
4	DIVICAJ / OFICIA HUACHO																	
2																		
4	CPNP LADERAS DE VILLA		LIMA	LIMA	12.19071667	-76.95762333	100M				0	1	1	0	2	URBANO	B	TIPO 1
5																		
3	CPNP LAS PRADERAS		LIMA	LIMA	12.11471833	-76.93712	100M				0	1	1	0	2	URBANO	B	TIPO 1
4																		
5	CPNP LAURA CALLER IBERICO		LIMA	LIMA	11.97065167	-77.07812833	100M				0	1	1	0	3	URBANO	B	TIPO 1
4																		
5	CPNP LINCE		LIMA	LIMA	12.08336833	-77.02702167	100M				0	1	1	0	3	URBANO	A	TIPO 1
4																		
5	CPNP LUNAHUANA		CAÑETE	LIMA	12.96356333	-76.14018833	100M				0	1	1	0	2	URBANO	B	TIPO 1
4																		
5	CPNP LURIN		LIMA	LIMA	-12.273685	-76.869174	100M				0	1	1	0	3	URBANO	B	TIPO 1
4																		
5	CPNP LURIN VILLA ALEJANDRO		LIMA	LIMA	-12.234075	-76.90772	100M				0	1	1	0	1	URBANO	B	TIPO 1
4																		
5	CPNP MAGDALENA DEL MAR		LIMA	LIMA	12.08816833	-77.07337167	100M				0	1	1	0	3	URBANO	A	TIPO 1
4																		
5	CPNP MALA		CAÑETE	LIMA	-12.860823	-76.632053	100M				0	1	1	0	3	URBANO	A	TIPO 1
4																		
5	CPNP MANCHAY		LIMA	LIMA	12.11613833	-76.87007167	100M				0	1	1	0	1	URBANO	B	TIPO 1
4																		
5	CPNP MARGANGA		LIMA	LIMA	-12.06987	-77.093015	100M				0	1	1	0	3	URBANO	B	TIPO 1
4																		
5	CPNP MARISCAL CACERES		LIMA	LIMA	-11.949195	-76.98108333	100M				0	1	1	0	3	URBANO	B	TIPO 1
4																		
5	CPNP MARQUEZ		CALLAO	LIMA	11.94473833	-77.13421333	100M				0	1	1	0	2	URBANO	B	TIPO 1
4																		
5	CPNP MATED FUMACAHUA		LIMA	LIMA	12.19204567	-76.98017667	100M				0	1	1	0	2	URBANO	B	TIPO 1
4																		
5	CPNP BARRANCO/CPNP TURISMO LIMA SUR		LIMA	LIMA	12.17025833	-77.0232515	150M				0	1	1	0	3	URBANO	A	TIPO 1
4																		
5	CPNP MATUCANA		HUACHO	LIMA	11.84371667	-76.38565	100M				0	1	1	0	2	URBANO	A	TIPO 1
4																		
5	CPNP MI PERU		CALLAO	LIMA	-11.854455	-77.12346667	100M				0	1	1	0	2	URBANO	B	TIPO 1
4																		
5	CPNP MIRONES ALTO		LIMA	LIMA	-12.051335	-77.06745	100M				0	1	1	0	3	URBANO	B	TIPO 1
4																		



5	CPNP MIRONES BAJO	JIRÓN MANUEL PEREZ DE TUDELA # 3344	LIMA	LIMA	-12038004	-77082207	100M			0	1	1	0	2	URBANO	B	TIPO 1
6	CPNP MONSERRATE	JIRÓN CALLAO # 891	LIMA	LIMA	12.04123812	-77.03937694	100M			0	1	1	0	3	URBANO	A	TIPO 1
1	CPNP MONTEERRICO	AV. MANUEL OIGUIN CUADRA 6	LIMA	LIMA	-12.094702	-76.973602	100M			0	1	1	0	3	URBANO	B	TIPO 1
2	CPNP NUEVA ESPERANZA	AV. 26 DE NOVIEMBRE 1391	LIMA	LIMA	12.16948454	-76.92875322	100M			0	1	1	0	3	URBANO	B	TIPO 1
3	CPNP NUEVO IMPERIAL	AV. AUGUSTO B. LEGUIA # 501	CAÑETE	LIMA	13.07597333	-76.311964167	100M			0	1	1	0	2	URBANO	B	TIPO 1
4	CENTRAL EMERGENCIA 105	AV. ESPAÑA 400-3ER. PISO (COSTADO PREFECTURA LIMA)	Lima	Lima	-12.05773	-77.0412	400M			0	0	1	0	0	URBANO	105	TIPO 1
5	CPNP NUEVO PROGRESO	Av. 2 Mz C-1 AAHH NUEVO PROGRESO/ TMA ZONA NUEVO MILENIO	LIMA	LIMA	-12.219249	-76.917878	100M			0	1	1	0	2	URBANO	D	TIPO 1
6	CPNP OQUEENDO	CALLE BUENOS AIRES Y BOLIVIA Y PARQUE N° 02 - EX FUNDO OQUEENDO CALLAO	CALLAO	CALLAO	11.97848143	-77.12322381	100M			0	1	1	0	1	URBANO	COMISARI A	TIPO 1
7	CPNP ORRANTIA DEL MAR	AV. AUGUSTO PEREZ ARANIBAR # 2075	LIMA	LIMA	12.10448833	-77.05733	100M			0	1	1	0	3	URBANO	B	TIPO 1
8	CPNP PACARAN	JR. MIRAFLORES 155	cañete	Lima	-12.985846	-76.054236	100M			0	1	1	0	2	URBANO	C	TIPO 1
9	CPNP PACHACUTEC	AV. DOSCIENTOS VEINTICINCO SN MZAW LT.13	CALLAO	CALLAO	11.83379167	-77.142075	100M			0	1	1	0	2	URBANO	B	TIPO 1
1	CPNP PALOMINO	CALLE SANTA JUSTINA # SN	LIMA	LIMA	12.06025333	-77.07249833	100M			0	1	1	0	2	URBANO	B	TIPO 1
2	CPNP PAMPLONA 1	CALLE SECTOR NUEVO HORIZONTE # SN	LIMA	LIMA	-12.148005	-76.96603	100M			0	1	1	0	2	URBANO	B	TIPO 1
3	CPNP PAMPLONA II	AV. EDILBERTO RAMOS # SN	LIMA	LIMA	12.13113667	-76.95800333	100M			0	1	1	0	2	URBANO	B	TIPO 1
4	CPNP PARAMONGA	AV. CENTRAL # 275	BARRANCA	LIMA	-10.67324	-77.81923167	100M			fx	1	1	0	2	URBANO	B	TIPO 1
5	CPNP PATIVILCA	AV. SIMON BOLIVAR # 117	BARRANCA	LIMA	-10.69596	-77.778336	100M			0	1	1	0	1	URBANO	B	TIPO 1
6	CPNP PAYET	JIRÓN PALLCAMARCA # SN	LIMA	LIMA	11.97195167	-77.04370667	100M			0	1	1	0	3	URBANO	B	TIPO 1
7	CPNP PETIT THOUARS	AV. PETIT THOUARS # 455	LIMA	LIMA	12.06866333	-77.03521167	100M			0	1	1	0	3	URBANO	A	TIPO 1
8	CPNP PIEDRA LIZA	PASAJE NUMERO UNO # SN	LIMA	LIMA	12.03974683	-77.01772481	100M			0	1	1	0	2	URBANO	B	TIPO 1
9																	



5	CPNP PLAYA RIMAC	JIRÓN MIGUEL GRAU # 200	CALLAO	CALLAO	LIMA	-12.03751	-77.09699833	100M				0	1	1	0	2	URBANO	B	TIPO 1
8	CPNP PRO	CALLE CONFRATERNIDAD # SN	LOS OLIVOS	LIMA	LIMA	-11.93454	-77.07757333	100M				0	1	1	0	3	URBANO	A	TIPO 1
1	CPNP PUCUSANA	JIRÓN UNION # SN	PUCUSANA	LIMA	LIMA	-12.48267	-76.796365	100M				0	1	1	0	1	URBANO	B	TIPO 1
2	CPNP PUEBLO LIBRE	PASAJE VIVANCO # 101	MAGDALENA VIEJA	LIMA	LIMA	12.07704667	-77.06560833	100M				0	1	1	0	3	URBANO	A	TIPO 1
5	CPNP PUEBLO NUEVO DE CONTA	AV. LOSTAUNAU SN MZ L1.2	NUEVO IMPERIAL	CAÑETE	LIMA	-13.018175	-76.33938	100M				0	1	1	0	1	URBANO	C	TIPO 1
8	CPNP PUENTE PIEDRA	AV. REP. DE VENEZUELA CON AV. BUENOS AIRES (REF. PLAZA DE ARMAS)	PUENTE PIEDRA	LIMA	LIMA	-11.866288	-77.0771672	100M				0	1	1	0	3	URBANO	A	TIPO 1
5	CPNP PUNTA HERMOSA	URB. EL CARMEN MZ "A-1" LT. "12-13"	PUNTA HERMOSA	LIMA	LIMA	12.31252333	-76.83720833	100M				0	1	1	0	1	URBANO	B	TIPO 1
8	CPNP PUNTA NEGRA	AV. GUANAY NORTE # SN	PUNTA NEGRA	LIMA	LIMA	12.36416167	-76.79570167	100M				0	1	1	0	1	URBANO	B	TIPO 1
5	CPNP QUILMANA	AV. LIMA # SN	QUILMANA	CAÑETE	LIMA	12.94971333	-76.38269333	100M				0	1	1	0	1	URBANO	C	TIPO 1
8	DEPINCRI CHORRILLOS-BARRANCO/TRANISTO/HALCONES	AV. SOL S/N CUADRA 16	CHORRILLOS	LIMA	LIMA	-12.181129	-76.992562	300M				0	1	1	0	3	URBANO	DIVINCI	TIPO 1
5	CPNP RAMON CASTILLA	JIRÓN TALARA # 200	CALLAO	CALLAO	LIMA	12.04407833	-77.12400667	100M				0	1	1	0	2	URBANO	B	TIPO 1
9	CPNP RICARDO PALMA	CALLE ANGEL BARACCO # SN	RICARDO PALMA	HUAROCHIRI	LIMA	11.92327612	-76.66508138	100M				0	1	1	0	1	RURAL	B	TIPO 1
1	CPNP RIMAC	JIRÓN CHICLAYO # 450	RIMAC	LIMA	LIMA	12.03948333	-77.027905	100M				0	1	1	0	3	URBANO	A	TIPO 1
2	CPNP SAGITARIO	AV. LAS GAVIOTA # SN	SURCO	LIMA	LIMA	-12.164779	-76.996769	100M				0	1	1	0	3	URBANO	B	TIPO 1
5	CPNP SALAMANCA	PASAJE LOS ATMARAS # 264	ATE	LIMA	LIMA	-12.0757	-76.98863	100M				0	1	1	0	4	URBANO	B	TIPO 1
9	CPNP SAN ANDRES	JIRÓN HUALLAGA # 852	CERCADO	LIMA	LIMA	12.05151667	-77.02353333	100M				0	1	1	0	3	URBANO	A	TIPO 1
5	CPNP SAN ANTONIO	AV. TOMAS MARZANO # 1180	MIRAFLORES	LIMA	LIMA	-12.11489	-77.010743	100M				0	1	1	0	2	URBANO	B	TIPO 1
6	CPNP SAN ANTONIO CAÑETE	AV. LIBERTAD # 433	SAN ANTONIO	CAÑETE	LIMA	12.64216333	-76.650745	100M				0	1	1	0	1	URBANO	C	TIPO 1
5	CPNP SAN ANTONIO DE JICAMARCA	AV. INCA YUPANQUI MZ AO / INTERSECCIÓN CON LA AV. LOS ANDES - ANEXO 22	SAN ANTONIO	HUAROCHIRI	LIMA	-11.925783	-76.966853	100M				0	1	1	0	1	URBANO	COMISARI A	TIPO 1



5	CPNP SAN BARTOLO	AV. SAN BARTOLO # SN	SAN BARTOLO	LIMA	LIMA	12.38746333	-76.77730667	100M				0	1	1	0	2	URBANO	B	TIPO 1
9																			
0	CPNP SAN BORJA	JR. FEDOROVICH STRANVINSKY CD 2 SN	SAN BORJA	LIMA	LIMA	12.10566833	-76.998985	100M				0	1	1	0	3	URBANO	A	TIPO 1
0																			
6	CPNP SAN CAJETANO	JIRÓN SUCRE # 100	EL AGUSTINO	LIMA	LIMA	-12.05681	-77.00803833	100M				0	1	1	0	2	URBANO	B	TIPO 1
0																			
1	CPNP SAN COSME	PASAJE ENRIQUE MEIGGS # 2125	LA VICTORIA	LIMA	LIMA	12.06457833	-77.00778	100M				0	1	1	0	2	URBANO	B	TIPO 1
6																			
2	CPNP SAN DAMIAN	JR. MANCO CAPAC # 199	SAN DAMIAN	LIMA	HUAROCHIRI	-12.0171162	-76.39168042	100M				0	1	1	0	1	URBANO	COMISARI A	TIPO 1
0																			
3	CPNP SAN FRANCISCO TABLADA LURIN	AV. SAN MARTIN # 170	VILLA MARIA DEL TRIUNFO	LIMA	LIMA	12.20009667	-76.92815833	100M				0	1	1	0	2	URBANO	B	TIPO 1
0																			
4	CPNP SAN GEARO	AV. PRINCIPAL # SN	CHORRILLOS	LIMA	LIMA	-12.193998	-77.020556	100M				0	1	1	0	2	URBANO	B	TIPO 1
0																			
5	CPNP SAN ISIDRO	CALLE ANTEQUERA # 116	SAN ISIDRO	LIMA	LIMA	12.09509476	-77.0923348	100M				0	1	1	0	3	URBANO	A	TIPO 1
0																			
6	CPNP SAN LUIS	JIRÓN JOSE ORENGO # 903	SAN LUIS	LIMA	LIMA	-12.073025	-76.99940667	100M				0	1	1	0	3	URBANO	A	TIPO 1
0																			
7	CPNP SAN LUIS CAÑETE	CALLE PLAZA DE ARMAS # 131	SAN LUIS	CAÑETE	LIMA	13.05075833	-76.430455	100M				0	1	1	0	1	URBANO	B	TIPO 1
0																			
8	CPNP SAN MATEO	JIRÓN LIMA # SN	SAN MATEO	HUAROCHIRI	LIMA	11.75930667	-76.29335667	100M				0	1	1	0	1	URBANO	B	TIPO 1
0																			
9	CPNP SAN MIGUEL	CALLE UNO # SN	SAN MIGUEL	LIMA	LIMA	12.08958667	-77.087785	100M				0	1	1	0	3	URBANO	B	TIPO 1
1																			
0	CPNP SAN PEDRO	AV. 15 DE ABRIL CDR. 3	EL AGUSTINO	LIMA	LIMA	12.05968333	-77.00317167	100M				0	1	1	0	2	URBANO	B	TIPO 1
1																			
6	CPNP SAN PEDRO DE CAPILLUCAS	CARRETERA CAÑETE AYUYOS KM 109	ALLAUCA	YALUYOS	LIMA	-12.707477	-75.969145	100M				0	1	1	0	1	URBANO	COMISARI A	TIPO 1
1																			
2	CPNP SAN VICENTE DE CAÑETE	JIRÓN SANTA RITA # SN	SAN VICENTE DE CAÑETE	CAÑETE	LIMA	-13.078295	-76.38896333	100M				0	1	1	0	2	URBANO	A	TIPO 1
6																			
1	CPNP SANTA ANITA	JIRÓN CIRO ALEGRIA # 555	SANTA ANITA	LIMA	LIMA	-12.044845	-76.97673833	100M				0	1	1	0	3	URBANO	A	TIPO 1
6																			
4	AREANDRO PNP MOQUEGUA	SECTOR MONTALVO CALALLUNA N°118-B VALLE	MARISCAL NIETO	MOQUEGUA	LIMA	-17.212073	-70.968232	100M				0	1	1	0	1		DIRANDR O	TIPO 1
6																			
1	CPNP SANTA CLARA	CARRETERA CENTRAL # 1	ATE	LIMA	LIMA	12.01683606	-76.88417226	100M				0	1	1	0	2	URBANO	B	TIPO 1
6																			
7	CPNP SANTA ELIZABETH	JR. NEVADO HUANDÓY SN MZ.F LT.18	SAN JUAN DE LURIGANCHO	LIMA	LIMA	-11.983885	-77.015015	100M				0	1	1	0	3	URBANO	B	TIPO 1



6	CPNP SANTA EULALIA	AV. JOSE BERNARDO ALCEDO # SN	SANTA EULALIA	HUAROCHIRI	LIMA	11.90092667	-76.66405167	100M		0	1	1	0	2	RURAL	B	TIPO 1
1																	
8																	
6	CPNP SANTA FELICIA	LOS CANARIOS. LA MOLINA 15024	LA MOLINA	LIMA	LIMA	-12.07221	-76.95523333	100M		0	1	1	0	2	URBANO	B	TIPO 1
1																	
9																	
2	CPNP SANTA ISABEL	AV. MARIA PARADO DE BELLIDO # SN	CARABAYLLO	LIMA	LIMA	11.96854221	-77.05675564	100M		0	1	1	0	3	URBANO	B	TIPO 1
0																	
6	CPNP SANTA LUZMILA	AV. GERARDO UNGER # 6500	COMAS	LIMA	LIMA	-11.94467	-77.06693533	100M		0	1	1	0	3	URBANO	B	TIPO 1
2																	
1																	
6	CPNP SANTA MARIA DEL MAR	AV. TERRAMAR # SN	SANTA MARIA DEL MAR	LIMA	LIMA	-12.399675	-76.773	100M		0	1	1	0	1	URBANO	B	TIPO 1
2																	
6	CPNP SANTA ROSA	AV. ALEJANDRO BERTELLO # SN	SANTA ROSA	LIMA	LIMA	-11.79655	-77.17104833	100M		0	1	1	0	2	URBANO	C	TIPO 1
3																	
6	UNIDAD DE EMERGENCIA CENTRO	AV. 28 DE JULIO 1650 // BAUSATE Y MESA	LA VICTORIA	LIMA	LIMA	-12.064016	-77.025725	150M		0	1	1	0	1	URBANO	EMERGENCIA	TIPO 1
2																	
4																	
6	CPNP SANTA ROSA IRRIGACION	AV. PRINCIPAL LA VILLA # SN - IRRIGACION SANTA ROSA	SAYAN	HUALAURA	LIMA	-11.235186	-77.381099	100M		0	1	1	0	1	URBANO	COMISARI A	TIPO 1
2																	
5																	
6	CPNP SANTIAGO DE SURCO	JIRÓN ARICA # 388	SURCO	LIMA	LIMA	-12.14538	-77.00303	100M		0	1	1	0	3	URBANO	A	TIPO 1
2																	
6	CPNP SANTOYO	JIRÓN CHIMBOTE # 2110	EL AGUSTINO	LIMA	LIMA	12.05135333	-77.00853333	100M		0	1	1	0	2	URBANO	B	TIPO 1
2																	
7																	
6	CPNP SARITA COLONIA	AV. VICTOR A. BELAUNDE # SN	CALLAO	CALLAO	LIMA	12.02369167	-77.13439	100M		0	1	1	0	2	URBANO	B	TIPO 1
2																	
8																	
6	CPNP SAYAN	OTRO PLAZA DE ARMAS # SN	SAYAN	HUALAURA	LIMA	11.13496833	-77.19262	100M		0	1	1	0	1	URBANO	B	TIPO 1
2																	
9																	
6	CPNP SECTORIAL OYON	CALLE COMERCIO # 481	OYON	OYON	LIMA	-10.669535	-76.76970833	100M		0	1	1	0	1	RURAL	A	TIPO 1
3																	
0																	
6	CPNP SOL DE ORO	AV. BUEN PASTOR # SN	LOS OLIVOS	LIMA	LIMA	11.99756333	-77.063925	100M		0	1	1	0	3	URBANO	A	TIPO 1
3																	
1																	
6	CPNP SUPE PUEBLO	JIRÓN SUCRE # 350	SUPE	BARRANCA	LIMA	10.79524833	-77.71631333	100M		0	1	1	0	1	URBANO	B	TIPO 1
3																	
2																	
6	CPNP SUPE PUERTO	CALLE CALLAO # 501	SUPE PUERTO	BARRANCA	LIMA	10.79698833	-77.7417	100M		0	1	1	0	1	URBANO	B	TIPO 1
3																	
3																	
6	CPNP SURQUILLO	JIRÓN SAN DIEGO # 401	SURQUILLO	LIMA	LIMA	-12.118732	-77.022453	100M		0	1	1	0	3	URBANO	A	TIPO 1
3																	
4																	
6	CPNP TAHUANTINSUYO	JIRÓN OLLANTAYTAMBO # SN	INDEPENDENCIA	LIMA	LIMA	-11.980585	-77.04887	100M		0	1	1	0	2	URBANO	B	TIPO 1
3																	
5																	
6	CPNP TUPAC AMARU	AV. TUPAC AMARU # 1121	COMAS	LIMA	LIMA	11.95521667	-77.05255167	100M		0	1	1	0	3	URBANO	A	TIPO 1
3																	
6																	



6	3	CPNP UNIDAD VECINAL NRO 3	AV. OSCAR BENAVIDES # SN	LIMA	LIMA	12.05137167	-77.08204333	100M			0	1	1	0	3	URBANO	B	TIPO 1
7	3	CPNP UNIVERSITARIA	AV. UNIVERSITARIA # SN	LIMA	LIMA	11.94744333	-77.06020667	100M			0	1	1	0	2	URBANO	B	TIPO 1
8	3	CPNP URB. PACHACAMAC	JR. JORGE CHAVEZ 181	LIMA	LIMA	-12.230055	-76.92323333	100M			0	1	1	0	2	URBANO	B	TIPO 1
9	3	CPNP VEGUETA	AV. GRAU # 133	HUAURA	LIMA	11.02339019	-77.64370143	100M			0	1	1	0	1	URBANO	B	TIPO 1
10	3	CPNP VENTANILLA	AV. PEDRO BELTRAN # 138	CALLAO	LIMA	11.87287667	-77.126185	100M			0	1	1	0	4	URBANO	A	TIPO 1
11	3	CPNP VILLA HERMOSA	JIRON RIO NANAY # SN	LIMA	LIMA	12.04147167	-76.98856667	100M			0	1	1	0	2	URBANO	B	TIPO 1
12	3	CPNP VILLA LOS REYES	MZ. C LT. 3 AA. HH. VILLA LOS REYES	CALLAO	LIMA	-11.83087	-77.121875	100M			0	1	1	0	3	URBANO	B	TIPO 1
13	3	CPNP VILLA MARIA DEL TRIUNFO	AV. EL TRIUNFO # 374	LIMA	LIMA	-12.165745	-76.94780833	100M			0	1	1	0	3	URBANO	A	TIPO 1
14	3	CPNP MIRAFLORES/DIVINCRI	CALLE GENERAL VIDAL # 230	LIMA	LIMA	12.11442333	-77.02813	150M			0	1	1	0	4	URBANO	A	TIPO 1
15	3	CPNP VILLA-CHORRILLOS	PROLONGACION HUAYLAS CDR. 1. DISTRITO DE CHORRILLOS	LIMA	LIMA	12.18578833	-77.00787833	100M			0	1	1	0	3	URBANO	B	TIPO 1
16	3	CPNP VITARTE	CARRITERA CENTRAL # SN	LIMA	LIMA	-12.02611	-76.91959	100M			0	1	1	0	2	URBANO	A	TIPO 1
17	3	CPNP YANGAS	KM 56 CARRETERA LIMA A CANTA	CANTA	LIMA	11.69488659	-76.84566417	100M			0	1	1	0	1	URBANO	COMISARI A	TIPO 1
18	3	CPNP YAUYES	JR. TRUJILLO S/N	YAUYES	LIMA	-12.4600538	-75.9187047	100M			0	1	1	0	1	URBANO	COMISARI A	TIPO 1
19	3	CPNP YERBATEROS	JIRON PABLO RISSO # 190	LIMA	LIMA	12.06471833	-76.99734	100M			0	1	1	0	2	URBANO	B	TIPO 1
20	3	CPNP ZAPALLAL	JIRON GALILEA # SN	LIMA	LIMA	-11.828025	-77.11752833	100M			0	1	1	0	3	URBANO	B	TIPO 1
21	3	CPNP ZARATE	AV. PIRAMIDE DEL SOL # 200	LIMA	LIMA	12.02703333	-77.00126333	100M			0	1	1	0	3	URBANO	A	TIPO 1
22	3	CPNP ZURIGA	AV. BERNARDO ALCEDO # 214	CAÑETE	LIMA	12.86029554	-76.0224031	100M			0	1	1	0	1	URBANO	COMISARI A	TIPO 1
23	3	DEPICA/DIVPOL CAÑETE	PLAZA SAN MARTIN 236 CERCADO CAÑETE	CAÑETE	LIMA	-13.076558	-76.385877	100M			0	1	1	0	2	URBANO	DIVINCRI	TIPO 1
24	3	DEPINCRI BARRANCA	URB LAS PALMERAS MZ. M LT.1	BARRANCA	LIMA	-10.741327	-77.765152	100M			0	1	1	0	1	URBANO	DEPINCRI	TIPO 1

Handwritten marks at the top left of the page.



Handwritten signature and initials on the left side of the page.

5	DEPINCR CALLAO.	JR. CONSTITUCIÓN CDA 2 S/N	CALLAO	CALLAO	LIMA	-12.059776	-77.147082	100M			0	1	1	0	3	URBANO	DIVINCR	TIPO 1
5	DEPINCR CARABAYLLO	AV. COLECTORA MZ H8 LOT 1.2.3.4 / URB SANTA MARIA. 1 ETAPA / CARABAYLLO	CARABAYLLO	LIMA	LIMA	-11.841079	-77.045862	100M			0	1	1	0	2	URBANO	DIVINCR	TIPO 1
5	DEPINCR CERCADO	JR. HUALLAGA Nº 876(310)	CERCADO	LIMA	LIMA	-12.051235	-77.023317	100M			0	1	1	0	3	URBANO	DIVINCR	TIPO 1
5	DEPINCR CHOSICA	AV. SANTA INÉS 316	LURIGANCHO	LIMA	LIMA	-11.972389	-76.755672	100M			0	1	1	0	2	URBANO	DIVINCR	TIPO 1
5	DEPINCR COMAS	AV. GUILLERMO DE LA FUENTE N°1058 URB VIREDOS	COMAS	LIMA	LIMA	-11.94755	-77.0518	100M			0	1	1	0	2	URBANO	DIVINCR	TIPO 1
5	DEPINCR EL AGUSTINO	BOULEVARD REPUBLICA 661 - EL AGUSTINO	EL AGUSTINO	LIMA	LIMA	-12.04979	-77.01014	100M			0	1	1	0	2	URBANO	DEPINCR	TIPO 1
5	DEPINCR LA MOLINA - CIENEGUITA	AV. MOLINA ESTE 2350 URB. MUSA	LA MOLINA	LIMA	LIMA	-12.9865443	-76.8938654	100M			0	1	1	0	2	URBANO	DEPINCR	TIPO 1
5	DEPINCR LOS OLIVOS	JR. MARCARÁ CON CHASQUITAMBO URB. NARANJAL	LOS OLIVOS	LIMA	LIMA	-11.9765162	-77.0692785	100M			0	1	1	0	3	URBANO	DIVINCR	TIPO 1
5	DIRLOG TELEMATICA	PSJE. SAN GERMAN CDA 2 COSTADO HOSPITAL BLEGUJA S/N	RIMAC	LIMA	LIMA	-12.033437	-77.032566	200M			0	1	1	0	1	URBANO	DIVLOG	TIPO 1
5	HOSPITAL POLICIAL "AUGUSTO B. LEGUIA"	PSJE. SAN GERMAN CDA. 2	RIMAC	LIMA	LIMA	-12.035265	-77.033962	200M			0	1	1	0	1	URBANO	HOSPITAL	TIPO 1
5	DEPINCR LURIN-PACHACAMAC Y BALNERIOS	ASOC. LOS CLAVES MZA N° LOTE 15	LURIN	LIMA	LIMA	-12.295489	-76.855269	100M			0	1	1	0	3	URBANO	DIVINCR	TIPO 1
5	DEPINCR NORTE SAN MARTIN DE PORRES	JR. JOAQUÍN CAPELLA 672 URB. INGENIERIA	SAN MARTIN DE PORRES	LIMA	LIMA	-12.0295084	-77.0567105	100M			0	1	1	0	2	URBANO	DIVINCR	TIPO 1
5	DEPINCR RIMAC	AV. EVITAMIENTO S/N. JR. GARCÍA RIBEYRO S/N	RIMAC	LIMA	LIMA	-12.036907	-77.041318	100M			0	1	1	0	1	URBANO	DIVINCR	TIPO 1
5	DEPINCR SAN BORJA/EFATURA AREA INVESTIGACION CRIMINAL-SUR	CALLE 2 N° 568	SAN BORJA	LIMA	LIMA	-12.089949	-76.984382	100M			0	1	1	0	2	URBANO	DIVINCR	TIPO 1
5	DEPINCR SAN JUAN DE MIRAFLORES	AV. JOSE R. ECHENIQUE 420-PAMPLONA	SAN JUAN DE MIRAFLORES	LIMA	LIMA	-12.148437	-76.975692	100M			0	1	1	0	2	URBANO	DIVINCR	TIPO 1
5	DEPINCR SAN MIGUEL	CALLE MANUELA MARTICORENA N° 163	SAN MIGUEL	LIMA	LIMA	-12.08254	-77.079573	100M			0	1	1	0	2	URBANO	DIVINCR	TIPO 1
5	DEPINCR SIL 1	INTERSECCION DE LA CALLE RIO UCAYALI CON RIO APURIMAC MZ. O LITE 20	SAN JUAN DE LURIGANCHO	LIMA	LIMA	11.97471874	-76.99548379	100M			0	1	1	0	0	URBANO	DIVINCR	TIPO 1
5	DEPINCR SIL 2	SAN HILARION ESTE, SAN JUAN DE LURIGANCHO 15434	SAN JUAN DE LURIGANCHO	LIMA	LIMA	-11.992401	-77.00857	100M			0	1	1	0	2	URBANO	DIVINCR	TIPO 1
5	DEPINCR VENTANILLA	CALLE TROMPETEROS 136 (ESPALDA DE LA CNP VENTANILLA)	VENTANILLA	CALLAO	LIMA	-11.872098	-77.126318	100M			0	1	1	0	2	URBANO	C	TIPO 1

Handwritten signature and initials at the top left of the page.



Handwritten signature and initials in the middle left of the page.

Handwritten signature and initials at the bottom left of the page.

6	CP DIVPOL NORTE 1 / UNEME NORTE-SOES NORTE	JR. LOS SILICOS 5534 PAN. NORTE PARADERO	LOS OLIVOS	LIMA	LIMA	-11.967957	-77.063192	400M	1	3	0	1	0	1	URBANO	COMPLEJO 1	TIPO 1
7	3/ TRANSITO NORTE / DITROVENORTE)	NISSAN PASANDO OVALO NARANJAL	VILLA MARIA DEL TRIUNFO	LIMA	LIMA	-12.201076	-76.928479	100M		0	1	1	0	2	URBANO	DEPINCRI	TIPO 1
6	DEPINCRI VILLA MARIA DEL TRIUNFO	AV. GENERAL VIDAL 300 MZ. 1-D. LOTE 17 P1	CALLAO	CALLAO	LIMA	-12.06849	-77.133575	100M		0	1	1	0	1	URBANO	FAMILIA	TIPO 1
6	DEPROVE CALLAO/ORIPACIU	OVALO CANADA S/N	MALA	CAÑETE	LIMA	12.71936667	-76.62937	100M		0	0	1	0	0	URBANO	CARRETERAS	TIPO 1
6	DESPICAR BUJAMA	CIL. PROGRESO SN MZ.D IT.6	CHICLA	HUAROCHIRI	LIMA	-11.704883	-76.268785	100M		0	0	1	0	0	RURAL	CARRETERAS	TIPO 1
6	DESPICAR CHICLA	CARR. CENTRAL KM 106 S/N PLAZA DE ARMAS -CHICLA	CHICLA	HUAROCHIRI	LIMA	-12.387248	-76.77745	100M		0	0	1	0	0	URBANO	CARRETERAS	TIPO 1
6	DESPICAR SAN BARTOLO	AV. EL GOLF S/N	SAN BARTOLO	LIMA	LIMA	-11.8841917	-76.4400617	100M		0	0	1	0	0	URBANO	CARRETERAS	TIPO 1
6	DESPICAR SAN JERONIMO SURCO	JIRON BOLOGNESI S/N SAN JERONIMO DE SURCO	SAN JERONIMO DE SURCO	HUAROCHIRI	LIMA	11.91117829	-76.58751726	100M		0	0	1	0	0	RURAL	CARRETERAS	TIPO 1
6	DESPICAR SANTA CRUZ DE COCACHACRA	CARRETERA CENTRAL # SN	SANTA CRUZ DE COCACHACRA	HUAROCHIRI	LIMA	-11.13467	-77.198538	100M		0	0	1	0	0	URBANO	CARRETERAS	TIPO 1
6	DESPICAR SAYAN	CARRETERA PENETRACION A SAYAN 45.6	SAYAN	HUAROCHIRI	LIMA	-11.728954	-76.968231	100M		0	0	1	0	0	URBANO	CARRETERAS	TIPO 1
6	DESPICAR STA ROSA	CARRETERA PANAMERICANA NORTE KM.42 DESTACAMENTO POLICIAL DE CARRETERA	SANTA ROSA	LIMA	LIMA	-11.792279	-77.1477796	100M		0	0	1	0	0	URBANO	CARRETERAS	TIPO 1
6	DESPICAR YANGAS	MZ C LOTE 11- CENTRO POBLADO BUENA VISTA- CARRETERA LIMA-CANTA	SANTA ROSA DE QUIVES	CANTA	LIMA	-12.061814	-77.051589	100M		0	1	1	0	1	URBANO	DIRANDRO	TIPO 1
6	DIRANDRO - DIVISION DE INVESTIGACION CONTRA EL DESVIO DE INSUMOS QUIMICOS	AV. RESTAURACION 600 PISO 3	CERCADO	LIMA	LIMA	-12.073168	-77.037185	100M		0	1	1	0	1	URBANO	DIRANDRO	TIPO 1
6	DIRANDRO - UN DE LOGISTICA - OFAD	AV. ARENALES 855	JESUS MARIA	LIMA	LIMA	-12.142931	-77.022374	100M		0	1	1	0	3	URBANO	DIRCOCO	TIPO 1
6	DIRECCION CONTRA LA CORRUPCION - DIRCOCOR PNP	AV. SAENZ PEÑA N° 116	BARRANCO	LIMA	LIMA	-12.082504	-77.040622	100M		0	1	1	0	1	URBANO	DIRPOLFI	TIPO 1
6	DIRECCION DE POLICIA FISCAL	AV. BELISARIO FLORES 565	LINCE	LIMA	LIMA	12.09548948	-77.06879294	100M		0	0	1	0	1	URBANO	TURISMO	TIPO 1
6	DIRECCION DE TURISMO PNP -DIRTUR PNP	JIRON MOORE 268	MAGDALENA	LIMA	LIMA	12.15793302	-76.97529227	150M		0	1	1	0	3	URBANO	A	TIPO 1
6	CPNP SAN JUAN DE MIRAFLORES	PASAJE SAN JUAN # SN	SAN JUAN DE MIRAFLORES	LIMA	LIMA	-12.1066635	-77.0238946	100M		0	1	1	1	1	URBANO	ENTIDAD DEL ESTADO	TIPO 1
6	DIRECCION NACIONAL DE ORDEN Y SEGURIDAD DIRNOS	AV. GRAL. RECAVARREN 1378	SURQUILLO	LIMA	LIMA	-12.113925	-76.984107	100M		0	1	1	0	1	URBANO	DIRPACIU	TIPO 1
6	DIRPACIU	AV. V. ASTETE 1131 URB. CH. DEL ESTANQUE	SURCO	LIMA	LIMA					0	1	1	0	1	URBANO		TIPO 1

[Handwritten signature]



[Handwritten signature]

6	DIRPOLFIS (POLICIA FISCAL)	AV. INGENIEROS 574	SURCO	LIMA	LIMA	-12.127852	-76.972709	100M				0	1	1	0	1	1	DIRPOLFIS	TIPO 1
4																			
6	DIRSAPOL PNP	AV. AREQUIPA N° 4898	MIRAFLORES	LIMA	LIMA	-12.11478	-77.02584	100M				0	1	1	0	1	1	SANIDAD	TIPO 1
5																			
6	DIVCMPA - DIVCTIPRN	AV. DEL BIERZO KM 1.5	VENTANILLA	CALLAO	LIMA	-11942471	-77117822	100M				0	1	1	0	1	1	DIRMEA MB	TIPO 1
6																			
9	CPNP SAN MARTIN DE PORRES	JIRON MANUEL VILLAR # 1	SAN MARTIN DE PORRES	LIMA	LIMA	-12.025688	-77.055866	150M				1	1	1	0	3	1	A	TIPO 1
7																			
6	DIVISION DE ASUNTOS SOCIALES /DEPARTAMENTO DE PROTECCION DE OBRAS CIVILES	JIRON LORETO 278	RIMAC	LIMA	LIMA	-12.042781	-77.028281	100M				0	0	1	0	1	1	DIPROC (DEPARTAMENTO DE PROTECCION DE OBRAS CIVILES)	TIPO 1
9																			
8																			
6	DIVISION DE INVESTIGACION CONTRA EL CRIMEN ORGANIZADO - DIRECCION DE MEDIO AMBIENTE PNP	ALAMEDA DEL PREMIO REAL MZ J LT 16 URB LA ENCANTADA DE VILLA CHORRILLOS	CHORRILLOS	LIMA	LIMA	-12.209203	-77.006881	100M				0	0	1	0	1	1		TIPO 1
9																			
9	DIVISION DE INVESTIGACION DE DELITOS CONTRA LOS DERECHOS INTELECTUALES	JR. JOSE PEZAT Y MONEL ANTES JR. TUPAC AMARU 1894	LINCE	LIMA	LIMA	-12.084551	-77.042691	100M				0	1	1	0	1	1	DIRPOLFIS	TIPO 1
7																			
0	DIVISION DE PROTECCION CONTRA LA VIOLENCIA FAMILIAR PNP - DIVPCVF	JR. CHOTA N°1434	LIMA	LIMA	LIMA	-12.058792	-77.040324	100M				0	1	1	0	2	1	DIVPCVF	TIPO 1
1																			
7	DIVISION DE PROTECCION DE BANCOS	AV. BOLOGNESI 282	SANTA ANITA	LIMA	LIMA	-12.054593	-76.969801	100M				0	1	1	0	1	1	AGUILAS NEGRAS	TIPO 1
2																			
7	DIVISION INVESTIGACION DE DELITOS CONTRA EL ESTADO - DIVICE	JR. ANTONIO ARRIETA 278	PUEBLO LIBRE	LIMA	LIMA	-12.074907	-77.055543	100M				0	1	1	0	1	1	DIRSEG	TIPO 1
3																			
7	DIVISION POLICIAL ESTE 1	JR. CELEDONIAS CDRA. 6 URB LAS FLORES DE PRIMAVERA PARADERO 13 DE LA AV. LAS FLORES SIL	SAN JUAN DE LURIGANCHO	LIMA	LIMA	-70.48133333	-70.48133333	100M				0	1	1	0	1	1	B	TIPO 1
4																			
7	DIVISION POLICIAL HUACHO	AV. 28 DE JULIO N° 210- ESQUINA DE 28 DE JULIO CON DOMINGO COLOMA	HUACHO	HUACHO	LIMA	-11.10713	-77.60638	100M				0	1	1	0	1	1	DIVPOL	TIPO 1
5																			
7	DIVPOL CHOSICA	PSJE. SOLEA 198 KM 32 CAT CENTRAL CHACACAYO	LURIGANCHO	LIMA	LIMA	-11.945102	-76.710469	100M				0	1	1	0	0	1	E	TIPO 1
6																			
7	DIVPOL HUARAL DEPICAI HUARAL	CALLE MANCO CAPAC S/N EL MILAGRO	HUARAL	HUARAL	LIMA	-11.49438	-77.216379	100M				0	1	1	0	2	1	DIVINCRI	TIPO 1
7																			
7	ESCUELA POSGRADO PNP	AV. GUARDIA CIVIL 800	CHORRILLOS	LIMA	LIMA	-12.177083	-76.995105	100M				0	1	1	0	1	1	ENF	TIPO 1
8																			
7	INTERPOL - SURCO	AV. MANUEL OLGUIN CUADRA 6 - PISO 2	SURCO	LIMA	LIMA	12.09479333	-76.97326333	100M				0	1	1	0	1	1	INTERPOL	TIPO 1
9																			
7	JEPOLTRAN - FENIX	AV. ALFONSO UGARTE CDA. 1	CERCADO	LIMA	LIMA	-12.039994	-77.043545	100M				0	1	1	0	1	1	TRANSITO	TIPO 1
1																			
7	JEPOLTRAN LIMA ESTE/POLICIA FISCAL	AV. 7 DE JUNIO - LOS FICUS	SANTA ANITA	LIMA	LIMA	-12.050294	-76.975754	100M				0	1	1	0	1	1	TRANSITO	TIPO 1
1																			

[Handwritten signatures and marks at the top left of the page]



[Handwritten signatures and marks in the middle left of the page]

7	1	MAESTRANZA	CA 13 S/N URB CARABAYLLO 5 METROPOLITANA MERCADO HYPER ESPALDA	COMAS	LIMA	-11.967624	-77.06003	100M			0	1	1	0	1	URBANO	DIVLOG	TIPO 1
7	1	MAESTRANZA 1	JR CHOTA 1322	CERCADO DE LIMA	LIMA	-12.0566854	-77.0408121	100M			0	1	1	0	1	URBANO	DIVLOG	TIPO 1
7	1	MAESTRANZA 2 Y 3	AV ARGENTINA CDA 15	CERCADO DE LIMA	LIMA	-12.04513	-77.05931	100M			0	1	1	0	1	URBANO	DIVLOG	TIPO 1
7	1	MINISTERIO PUBLICO	AV. ABANCAY CDRA. 5 S/N PISO 11 - LIMA	CERCADO	LIMA	-12.05166	-77.02842	100M			0	1	1	0	1	URBANO	ENTIDAD DEL ESTADO	TIPO 1
7	1	OFICRI DIRANDRO LIMA	CALLE RAMON DAGUINO N°442 - RESIDENCIAL PIO XII - 2DO BLOCK PRIMER PISO	JESUS MARIA	LIMA	-12.071542	-77.038015	100M			0	1	1	0	1	URBANO	OFICRI	TIPO 1
7	1	POLICIA JUDICIAL CALLAO	AV. 2 DE MAYO S/N CDA 5	CALLAO	LIMA	-12.056804	-77.142677	100M			0	1	1	0	1	URBANO	POJUS	TIPO 1
7	1	POLICLINICO POLICIAL - SEDE ESCUELA DE SAN BARTOLO	AV. EL GOLF S/N SAN BARTOLO	SAN BARTOLO	LIMA	-12.384413	-76.7799	100M			0	1	1	0	1	URBANO	POSTA MEDICA	TIPO 1
7	1	POLICLINICO POLICIAL CAÑETE	AV. PROLONG. AUGUSTO B LEGUIA S/N S/N	CAÑETE	LIMA	-13.076097	-76.316168	100M			0	1	1	0	1	URBANO	POSTA MEDICA	TIPO 1
7	2	POLICLINICO POLICIAL CARABAYLLO	MZ G1 L15 S/N MZ G1 LOTE KM.	CARABAYLLO	LIMA	-11.888395	-77.038235	100M			0	1	1	0	1	URBANO	POSTA MEDICA	TIPO 1
7	2	POLICLINICO POLICIAL SAN DIEGO	CALLE SANTO TOMAS DE AQUINO CDA 3 S/N	SAN MARTIN DE PORRES	LIMA	-11.941602	-77.086059	100M			0	1	1	0	1	URBANO	POLICLINICO	TIPO 1
7	2	CPNP VILLA EL SALVADOR/DIVINCI/CONTRA INVASIONES	AV. CESAR VALLEJO # 5N	VILLA EL SALVADOR	LIMA	12.21295758	-76.9366765	150M			0	1	1	0	3	URBANO	A	TIPO 1
7	2	POLICLINICO POLICIAL VIPOL	CALLE LOS NENUFAR S/N	CALLAO	CALLAO	-12.012214	-77.097921	100M			0	1	1	0	1	URBANO	POLICLINICO	TIPO 1
7	2	POLICLINIO POLICIAL CALLAO	AV. LA PAZ S/N	LA PERLA	CALLAO	-12.072372	-77.124381	100M			0	1	1	0	1	URBANO	POLICLINICO	TIPO 1
7	2	POSTA MEDICA POLICIAL HUACHO	CALLE 28 DE JULIO 103	HUACHO	LIMA	-11.10795	-77.585091	100M			0	1	1	0	1	URBANO	POSTA MEDICA	TIPO 1
7	2	POSTA MEDICA POLICIAL VENTANILLA	AV. PEDRO BELTRAN CDA 10 S/N	VENTANILLA	CALLAO	-11.87153	-77.122556	100M			0	1	1	0	1	URBANO	POSTA MEDICA	TIPO 1
7	2	SEDE RENIEC CONEXIÓN SEDE PRINCIPAL PNP	JR. TIZIANO VECILLIO 245, SAN BORJA	SAN BORJA	LIMA	12.0845065	-77.00122831	100M			0	1	1	0	1	URBANO	ENTIDAD DEL ESTADO	TIPO 1
7	2	SOPORTE TECNICO - DIRTIC PNP	AV. ANDRÉS ARAMBURU N° 550 (CP WALTER ROSALES LEÓN, PISO 7)	SURQUILLO	LIMA	-12.102790	-77.02502	100M			0	1	1	0	1	URBANO	DIRTIC	TIPO 1
7	2	UNIDAD DE EMERGENCIA CALLAO - UNEME CALLAO	AV. LA PAZ Nº 2685	LA PERLA	CALLAO	-12.07715	-77.110172	100M			0	1	1	0	1	URBANO	EMERGENCIA	TIPO 1
7	3	UNIDAD DE EMERGENCIA ESTE 1	AV. FERNANDO WIESE 313	SAN JUAN DE LURIGANCHO	LIMA	-11.980552	-77.005478	100M			0	1	1	0	1	URBANO	EMERGENCIA	TIPO 1

Handwritten signatures and initials at the top left of the page.

Handwritten signatures and initials in the middle left of the page.



7	UNIDAD DE EMERGENCIA ESTE 2	AV. JOSÉ C. MARIATEGUI 68	ATE	LIMA	LIMA	-12.011854	-76.827383	100M				0	1	1	0	1	URBANO	EMERGENCIA	TIPO 1
3	UNIDAD DE EMERGENCIA SUR 1	AV. REPÚBLICA DE PANAMÁ 4450	SURQUILLO	LIMA	LIMA	-12.109228	-77.018509	100M				0	1	1	0	1	URBANO	EMERGENCIA	TIPO 1
3	UNIDAD DE EMERGENCIA SUR 2 - UNEME SUR 2	AV. PACHACUTEC 2220 URB VILLA JARDIN	VILLA MARIA DEL TRIUNFO	LIMA	LIMA	12.167383976	76.95190853	100M				0	1	1	0	1	URBANO	UNEME	TIPO 1
3	UNIDAD FUNCIONAL DE CRIMINALISTICA ESTE 1 - UNIFUCRI ESTE 1	CALLE LOS NARANJOS 126 (5 to piso)	SAN JUAN DE LURIGANCHO	LIMA	LIMA	-11.981027	-77.011369	150M				0	1	1	0	1	URBANO	DIRCRI	TIPO 1
3	UNIDAD PREVENCIÓN E INVESTIGACIÓN DE ROBO DE VEHICULOS - UNIPRV BARRANCA	JIRÓN STA. ZORAIDA # SN	BARRANCA	BARRANCA	LIMA	-10.750620	-77.764824	100M				0	1	1	0	2	RURAL	B	TIPO 1
3	UNINST - DIRTIC PNP	JR. CRISANTEMOS 164 MZ PI-LT-9	LA MOLINA	LIMA	LIMA	-12.085208	-76.958033	100M				0	1	1	0	0	URBANO	ETS	TIPO 1
3	CPNP ALTO AMAZONAS - YURIMAGUAS/DIVPOL	CALLE CONDAMINE # SN	YURIMAGUAS	ALTO AMAZONAS	LORETO	5.897408333	-76.11445167	100M				0	1	1	0	2	URBANO	B	TIPO 1
3	CPNP SECTORIAL LORETO - NAUTA	CALLE MANUEL PACAYA # 345	NAUTA	LORETO	LORETO	4.506838333	-73.57502167	100M				0	1	1	0	1	URBANO	B	TIPO 1
3	CPNP 9 DE OCTUBRE	CALLE TAHUANTINSUYO # SN	BELEN	MAYNAS	LORETO	3.766379621	-73.26099336	100M				0	1	1	0	1	URBANO	B	TIPO 1
3	CPNP BELEN	CALLE SEIS # SN	BELEN	MAYNAS	LORETO	3.760801667	-73.24907	100M				0	1	1	0	1	URBANO	B	TIPO 1
3	CPNP TAMSHYACU	CALLE ALAYZA PAZ SOLDAN # 107	FERNANDO LORES	MAYNAS	LORETO	4.002231667	-73.15991833	100M				0	1	1	0	1	RURAL	C	TIPO 1
3	CPNP AEROPUERTO INTERNACIONAL FRANCISCO SECADA VIGNETTA	OTRO INSTALACIONES DEL AEROPUERTO INTERNACIONAL # 1	IQUITOS	MAYNAS	LORETO	3.784341667	-73.30262167	100M				0	1	1	0	0	URBANO	C	TIPO 1
3	CPNP IQUITOS	CALLE MORONA # 120	IQUITOS	MAYNAS	LORETO	3.752266766	-73.24464664	100M				0	1	1	0	1	URBANO	A	TIPO 1
3	CPNP MORONACOCCHA/CPNP FAMILIA/DIRCOCOR MAYNAS	AV. MARISCAL CACERES 2200	IQUITOS	MAYNAS	LORETO	-3.745247	-73.264983	100M				0	1	1	0	2	URBANO	A	TIPO 1
3	DIVTURMA IQUITOS	PROLONGACIÓN PUTUMAYO Nº 1658	IQUITOS	MAYNAS	LORETO	-3.799301	-73.256882	100M				0	1	1	0	1	URBANO	TURISMO	TIPO 1
3	ETS PNP IQUITOS	ALTURA DEL KM. 5.100. DE LA CARRETERA IQUITOS - NAUTA. CASERÍO DE QUISTOCOCCHA	IQUITOS	MAYNAS	LORETO	-3.81905	-73.32346	100M				0	1	1	0	5	URBANO	ETS	TIPO 1
3	OFICRI IQUITOS	JR. PROSPERO Nº 565 - IQUITOS	IQUITOS	MAYNAS	LORETO	-3.75354	-73.24635	100M				0	1	1	0	1	URBANO	OFICRI	TIPO 1
3	RQ AEROPUERTO CRNL - FAP FRANCISCO SECADA VINEA	AV. A. QUIÑONES KM 6-AEROPUERTO	IQUITOS	MAYNAS	LORETO	-3.785033	-73.303278	100M				0	1	1	0	1	URBANO	RQ	TIPO 1
3	UNIPRCAR IQUITOS	CALLE PUTUMAYO 762	IQUITOS	MAYNAS	LORETO	-3.74613	-73.248669	100M				0	1	1	0	0	URBANO	CARRETE RAS	TIPO 1

7	5	REGPOL LORETO	AV. BRASIL 147 IQUITOS	IQUITOS	MAYNAS	LORETO	-3.753337	-73.245438	150M			0	1	1	0	1	URBANO	REGPOL	TIPO 1
7	5	CPNP PUNCHANA	AV. LA MARINA # 1101	PUNCHANA	MAYNAS	LORETO	3.729163333	-73.24078657	100M			0	1	1	0	1	URBANO	A	TIPO 1
7	5	DIVINCRI IQUITOS	CALLE 28 DE JULIO 103	PUNCHANA	MAYNAS	LORETO	-3.7287735	-73.2409193	100M			0	1	1	0	2	URBANO	DIVINCRI	TIPO 1
7	5	POLICLINICO POLICIAL IQUITOS	CALLE ABELARDO QUIÑONEZ KM 2.5	SAN JUAN BAUTISTA	MAYNAS	LORETO	-3.769623	-73.277574	100M			0	1	1	0	1	URBANO	POLICLINICO	TIPO 1
7	5	DIVTURMA MADRE DE DIOS	JR. DANIEL ALCIDES CARRION 440	TAMBOPATA	MADRE DE DIOS	MADRE DE DIOS	-12.593326	-69.178204	100M			0	0	1	0	1	URBANO	TURISMO	TIPO 1
7	5	CPNP RURAL IBERIA	AV. JORGE CHAVEZ # 986	IBERIA	TAHUAMANU	MADRE DE DIOS	11.40535167	-69.489645	100M			0	1	1	0	1	RURAL	D	TIPO 1
7	5	FRONTERIZO INAPARI	AV. HAYA DE LA TORRE CON A. BOLIVIA	INAPARI	TAHUAMANU	MADRE DE DIOS	-10.944700	-69.57594	100M			0	0	1	0	1	RURAL	CEBAF	TIPO 1
7	5	CPNP MAZUKO	AV. INAMBARI SN MZLL LT.1	INAMBARI	TAMBOPATA	MADRE DE DIOS	-13.100475	-70.36712667	100M			0	1	1	0	1	RURAL	D	TIPO 1
7	5	CPNP PLANCHON	CARR. CARRET INTEROCEANICA SN	LAS PIEDRAS	TAMBOPATA	MADRE DE DIOS	12.27572667	-69.15207833	100M			0	1	1	0	1	URBANO	C	TIPO 1
7	5	CPNP DE LA FAMILIA MALDONADO	AV. APURIMAC S/N CRUCE CON AV. ERNESTO RIVERO	TAMBOPATA	TAMBOPATA	MADRE DE DIOS	12.60154167	-69.18897833	100M			0	1	1	0	1	RURAL	FAMILIA	TIPO 1
7	6	CPNP PUERTO MALDONADO - TAMBOPATA	JIRÓN DANIEL ALCIDES CARRION # 410	TAMBOPATA	TAMBOPATA	MADRE DE DIOS	-12.59345	-69.17810333	100M			0	1	1	0	2	RURAL	A	TIPO 1
7	6	CPNP TAMBOPATA	AV. 2 DE MAYO S/N - ÓVALO CARRETERA INTEROCEÁNICA	TAMBOPATA	TAMBOPATA	MADRE DE DIOS	12.58328667	-69.19316333	100M			0	1	1	0	1	RURAL	B	TIPO 1
7	6	DIRCOCOR TAMBOPATA	JR. CUSCO CON JR. MARCO RUIZ	TAMBOPATA	TAMBOPATA	MADRE DE DIOS	-12.582317	-69.19138	100M			0	1	1	0	1	RURAL	DIRCOCOR	TIPO 1
7	6	DIVINCRI MADRE DE DIOS/DEPOTAD MADRE DE DIOS	JR. BILLINGHURST 387	TAMBOPATA	TAMBOPATA	MADRE DE DIOS	-12.592228	-69.176611	100M			0	1	1	0	2	RURAL	DIVINCRI	TIPO 1
7	6	REGPOL MADRE DE DIOS	AV. ELMER FAUCETT S/N - URB. LA JOYA	TAMBOPATA	TAMBOPATA	MADRE DE DIOS	-12.596938	-69.220247	100M			0	1	1	0	1	RURAL	DIRCOCOR	TIPO 1
7	6	DIVIDA Y DIVIDCOERM	Av. GUARDIA CIVIL N° 377-B LA CAMPIÑA	CHORRILLOS	LIMA	LIMA	-12.183471	-77.001334	100M			0	1	1	0	1	RURAL	C	TIPO 1
7	6	CPNP SECTORIAL OMATE / COMISARIA RURAL OMATE	CALLE IGNACIO JOVE# S/N	OMATE	GENERAL SANCHEZ CERRO	MOQUEGUA	-16.6743414	-70.9699805	100M			0	1	1	0	1	RURAL	B	TIPO 1
7	6	CPNP ILO/POSTA MÉDICA (IMPLEMENTADO EN LA CPNP ILO SOLAMENTE)	CALLE PICHINCHA # 327	ILO	ILO	MOQUEGUA	-17.64465	-71.343747	100M			0	1	1	0	2	URBANO	A	TIPO 1
7	6	CPNP PAMPA INALAMBICA	AV. BOULEVAR # SN	ILO	ILO	MOQUEGUA	-17.65242	-71.32462	100M			0	1	1	0	1	URBANO	B	TIPO 1

[Handwritten signatures and marks]



[Handwritten signatures and marks]

7	6	CPNP SECTORIAL ILO/OFICRI	AV. MARIANO LINO URQUIETA # 301	ILO	ILO	MOQUEGUA	-17.64211	-71.3408333	100M			0	1	1	0	2	URBANO	A	TIPO 1
9	7	DIVINCRI ILO/DIVANDRO ILO	AV. MARIANO LINO URQUIETA # 319	ILO	ILO	MOQUEGUA	-17.641502	-71.340665	100M			0	1	1	0	2	URBANO	DIVINCRI	TIPO 1
7	7	DIVTURMA ILO (IMPLEMENTO TAMBIEN EN LA POSTA MEDICA ILO)	JR. ZEPITA 602	ILO	ILO	MOQUEGUA	-17.644377	-71.343389	100M			0	0	1	0	1	URBANO	TURISMO	TIPO 1
1	7	CPNP DE LA FAMILIA MOQUEGUA	CALLE AYACUCHO # SN	MOQUEGUA	MARISCAL NIETO	MOQUEGUA	-17.191175	-70.929683	100M			0	1	1	0	1	URBANO	FAMILIA	TIPO 1
2	7	CPNP LOS ANGELES	CALLE 2 DE MAYO # 302	MOQUEGUA	MARISCAL NIETO	MOQUEGUA	17.16958751	-70.90695067	100M			0	1	1	0	1	URBANO	C	TIPO 1
3	7	CPNP MOQUEGUA	CALLE AYACUCHO # 308	MOQUEGUA	MARISCAL NIETO	MOQUEGUA	-17.199003	-70.99254833	100M			0	1	1	0	3	URBANO	B	TIPO 1
4	7	UNIPOMON TACALA / DIVSESP	MZ V.T. 19 CALLE LOS SAUCES - AA.HH. VILLA TACALA	CHORRILLOS	LIMA	LIMA	-12.186807	-76.988297	100M			0	1	1	0	1	URBANO	B	TIPO 1
5	7	DIVINCRI MOQUEGUA/REGION POLICIAL/OFICRI (AFIS)	CALLE AMAZONAS S/N	MOQUEGUA	MARISCAL NIETO	MOQUEGUA	-17.1889709	-70.9332212	100M			0	1	1	0	3	URBANO	DIVINCRI	TIPO 1
6	7	CPNP SAMEGUA	AV. EMANCIPACION SN MZ 2 IT.12	SAMEGUA	MARISCAL NIETO	MOQUEGUA	17.18233178	-70.8945316	100M			0	1	1	0	2	URBANO	B	TIPO 1
7	7	POL PNP MOQUEGUA	AV. ANDRES AVELINO CACERES S/N	SAMEGUA	MARISCAL NIETO	MOQUEGUA	-17.186757	-70.907793	100M			0	1	1	0	1	URBANO	POLICLINO	TIPO 1
8	7	CPNP TORATA	CALLE GRAU # 5	TORATA	MARISCAL NIETO	MOQUEGUA	17.0776833	-70.84528	100M			0	1	1	0	1	RURAL	D	TIPO 1
9	7	CPNP SECTORIAL DANIEL CARRION YANAHUANCA	JIRON 28 DE JULIO # SN	YANAHUANCA	DANIEL ALCIDES CARRION	PASCO	10.49133657	-76.51449333	100M			0	1	1	0	1	RURAL	B	TIPO 1
0	7	CPNP COMANDANCIA RURAL OXAPAMPA	JIRON ENRIQUE BOTTGER # 338	OXAPAMPA	OXAPAMPA	PASCO	10.57610167	-75.40269833	100M			0	1	1	0	2	RURAL	A	TIPO 1
1	7	CPNP VILLA RICA/DESPROCAR SAN LUIS DE SHUARO	AV. PADRE SALAS # SN	VILLA RICA	OXAPAMPA	PASCO	10.73776667	-75.26921	100M			0	1	1	0	1	RURAL	B	TIPO 1
2	7	CPNP CHAUPIMARCA	JIRON YALLI # 180	CHAUPIMARCA	PASCO	PASCO	10.68513167	-76.25437833	100M			0	1	1	0	1	RURAL	B	TIPO 1
3	7	CPNP LA ESPERANZA	AV. PROGRESO SN	SIMON BOLIVAR	PASCO	PASCO	-10.703602	-76.291688	100M			0	1	1	0	1		C	TIPO 1
4	7	CPNP HUARIACA	PASAJE HEROES DE LA GUERRA DEL PASIFICO # SN	HUARIACA	PASCO	PASCO	10.44492667	-76.18642	100M			0	1	1	0	1	RURAL	C	TIPO 1
5	7	CPNP HUAYLLAY	JIRON PASCO # SN	HUAYLLAY	PASCO	PASCO	-11.000105	-76.36158167	100M			0	1	1	0	1	RURAL	C	TIPO 1
6	7	POSTA MEDICA POLICIAL CERRO DE PASCO	AV. LOS PROCERES Y LOPEZ ALBUJAR S/N	LLANACANCHA	PASCO	PASCO	-10.662433	-76.251784	100M			0	1	1	0	1	RURAL	POLICLINO	TIPO 1

Handwritten signatures and initials at the top left of the page.



Handwritten signatures and initials on the left side of the page.

7	UNIPRCA LIMA SUR	KM 56 PANAMERICANA SUR	PUCUSANA	LIMA	LIMA	-12.455439	-76.753394	100M			0	0	1	0	0	URBANO	CARRETE RAS	TIPO 1
8	DIVINCI PASCO/DFCRI (AFIS)	AV. LOS INCAS CUADRA 1	PASCO	PASCO	PASCO	-10.667373	-76.252363	100M			0	1	1	0	2	RURAL	DIVINCI	TIPO 1
9	CPNP SAN FRANCISCO DE ASIS DE YARUSYACAN	JIRÓN LIBERTAD # SN	SAN FRANCISCO DE ASIS DE YARUSYACAN	PASCO	PASCO	-10.49098	-76.197259	100M			0	1	1	0	0	RURAL	E	TIPO 1
9	CPNP SECTORIAL TINYAHUARCO COLQUIJRCA	AV. 28 DE JULIO # SN	TINYAHUARCO	PASCO	PASCO	-10.754995	-76.26485667	100M			0	1	1	0	1	RURAL	C	TIPO 1
9	CPNP LA QUINUA / DESPRECAR LA QUINUA	CARRETERA CENTRAL VIA OROYA - HUANUCO # SN / FRENTE A PLAZA LA MONEDA	YANACANCHA	PASCO	PASCO	-10.614818	-76.179603	100M			0	1	1	0	1	URBANO	COMISARI A	TIPO 1
9	CPNP YANACANCHA	AV. LOS PROCERES # 203	YANACANCHA	PASCO	PASCO	10.66606029	-76.253196	100M			0	1	1	0	2	RURAL	B	TIPO 1
9	REGPOL PASCO/DIVTURMA PASCO YANACANCHA	AV. LOS PROCERES 906	YANACANCHA	PASCO	PASCO	-10.662712	-76.252213	100M			0	0	1	0	1	RURAL	TURISMO	TIPO 1
9	CPNP SECTORIAL AYABACA	CALLE CACERES S/N AYABACA	AYABACA	AYABACA	PIURA	-4.641835	-79.715373	100M			0	1	1	0	1	URBANO	B	TIPO 1
9	CPNP HUANCABAMBA	AV. CENTENARIO # 390	HUANCABAMBA	HUANCABAMBA	PIURA	-5.23635	-79.45303333	100M			0	1	1	0	1	RURAL	B	TIPO 1
9	CPNP KILOMETRO 50	CARR. CARRETERA CHULUCANAS KM50 SN MZC LT.277	CHULUCANAS	MORROPON	PIURA	-5.169395	-80.18613167	100M			0	1	1	0	1	URBANO	D	TIPO 1
9	CPNP PACCHA	AV. CALLE PRINCIPAL # SN	CHULUCANAS	MORROPON	PIURA	-5.01628	-80.22088667	100M			0	1	1	0	1	URBANO	D	TIPO 1
9	CPNP SECTORIAL CHULUCANAS	AV. RAMON CASTILLA # 1300	CHULUCANAS	MORROPON	PIURA	5.100871868	-80.1671277	100M			0	1	1	0	2	URBANO	A	TIPO 1
9	CPNP RURAL MATANZA	AV. 27 DE NOVIEMBRE # 236	LA MATANZA	MORROPON	PIURA	5.214901667	-80.090435	100M			0	1	1	0	1	RURAL	D	TIPO 1
9	CPNP SECTORIAL MORROPON	JIRÓN LOPEZ # 201	MORROPON	MORROPON	PIURA	-5.188795	-79.97140167	100M			0	1	1	0	2	URBANO	B	TIPO 1
9	CPNP SAN JUAN DE BIGOTE	AV. VICTOR RAUL HAYA DE LA TORRE # SN	SAN JUAN DE BIGOTE	MORROPON	PIURA	5.318746667	-79.78662167	100M			0	1	1	0	1	RURAL	D	TIPO 1
9	CPNP SAN LUCAS DE COLAN	CARRETERA SULLANA A PAITA - SAN LUCAS DE COLAN # SN	COLAN	PAITA	PIURA	5.007066667	-81.05663333	100M			0	1	1	0	1	RURAL	D	TIPO 1
9	CPNP CIUDAD DEL PESCADOR PIURA	AV. VICTOR RAUL HAYA DE LA TORRE SN MZC LT.1	PAITA	PAITA	PIURA	-5.09461	-81.10010333	100M			0	1	1	0	1	URBANO	C	TIPO 1
9	CPNP SECTORIAL PAITA	JIRÓN INDEPENDENCIA # 427	PAITA	PAITA	PIURA	5.086381667	-81.110685	100M			0	1	1	0	1	URBANO	B	TIPO 1
9	CPNP AEROPUERTO PIURA	AV. CORPAC # SN	CASTILLA	PIURA	PIURA	5.209938076	-80.61650249	100M			0	1	1	0	0	URBANO	A	TIPO 1



8	0	CPNP CASTILLA	AV. CORPAC # 100	CASTILLA	PIURA	PIURA	-5.2055966	-80.6206591	100M			0	1	1	0	1	URBANO	B	TIPO 1
7	0	CPNP EL INDIO	CALLE D # 261	CASTILLA	PIURA	PIURA	5.224608333	-80.61843833	100M			0	1	1	0	1	URBANO	C	TIPO 1
8	0	CPNP LOS ALGARROBOS	AV. AV 289 DE JULIO SN MZ.6 LT.1	CASTILLA	PIURA	PIURA	5.172515131	-80.64975567	100M			0	1	1	0	2	URBANO	B	TIPO 1
9	0	CPNP TACALA	AV. LOS BRILLANTES # SN	CASTILLA	PIURA	PIURA	5.187088333	-80.59857	100M			0	1	1	0	1	URBANO	C	TIPO 1
8	1	POL RNP ALMIRANTE MIGUEL GRAU (PIURA)	AV. CAJETANO HEREDIA S/N	CASTILLA	PIURA	PIURA	-5.195287	-80.52068	100M			0	1	1	0	1	URBANO	POLICIA	TIPO 1
1	1	CPNP SECTORIAL CATACAOS	AV. FRANCISCO BOLOGNESI # SN	CATACAOS	PIURA	PIURA	5.266191667	-80.67180167	100M			0	1	1	0	1	URBANO	B	TIPO 1
8	1	CPNP CUCUNGARA	AV. GRAU # 715	CURA MORI	PIURA	PIURA	5.324648333	-80.66487333	100M			0	1	1	0	1	URBANO	D	TIPO 1
3	1	CPNP LA ARENA	JIRÓN COMERCIO # 930	LA ARENA	PIURA	PIURA	-5.347885	-80.71320833	100M			0	1	1	0	1	URBANO	C	TIPO 1
8	1	CPNP LAS LOMAS	JIRÓN MIGUEL GRAU # 599	LAS LOMAS	PIURA	PIURA	4.656596667	-80.24405167	100M			0	1	1	0	1	URBANO	D	TIPO 1
5	1	CPNP PIURA	AV. SANCHEZ CERRO # 1381	PIURA	PIURA	PIURA	-5.190595	-80.63419	100M			0	1	1	0	2	URBANO	A	TIPO 1
6	1	CPNP SAN MARTIN	AV. JOSE CARLOS MARIATEGUI # 304	PIURA	PIURA	PIURA	5.185460052	-80.66849224	100M			0	1	1	0	1	URBANO	B	TIPO 1
7	1	DEPEME PIURA	CALLE 5 URB. SAN JOSE	PIURA	PIURA	PIURA	-5.193431	-80.644795	100M			0	1	1	0	1	URBANO	EMERGENCIA	TIPO 1
8	1	COMTUR PIURA / DIVIMA PIURA	AV. LOS COCOS 250 URBANIZACION CLUB GRAU	PIURA	PIURA	PIURA	-5.190867	-80.634336	100M			0	0	1	0	1	URBANO	TURISMO	TIPO 1
9	2	REGPOL PIURA	CARRERA PIURA-SULLANA KM. 3.5 ZONA INDUSTRIAL	PIURA	PIURA	PIURA	-5.182270	-80.654212	150M			0	1	1	0	1	URBANO	REGPOL	TIPO 1
8	2	POSTA RNP SULLANA	CALLE UGARTECHE 416	SULLANA	PIURA	PIURA	-4.88877	-80.684876	100M			0	1	1	0	1	URBANO	POSTA MEDICA	TIPO 1
1	2	CPNP CRUCETA	AV. JESUS MARIA # SN	TAMBO GRANDE	PIURA	PIURA	4.837078333	-80.270185	100M			0	1	1	0	1	URBANO	D	TIPO 1
2	2	CPNP TAMBOGRANDE	JIRÓN PAITA # 759	TAMBO GRANDE	PIURA	PIURA	4.93213333	-80.34211333	100M			0	1	1	0	1	URBANO	B	TIPO 1
3	2	CPNP LA UNION	CALLE UNION # 501	LA UNION	PIURA	PIURA	5.402346989	-80.74340366	100M			0	1	1	0	1	URBANO	C	TIPO 1
8	2	CPNP SECTORIAL SECHURA	CALLE SUCRE # 221	SECHURA	SECHURA	PIURA	5.554587896	-80.82269311	100M			0	1	1	0	2	URBANO	B	TIPO 1

8	CPNP BELLAVISTA PIURA	CALLE PUNO # 251	BELLAVISTA	SULLANA	PIURA	-4.891266	-80.68181	100M		0	1	1	0	2	RURAL	B	TIPO 1
2	CPNP SAN JACINTO	CALLE LOS LAURELES # SN	IGNACIO ESCUDERO	SULLANA	PIURA	4.84741667	-80.87356	100M		0	1	1	0	1	URBANO	D	TIPO 1
7	CPNP MARCAVELICA	CARRETERA PANAMERICANA NORTE # SN	MARCAVELICA	SULLANA	PIURA	4.881943333	-80.70671667	100M		0	1	1	0	1	URBANO	C	TIPO 1
8	DESPRCAR MARCAVELICA	CARRETERA PANAMERICANA NORTE # SN	MARCAVELICA	SULLANA	PIURA	4.885948333	-80.69810833	100M		0	0	1	0	0	URBANO	CARRETERAS	TIPO 1
9	CPNP SECTORIAL QUERECOTILLO	CALLE RODRIGUEZ # 485	QUERECOTILLO	SULLANA	PIURA	4.841468333	-80.65206667	100M		0	1	1	0	1	URBANO	C	TIPO 1
8	CPNP EL OBRERO	CALLE 13 DE DICIEMBRE # SN	SULLANA	SULLANA	PIURA	4.910501667	-80.68254833	100M		0	1	1	0	0	URBANO	E	TIPO 1
1	CPNP SULLANA	PASAJE LAS CAPULLANAS # 107	SULLANA	SULLANA	PIURA	4.899063333	-80.69023833	100M		0	1	1	0	2	URBANO	B	TIPO 1
8	SEINCRI SULLANA	AV. JOSE DE LAMA C/8 AA.HH SANCHEZ CERRO	SULLANA	SULLANA	PIURA	-4.8997971	-80.6935268	100M		0	1	1	0	1	URBANO	DIVINCRI	TIPO 1
3	CPNP EL ALTO	AV. BOLOGNESI # SN	EL ALTO	TALARA	PIURA	4.266716667	-81.21316833	100M		0	1	1	0	1	URBANO	D	TIPO 1
3	CPNP NEGRITOS	AV. MIGUEL GRAU # 349	LA BREA	TALARA	PIURA	-4.654365	-81.30501167	100M		0	1	1	0	1	RURAL	D	TIPO 1
5	CPNP LOS ORGANOS	AV. TUPAC AMARU # 519	LOS ORGANOS	TALARA	PIURA	4.179346667	-81.129755	100M		0	1	1	0	1	URBANO	D	TIPO 1
8	CPNP MANCORA	AV. PIURA # 625	MANCORA	TALARA	PIURA	-4.106995	-81.05293667	100M		0	1	1	0	1	URBANO	D	TIPO 1
7	DIVTURMA SULLANA CAMBIADO SECTOR MANCORA	AV. PIURA N°330	MANCORA	TALARA	PIURA	4.107363883	-81.05694334	100M		0	0	1	0	1	URBANO	TURISMO	TIPO 1
8	CPNP SECTORIAL TALARA	AV. BOLOGNESI # SN	PARIÑAS	TALARA	PIURA	-4.576145	-81.27648833	100M		0	1	1	0	2	URBANO	B	TIPO 1
9	CPNP TALARA ALTA	AV. A # 55	PARIÑAS	TALARA	PIURA	-4.589485	-81.25667167	100M		0	1	1	0	1	URBANO	C	TIPO 1
4	CPNP RURAL ASILLO (E)	JIRÓN BOLOGNESI # SN	ASILLO	AZANGARO	PUNO	14.78636167	-70.35442833	100M		0	1	1	0	1	RURAL	C	TIPO 1
1	CPNP SECTORIAL AZANGARO	JIRÓN TACNA # 313	AZANGARO	AZANGARO	PUNO	14.90983667	-70.196465	100M		0	1	1	0	1	RURAL	B	TIPO 1
8	CPNP RURAL JOSE DOMINGO CHOQUEHUANCA	JR. CUSCO N° 710	JOSE DOMINGO CHOQUEHUANCA	AZANGARO	PUNO	-15.030921	-70.340838	100M		0	1	1	0	1	RURAL	B	TIPO 1
4	CPNP MACUSANI	COPACABANA N° 242 - COSTADO DE TERMINAL	MACUSANI	CABABAYA	PUNO	-14.064695	-70.434991	100M		0	1	1	0	1	RURAL	B	TIPO 1
4																	

Handwritten signatures and initials at the top left of the page.



8	CPNP SECTORIAL DESAGUADERO/CARRETERA	AV. 28 DE JULIO # 325	DESAGUADERO	CHUCUITO	PUNO	-16.564245	-69.03947833	100M			0	1	1	0	2	RURAL	B	TIPO 1
4	DESAGUADERO /CEM																	
4	CPNP POMATA	JIRÓN LIMA NORTE # SN	POMATA	CHUCUITO	PUNO	16.27190833	-69.29286833	100M			0	1	1	0	1	RURAL	C	TIPO 1
4																		
4	CPNP SECTORIAL ILAVE/DIVPOL ILAVE	JIRÓN ANDINO # 412	ILAVE	EL COLLAO	PUNO	16.08573333	-69.63805833	100M			0	1	1	0	2	RURAL	A	TIPO 1
4																		
4	CPNP SECTORIAL HUANCANE	JIRÓN PECOSANI # 109	HUANCANE	HUANCANE	PUNO	15.20135167	-69.7656	100M			0	1	1	0	1	RURAL	B	TIPO 1
4																		
4	CPNP SECTORIAL LAMPA	JIRÓN JOSE MANUEL RIOS # 232	LAMPA	LAMPA	PUNO	15.36360667	-70.36710833	100M			0	1	1	0	1	RURAL	B	TIPO 1
4																		
4	CPNP SANTA LUCIA	JR. MANUEL CERVANTES N° 520	SANTA LUCIA	LAMPA	PUNO	-15.701796	-70.609044	100M			0	1	1	0	1	RURAL	D	TIPO 1
4																		
4	CPNP SECTORIAL AYAVIRI	JIRÓN 2 DE MAYO # 581	AYAVIRI	MELGAR	PUNO	14.88188333	-70.59221667	100M			0	1	1	0	2	RURAL	A	TIPO 1
4																		
4	DESPPCAR AYAVIRI	CALLE UMACHIRI # SN	AYAVIRI	MELGAR	PUNO	14.88466333	-70.59669667	100M			0	0	1	0	0	RURAL	CARRERE RAS	TIPO 1
4																		
4	CPNP ORURILLO	JIRÓN PIMENTEL # SN	ORURILLO	MELGAR	PUNO	14.72741068	-70.51095128	100M			0	1	1	0	1	RURAL	C	TIPO 1
4																		
4	CPNP RURAL SANTA ROSA	AV. MANCO CAPAC # 104	SANTA ROSA	MELGAR	PUNO	14.60809667	-70.79126667	100M			0	1	1	0	1	RURAL	C	TIPO 1
4																		
4	CPNP RURAL MOHO	AV. AREQUIPA # 105	MOHO	MOHO	PUNO	15.35911167	-69.48870167	100M			0	1	1	0	1	RURAL	C	TIPO 1
4																		
4	CPNP ACORA	AV. RAMON CASTILLA # 480	ACORA	PUNO	PUNO	-15.976265	-69.796665	100M			0	1	1	0	1	RURAL	B	TIPO 1
4																		
4	CPNP CAPACHICA	JIRÓN AREQUIPA # SN	CAPACHICA	PUNO	PUNO	15.64186686	-69.83118832	100M			0	1	1	0	1	RURAL	C	TIPO 1
4																		
4	CPNP CHUCUITO	JR. PASION N° 611	CHUCUITO	PUNO	PUNO	-15.894796	-69.889785	100M			0	1	1	0	1	RURAL	C	TIPO 1
4																		
4	CPNP ALTO PUNO	JR. MILLER FULLER MZA. N LOTE 8	PUNO	PUNO	PUNO	-15.820018	-70.029527	100M			0	1	1	0	1	URBANO	D	TIPO 1
4																		
4	CPNP DE LA FAMILIA PUNO	JR. DEUSTIA N° 536	PUNO	PUNO	PUNO	-15.840424	-70.02852	100M			0	1	1	0	1	URBANO	FAMILIA	TIPO 1
4																		
4	CPNP HUASCAR TIPO D / POLICLINICO	AV. JULIACA # SN	PUNO	PUNO	PUNO	15.82776333	-70.02424	100M			0	1	1	0	2	URBANO	C	TIPO 1
4																		
4	CPNP ICHU / DESPPCAR PUNO	PANAMERICANA SUR N° 1372 PUNO-CHUCUITO	PUNO	PUNO	PUNO	-15.875469	-69.9278321	100M			0	1	1	0	2	RURAL	B	TIPO 1
4																		
4	CPNP SECTORIAL PUNO/DECOTE/ESC VERDE/DIVPOL/MEDIO AMBIENTE	JIRÓN DEUSTIA # 536 - 538	PUNO	PUNO	PUNO	-15.840445	-70.028503	100M			0	1	1	0	3	URBANO	A	TIPO 1

Handwritten signature and initials at the top left of the page.

Handwritten signature and initials on the left side of the page.



8	6	DEPINCRI - PUNO	JR. RICARDO PALMA 225	PUNO	PUNO	PUNO	-15.8414262	-70.0209345	100M		0	1	1	0	2	URBANO	DIVINCRI	TIPO 1
4	8																	
6	5	OTITIC PUNO	JR. TACNA SN ESQUINA CON JR. RICARDO PALMA	PUNO	PUNO	PUNO	-15.842977	-70.023324	100M		0	1	1	0	2	RURAL	OTITIC	TIPO 1
8	6																	
6	6	REGPOL PUNO	AV. EL SOL 450	PUNO	PUNO	PUNO	-15.835892	-70.023276	200M		0	1	1	0	1	URBANO	REGPOL	TIPO 1
8	6																	
6	6	CPNP LA RINCONADA	CALLE COLOMBIA # SN	ANANEA	SAN ANTONIO DE PUTINA	PUNO	-14.63425	-69.44711167	100M		0	1	1	0	1	RURAL	C	TIPO 1
7	8																	
8	6	CPNP SECTORIAL SAN ANTONIO DE PUTINA	AV. LIBERTAD # SN	PUTINA	SAN ANTONIO DE PUTINA	PUNO	14.91622667	-69.86633167	100M		0	1	1	0	1	RURAL	A	TIPO 1
8	6																	
6	6	CPNP CABANILLAS	JIRÓN SAN MARTÍN # 221	CABANILLAS	SAN ROMAN	PUNO	-15.643775	-70.35106833	100M		0	1	1	0	1	RURAL	C	TIPO 1
9	8																	
6	7	CPNP CARACOTO	AV. LIMA # SN	CARACOTO	SAN ROMAN	PUNO	15.56645833	-70.10168167	100M		0	1	1	0	1	RURAL	D	TIPO 1
8	0																	
7	7	CPNP AEROPUERTO INCA MANCO CAPAC	AV. AEROPUERTO # SN	JULIACA	SAN ROMAN	PUNO	-15.47020333	-70.15710333	100M		0	1	1	0	0	URBANO	A	TIPO 1
1	8																	
8	7	CPNP JULIACA/DIVPOL JULIACA/ OFICRI/ FAMILIA JULIACA/ OFICINA DISCIPLINA/ USE	JIRON RAMON CASTILLA N° 723 CON JR. SAN MARTIN	JULIACA	SAN ROMAN	PUNO	-15.492894	-70.128058	200M		1	1	1	0	3	URBANO	A	TIPO 1
2	7																	
8	7	CPNP SANTA BARBARA/105, ESCUADRON DE EMERGENCIA	JIRÓN LOS OLIVOS # SN	JULIACA	SAN ROMAN	PUNO	15.50538167	-70.12800167	150M		1	1	1	0	1	URBANO	B	TIPO 1
3	8																	
7	8	DEPINCRI PNP JULIACA	JIRON ARICA 100 URB. LA RINCONADA	JULIACA	SAN ROMAN	PUNO	-15.496631	-70.132408	150M		0	1	1	0	2	URBANO	DIVINCRI	TIPO 1
4	8																	
8	7	DESPICAR JULIACA	AV. CIRCUNVALACION ESTE N° 924	JULIACA	SAN ROMAN	PUNO	-15.49205	-70.121199	100M		0	0	1	0	0	URBANO	CARRETE RAS	TIPO 1
5	8																	
7	7	TRANSITO / DEPROVE	AV. C. TELLO CUADRA 8 - LA CAPILLA (JIRON CAHUIDE 947)	JULIACA	SAN ROMAN	PUNO	-15.487185	-70.132289	200M		0	1	1	0	1	URBANO	DIPROVE	TIPO 1
6	8																	
8	7	CPNP SECTORIAL PNP YUNGUYO	JIRÓN AUDIBERT # 253	YUNGUYO	YUNGUYO	PUNO	16.24377667	-69.09166667	100M		0	1	1	0	1	RURAL	B	TIPO 1
7	8																	
8	7	CPNP SANDIA	JIRON ARICA N° 318	SANDIA	SANDIA	PUNO	-14.322222	-69.465822	100M		0	1	1	0	2	URBANO	A	TIPO 1
8	8																	
7	8	CPNP BELLAVISTA	JIRÓN RICARDO PALMA # SN	BELLAVISTA	BELLAVISTA	SAN MARTIN	7.066226667	-76.58458833	100M		0	1	1	0	1	URBANO	B	TIPO 1
9	8																	
8	8	CPNP SAPOSOA	AV. LIMA # 428	SAPOSOA	HUALLAGA	SAN MARTIN	-6.93632109	-76.77129954	100M		0	1	1	0	1	URBANO	B	TIPO 1
8	0																	
8	8	CPNP LAMAS	JR. SAN MARTÍN N° 661	LAMAS	LAMAS	SAN MARTIN	-6.423028	-76.513491	100M		0	1	1	0	1	URBANO	B	TIPO 1
8	1																	
8	8	CPNP SORITOR	CARRETERA FERNANDO BELAUDE TERRY # SN	SORITOR	LAMAS	SAN MARTIN	6.387603333	-76.62985333	100M		0	1	1	0	1	URBANO	B	TIPO 1
2	8																	



8	CPNP Sectorial JUANUI	JIRÓN TRIUNFO CUANDRA 6	JUANUI	MARISCAL CACERES	SAN MARTIN	7.179836667	-76.72648667	100M			0	1	1	0	1	URBANO	B	TIPO 1
3																		
8	CPNP CALZADA	JIRÓN INDEPENDENCIA # SN	CALZADA	MOYOBAMBA	SAN MARTIN	6.030496667	-77.06685	100M			0	1	1	0	1	RURAL	D	TIPO 1
4																		
8	CPNP JEPOLACIO	JIRÓN BOLOGNESI # 360	JEPOLACIO	MOYOBAMBA	SAN MARTIN	6.108213945	-76.91335763	100M			0	1	1	0	1	RURAL	D	TIPO 1
5																		
8	CPNP MOYOBAMBA	JIRÓN PEDRO CANGA # 298	MOYOBAMBA	MOYOBAMBA	SAN MARTIN	6.034482191	-76.57407991	100M			0	1	1	0	2	URBANO	A	TIPO 1
6																		
8	CPNP UCHUGELA	AV. ALMIRANTE GRAU # SN	MOYOBAMBA	MOYOBAMBA	SAN MARTIN	-6.04775	-76.97178	100M			0	1	1	0	1	URBANO	C	TIPO 1
7																		
8	CPNP TABALOSOS	AV. MIGUEL GRAU # SN	SORTOR	MOYOBAMBA	SAN MARTIN	6.195030497	-77.10041933	100M			0	1	1	0	1	URBANO	C	TIPO 1
8																		
8	CPNP PICOTA	CARRETERA FERNANDO BELAUNDE TERRY # SN	PICOTA	PICOTA	SAN MARTIN	-6.91891	-76.33226	100M			0	1	1	0	1	URBANO	C	TIPO 1
9																		
8	CPNP SAN HILARION	CARRETERA FERNANDO BELAUNDE TERRY # SN	SAN HILARION	PICOTA	SAN MARTIN	6.999921667	-76.444995	100M			0	1	1	0	1	RURAL	D	TIPO 1
0																		
8	CPNP SEGUNDA JERUSALEN	AV. GALILEA # 420	ELIAS SOPLIN VARGAS	RIOJA	SAN MARTIN	5.988013333	-77.27754833	100M			0	1	1	0	1	RURAL	D	TIPO 1
1																		
8	CPNP NUEVA CAJAMARCA	AV. CAJAMARCA SUR # 595	NUEVA CAJAMARCA	RIOJA	SAN MARTIN	-5.943097	-77.306147	100M			0	1	1	0	1	URBANO	B	TIPO 1
2																		
8	CPNP NARANJOS	AV. PARDO MIGUEL Y JR. LOS ANGELES S/N	PARDO MIGUEL	RIOJA	SAN MARTIN	5.740482213	-77.50366867	100M			0	1	1	0	1	RURAL	C	TIPO 1
3																		
8	CPNP RIOJA	JIRÓN SAN MARTIN # 1190	RIOJA	RIOJA	SAN MARTIN	-6.0638	-77.167896	100M			0	1	1	0	1	URBANO	B	TIPO 1
4																		
8	CPNP YURACYACU	AV. RIOJA NRO. 1410	YURACYACU	RIOJA	SAN MARTIN	5.928282122	-77.22725697	100M			0	1	1	0	1	RURAL	D	TIPO 1
5																		
8	DIYMA TARAPOTO	AV. CARRETERA TARAPOTO - YURIMAGUAS KM 5.5 S/N	BANDA DE SHILCAYO	SAN MARTIN	SAN MARTIN	-6.482214	-76.328804	100M			0	0	1	0	1	URBANO	TURISMO	TIPO 1
6																		
8	CPNP LA BANDA DE SHILCAYO	JIRÓN SANTA MARIA # 180	LA BANDA DE SHILCAYO	SAN MARTIN	SAN MARTIN	-6.4907	-76.354037	100M			0	1	1	0	1	URBANO	C	TIPO 1
7																		
8	CPNP MORALES/COM CAR TARAPOTO	AV. SALAVERRY # 213 # 225	MORALES	SAN MARTIN	SAN MARTIN	6.479423333	-76.38295167	100M			0	1	1	0	2	URBANO	B	TIPO 1
8																		
8	DEPOTAD MORALES	JR. SEVILLA 351	MORALES	SAN MARTIN	SAN MARTIN	-6.473491	-76.388949	100M			0	1	1	0	1	URBANO	DURANDR	TIPO 1
9																		
0	POL PNP MOYOBAMBA	AV. GRAU BARRIO CALVARIO 451	MOYOBAMBA	SAN MARTIN	SAN MARTIN	-6.044314	-76.970821	100M			0	1	1	0	1	URBANO	POLICIA	TIPO 1
0																		
8	CPNP AEROPUERTO TARAPOTO	JIRÓN JORGE CHAVEZ # SN	TARAPOTO	SAN MARTIN	SAN MARTIN	6.511053333	-76.36914333	100M			0	1	1	0	0	URBANO	A	TIPO 1
1																		



9	0	CPNP DE LA FAMILIA TARAPOTO	JIRON MATEO PUMACAHUA # SN	TARAPOTO	SAN MARTIN	SAN MARTIN	6.486328333	-76.37376333	100M			0	1	1	0	1	URBANO	FAMILIA	TIPO 1
2	0	CPNP TARAPOTO/DEPANDRO/REG POL SAN MARTIN	JIRON RAMIREZ HURTADO # 298	TARAPOTO	SAN MARTIN	SAN MARTIN	-6.48673	-76.35915	300M			3	1	1	0	3	URBANO	A	TIPO 1
3	0	DIVINCI-API-T OFICRI TARAPOTO	JR. LEONCIO PRADO 349	TARAPOTO	SAN MARTIN	SAN MARTIN	-6.484855	-76.360652	150M			3	1	1	0	2	URBANO	DIVINCI/ OFICRI	TIPO 1
4	0	DIVISION DE EMERGENCIA - TARAPOTO	C12 ALFONSO UGARTE	TARAPOTO	SAN MARTIN	SAN MARTIN	-6.492159	-76.371773	100M			0	1	1	0	1	URBANO	EMERGEN CIA	TIPO 1
5	0	OFICINA DE INTELIGENCIA TERRITORIAL	AV. SAN MARTIN N° 614	TARAPOTO	SAN MARTIN	SAN MARTIN	-6.493590	-76.353700	100M			0	0	1	0	1	URBANO	ORI	TIPO 1
6	0	POL PNP TARAPOTO	JR. LOS GIRASOLES 300	TARAPOTO	SAN MARTIN	SAN MARTIN	-6.493199	-76.372249	100M			0	1	1	0	1	URBANO	POLICINI CO	TIPO 1
7	0	CPNP NUEVO PROGRESO	CARRETERA FERNANDO BELAUDE TERRY # SN	NUEVO PROGRESO	TOCACH	TOCACH	8.453321667	-76.32424833	100M			0	1	1	0	1	RURAL	C	TIPO 1
8	0	DEPOTAD SANTA LUCIA (Antes DEPOTAD UCHIZA)	AV. LAS PALMAS 04 S/N-INTERIOR DE LA ETS SANTA LUCIA	SANTA LUCIA (Antes Uchiza)	TOCACH	TOCACH	-8.340909	-76.387207	100M			0	1	1	0	1	RURAL	DIRANDR O	TIPO 1
9	0	CPNP SECTORIAL TOCACH	JIRON FREDY ALIAGA # SN	TOCACH	SAN MARTIN	TOCACH	8.188316667	-76.51220167	100M			0	1	1	0	1	RURAL	B	TIPO 1
1	0	DESPPCAR TOCACH	JIRON SAN MARTIN # SN	TOCACH	SAN MARTIN	TOCACH	8.191158333	-76.51072333	100M			0	0	1	0	0	RURAL	CARRETE RAS	TIPO 1
2	0	CPNP UCHIZA	AV. MARCELINO ALVAREZ # SN	UCHIZA	SAN MARTIN	TOCACH	8.450521667	-76.46213167	100M			0	1	1	0	1	RURAL	C	TIPO 1
3	0	POSTA PNP SANTA LUCIA	AV. LAS PALMAS S/N	UCHIZA	SAN MARTIN	TOCACH	-8.340989	-76.387246	100M			0	1	1	0	1	RURAL	POSTA MEDICA	TIPO 1
4	0	COMISARIA DE TURISMO SAN MARTIN	JR. TOMAS MEZA N° 134	TARAPOTO	SAN MARTIN	SAN MARTIN	6.484122205	-76.36340723	100M			0	0	1	0	1	URBANO	AMBIENT E	TIPO 1
5	0	CPNP RURAL CANDARAVE	CALLE ARICA # 407	CANDARAVE	CANDARAVE	CANDARAVE	-17.271326	-70.25253667	100M			0	1	1	0	1	RURAL	B	TIPO 1
6	0	CPNP TOQUEPALA	OTRO SIN NOMBRE # SN	ILABAYA	JORGE BASADRE	JORGE BASADRE	17.27930166	-70.630985	100M			0	1	1	0	1	RURAL	B	TIPO 1
7	0	CPNP ITE	AV. PRINCIPAL # SN	ITE	JORGE BASADRE	JORGE BASADRE	17.86247333	-70.96448333	100M			0	1	1	0	1	RURAL	D	TIPO 1
8	0	CPNP LOCUMBA	CALLE SUCRE # SN	LOCUMBA	JORGE BASADRE	JORGE BASADRE	17.61183667	-70.76209667	100M			0	1	1	0	1	RURAL	C	TIPO 1
9	0	COMISARIA PNP ESPECIAL CAMIARA	CARRETERA PANAMERICANA SUR SN. KM 1204	LUCUMBA	JORGE BASADRE	JORGE BASADRE	-17.647509	-70.900123	100M			0	1	1	0	1	RURAL	COMISARI A	TIPO 1
0	0	CPNP ALTO DE LA ALIANZA	CALLE MARIANO SANTOS S/N	ALTO DE LA ALIANZA	TACNA	TACNA	-17.987995	-70.24142667	100M			0	1	1	0	1	URBANO	C	TIPO 1



9	2	CPNP CALANA	AV. GENERAL VARELA # SN	CALANA	TACNA	TACNA	-17.940615	-70.18695667	100M				0	1	1	0	1	URBANO	D	TIPO 1
2	1	REGPOL TACNA	PASAJE CALDERON DE LA BARCA 353	CERCADO	TACNA	TACNA	-18.010183	-70.249024	200M				0	1	1	0	1	URBANO	RESPOL	TIPO 1
2	2	CPNP CIUDAD NUEVA	CLL CASIMIRO ESPEJO SN	CIUDAD NUEVA	TACNA	TACNA	17.97890667	-70.236505	100M				0	1	1	0	1	URBANO	B	TIPO 1
9	2	CPNP AEROPUERTO TACNA	OTRO PANAMERICANA SUR # SN	CORONEL GREGORIO ALBARRACIN LANCHIPA	TACNA	TACNA	-18.049135	-70.2765	100M				0	1	1	0	0	RURAL	A	TIPO 1
2	4	CPNP CORONEL GREGORIO ALBARRACIN LANCHIPA	AV. MUNICIPAL # SN	CORONEL GREGORIO ALBARRACIN LANCHIPA	TACNA	TACNA	18.04194167	-70.25118833	100M				0	1	1	0	2	RURAL	B	TIPO 1
9	5	DEFINCRI TACNA	ASOCIACION VIV 24 DE JUNIO MZ 4 LTE 02	CORONEL GREGORIO ALBARRACIN LANCHIPA	TACNA	TACNA	18.05646754	-70.25492907	100M				0	1	1	0	2	URBANO	DIVINCRI	TIPO 1
2	6	CPNP SAMA INCLAN	AV. LAS VILCAS # SN	INCLAN	TACNA	TACNA	-17.79488	-70.49471	100M				0	1	1	0	1	RURAL	C	TIPO 1
9	7	COMISARIA DE TURISMO PNP TACNA	AV. GRAU NRO. 57 CERCADO DE TACNA	TACNA	TACNA	TACNA	-18.016811	-70.253939	100M				0	0	1	0	1	URBANO	TURISMO	TIPO 1
2	8	CPNP POCOLLAY	AV. CELESTINO VARGAS # 1145	POCOLLAY	TACNA	TACNA	-17.99519	-70.22024333	100M				0	1	1	0	1	URBANO	C	TIPO 1
9	9	CPNP BOCA DEL RIO	AV. GRAU SN	SAMA	TACNA	TACNA	18.15800167	-70.57884	100M				0	1	1	0	1	RURAL	D	TIPO 1
3	0	CPNP SAMA LAS VARAS	AV. HEROES DE LA GUERRA DEL PACIFICO, CRUCE CA. SIMON BOLIVAR # SN	SAMA	TACNA	TACNA	-17.862837	-70.560151	100M				0	1	1	0	1	RURAL	C	TIPO 1
9	1	DESPCAR BOCA DEL RIO	CARRETERA COSTANERA SUR # SN	SAMA	TACNA	TACNA	-17.89716	-70.9683	100M				0	0	1	0	0	RURAL	CARRETERAS	TIPO 1
2	2	CPNP AUGUSTO B. LEGUIA	AV. 200 MILLAS CON CALLE JOSE GÁLVEZ SN	TACNA	TACNA	TACNA	-18.03444	-70.27667	100M				0	1	1	0	1	URBANO	C	TIPO 1
9	3	CPNP CENTRAL TACNA	CALLE CALLAO # 121	TACNA	TACNA	TACNA	-18.014794	-70.251762	100M				0	1	1	0	2	URBANO	A	TIPO 1
3	4	CPNP DE LA FAMILIA TACNA	AV. HIPOLITO UNANUE # 970	TACNA	TACNA	TACNA	18.00758016	-70.25539041	100M				0	1	1	0	1	URBANO	FAMILIA	TIPO 1
9	5	CPNP GONZALES VIGIL	AV. INDUSTRIAL # SN	TACNA	TACNA	TACNA	17.99740591	-70.24562985	100M				0	1	1	0	2	URBANO	A	TIPO 1
2	6	CPNP LA NATIVIDAD	CALLE 8 DE SETIEMBRE # 1937	TACNA	TACNA	TACNA	-18.011672	-70.233148	100M				0	1	1	0	1	URBANO	B	TIPO 1
9	7	CPNP RURAL LA CONCORDIA	OTRO PANAMERICANA SUR # SN	TACNA	TACNA	TACNA	18.30772333	-70.313745	100M				0	1	1	0	1	URBANO	A	TIPO 1
3	8	CPNP TERMINAL TERRESTRE MANUEL A. ODRIA	AV. HIPOLITO UNANUE # SN	TACNA	TACNA	TACNA	18.00545833	-70.25773167	100M				0	1	1	0	1	URBANO	C	TIPO 1

Handwritten signatures and marks at the top left of the page.



Handwritten signatures and initials in the middle left margin.

9	DESPPCAR TACNA	AV. MANUEL A. ODRÍA S/N	TACNA	TACNA	TACNA	-18.026376	-70.261768	100M			0	0	1	0	0	URBANO	CARRETE RAS	TIPO 1
4																		
4	DIRCOCOR TACNA	URB VILLA DEL SOL MZ C1 LOTE 11 CENTRO POBLADO LA NATIVIDAD	TACNA	TACNA	TACNA	-18.016749	-70.266578	100M			0	1	1	0	0	URBANO	DIRCOCO R	TIPO 1
1																		
4	DIVINCRI TACNA	AV. TOMAS MARZANO S/N CON INTERSECCION AV. LIBERTADORA	TACNA	TACNA	TACNA	-18.056493	-70.254795	100M			0	1	1	0	0	URBANO	DIVINCRI	TIPO 1
2																		
9	OFICRI TACNA	AV. ARIAS Y ARAGÓES S/N	TACNA	TACNA	TACNA	-18.002836	-70.257759	100M			0	1	1	0	0	URBANO	OFICRI	TIPO 1
4																		
4	POL PNP TACNA	CALLE BLONDELL 110	TACNA	TACNA	TACNA	-18.015675	-70.254338	100M			0	1	1	0	0	URBANO	POLICLINICO	TIPO 1
4																		
9	CPNP RURAL TARATA	CALLE PRIMERO DE SETIEMBRE # SN	TARATA	TARATA	TACNA	17.47254833	-70.03111833	100M			0	1	1	0	0	RURAL	B	TIPO 1
4																		
9	CPNP SECTORIAL ZORRITOS	AV. REPUBLICA DEL PERU # SN	ZORRITOS	CONTRALMIR ANTE VILLAR	TUMBS	-3.68048	-80.675705	100M			0	1	1	0	0	URBANO	B	TIPO 1
6																		
9	CPNP CORRALES	CALLE SAN PEDRO # 600	CORRALES	TUMBS	TUMBS	3.601816667	-80.48098833	100M			0	1	1	0	0	URBANO	B	TIPO 1
4																		
9	CPNP LA CRUZ	AV. PIURA # 422	LA CRUZ	TUMBS	TUMBS	-3.637655	-80.59297167	100M			0	1	1	0	0	URBANO	C	TIPO 1
4																		
9	COMISARIA DE TURISMO TUMBS	CARRETERA PANAMERICANA NORTE KM. 4.5 (INTERIOR DE LA EX.EESTPP-TUMBS)	TUMBS	TUMBS	TUMBS	3.553624466	-80.42995158	100M			0	0	1	0	0	URBANO	TURISMO	TIPO 1
4																		
9	CPNP ANDRES ARAUJO MORAN	CLL. MAXIMILIANO MORAN SN MZ 18 LT. SN	TUMBS	TUMBS	TUMBS	3.560051667	-80.42805833	100M			0	1	1	0	0	URBANO	C	TIPO 1
0																		
9	CPNP DE LA FAMILIA TUMBS	AV. TUPAC AMARU # SN	TUMBS	TUMBS	TUMBS	3.572066667	-80.45198333	100M			0	1	1	0	0	URBANO	FAMILIA	TIPO 1
5																		
9	CPNP EL TABLAZO	CALLE HILARIO CARRASCO # 515	TUMBS	TUMBS	TUMBS	3.568281667	-80.450175	100M			0	1	1	0	0	URBANO	C	TIPO 1
5																		
9	CPNP PUERTO PIZARRO	CALLE JOSE OLAYA # 202	TUMBS	TUMBS	TUMBS	3.503021667	-80.39119833	100M			0	1	1	0	0	URBANO	C	TIPO 1
5																		
9	CPNP SAN JOSE - TUMBS	CALLE ZARUMILLA # 301	TUMBS	TUMBS	TUMBS	3.562988333	-80.460245	100M			0	1	1	0	0	URBANO	A	TIPO 1
5																		
9	REGPOL TUMBS	AV. PANAMERICANA NORTE S/N 1033	TUMBS	TUMBS	TUMBS	-3.557394	-80.451689	200M			1	0	1	0	0	URBANO	PRENTE	TIPO 1
5																		
9	POL PNP TUMBS	AV. TUMBS 706 (AV. TUMBS CON AV. JOSE OLAYA)	TUMBS	TUMBS	TUMBS	-3.565818	-80.457418	100M			0	1	1	0	0	URBANO	POLICLINICO	TIPO 1
6																		
9	CPNP AGUAS VERDES	AV. REPUBLICA DEL PERU # 254	AGUAS VERDES	ZARUMILLA	TUMBS	3.481631816	-80.24548441	100M			0	1	1	0	0	URBANO	C	TIPO 1
5																		
9	CEBAF - CONTROL POLICIAL ZARUMILLA	PAN. NORT KM 1268 (4KM DE FRONT ECUADOR)	ZARUMILLA	ZARUMILLA	TUMBS	-3.510765	-80.250539	100M			0	0	1	0	0	URBANO	CEBAF	TIPO 1
5																		



9	CPNP ZARUMILLA	CALLE TUMBES # 304	ZARUMILLA	ZARUMILLA	TUMBES	-3.50163	-80.27586167	100M				0	1	1	0	2	URBANO	A	TIPO 1
5																			
5	BRECC-LIMA NORTE	JR. ANDRÉS TORRES PAZ N° 116 - URBANIZACIÓN CONDEVILLA SEÑOR	SAN MARTIN DE PORRES	LIMA	LIMA	-12.018940	-77.088923	100M				0	1	1	0	0	RURAL	E	TIPO 1
6																			
0																			
9	CPNP PUCALLPA	JIRÓN INDEPENDENCIA # 360	CALLERIA	CORONEL PORTILLO	UCAYALI	-8.38211939	-74.5240871	100M				0	1	1	0	2	URBANO	A	TIPO 1
6																			
6	POL PNP PUCALLPA	JR. SUCRE CDA 4 S/N	CALLERIA	CORONEL PORTILLO	UCAYALI	-8.383793	-74.531983	100M				0	1	1	0	1	URBANO	POLICIA CO	TIPO 1
2																			
9	REGPOL UCAYALI	AV. SAN MARTIN 466	CALLERIA	CORONEL PORTILLO	UCAYALI	-8.384316	-74.531174	150M				0	1	1	0	1	URBANO	REGPOL	TIPO 1
6																			
3																			
9	CPNP CAMPO VERDE/COM CAR CAMPO VERDE	AV. 1 DE JUNIO # SN	CAMPOVERDE	CORONEL PORTILLO	UCAYALI	8.473743849	-74.80449468	100M				0	1	1	0	1	URBANO	C	TIPO 1
6																			
4																			
9	CPNP SAN FERNANDO (MANANTAY)	JIRÓN LOS MANGOS # 572	MANANTAY	CORONEL PORTILLO	UCAYALI	-8.39809	-74.536905	100M				0	1	1	0	1	RURAL	B	TIPO 1
5																			
9	COMISARIA DE TURISMO UCAYALI	AA. HH. FAUSTINO MALDONADO MZ. D LT. 7 - YARINACCOCHA	YARINACCOCHA	CORONEL PORTILLO	UCAYALI	-8.378077	-74.558173	100M				0	0	1	0	1	URBANO	TURISMO	TIPO 1
6																			
6	CPNP YARINACCOCHA	AV. YARINACCOCHA # 376	YARINACCOCHA	CORONEL PORTILLO	UCAYALI	8.555034915	-74.57652166	100M				0	1	1	0	1	URBANO	B	TIPO 1
7																			
9	DEP. UNIDAD DESCONCENTRADO DE PROTECCION DEL MEDIO AMBIENTE	CARRETERA FEDERICO BASADRE 10.5	YARINACCOCHA	CORONEL PORTILLO	UCAYALI	-8.401911	-74.619968	100M				0	0	1	0	1	URBANO	MEDIO AMBIENTE	TIPO 1
6																			
8																			
9	RQ AEROPUERTO CAP. FAP DAVID ABENSUR RENGIFO	CARRETERA FEDERICO BASADRE	YARINACCOCHA	CORONEL PORTILLO	UCAYALI	-8.384974	-74.573885	100M				0	1	1	0	1	URBANO	RQ	TIPO 1
9																			
7	CPNP ALEJANDER VON HUMBOLDT	CARRETERA REGIONAL FEDERICO BASADRE # SN	IRAZOLA	PADRE ABAD	UCAYALI	-8.82504	-75.05160833	100M				0	1	1	0	1	RURAL	B	TIPO 1
0																			
9	CPNP NESHUYA HUALLAGA	CARRETERA FEDERICO BASADRE # SN	IRAZOLA	PADRE ABAD	UCAYALI	8.642201667	-74.96223167	100M				0	1	1	0	1	RURAL	C	TIPO 1
7																			
9	CPNP SAN ALEJANDRO	CALLE REGIONAL FEDERICO BASADRE # SN	IRAZOLA	PADRE ABAD	UCAYALI	-8.82949	-75.21611667	100M				0	1	1	0	1	RURAL	C	TIPO 1
2																			
7	DESPCAR VON HUMBOLT	AV. 1 DE JUNIO # SN	IRAZOLA	PADRE ABAD	UCAYALI	8.825125905	-75.05201966	100M				0	0	1	0	0	RURAL	CARRERAS	TIPO 1
3																			
9	CPNP SECTORIAL PADRE ABAD - AGUAYTIA/COM CAR AGUAYTIA	CARRETERA FEDERICO BASADRE KM 162 - AGUAYTIA	PADRE ABAD	PADRE ABAD	UCAYALI	-9.037793	-75.5069754	100M				0	1	1	0	1	RURAL	B	TIPO 1
7																			
4																			
9	CPNP SECTORIAL UCAYALI CONTAMANA	CALLE MANUEL E. ROJAS # 315	CONTAMANA	UCAYALI	UCAYALI	7.349791667	-75.00849833	100M				0	1	1	0	2	RURAL	B	TIPO 1
7																			
5																			

[Handwritten signature]

[Handwritten signature]

[Handwritten signature]



[Handwritten signature]

[Handwritten signature]

ANEXO B2 43 UNIDADES SEDES TIPO 2

N°	SEDE	DIRECCIÓN ACTUAL	DISTRITO	PROVINCIA	DPTO	LATITUD	LONGITUD	ANC HO BAN DA	SWITCH H LAN Y GABINETE PRINCIPAL	SWITCH LAN DE 48 PUERTOS Y GABINETE DE DISTRIBUCION	SWITCH DE 24 PUERTOS Y GABINETE PRINCIPAL	FIREWALL	FIREWALL DE PROXIMA GENERACION	N° DE ACCESOS	Zonificación	TIPO DE UNIDAD	TIP O	
1	REGPOL AMAZONAS	JIRON AYACUCHO C 10	CHACHAPOYAS	CHACHAPOYAS	AMAZONAS	6.228965	- 77.87336 9	100 M	1	1	0	1	0	0	5	URBA NO	UNIDAD PNP	TIP O 2
2	DEFUNEME-DEPSEFEN-DEPTA-DEPSESP-DEPERPROC-DEPROVE-DEPAJUS	AV. JOSE PARDO CUADRA 26	CHIMBOTE	SANTA	ANCASH	9.086921	- 78.57242 8	200 M	1	1	0	1	0	0	5	URBA NO	UNIDAD PNP	TIP O 2
3	DEPICA/COMPLEJO POLICIAL CAMANA/INSPECTORIA CAMANA	AV. MARISCAL CASTILLA 735 MZ LOTE 9 KM.	CAMANA	CAMANA	AREQUIPA	- 16.62974 4	- 72.71194 1	200 M	1	1	0	1	0	0	3	URBA NO	UNIDAD PNP	TIP O 2
4	DIVINCRI AYACUCHO/COMPLEJO WALTER ROSALES LEON	JR. LIMA 330	AYACUCHO	HUAMANGA	AYACUCHO	- 13.16020 7	- 74.22924	200 M	1	2	0	1	0	0	3	URBA NO	UNIDAD PNP	TIP O 2
5	DIVINCRI/DIVTURMA/DEPROVE CAJAMARCA	JR. DEL COMERCIO 1021	CAJAMARCA	CAJAMARCA	CAJAMARC A	- 7.158129	- 78.51708 2	200 M	1	3	0	1	0	0	3	URBA NO	UNIDAD PNP	TIP O 2
6	CPNP DE LA FAMILIA/DEPINCRI/DIVCOTER/DIPOLFIS (AHORA SEGURIDAD DE ESTADO)	CALLE JORGE OCHOA # 345	SANTIAGO	CUSCO	CUSCO	- 13.52431 171	- 71.98421 158	200 M	1	2	0	1	0	0	3	URBA NO	UNIDAD PNP	TIP O 2
7	DIVINCRI ICA/COM FAMILIA ICA	CALLE LIBERTAD 384	ICA	ICA	ICA	- 14.06532 5	- 75.73204	200 M	1	2	0	1	0	0	3	URBA NO	UNIDAD PNP	TIP O 2
8	DIRECCION DE BIENESTAR Y APOYO AL POLICIA - DIRBAP	JR. MELLO FRANCO N° 155	JESUS MARIA	LIMA	LIMA	- 12.07447 8	- 77.05233	200 M	1	3	0	1	0	0	3	URBA NO	UNIDAD PNP	TIP O 2
9	DIVINCRI + SEANDRO JUANIUI+DIVPOL	CALLE LA MERCED 428 SE TRASLADÓ A LA COMISARIA DE JUANIUI	JUANIUI	MARISCAL CACERES	SAN MARTIN	- 7.179839	- 76.72649 6	200 M	1	3	0	1	0	0	3	URBA NO	UNIDAD PNP	TIP O 2
10	TRANSITO DEPROVE DEPIAT	AV. ARIAS Y ARAGÓES 1115	TACNA	TACNA	TACNA	18.00245 6	- 70.25937 2	200 M	1	2	0	1	0	0	4	URBA NO	UNIDAD PNP	TIP O 2
11	REGPOL ICA/OFICRI	JR. J. ELIAS S/N (CUADRA 06)	ICA	ICA	ICA	- 14.07296 6	- 75.73227 3	200 M	1	3	0	1	0	0	5	URBA NO	COMPLEJO FRENTE	TIP O 2
12	REGPOL JUNIN - HUANCAYO / OFICRI / INSPECTORIA	JR. CUSCO 666 , ESQUINA DE JR. CUSCO CON JR. LIBERTAD	HUANCAYO	HUANCAYO	JUNIN	- 12.06679 6	- 75.22047 7	200 M	1	2	0	1	0	0	5	URBA NO	COMPLEJO MACRE	TIP O 2
13	CP SAN MARTIN DIVINCRI/DIRTUMA/OFICRI	JR. SAN MARTIN CDA 7	RESTAURACION	HUARAZ	ANCASH	- 9.529525	- 77.53004 5	200 M	1	1	0	1	0	0	3	RURA L	COMPLEJO 1	TIP O 2
14	CP ALCIDES VIGO HURTADO/DIRCOCOR/DEINCRI/CARRTERAS/OFICRI	JR. CALICANTO 18 CUADRA S/N	AMARILIS	HUANUCO	HUANUCO	- 9.953296	- 76.23564 4	200 M	1	2	0	1	0	0	3	URBA NO	COMPLEJO 1	TIP O 2
15	CP ALCIDES VIGO HURTADO (DEPINCRI SEG. ESTADO. DIVICOTE. DIVANDRO. OFICRI) - LA LIBERTAD	CALLE SANTO TORIBIO DE MOGROVEJO 387 URB.SAN ANDRES	TRUJILLO	TRUJILLO	LA LIBERTAD	- 8.117851 2	- 79.03511 51	200 M	1	2	0	1	0	0	5	URBA NO	COMPLEJO 1	TIP O 2
16	CP 7 DE AGOSTO (DIVOPUS/DIVISION POLICIA COMUNITARIA, SEGURIDAD ESTADO, UNITIC)	AV. JOSE BALTA 80	CHICLAYO	CHICLAYO	LAMBAYEQ UE	- 6.777582	- 79.83885 8	200 M	1	2	0	1	0	0	5	URBA NO	COMPLEJO 1	TIP O 2



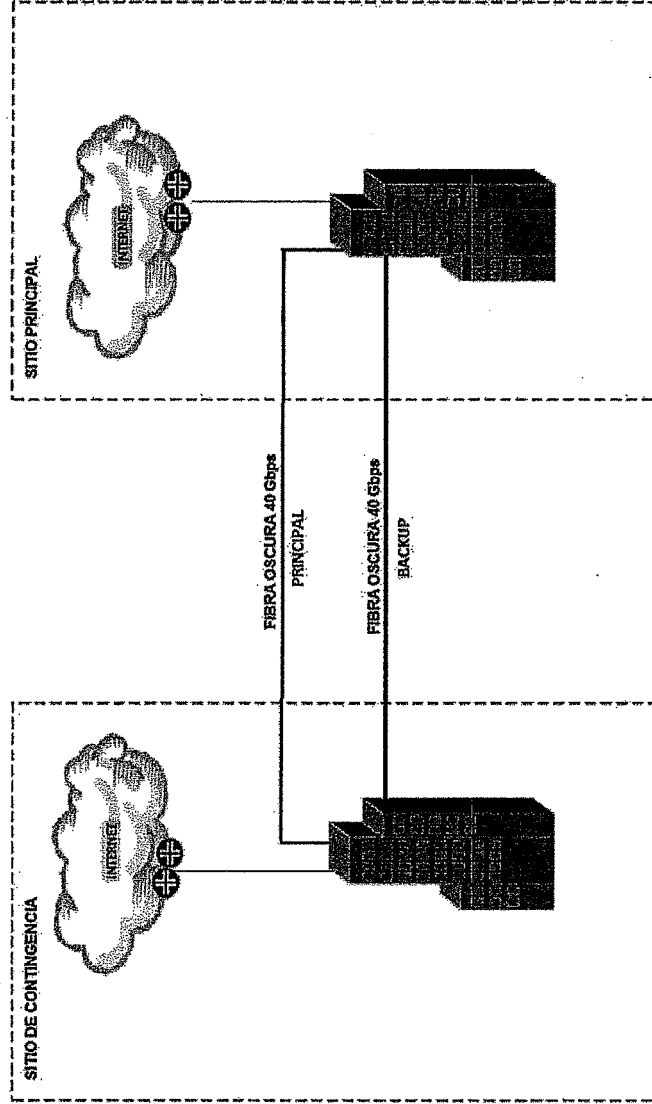
1	7	CPNP LA VICTORIA	AV. 28 DE JULIO # 1600	LA VICTORIA	LIMA	LIMA	12.05309 657	-77.0261 M	100	1		3	0	1	0	3	URBA NO	A	TIP O 2
1	8	CPNP BREÑA/DIVINCRI	JIRÓN GENERAL FELIPE VARELA # 1978	BREÑA	LIMA	LIMA	12.06719 667	-77.05289 833	150		1	3	0	1	0	3	URBA NO	A	TIP O 2
1	9	CP MY. PNP FELIX TELLO ROJAS (DIVINCRI. DEPROVE. OFICRI CHICLAYO)	AV. SALAVERRY CON PL. JOSE OLAYA 929	CHICLAYO	CHICLAYO	LAMBAYEQUE	6.770414	79.85462	200		1	2	0	1	0	5	URBA NO	COMPLEJO 1	TIP O 2
2	0	CP SANTA MARINA OFICRI	JR. SUPE 3 AV. FERNANDINI	CALLAO	CALLAO	LIMA	12.05467 2	-77.12925 7	200		1	2	0	1	0	5	URBA NO	COMPLEJO 1	TIP O 2
2	1	DIRECCION DE AVIACION POLICIAL - DIRAVPOL	AV. ELMER FAUCCETT S/N. AL COSTADO DEL AUCH	CALLAO	CALLAO	LIMA	12.02717 9	-77.10360 1	200		1	3	0	0	2	3	URBA NO	COMPLEJO 1	TIP O 2
2	2	CP ALIPIO PONCE VASQUEZ	JR. APURIMAC 647	CERCADO	CALLAO	LIMA	12.06331 3	-77.13714 8	400	1		4	0	0	2	5	URBA NO	COMPLEJO 1	TIP O 2
2	3	CPNP INDEPENDENCIA/DIVINCRI/DIVPOL	AV. TUPAC AMARU KM. 4.5	INDEPENDENCIA	LIMA	LIMA	11.99628 593	-77.05482 781	150		1	3	0	1	0	3	URBA NO	A	TIP O 2
2	4	CP ALCIDES VIGO HURTADO DIRINCRI / OFICRI DIRINCRI 5TO PISO OFICRI DIRCOTE PISO 12	AV. ESPAÑA CDRA. 03 PISO 4	CERCADO	LIMA	LIMA	12.05829 6	-77.04004 6	400		1	2	0	0	2	5	URBA NO	COMPLEJO 1	TIP O 2
2	5	DIPROVE / OFICRI	JR. CONCHUCOS 666 BARRIOS ALTOS PISO 2	CERCADO	LIMA	LIMA	12.04866 1	-77.01162 8	400		1	2	0	0	2	3	URBA NO	COMPLEJO 1	TIP O 2
2	6	CPNP APOLO/DIVINCRI	JIRÓN 3 DE FEBRERO # 1050	LA VICTORIA	LIMA	LIMA	12.07135 201	-77.00980 291	150		1	3	0	1	0	3	URBA NO	A	TIP O 2
2	7	REGPOL LIMA - (105)/DIRCOTE	AV. ESPAÑA CDRA 4 S/N	CERCADO	LIMA	LIMA	12.05799 8	-77.04098 2	400	1		4	0	0	2	5	URBA NO	COMPLEJO 1	TIP O 2
2	8	ESCUELA DE OFICIALES	AV. GUARDIA CIVIL S/N	CHORRILLOS	LIMA	LIMA	12.17524 3	-76.99358 7	200	1		4	0	0	2	2	URBA NO	COMPLEJO 1	TIP O 2
2	9	HOSPITAL NACIONAL PNP "LUIS N. SAENZ"	AV. DE LA POLICIA N° 335	JESUS MARIA	LIMA	LIMA	12.08562 785	-77.05989 198	400	1		4	0	0	2	0	URBA NO	COMPLEJO 1	TIP O 2
3	0	DIRSEVI - DIVPOLTRAN	AV. 28 DE JULIO Y LA MAR 2090	LA VICTORIA	LIMA	LIMA	12.06194 9	-77.01986 1	400	1		4	0	0	2	3	URBA NO	COMPLEJO 1	TIP O 2
3	1	ETS PNP PUENTE PIEDRA	AV. PANAMERICANA NORTE KM. 26.5	PUENTE PIEDRA	LIMA	LIMA	11.89582	-77.05846	400	1		5	0	0	2	8	URBA NO	COMPLEJO 1	TIP O 2
3	2	DEPARTAMENTO DE REQUISITORIAS	JR. LOS TORDOS N°1042	SAN JUAN DE LURIGANCHO	LIMA	LIMA	12.01604 2	-76.99780 5	150		1	1	0	1	0	2	URBA NO	RQ/OFICRI	TIP O 2
3	3	CP JUAN BENITEZ LUINA CIBELES	CALLE LOS CIBELES 150	RIMAC	LIMA	LIMA	12.03354 8	-77.03254 7	400	1		5	0	0	2	12	URBA NO	COMPLEJO 1	TIP O 2
3	4	DIRANDRO	CALLE LOS CISNES 594 PISO 10 ARAMBURU	SAN ISIDRO	LIMA	LIMA	12.10228 1	-77.02356 2	400	1		4	0	0	2	5	URBA NO	COMPLEJO 1	TIP O 2
3	5	DIRINT	AV. PASEO DE LA REPUBLICA 3681 PISO 7	SAN ISIDRO	LIMA	LIMA	12.10065 6	-77.02646 6	400	1		1	0	0	1	0	URBA NO	COMPLEJO 1	TIP O 2
3	6	DIVISION DE PROTECCION DE CARRETERAS - DIVPRCAR	AV. VARGAS MACHUCA CDA. 4 - JUNTO A LA CT	SAN JUAN DE MIRAFLORES	LIMA	LIMA	12.16563 2	-76.97361	400		1	3	0	0	2	3	URBA NO	COMPLEJO 1	TIP O 2

37	CP WALTER ROSALES LEON ARAMBURU	AV. ARAMBURU 550 - PISO 4	SURQUILLO	LIMA	LIMA	12.102718	77.025027	400 M	1	5	0	0	2	8	URBA NO	COMPLEJO 1	TIP O2
38	CP USE PNP/SEGURIDAD DEL ESTADO/DIPOLCA/OFICRI	JR ICA Y PARDO DE MIGUEL	TAMBOPATA	TAMBOPATA	MADRE DE DIOS	12.587636	69.194441	200 M	1	2	0	1	0	5	RURA L	COMPLEJO 1	TIP O2
39	CP JUAN BENITEZ LUNA DEPOTAD DIVSEG PIURA SSEE	CALLE MONITOR HUASCAR 220 URB. LA ALBORADA	PIURA	PIURA	PIURA	5.185474	80.65227	200 M	1	5	0	1	0	4	URBA NO	COMPLEJO 1	TIP O2
40	CP MAY ROBERTO MORALES ROJAS /DIVINCRI/OFICRI/DIVANDRO/DEPROVE	AV. PROLONGACION SANCHEZ CERRO S/N CARRETERA PIURA SULLANA. S/N	PIURA	PIURA	PIURA	5.185024	80.647686	400 M	1	1	0	1	0	3	URBA NO	COMPLEJO 1	TIP O2
41	CP PNP WALTER PINEDO JIMENEZ/ COM CAR MOYOBAMBA /DIRCOCOR /DIVINCRI	JR. CRNL SECADA 113	MOYOBAMBA	MOYOBAMBA	SAN MARTIN	6.038981	76.97029	200 M	1	1	0	1	0	3	URBA NO	COMPLEJO 1	TIP O2
42	CP Tnte JORGE TAPE TABAZONA (DIVTRAN DIVINCRI DIVANDRO	AV. PANAMERICANA NORTE KM 1322	TUMBES	TUMBES	TUMBES	3.555376	80.437942	200 M	1	2	0	1	0	3	URBA NO	COMPLEJO 1	TIP O2
43	CP SOTI PNP ARTEMIO SANCHEZ PAREDES DIVINCRI/OFICRI PUCALLPA	AV. 9 DE OCTUBRE N°167	CALLERIA	CORONEL PORTILLO	UCAYALI	8.9877901	74.5444298	200 M	1	2	0	1	0	3	URBA NO	COMPLEJO 1	TIP O2

ANEXO C

DISEÑO DE RED PROPUESTO

INTERCONEXION ENTRE SITIOS



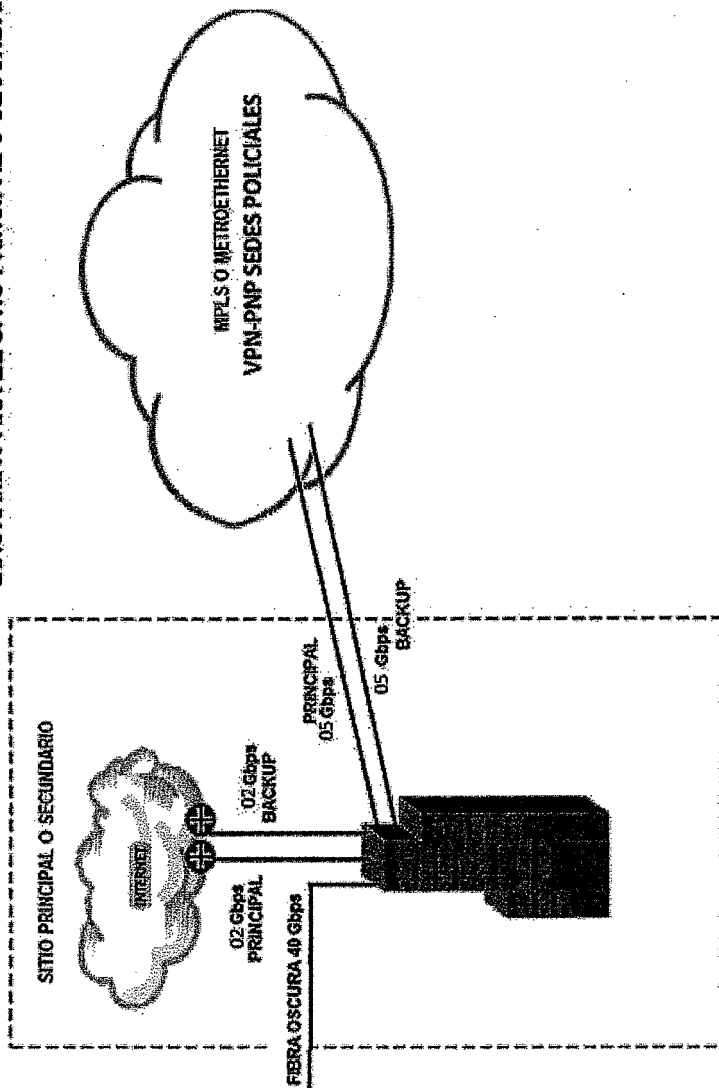
[Handwritten signatures]



[Handwritten signature]

[Handwritten signature]

DIAGRAMA PARA EL SITIO PRINCIPAL O SECUNDARIO

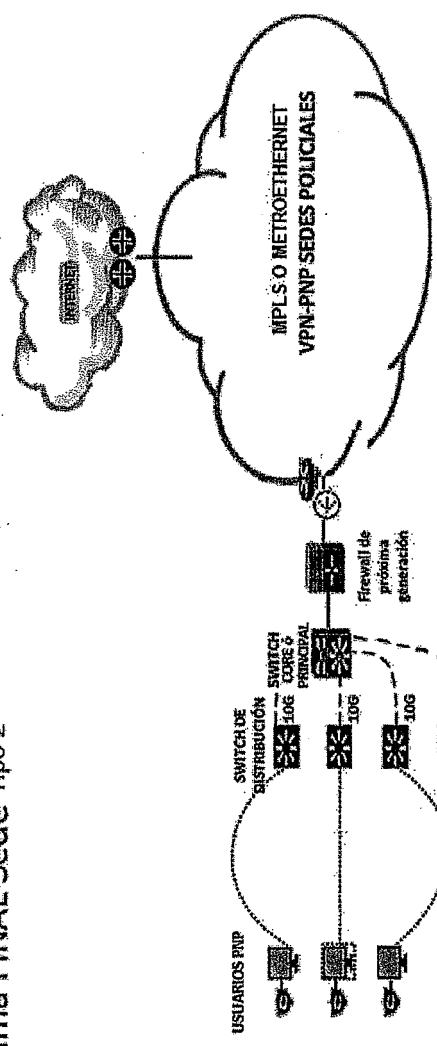


Handwritten marks and signatures at the top left of the page.



Handwritten signature and initials 'M. W.' in the top left margin.

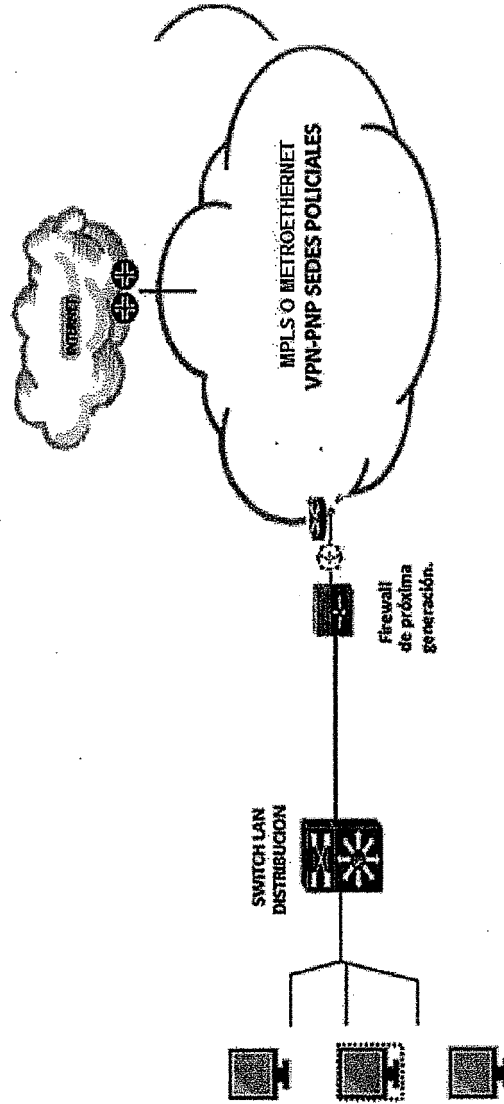
Diagrama FINAL Sede Tipo 2



REPRESENTACION	DESCRIPCION
Una pinta de color azul indica una bodega de tránsito, la cual no deberá ser utilizada para almacenar mercancías.	
Una pinta de color rojo indica una bodega de tránsito, la cual no deberá ser utilizada para almacenar mercancías.	
Una pinta de color verde indica una bodega de tránsito, la cual no deberá ser utilizada para almacenar mercancías.	

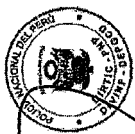
SW CORE : SW 48 PTO. L3
 SW PRINCIPAL : SW 48 PTO. L2
 SW DE DISTRIBUCION : SW 48 PTO. L2
 INTERCONEXION ENTRE SW: Fibra de 10GB

Diagrama FINAL Sede
Remota Tipo 1 y Tipo 2



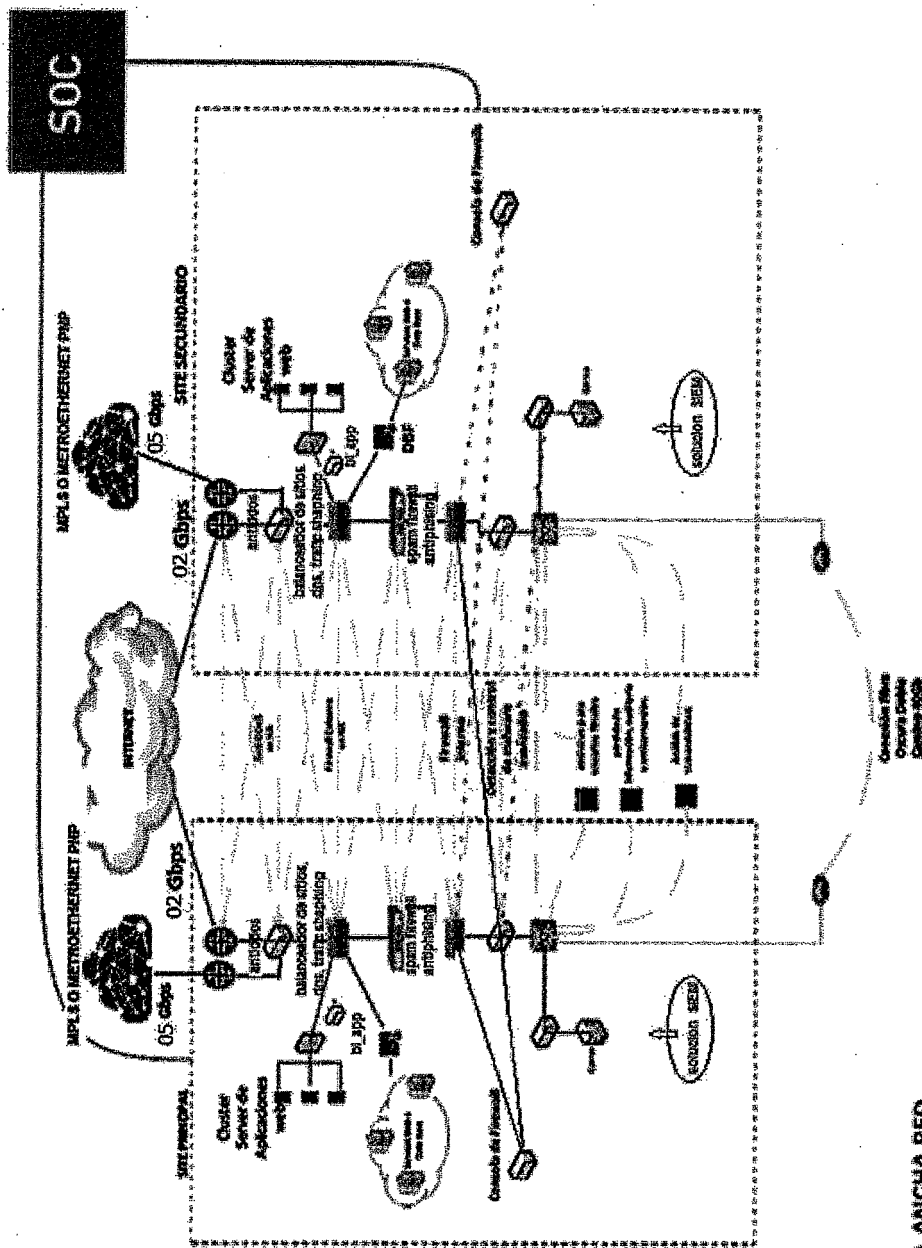
INTERCONEXIÓN BANDA ANCHA RED
POLICÍA NACIONAL DEL PERÚ

Handwritten signature and initials at the top left of the page.



ANEXO D

DIAGRAMA DE ENLACES DE DATOS PARA PNP



INTERCONEXIÓN BANDA ANCHA RED
POLICÍA NACIONAL DEL PERÚ

CONDICIONES Y DISPOSICIONES DE SEGURIDAD Y SALUD EN EL TRABAJO PARA COMPRAS EN INSTALACIONES EXISTENTES DE LA PNP

En el marco del artículo 68 de la Ley N° 29783, Ley de Seguridad y Salud en el Trabajo, a continuación, se precisan las condiciones y disposiciones en materia de Seguridad y Salud en el Trabajo a considerar durante la ejecución del servicio:

CONDICIONES DE SEGURIDAD Y SALUD EN EL TRABAJO:

El CONTRATISTA debe presentar al inicio de la implementación de la prestación principal:

Constancias del Seguro Complementario de Trabajo de Riesgo (SCTR) SALUD Y PENSIÓN de todo el personal declarado.

Declaración Jurada sobre el buen estado de salud¹ por cada trabajador.

En caso de aplicar, los trabajadores del CONTRATISTA deberán contar con sus respectivos Equipos de Protección Personal (EPP's). El no uso de los EPP's podrá ser causal de paralización del servicio, y por ende de aplicación de penalidad. En ese sentido, los EPP's básicos necesarios son los siguientes:

Ropa de trabajo (pantalón, polo manga larga u otros).

Casco de seguridad.

Zapatos de seguridad con puntera composite o caso contrario punta de acero

Lentes de seguridad.

Tapones auditivos u orejeras.

Mascarillas quirúrgicas o comunitarias.

Alcohol gel al 60%.

Entre otros que correspondan de acuerdo con el tipo de trabajo que realicen.

De igual forma, deberán tener los Registros de Entrega de Equipos de Protección Personal (EPP's) en virtud del artículo 33 inciso f) del Reglamento de la Ley N° 29783, Ley de Seguridad y Salud en el Trabajo aprobado por el Decreto Supremo N° 005-2012-TR y de la Resolución Ministerial N° 050-2013-TR.

CAPÍTULO IV FACTORES DE EVALUACIÓN

La evaluación se realiza sobre la base de cien (100) puntos.

Para determinar la oferta con el mejor puntaje y el orden de prelación de las ofertas, se considera lo siguiente:

FACTOR DE EVALUACIÓN	PUNTAJE / METODOLOGÍA PARA SU ASIGNACIÓN
A. PRECIO	
<u>Evaluación:</u> Se evaluará considerando el precio ofertado por el postor. <u>Acreditación:</u> Se acreditará mediante el documento que contiene el precio de la oferta (Anexo N° 6).	La evaluación consistirá en otorgar el máximo puntaje a la oferta de precio más bajo y otorgar a las demás ofertas puntajes inversamente proporcionales a sus respectivos precios, según la siguiente fórmula: $P_i = \frac{O_m \times PMP}{O_i}$ i = Oferta P_i = Puntaje de la oferta a evaluar O_i = Precio i O_m = Precio de la oferta más baja PMP = Puntaje máximo del precio 100 puntos

Importante

Los factores de evaluación elaborados por el comité de selección son objetivos y guardan vinculación, razonabilidad y proporcionalidad con el objeto de la contratación. Asimismo, estos no pueden calificar con puntaje el cumplimiento de los Términos de Referencia ni los requisitos de calificación.

CAPÍTULO V PROFORMA DEL CONTRATO

Importante

Dependiendo del objeto del contrato, de resultar indispensable, puede incluirse cláusulas adicionales o la adecuación de las propuestas en el presente documento, las que en ningún caso pueden contemplar disposiciones contrarias a la normativa vigente ni a lo señalado en este capítulo.

Conste por el presente documento, la contratación del servicio de [CONSIGNAR LA DENOMINACIÓN DE LA CONVOCATORIA], que celebra de una parte [CONSIGNAR EL NOMBRE DE LA ENTIDAD], en adelante LA ENTIDAD, con RUC N° [.....], con domicilio legal en [.....], representada por [.....], identificado con DNI N° [.....], y de otra parte [.....], con RUC N° [.....], con domicilio legal en [.....], inscrita en la Ficha N° [.....] Asiento N° [.....] del Registro de Personas Jurídicas de la ciudad de [.....], debidamente representado por su Representante Legal, [.....], con DNI N° [.....], según poder inscrito en la Ficha N° [.....], Asiento N° [.....] del Registro de Personas Jurídicas de la ciudad de [.....], a quien en adelante se le denominará EL CONTRATISTA en los términos y condiciones siguientes:

CLÁUSULA PRIMERA: ANTECEDENTES

Con fecha [.....], el comité de selección adjudicó la buena pro del **CONCURSO PÚBLICO N° [CONSIGNAR NOMENCLATURA DEL PROCEDIMIENTO DE SELECCIÓN]** para la contratación de [CONSIGNAR LA DENOMINACIÓN DE LA CONVOCATORIA], a [INDICAR NOMBRE DEL GANADOR DE LA BUENA PRO], cuyos detalles e importe constan en los documentos integrantes del presente contrato.

CLÁUSULA SEGUNDA: OBJETO

El presente contrato tiene por objeto [CONSIGNAR EL OBJETO DE LA CONTRATACIÓN].

CLÁUSULA TERCERA: MONTO CONTRACTUAL

El monto total del presente contrato asciende a [CONSIGNAR MONEDA Y MONTO], que incluye todos los impuestos de Ley.

Este monto comprende el costo del servicio, todos los tributos, seguros, transporte, inspecciones, pruebas y, de ser el caso, los costos laborales conforme a la legislación vigente, así como cualquier otro concepto que pueda tener incidencia sobre la ejecución del servicio materia del presente contrato.

CLÁUSULA CUARTA: DEL PAGO¹¹

LA ENTIDAD se obliga a pagar la contraprestación a EL CONTRATISTA en [INDICAR MONEDA], en [INDICAR SI SE TRATA DE PAGO ÚNICO, PAGOS PARCIALES O PAGOS PERIÓDICOS], luego de la recepción formal y completa de la documentación correspondiente, según lo establecido en el artículo 171 del Reglamento de la Ley de Contrataciones del Estado.

Para tal efecto, el responsable de otorgar la conformidad de la prestación deberá hacerlo en un plazo que no excederá de los siete (7) días de producida la recepción, salvo que se requiera efectuar pruebas que permitan verificar el cumplimiento de la obligación, en cuyo caso la conformidad se emite en un plazo máximo de quince (15) días, bajo responsabilidad de dicho funcionario.

LA ENTIDAD debe efectuar el pago de las contraprestaciones pactadas a favor del CONTRATISTA dentro de los diez (10) días calendario siguientes de otorgada la conformidad de los servicios, siempre que se verifiquen las condiciones establecidas en el contrato para ello, bajo responsabilidad del funcionario competente.

¹¹ En cada caso concreto, dependiendo de la naturaleza del contrato, podrá adicionarse la información que resulte pertinente a efectos de generar el pago.

En caso de retraso en el pago por parte de LA ENTIDAD, salvo que se deba a caso fortuito o fuerza mayor, EL CONTRATISTA tendrá derecho al pago de intereses legales conforme a lo establecido en el artículo 39 de la Ley de Contrataciones del Estado y en el artículo 171 de su Reglamento, los que se computan desde la oportunidad en que el pago debió efectuarse.

CLÁUSULA QUINTA: DEL PLAZO DE LA EJECUCIÓN DE LA PRESTACIÓN

El plazo de ejecución del presente contrato es de [.....], el mismo que se computa desde [CONSIGNAR SI ES DEL DÍA SIGUIENTE DEL PERFECCIONAMIENTO DEL CONTRATO, DESDE LA FECHA QUE SE ESTABLEZCA EN EL CONTRATO O DESDE LA FECHA EN QUE SE CUMPLAN LAS CONDICIONES PREVISTAS EN EL CONTRATO PARA EL INICIO DE LA EJECUCIÓN, DEBIENDO INDICAR LAS MISMAS EN ESTE ÚLTIMO CASO].

El plazo para la [CONSIGNAR LAS ACTIVIDADES PREVIAS PREVISTAS EN LOS TÉRMINOS DE REFERENCIA] es de [.....], el mismo que se computa desde [INDICAR CONDICIÓN CON LA QUE DICHAS ACTIVIDADES SE INICIAN].”

CLÁUSULA SEXTA: PARTES INTEGRANTES DEL CONTRATO

El presente contrato está conformado por las bases integradas, la oferta ganadora, así como los documentos derivados del procedimiento de selección que establezcan obligaciones para las partes.

CLÁUSULA SÉTIMA: GARANTÍAS

EL CONTRATISTA entregó al perfeccionamiento del contrato la respectiva garantía incondicional, solidaria, irrevocable, y de realización automática en el país al solo requerimiento, a favor de LA ENTIDAD, por los conceptos, montos y vigencias siguientes:

- De fiel cumplimiento del contrato: [CONSIGNAR EL MONTO], a través de la [INDICAR EL TIPO DE GARANTÍA PRESENTADA] N° [INDICAR NÚMERO DEL DOCUMENTO] emitida por [SEÑALAR EMPRESA QUE LA EMITE]. Monto que es equivalente al diez por ciento (10%) del monto del contrato original, la misma que debe mantenerse vigente hasta la conformidad de la recepción de la prestación.

Importante

Al amparo de lo dispuesto en el numeral 149.4 del artículo 149 del Reglamento de la Ley de Contrataciones del Estado, en el caso de contratos periódicos de prestación de servicios en general, si el postor ganador de la buena pro solicita la retención del diez por ciento (10%) del monto del contrato original como garantía de fiel cumplimiento de contrato, debe consignarse lo siguiente:

“De fiel cumplimiento del contrato: [CONSIGNAR EL MONTO], a través de la retención que debe efectuar LA ENTIDAD, durante la primera mitad del número total de pagos a realizarse, de forma prorrateada, con cargo a ser devuelto a la finalización del mismo.”

Importante

En los contratos derivados de procedimientos de selección por relación de ítems, cuando el monto del ítem adjudicado o la sumatoria de los montos de los ítems adjudicados sea igual o menor a doscientos mil Soles (S/ 200,000.00), no corresponde presentar garantía de fiel cumplimiento de contrato ni garantía de fiel cumplimiento por prestaciones accesorias, conforme a lo dispuesto en el literal a) del artículo 152 del Reglamento.

CLÁUSULA OCTAVA: EJECUCIÓN DE GARANTÍAS POR FALTA DE RENOVACIÓN

LA ENTIDAD puede solicitar la ejecución de las garantías cuando EL CONTRATISTA no las hubiere renovado antes de la fecha de su vencimiento, conforme a lo dispuesto por el literal a) del numeral 155.1 del artículo 155 del Reglamento de la Ley de Contrataciones del Estado.

CLÁUSULA DÉCIMA: CONFORMIDAD DE LA PRESTACIÓN DEL SERVICIO

La conformidad de la prestación del servicio se regula por lo dispuesto en el artículo 168 del Reglamento de la Ley de Contrataciones del Estado. La conformidad será otorgada por [CONSIGNAR EL ÁREA O UNIDAD ORGÁNICA QUE OTORGARÁ LA CONFORMIDAD] en el plazo máximo de [CONSIGNAR SIETE (7) DÍAS O MÁXIMO QUINCE (15) DÍAS, EN CASO SE

REQUIERA EFECTUAR PRUEBAS QUE PERMITAN VERIFICAR EL CUMPLIMIENTO DE LA OBLIGACIÓN] días de producida la recepción.

De existir observaciones, LA ENTIDAD las comunica al CONTRATISTA, indicando claramente el sentido de estas, otorgándole un plazo para subsanar no menor de dos (2) ni mayor de ocho (8) días. Dependiendo de la complejidad o sofisticación de las subsanaciones a realizar el plazo para subsanar no puede ser menor de cinco (5) ni mayor de quince (15) días. Si pese al plazo otorgado, EL CONTRATISTA no cumpliera a cabalidad con la subsanación, LA ENTIDAD puede otorgar al CONTRATISTA periodos adicionales para las correcciones pertinentes. En este supuesto corresponde aplicar la penalidad por mora desde el vencimiento del plazo para subsanar.

Este procedimiento no resulta aplicable cuando los servicios manifiestamente no cumplan con las características y condiciones ofrecidas, en cuyo caso LA ENTIDAD no otorga la conformidad, debiendo considerarse como no ejecutada la prestación, aplicándose la penalidad que corresponda por cada día de atraso.

CLÁUSULA UNDÉCIMA: DECLARACIÓN JURADA DEL CONTRATISTA

EL CONTRATISTA declara bajo juramento que se compromete a cumplir las obligaciones derivadas del presente contrato, bajo sanción de quedar inhabilitado para contratar con el Estado en caso de incumplimiento.

CLÁUSULA DUODÉCIMA: RESPONSABILIDAD POR VICIOS OCULTOS

La conformidad del servicio por parte de LA ENTIDAD no enerva su derecho a reclamar posteriormente por defectos o vicios ocultos, conforme a lo dispuesto por los artículos 40 de la Ley de Contrataciones del Estado y 173 de su Reglamento.

El plazo máximo de responsabilidad del contratista es de [CONSIGNAR TIEMPO EN AÑOS, NO MENOR DE UN (1) AÑO] año(s) contado a partir de la conformidad otorgada por LA ENTIDAD.

CLÁUSULA DÉCIMA TERCERA: PENALIDADES

Si EL CONTRATISTA incurre en retraso injustificado en la ejecución de las prestaciones objeto del contrato, LA ENTIDAD le aplica automáticamente una penalidad por mora por cada día de atraso, de acuerdo a la siguiente fórmula:

$$\text{Penalidad Diaria} = \frac{0.10 \times \text{monto vigente}}{F \times \text{plazo vigente en días}}$$

Donde:

F = 0.25 para plazos mayores a sesenta (60) días o;

F = 0.40 para plazos menores o iguales a sesenta (60) días.

El retraso se justifica a través de la solicitud de ampliación de plazo debidamente aprobado. Adicionalmente, se considera justificado el retraso y en consecuencia no se aplica penalidad, cuando EL CONTRATISTA acredite, de modo objetivamente sustentado, que el mayor tiempo transcurrido no le resulta imputable. En este último caso la calificación del retraso como justificado por parte de LA ENTIDAD no da lugar al pago de gastos generales ni costos directos de ningún tipo, conforme el numeral 162.5 del artículo 162 del Reglamento de la Ley de Contrataciones del Estado.

Importante

De haberse previsto establecer penalidades distintas a la penalidad por mora, incluir dichas penalidades, los supuestos de aplicación de penalidad, la forma de cálculo de la penalidad para cada supuesto y el procedimiento mediante el cual se verifica el supuesto a penalizar, conforme el artículo 163 del Reglamento de la Ley de Contrataciones del Estado.

OTRAS PENALIDADES

Asimismo, conforme al artículo 163° del Reglamento de la Ley de Contrataciones del Estado, y a las características del servicio a contratar, se considera necesario establecer penalidades distintas a la penalidad por mora conforme al siguiente detalle:

6.10.1 SERVICIO BRINDADO

6.10.1.1 DISPONIBILIDAD DE ACUERDOS

Para el cálculo de la penalidad se considerará como sigue:

Penalidad Disponibilidad (DIS) ITEM1 = Penalidad Disponibilidad (DIS) $C_{1,2,4,5}$ +

Penalidad Disponibilidad (DIS) C_3

6.10.1.1.1 PARA COMPONENTES 1, 2, 4 y 5 ($C_{1,2,4,5}$):

Disponibilidad de acuerdo al SLA (99.7%): El contratista será responsable de la operatividad de los servicios por cada componente 1, 2, 4 y 5 necesarios para la prestación del servicio (implica a cada equipamiento instalado), los cuales deben estar disponibles y operativos las veinticuatro (24) horas del día, los siete (07) días a la semana y trescientos sesenta y cinco (365) días del año. El nivel de disponibilidad debe ser como mínimo del 99.7% (SLA) para los siguientes servicios:

N°	DISPONIBILIDAD PROMEDIO MEDIDOS MES A MES (DIS)	PENALIDAD	PROCEDIMIENTO
01	$\leq 99.7\%$ y $> 95\%$	20% de 4UIT	Personal técnico de la DIRTIC PNP a través del acceso web, monitorea,

02	$\leq 95\%$ y $> 90\%$	30% de 4UIT	registra e informa la disponibilidad de los enlaces y en comparación con la información descrita en la presente tabla, LA ENTIDAD procede a solicitar la penalización, emitiendo el informe correspondiente.
03	$\leq 90\%$ y $> 80\%$	40% de 4UIT	
04	$\leq 80\%$	50% de 4UIT	

6.10.1.1.2 PARA COMPONENTES 3 C_3 :

Disponibilidad de acuerdo al SLA (99.5%): El contratista será responsable de la disponibilidad de los servicios brindados en el componente 3 necesarios para la prestación del servicio (implica a cada equipamiento instalado), los cuales deben estar disponibles y operativos las veinticuatro (24) horas del día, los siete (07) días a la semana y trescientos sesenta y cinco (365) días del año. El nivel de disponibilidad debe ser como mínimo del 99.5% (SLA) para los siguientes servicios:

N°	DISPONIBILIDAD PROMEDIO MEDIDOS MES A MES (DIS)	PENALIDAD	PROCEDIMIENTO
01	$\leq 99.5\%$ y $> 93\%$	20% de 3UIT	Personal técnico de la DIRTIC PNP a través del acceso web, monitorea, registra e informa la disponibilidad de los enlaces. LA ENTIDAD procede a solicitar la penalización, emitiendo el informe correspondiente, tomando en consideración la información indicada en el presente cuadro.
02	$\leq 93\%$ y $> 90\%$	30% de 3UIT	
03	$\leq 90\%$ y $> 80\%$	40% de 3UIT	
04	$\leq 80\%$	50% de 3UIT	

6.10.1.2 CALIDAD DE ATENCIÓN ANTE AVERÍAS

6.10.1.2.1 PARA COMPONENTE 1, 2, 4 Y 5:

N°	CONCEPTO- THE	PENALIDAD	PROCEDIMIENTO
01	Demora de mayor a una (01) horas hasta cinco (05) horas para la subsanación de averías de los siguientes servicios: COMPONENTE 1: Servicio de acceso de internet para la sede principal y secundario (sitio principal y secundario). COMPONENTE 2: Servicio de fibra óptica entre el Datacenter principal y secundario de la PNP COMPONENTE 4: Servicio de seguridad de la información y seguridad informática gestionada. COMPONENTE 5: Servicio de housing para el Datacenter secundario PNP	20% de 4UIT por ocurrencia	Cuando La Entidad reporte una falla en los enlaces y/o equipamientos de los Data Center, registrará la fecha y hora de la llamada. El contratista deberá crear un ticket por cada incidente reportado y resolverlo dentro de una (01) hora. Si no se soluciona, el personal de la DIRTIC PNP

02	Demora de mayor a cinco (05) horas para la subsanación de averías de los siguientes servicios: COMPONENTE 1: Servicio de acceso de internet para la sede principal y secundario (sitio principal y secundario). COMPONENTE 2: Servicio de fibra oscura entre el Datacenter principal y secundario de la PNP COMPONENTE 4: Servicio de seguridad de la información y seguridad informática gestionada. COMPONENTE 5: Servicio de housing para el Datacenter secundario PNP	30% de 4UIT por ocurrencia	informará sobre la demora y emitirá un informe solicitando la penalización correspondiente, según lo establecido. Además, se pedirá la penalización si ocurre otra falla similar.
03	El personal designado para los trabajos necesarios para la implementación del servicio no cuenta con uniforme o implementos de seguridad y seguro complementario de trabajo de riesgo.	20% de 1UIT por ocurrencia, asimismo, no se permitirá el ingreso del personal del contratista en los Datacenter PNP	

6.10.1.2.2 PARA COMPONENTE 3:

N°	CONCEPTO- THE	PENALIDAD	PROCEDIMIENTO
01	COMPONENTE 3: "Plataforma digital de servicios para transmisión de voz, video y datos para las sedes desconcentradas PNP, a nivel nacional"; en la que se debe considerar, para la subsanación de averías de las líneas de conexión a internet, intranet y sus equipos de conectividad, así como los equipos de seguridad gestionada: <ul style="list-style-type: none">Demora de mayor a cuatro (04) horas hasta nueve (09) horas para la subsanación de averías en zonas urbanas.Demora de mayor a doce (12) horas hasta dieciséis (16) horas para la subsanación de averías en zonas rurales.	20% de 2UIT por ocurrencia	La Entidad anotará el día y la hora en la cual realiza la llamada reportando la ocurrencia, falla y/o avería en el servicio. Ante cada falla en el servicio el contratista debe generar un ticket por el incidente reportado y solucionarlo en cuatro (04) hora, de no darse la solución del incidente, el personal de la DIRTIC PNP informará la demora de la solución de la avería, emitiendo el informe correspondiente solicitando la penalización respectiva considerando la información descrita en el presente cuadro.
02	COMPONENTE 3: "Plataforma digital de servicios para transmisión de voz, video y datos para las sedes desconcentradas PNP, a nivel nacional"; en la que se debe considerar, para la subsanación de averías de las líneas de conexión a internet, intranet y sus equipos de conectividad, así como los equipos de seguridad gestionada: <ul style="list-style-type: none">Demora de mayor a nueve (09) horas hasta catorce (14) horas para la subsanación de averías en zonas urbanas.Demora de mayor a dieciséis (16) horas hasta veinte (20) horas para la subsanación de averías en zonas rurales.	30% de 2UIT por ocurrencia	La Entidad anotará el día y la hora en la cual realiza la llamada reportando la ocurrencia, falla y/o avería en el servicio. Ante cada falla en el servicio el contratista debe generar un ticket por el incidente reportado y solucionarlo en cuatro (04) horas, de no darse la solución del incidente, el personal de la DIRTIC PNP informará la demora de la solución de la avería, emitiendo el informe correspondiente solicitando la penalización respectiva considerando la información descrita en el presente cuadro.
03	COMPONENTE 3: "Plataforma digital de servicios para transmisión de voz, video y datos para las sedes desconcentradas PNP, a nivel nacional"; por lo que se debe considerar, para la subsanación de averías de las líneas de conexión a internet, intranet y sus equipos	40% de 2UIT por ocurrencia	

	de conectividad, así como los equipos de seguridad gestionada: <ul style="list-style-type: none"> • Demora de mayor a catorce (14) horas para la subsanación de averías en zonas urbanas. • Demora de mayor a veinte (20) horas para la subsanación de averías en zonas rurales. 		
04	El personal designado para los trabajos necesarios para la implementación del servicio no cuenta con uniforme o implementos de seguridad y seguro complementario de trabajo de riesgo.	20% de 3UIT por ocurrencia Asimismo, no se permitirá el ingreso del personal del contratista en los Datacenter PNP	De verificar esta ocurrencia, se solicitará la penalización emitiendo el informe correspondiente solicitando la penalización respectiva considerando la información descrita en el presente cuadro (punto 04).

*El cálculo de penalidad se realizará por cada sobre el cual no se cumpla el acuerdo de nivel de servicio. La penalidad se calculará de acuerdo con la siguiente fórmula:

$$\text{Tiempo de solución} = \text{Fecha y hora de solución del incidente} - \text{Fecha y hora de generación del ticket de Incidente} - \text{Duración de parada de reloj}$$

Dónde: Parada de Reloj es el retraso en la atención de averías por motivos no atribuibles al contratista, y que se encuentran específicamente detallados en las Bases Integradas, el cual será registrado en la herramienta de gestión de averías.

La penalidad total mensual por este concepto se obtiene sumando las penalidades obtenidas de las líneas de conexión a internet, fibra oscura, plataforma digital de servicios para transmisión de voz, video y datos para las sedes desconcentrada PNP a nivel nacional, servicio de seguridad de la información, servicio sms y servicio de autenticación, servicio de housing para el datacenter secundario. Por ejemplo:

Penalidad Total (THE) ITEM1 = THE por Equipo1 * penalidad +

THE por Equipo2 * penalidad + THE por EquipoXX * penalidadXX

Frecuencia de caída Mensual (FCM) del servicio, al mes: Medido por la cantidad de veces en que está fuera de servicio la línea a internet e intranet, la fibra oscura o los equipos de comunicación y seguridad de las sedes a nivel nacional, así como los comprendidos en el servicio de seguridad gestionada.

Cuadro de penalidad

FCM	Penalidad	PROCEDIMIENTO
-----	-----------	---------------

3 o 4	10% de una UIT	El personal de la DIRTIC PNP informará de las caídas mensuales del servicio (contados según ticket de avería) emitiendo el informe respectivo solicitando la penalización del servicio considerando la información indicada en el presente cuadro.
5 o 6	20% de una UIT	
7 u 8	30% de una UIT	
Mayor a 8	35% de una UIT	

Si la FCM es mayor a 4 caídas del servicio, se considera como una falta grave, y se acumula para efectos de resolver el Contrato.

De presentarse una situación excepcional que impida al CONTRATISTA cumplir con los plazos de respuesta establecidos, éste podrá enviar una Carta y un correo electrónico a LA ENTIDAD y a la Unidad Usaria (DIRTIC PNP) en un plazo no mayor a cuarenta y ocho (48) horas de comunicado la avería, exponiendo los motivos técnicos que originaron la situación. LA ENTIDAD evaluará dicha justificación en un plazo no mayor a setenta y dos (72) horas. Si LA ENTIDAD encuentra justificadas y aprueba las razones expuestas, no se contabilizarán las horas de exceso incurridas para el cálculo del UPTIME.

Del mismo modo, si la Entidad excede el plazo máximo de setenta y dos (72) horas en dar respuesta a las razones expuestas en la comunicación del contratista, no se contabilizarán las horas de exceso incurridas para el cálculo del UPTIME y se procederá a la parada de reloj.

Pérdida de Paquetes (PPKT)

La pérdida de paquetes se calcula producto de la ejecución del comando ping en el circuito de datos (Entre el equipo de comunicación del circuito de datos de la Unidad Remota y el equipo de comunicación del circuito de datos del Nodo Central), sobre una muestra de 1,000 paquetes de tamaño estándar (32 Bytes), la pérdida de paquetes no debe ser mayor al 1 %.

Las pruebas se realizarán sobre un enlace que no exceda un consumo del 80%, en cuanto al periodo de muestreo este podrá ser mayor a tres minutos, la medición de pérdida de paquetes se deberá realizar una (01) vez al mes por cada enlace de datos.

La medición de este factor de calidad será medida en condiciones climáticas normales.

Cuadro de Penalidad:

PPKT	Penalidad	PROCEDIMIENTO
>1% y < 2%	5% de una UIT	El personal de la DIRTIC PNP informará sobre la pérdida de paquetes de acuerdo al reporte obtenido del sistema de monitoreo o de acuerdo el reporte brindado por el contratista, la DIRTIC PNP emitirá un informe solicitando la penalización tomando en consideración la información indicada en el presente cuadro.
>= 2% y < 3%	10% de una UIT	
>= 3% y < 4%	20% de una UIT	
>= 4%	30% de una UIT	

Si el PPKT es mayor a 4%, se considera como una falta grave, y se acumula para efectos de resolver el Contrato. Ante una caída total del servicio, no se considerará la penalidad por pérdida de paquetes

ya que esta penalidad se aplica cuando el enlace está operativo, pero con ciertas limitantes de conectividad.

6.10.1.2.3 PARA EL COMPONENTE 3 LATENCIA

El contratista será responsable de mantener la latencia según lo solicitado por la entidad, los servicios brindados en el componente 3 necesarios para la prestación del servicio implica la implementación de un red corporativa la misma que requiere mantener latencia bajas para el normal funcionamiento de los sistemas policiales, interoperabilidad entre entidades nacionales e internacionales, soluciones de videoconferencia y acceso a herramientas de investigación propias de las Unidades Operativas PNP, servicio que debe estar controlado las veinticuatro (24) horas del día, los siete (07) días a la semana y trescientos sesenta y cinco (365) días del año.

N°	LATENCIA	PENALIDAD	PROCEDIMIENTO
01	>20ms y 40ms> (Lima Metropolitana F.O.) >40ms y 60ms> (Provincia F.O.) ≥60ms y 120ms> (Radio Enlace)	10% de 3UIT	El personal de la DIRTIC PNP informara sobre la perdida de paquetes de acuerdo al reporte obtenido del sistema de monitoreo o de acuerdo al reporte brindado por le contratista. La DIRTIC PNP emitirá un informe solicitando la penalización tomando en consideración la informacion indicada en el presente cuadro.
02	≥40ms y 60ms> (Lima Metropolitana F.O.) ≥60ms y 90ms> (Provincia F.O.) ≥120ms y 180ms> (Radio Enlace)	20% de 3UIT	
03	≥60ms y 90ms> (Lima Metropolitana F.O.) ≥90ms y 130ms> (Provincia F.O.) ≥180ms y 240ms> (Radio Enlace)	40% de 3UIT	
04	≥90ms y 150ms> (Lima Metropolitana F.O.) ≥130ms y 210ms> (Provincia F.O.) ≥240ms y 300ms> (Radio Enlace)	50% de 3UIT	
05	≥150ms (Lima Metropolitana F.O.) ≥210ms (Provincia F.O.) ≥300ms (Radio Enlace)	60% de 3UIT	

Estas penalidades se deducen de los pagos a cuenta o del pago final, según corresponda; o si fuera necesario, se cobra del monto resultante de la ejecución de la garantía de fiel cumplimiento.

Estos dos (2) tipos de penalidades pueden alcanzar cada una un monto máximo equivalente al diez por ciento (10%) del monto del contrato vigente, o de ser el caso, del ítem que debió ejecutarse.

Cuando se llegue a cubrir el monto máximo de la penalidad por mora o el monto máximo para otras penalidades, de ser el caso, LA ENTIDAD puede resolver el contrato por incumplimiento.

CLÁUSULA DÉCIMA CUARTA: RESOLUCIÓN DEL CONTRATO

Cualquiera de las partes puede resolver el contrato, de conformidad con el numeral 32.3 del artículo 32 y artículo 36 de la Ley de Contrataciones del Estado, y el artículo 164 de su Reglamento. De darse el caso, LA ENTIDAD procederá de acuerdo a lo establecido en el artículo 165 del Reglamento de la Ley de Contrataciones del Estado.

CLÁUSULA DÉCIMA QUINTA: RESPONSABILIDAD DE LAS PARTES

Cuando se resuelva el contrato por causas imputables a algunas de las partes, se debe resarcir los daños y perjuicios ocasionados, a través de la indemnización correspondiente. Ello no obsta la aplicación de las sanciones administrativas, penales y pecuniarias a que dicho incumplimiento diere lugar, en el caso que éstas correspondan.

Lo señalado precedentemente no exime a ninguna de las partes del cumplimiento de las demás obligaciones previstas en el presente contrato.

CLÁUSULA DÉCIMA SEXTA: ANTICORRUPCIÓN

EL CONTRATISTA declara y garantiza no haber, directa o indirectamente, o tratándose de una persona jurídica a través de sus socios, integrantes de los órganos de administración, apoderados, representantes legales, funcionarios, asesores o personas vinculadas a las que se refiere el artículo 7 del Reglamento de la Ley de Contrataciones del Estado, ofrecido, negociado o efectuado, cualquier pago o, en general, cualquier beneficio o incentivo ilegal en relación al contrato.

Asimismo, el CONTRATISTA se obliga a conducirse en todo momento, durante la ejecución del contrato, con honestidad, probidad, veracidad e integridad y de no cometer actos ilegales o de corrupción, directa o indirectamente o a través de sus socios, accionistas, participacionistas, integrantes de los órganos de administración, apoderados, representantes legales, funcionarios, asesores y personas vinculadas a las que se refiere el artículo 7 del Reglamento de la Ley de Contrataciones del Estado.

Además, EL CONTRATISTA se compromete a i) comunicar a las autoridades competentes, de manera directa y oportuna, cualquier acto o conducta ilícita o corrupta de la que tuviera conocimiento; y ii) adoptar medidas técnicas, organizativas y/o de personal apropiadas para evitar los referidos actos o prácticas.

Finalmente, EL CONTRATISTA se compromete a no colocar a los funcionarios públicos con los que deba interactuar, en situaciones reñidas con la ética. En tal sentido, reconoce y acepta la prohibición de ofrecerles a éstos cualquier tipo de obsequio, donación, beneficio y/o gratificación, ya sea de bienes o servicios, cualquiera sea la finalidad con la que se lo haga.

CLÁUSULA DÉCIMA SÉTIMA: MARCO LEGAL DEL CONTRATO

Sólo en lo no previsto en este contrato, en la Ley de Contrataciones del Estado y su Reglamento, en las directivas que emita el OSCE y demás normativa especial que resulte aplicable, serán de aplicación supletoria las disposiciones pertinentes del Código Civil vigente, cuando corresponda, y demás normas de derecho privado.

CLÁUSULA DÉCIMA OCTAVA: SOLUCIÓN DE CONTROVERSIAS¹²

Las controversias que surjan entre las partes durante la ejecución del contrato se resuelven mediante conciliación o arbitraje, según el acuerdo de las partes.

Cualquiera de las partes tiene derecho a iniciar el arbitraje a fin de resolver dichas controversias dentro del plazo de caducidad previsto en la Ley de Contrataciones del Estado y su Reglamento.

Facultativamente, cualquiera de las partes tiene el derecho a solicitar una conciliación dentro del plazo de caducidad correspondiente, según lo señalado en el artículo 224 del Reglamento de la Ley de Contrataciones del Estado, sin perjuicio de recurrir al arbitraje, en caso no se llegue a un acuerdo entre ambas partes o se llegue a un acuerdo parcial. Las controversias sobre nulidad del contrato solo pueden ser sometidas a arbitraje.

El Laudo arbitral emitido es inapelable, definitivo y obligatorio para las partes desde el momento de su notificación, según lo previsto en el numeral 45.21 del artículo 45 de la Ley de Contrataciones del Estado.

Las partes se someten al fuero jurisdiccional de Lima¹³.

CLÁUSULA DÉCIMA NOVENA: FACULTAD DE ELEVAR A ESCRITURA PÚBLICA

Cualquiera de las partes puede elevar el presente contrato a Escritura Pública corriendo con todos los gastos que demande esta formalidad.

CLÁUSULA VIGÉSIMA: DOMICILIO PARA EFECTOS DE LA EJECUCIÓN CONTRACTUAL

Las partes declaran el siguiente domicilio para efecto de las notificaciones que se realicen durante la ejecución del presente contrato:

¹² De acuerdo con el numeral 225.3 del artículo 225 del Reglamento, las partes pueden recurrir al arbitraje ad hoc cuando las controversias deriven de procedimientos de selección cuyo valor estimado sea menor o igual a cinco millones con 00/100 soles (S/ 5 000 000,00).

¹³ Contenido de clausula modificado de conformidad al MEMORANDUM N°697-2024-DIRADM-DIVLOG-PNP/SEC de fecha 21OCT2024 y OFICIO N°005542-2024-IN-PSI de fecha 17JUL2024.

DOMICILIO DE LA ENTIDAD: [REDACTED]

DOMICILIO DEL CONTRATISTA: [CONSIGNAR EL DOMICILIO SEÑALADO POR EL POSTOR GANADOR DE LA BUENA PRO AL PRESENTAR LOS REQUISITOS PARA EL PERFECCIONAMIENTO DEL CONTRATO]

La variación del domicilio aquí declarado de alguna de las partes debe ser comunicada a la otra parte, formalmente y por escrito, con una anticipación no menor de quince (15) días calendario.

De acuerdo con las bases integradas, la oferta y las disposiciones del presente contrato, las partes lo firman por duplicado en señal de conformidad en la ciudad de [.....] al [CONSIGNAR FECHA].

"LA ENTIDAD"

"EL CONTRATISTA"

Importante

Este documento puede firmarse digitalmente si ambas partes cuentan con firma digital, según la Ley N° 27269, Ley de Firmas y Certificados Digitales¹⁴.

¹⁴ Para mayor información sobre la normativa de firmas y certificados digitales ingresar a: <https://www.indecopi.gob.pe/web/firmas-digitales/firmar-y-certificados-digitales>

ANEXOS

ANEXO N° 1

DECLARACIÓN JURADA DE DATOS DEL POSTOR

Señores
COMITÉ DE SELECCIÓN
CONCURSO PÚBLICO N° 02-2025-DIRECFIN-PNP-1

Presente.-

El que se suscribe, [...], postor y/o Representante Legal de [CONSIGNAR EN CASO DE SER PERSONA JURÍDICA], identificado con [CONSIGNAR TIPO DE DOCUMENTO DE IDENTIDAD] N° [CONSIGNAR NÚMERO DE DOCUMENTO DE IDENTIDAD], con poder inscrito en la localidad de [CONSIGNAR EN CASO DE SER PERSONA JURÍDICA] en la Ficha N° [CONSIGNAR EN CASO DE SER PERSONA JURÍDICA] Asiento N° [CONSIGNAR EN CASO DE SER PERSONA JURÍDICA], **DECLARO BAJO JURAMENTO** que la siguiente información se sujeta a la verdad:

Nombre, Denominación o Razón Social :				
Domicilio Legal :				
RUC :		Teléfono(s) :		
MYPE ¹⁵		Sí	No	
Correo electrónico :				

Autorización de notificación por correo electrónico:

Autorizo que se notifiquen al correo electrónico indicado las siguientes actuaciones:

1. Solicitud de la descripción a detalle de todos los elementos constitutivos de la oferta.
2. Solicitud de reducción de la oferta económica.
3. Solicitud de subsanación de los requisitos para perfeccionar el contrato.
4. Solicitud para presentar los documentos para perfeccionar el contrato, según orden de prelación, de conformidad con lo previsto en el artículo 141 del Reglamento.
5. Respuesta a la solicitud de acceso al expediente de contratación.
6. Notificación de la orden de servicios¹⁶

Asimismo, me comprometo a remitir la confirmación de recepción, en el plazo máximo de dos (2) días hábiles de recibida la comunicación.

[CONSIGNAR CIUDAD Y FECHA]

.....
Firma, Nombres y Apellidos del postor o Representante legal, según corresponda

Importante

La notificación dirigida a la dirección de correo electrónico consignada se entenderá válidamente efectuada cuando la Entidad reciba acuse de recepción.

¹⁵ Esta información será verificada por la Entidad en la página web del Ministerio de Trabajo y Promoción del Empleo en la sección consulta de empresas acreditadas en el REMYPE en el link <http://www2.trabajo.gob.pe/servicios-en-linea-2-2/> y se tendrá en consideración, en caso el postor ganador de la buena pro solicite la retención del diez por ciento (10%) del monto del contrato, en calidad de garantía de fiel cumplimiento, en los contratos periódicos de prestación de servicios, según lo señalado en el numeral 149.4 del artículo 149 y numeral 151.2 del artículo 151 del Reglamento.

¹⁶ Consignar en el caso de procedimientos de selección por relación de ítems, cuando el monto del valor estimado del ítem no supere los doscientos mil Soles (S/ 200 000.00), cuando se haya optado por perfeccionar el contrato con una orden de servicios.

Importante

Cuando se trate de consorcios, la declaración jurada es la siguiente:

ANEXO N° 1

DECLARACIÓN JURADA DE DATOS DEL POSTOR

Señores
COMITÉ DE SELECCIÓN
CONCURSO PÚBLICO N° 02-2025-DIRECFIN-PNP-1
Presente.-

El que se suscribe, [...], representante común del consorcio [CONSIGNAR EL NOMBRE DEL CONSORCIO], identificado con [CONSIGNAR TIPO DE DOCUMENTO DE IDENTIDAD] N° [CONSIGNAR NÚMERO DE DOCUMENTO DE IDENTIDAD], **DECLARO BAJO JURAMENTO** que la siguiente información se sujeta a la verdad:

Datos del consorciado 1				
Nombre, Denominación o Razón Social :				
Domicilio Legal :				
RUC :	Teléfono(s) :			
MYPE ¹⁷		Sí	No	
Correo electrónico :				

Datos del consorciado 2				
Nombre, Denominación o Razón Social :				
Domicilio Legal :				
RUC :	Teléfono(s) :			
MYPE ¹⁸		Sí	No	
Correo electrónico :				

Datos del consorciado ...				
Nombre, Denominación o Razón Social :				
Domicilio Legal :				
RUC :	Teléfono(s) :			
MYPE ¹⁹		Sí	No	
Correo electrónico :				

Autorización de notificación por correo electrónico:

Correo electrónico del consorcio:


Autorizo que se notifiquen al correo electrónico indicado las siguientes actuaciones:

1. Solicitud de la descripción a detalle de todos los elementos constitutivos de la oferta.
2. Solicitud de reducción de la oferta económica.
3. Solicitud de subsanación de los requisitos para perfeccionar el contrato.

¹⁷ En los contratos periódicos de prestación de servicios, esta información será verificada por la Entidad en la página web del Ministerio de Trabajo y Promoción del Empleo en la sección consulta de empresas acreditadas en el REMYPE en el link <http://www2.trabajo.gob.pe/servicios-en-linea-2-2/> y se tendrá en consideración, en caso el consorcio ganador de la buena pro solicite la retención del diez por ciento (10%) del monto del contrato, en calidad de garantía de fiel cumplimiento, según lo señalado en el numeral 149.4 del artículo 149 y numeral 151.2 del artículo 151 del Reglamento. Para dicho efecto, todos los integrantes del consorcio deben acreditar la condición de micro o pequeña empresa.

¹⁸ Ibidem.

¹⁹ Ibidem.

- 
4. Solicitud para presentar los documentos para perfeccionar el contrato, según orden de prelación, de conformidad con lo previsto en el artículo 141 del Reglamento.
 5. Respuesta a la solicitud de acceso al expediente de contratación.
 6. Notificación de la orden de servicios²⁰

Asimismo, me comprometo a remitir la confirmación de recepción, en el plazo máximo de dos (2) días hábiles de recibida la comunicación.



[CONSIGNAR CIUDAD Y FECHA]



.....
**Firma, Nombres y Apellidos del representante
común del consorcio**

Importante

La notificación dirigida a la dirección de correo electrónico consignada se entenderá válidamente efectuada cuando la Entidad reciba acuse de recepción.

²⁰ Consignar en el caso de procedimientos de selección por relación de ítems, cuando el monto del valor estimado del ítem no supere los doscientos mil Soles (S/ 200 000.00), cuando se haya optado por perfeccionar el contrato con una orden de servicios.

ANEXO N° 2

**DECLARACIÓN JURADA
(ART. 52 DEL REGLAMENTO DE LA LEY DE CONTRATACIONES DEL ESTADO)**

Señores
COMITÉ DE SELECCIÓN
CONCURSO PÚBLICO N° 02-2025-DIRECFIN-PNP-1
Presente.-

Mediante el presente el suscrito, postor y/o Representante Legal de [CONSIGNAR EN CASO DE SER PERSONA JURÍDICA], declaro bajo juramento:

- i. No haber incurrido y me obligo a no incurrir en actos de corrupción, así como a respetar el principio de integridad.
- ii. No tener impedimento para postular en el procedimiento de selección ni para contratar con el Estado, conforme al artículo 11 de la Ley de Contrataciones del Estado.
- iii. Conocer las sanciones contenidas en la Ley de Contrataciones del Estado y su Reglamento, así como las disposiciones aplicables de la Ley N° 27444, Ley del Procedimiento Administrativo General.
- iv. Participar en el presente proceso de contratación en forma independiente sin mediar consulta, comunicación, acuerdo, arreglo o convenio con ningún proveedor; y, conocer las disposiciones del Decreto Legislativo N° 1034, Decreto Legislativo que aprueba la Ley de Represión de Conductas Anticompetitivas.
- v. Conocer, aceptar y someterme a las bases, condiciones y reglas del procedimiento de selección.
- vi. Ser responsable de la veracidad de los documentos e información que presento en el presente procedimiento de selección.
- vii. Comprometerme a mantener la oferta presentada durante el procedimiento de selección y a perfeccionar el contrato, en caso de resultar favorecido con la buena pro.

[CONSIGNAR CIUDAD Y FECHA]

.....
**Firma, Nombres y Apellidos del postor o
Representante legal, según corresponda**

Importante

En el caso de consorcios, cada integrante debe presentar esta declaración jurada, salvo que sea presentada por el representante común del consorcio.

ANEXO N° 3

DECLARACIÓN JURADA DE CUMPLIMIENTO DE LOS TÉRMINOS DE REFERENCIA

Señores

COMITÉ DE SELECCIÓN

CONCURSO PÚBLICO N° 02-2025-DIRECFIN-PNP-1

Presente.-

Es grato dirigirme a usted, para hacer de su conocimiento que luego de haber examinado las bases y demás documentos del procedimiento de la referencia y, conociendo todos los alcances y las condiciones detalladas en dichos documentos, el postor que suscribe ofrece el servicio de **[CONSIGNAR OBJETO DE LA CONVOCATORIA]**, de conformidad con los Términos de Referencia que se indican en el numeral 3.1 del Capítulo III de la sección específica de las bases y los documentos del procedimiento.

[CONSIGNAR CIUDAD Y FECHA]

.....
**Firma, Nombres y Apellidos del postor o
Representante legal o común, según corresponda**

Importante

Adicionalmente, puede requerirse la presentación de documentación que acredite el cumplimiento de los términos de referencia, conforme a lo indicado en el acápite relacionado al contenido de las ofertas de la presente sección de las bases.

ANEXO N° 4

DECLARACIÓN JURADA DE PLAZO DE PRESTACIÓN DEL SERVICIO

Señores

COMITÉ DE SELECCIÓN

CONCURSO PÚBLICO N° 02-2025-DIRECFIN-PNP-1

Presente. -

Mediante el presente, con pleno conocimiento de las condiciones que se exigen en las bases del procedimiento de la referencia, me comprometo a prestar el servicio objeto del presente procedimiento de selección en el plazo de [CONSIGNAR EL PLAZO OFERTADO].

[CONSIGNAR CIUDAD Y FECHA]

.....
**Firma, Nombres y Apellidos del postor o
Representante legal o común, según corresponda**

ANEXO N° 5

PROMESA DE CONSORCIO

(Sólo para el caso en que un consorcio se presente como postor)

Señores

COMITÉ DE SELECCIÓN

CONCURSO PÚBLICO N° 02-2025-DIRECFIN-PNP-1

Presente.-

Los suscritos declaramos expresamente que hemos convenido en forma irrevocable, durante el lapso que dure el procedimiento de selección, para presentar una oferta conjunta al **CONCURSO PÚBLICO N° [CONSIGNAR NOMENCLATURA DEL PROCEDIMIENTO]**.

Asimismo, en caso de obtener la buena pro, nos comprometemos a formalizar el contrato de consorcio, de conformidad con lo establecido por el artículo 140 del Reglamento de la Ley de Contrataciones del Estado, bajo las siguientes condiciones:

a) Integrantes del consorcio

1. [NOMBRE, DENOMINACIÓN O RAZÓN SOCIAL DEL CONSORCIADO 1].
2. [NOMBRE, DENOMINACIÓN O RAZÓN SOCIAL DEL CONSORCIADO 2].

b) Designamos a [CONSIGNAR NOMBRES Y APELLIDOS DEL REPRESENTANTE COMÚN], identificado con [CONSIGNAR TIPO DE DOCUMENTO DE IDENTIDAD] N° [CONSIGNAR NÚMERO DE DOCUMENTO DE IDENTIDAD], como representante común del consorcio para efectos de participar en todos los actos referidos al procedimiento de selección, suscripción y ejecución del contrato correspondiente con [CONSIGNAR NOMBRE DE LA ENTIDAD].

Asimismo, declaramos que el representante común del consorcio no se encuentra impedido, inhabilitado ni suspendido para contratar con el Estado.

c) Fijamos nuestro domicilio legal común en [.....].

d) Las obligaciones que corresponden a cada uno de los integrantes del consorcio son las siguientes:

1. OBLIGACIONES DE [NOMBRE, DENOMINACIÓN O RAZÓN SOCIAL DEL CONSORCIADO 1] [%]²¹

[DESCRIBIR LAS OBLIGACIONES DEL CONSORCIADO 1]

2. OBLIGACIONES DE [NOMBRE, DENOMINACIÓN O RAZÓN SOCIAL DEL CONSORCIADO 2] [%]²²

[DESCRIBIR LAS OBLIGACIONES DEL CONSORCIADO 2]

TOTAL OBLIGACIONES

100%²³

[CONSIGNAR CIUDAD Y FECHA]

²¹ Consignar únicamente el porcentaje total de las obligaciones, el cual debe ser expresado en número entero, sin decimales.

²² Consignar únicamente el porcentaje total de las obligaciones, el cual debe ser expresado en número entero, sin decimales.

²³ Este porcentaje corresponde a la sumatoria de los porcentajes de las obligaciones de cada uno de los integrantes del consorcio.

.....
Consociado 1
Nombres, apellidos y firma del Consorciado 1
o de su Representante Legal
Tipo y N° de Documento de Identidad

.....
Consociado 2
Nombres, apellidos y firma del Consorciado 2
o de su Representante Legal
Tipo y N° de Documento de Identidad

Importante

De conformidad con el artículo 52 del Reglamento, las firmas de los integrantes del consorcio deben ser legalizadas.

Importante para la Entidad

En caso de la prestación de servicios bajo el sistema a suma alzada incluir el siguiente anexo:

Esta nota deberá ser eliminada una vez culminada la elaboración de las bases

ANEXO N° 6

PRECIO DE LA OFERTA

Señores
COMITÉ DE SELECCIÓN
CONCURSO PÚBLICO N° 02-2025-DIRECFIN-PNP-1
Presente.-

Es grato dirigirme a usted, para hacer de su conocimiento que, de acuerdo con las bases, mi oferta es la siguiente:

CONCEPTO	PRECIO TOTAL
TOTAL	

El precio de la oferta [CONSIGNAR LA MONEDA DE LA CONVOCATORIA] incluye todos los tributos, seguros, transporte, inspecciones, pruebas y, de ser el caso, los costos laborales conforme a la legislación vigente, así como cualquier otro concepto que pueda tener incidencia sobre el costo del servicio a contratar; excepto la de aquellos postores que gocen de alguna exoneración legal, no incluirán en el precio de su oferta los tributos respectivos.

[CONSIGNAR CIUDAD Y FECHA]

.....
Firma, Nombres y Apellidos del postor o
Representante legal o común, según corresponda

Importante

- *El postor debe consignar el precio total de la oferta, sin perjuicio que, de resultar favorecido con la buena pro, presente el detalle de precios unitarios para el perfeccionamiento del contrato.*
- *El postor que goce de alguna exoneración legal, debe indicar que su oferta no incluye el tributo materia de la exoneración, debiendo incluir el siguiente texto:*

Mi oferta no incluye [CONSIGNAR EL TRIBUTO MATERIA DE LA EXONERACIÓN]"



ANEXO N° 8

EXPERIENCIA DEL POSTOR EN LA ESPECIALIDAD

Señores
COMITÉ DE SELECCIÓN
CONCURSO PÚBLICO N° 02-2025-DIRECFIN-PNP-1
Presente.-

Mediante el presente, el suscrito detalla la siguiente EXPERIENCIA EN LA ESPECIALIDAD:

N°	CLIENTE	OBJETO DEL CONTRATO	N° CONTRATO / O/S / COMPROBANTE DE PAGO	FECHA DEL CONTRATO O CP ²⁴	FECHA DE LA CONFORMIDAD DE SER EL CASO ²⁵	EXPERIENCIA PROVENIENTE ²⁶ DE:	MONEDA	IMPORTE ²⁷	TIPO DE CAMBIO VENTA ²⁸	MONTO FACTURADO ACUMULADO ²⁹
1										
2										
3										
4										

²⁴ Se refiere a la fecha de suscripción del contrato, de la emisión de la Orden de Servicios o de cancelación del comprobante de pago, según corresponda.


²⁵ Únicamente, cuando la fecha del perfeccionamiento del contrato, sea previa a los ocho (8) años anteriores a la fecha de presentación de ofertas, caso en el cual el postor debe acreditar que la conformidad se emitió dentro de dicho período.

²⁶ Si el titular de la experiencia no es el postor, consignar si dicha experiencia corresponde a la matriz en caso que el postor sea sucursal, o fue transmitida por reorganización societaria, debiendo acompañar la documentación sustentatoria correspondiente. Al respecto, según la Opinión N° 216-2017/DTN "Considerando que la sociedad matriz y la sucursal constituyen la misma persona jurídica, la sucursal puede acreditar como suya la experiencia de su matriz". Del mismo modo, según lo previsto en la Opinión N° 010-2013/DTN, "... en una operación de reorganización societaria que comprende tanto una fusión como una escisión, la sociedad resultante podrá acreditar como suya la experiencia de la sociedad incorporada o absorbida, que se extingue producto de la fusión; asimismo, si en virtud de la escisión se transfiere un bloque patrimonial consistente en una línea de negocio completa, la sociedad resultante podrá acreditar como suya la experiencia de la sociedad escindida, correspondiente a la línea de negocio transmitida. De esta manera, la sociedad resultante podrá emplear la experiencia transmitida, como consecuencia de la reorganización societaria antes descrita, en los futuros procesos de selección en los que participe".

²⁷ Se refiere al monto del contrato ejecutado incluido adicionales y reducciones, de ser el caso.

²⁸ El tipo de cambio venta debe corresponder al publicado por la SBS correspondiente a la fecha de suscripción del contrato, de la emisión de la Orden de Servicios o de cancelación del comprobante de pago, según corresponda.

²⁹ Consignar en la moneda establecida en las bases.

N°	CLIENTE	OBJETO DEL CONTRATO	N° CONTRATO / O/S / COMPROBANTE DE PAGO	FECHA DEL CONTRATO O CP 24	FECHA DE LA CONFORMIDAD DE SER EL CASO 25	EXPERIENCIA PROVENIENTE 26 DE:	MONEDA	IMPORTE 27	TIPO DE CAMBIO VENTA 28	MONTO FACTURADO ACUMULADO 29
5										
6										
7										
8										
9										
10										
...										
20										
TOTAL										

[CONSIGNAR CIUDAD Y FECHA]

.....
Firma, Nombres y Apellidos del postor o
Representante legal o común, según corresponda

ANEXO N° 9

**DECLARACIÓN JURADA
(NUMERAL 49.4 DEL ARTÍCULO 49 DEL REGLAMENTO)**

Señores
COMITÉ DE SELECCIÓN
CONCURSO PÚBLICO N° 02-2025-DIRECFIN-PNP-1
Presente.-

Mediante el presente el suscrito, postor y/o Representante Legal de [CONSIGNAR EN CASO DE SER PERSONA JURÍDICA], declaro que la experiencia que acredito de la empresa [CONSIGNAR LA DENOMINACIÓN DE LA PERSONA JURÍDICA] como consecuencia de una reorganización societaria, no se encuentra en el supuesto establecido en el numeral 49.4 del artículo 49 del Reglamento.

[CONSIGNAR CIUDAD Y FECHA]

.....
**Firma, Nombres y Apellidos del postor o
Representante legal, según corresponda**

Importante

A efectos de cautelar la veracidad de esta declaración, el postor puede verificar la información de la Relación de Proveedores Sancionados por el Tribunal de Contrataciones del Estado con Sanción Vigente en <http://portal.osce.gob.pe/rnp/content/relación-de-proveedores-sancionados>.

También le asiste dicha facultad al órgano encargado de las contrataciones o al órgano de la Entidad al que se le haya asignado la función de verificación de la oferta presentada por el postor ganador de la buena pro.

ANEXO N° 12

**AUTORIZACIÓN DE NOTIFICACIÓN DE LA DECISIÓN DE LA ENTIDAD SOBRE LA
SOLICITUD DE AMPLIACIÓN DE PLAZO MEDIANTE MEDIOS ELECTRÓNICOS DE
COMUNICACIÓN**

(DOCUMENTO A PRESENTAR EN EL PERFECCIONAMIENTO DEL CONTRATO)

Señores
COMITÉ DE SELECCIÓN
CONCURSO PÚBLICO N° 02-2025-DIRECFIN-PNP-1
Presente.-

El que se suscribe, [...], postor adjudicado y/o Representante Legal de [CONSIGNAR EN CASO DE SER PERSONA JURÍDICA], identificado con [CONSIGNAR TIPO DE DOCUMENTO DE IDENTIDAD] N° [CONSIGNAR NUMERO DE DOCUMENTO DE IDENTIDAD], autorizo que durante la ejecución del contrato se me notifique al correo electrónico [INDICAR EL CORREO ELECTRÓNICO] lo siguiente:

✓ Notificación de la decisión de la Entidad respecto a la solicitud de ampliación de plazo.

[CONSIGNAR CIUDAD Y FECHA]

.....
**Firma, Nombres y Apellidos del postor o
Representante legal o común, según
corresponda**

Importante

La notificación de la decisión de la Entidad respecto a la solicitud de ampliación de plazo se efectúa por medios electrónicos de comunicación, siempre que se cuente con la autorización correspondiente y sea posible obtener un acuse de recibo a través del mecanismo utilizado.