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

CONCURSO PÚBLICO Nº 002-2024-MIDIS/PNPAIS

PRIMERA CONVOCATORIA

CONTRATACIÓN DE SERVICIO DE INTERNET PARA SEDE CENTRAL – UNIDADES TERRITORIALES, SERVICIOS EN LA NUBE Y ENTORNOS COLABORATIVOS (CORREOS ELECTRÓNICOS) PARA EL PROGRAMA NACIONAL "PLATAFORMAS DE ACCIÓN PARA LA INCLUSIÓN SOCIAL – PAIS

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 INDECOPI, 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 INDECOPI 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 INDECOPI 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 Nº 27269, Ley de Firmas y Certificados Digitales[1]). 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*

[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

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

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 accesoria, 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	:	PROGRAMA NACIONAL "PLATAFORMAS DE ACCIÓN PARA LA INCLUSIÓN SOCIAL – PAIS
RUC Nº	:	20601993181
Domicilio legal	:	Av. Vía Expresa Luís Fernán Bedoya Reyes N° 3245
Teléfono:	:	3906790 - anexo 6790
Correo electrónico:	:	falvites@pais.gob.pe

1.2. OBJETO DE LA CONVOCATORIA

El presente procedimiento de selección tiene por objeto la contratación del SERVICIO DE INTERNET PARA SEDE CENTRAL – UNIDADES TERRITORIALES, SERVICIOS EN LA NUBE Y ENTORNOS COLABORATIVOS (CORREOS ELECTRÓNICOS) PARA EL PROGRAMA NACIONAL "PLATAFORMAS DE ACCIÓN PARA LA INCLUSIÓN SOCIAL – PAIS

Ítem	Detalle	Unidad de Medida
1	SERVICIO DE INTERNET, CONECTIVIDAD ENTRE CENTRO DE DATOS, HOSTING DEDICADO DE CENTRO DE DATOS PRINICPAL Y CONTIGENCIAS, SEGURIDAD INFORMATICA, EQUIPAMIENTO DE SERVIDORES Y COMPONENTES DE RESPALDO DE INFORMACION. PARA LA SEDE CENTRAL, UNIDADES TERRITORIALES Y SEDES LIMA	Servicio
2	SERVICIO DE ENTORNOS COLABORATIVOS CORREOS ELECTRÓNICOS)	Servicio

1.3. EXPEDIENTE DE CONTRATACIÓN

El expediente de contratación fue aprobado mediante Aprobación de expediente N° 024-2024-MIDIS/PNPAIS-UA de fecha 15 de abril de 2024.

1.4. FUENTE DE FINANCIAMIENTO

Recursos Ordinarios

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

No Corresponde

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 en el plazo es de mil noventa y cinco (1095) días calendario.

a) PLAZO DE IMPLEMENTACION PARA ITEM 1, el plazo de implementación del servicio será de ciento veinte (120) días calendarios contado a partir de firmado el contrato.

b) PLAZO DE IMPLEMENTACION PARA ITEM 2, el plazo de implementación del servicio será de cinco (05) días calendarios contado a partir de firmado el contrato

En concordancia con lo establecido en el expediente de contratación.

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 la suma de S/. 5.00 (Cinco con 00/100 soles) en la Caja de la Entidad. La copia se entregará en la Coordinación de Abastecimiento, sito en el cuarto piso de la Sede Central del PNPAIS (Av. Vía Expresa Luis Fernán Bedoya Reyes N° 3245), en el horario de 08:30 a 17:30 horas].

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

1.10. BASE LEGAL

- Ley Nº 31953 Ley de Presupuesto del Sector Público para el Año Fiscal 2024.
- Ley Nº 31954 Ley de Equilibrio Financiero del Presupuesto del Sector Público del año fiscal2024.
- Política de Sistema Integrado de Gestión OSCE - Directivas y opiniones del OSCE.
- Código Civil.
- Cualquier otra disposición legal vigente que permita desarrollar el objeto de la convocatoria que no contravéngalo regulado por la Ley de Contrataciones del Estado.

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 documentos[2], 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 Nº 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 – PIDE[3] 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 Nº 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 Nº 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) Declaración jurada de plazo de prestación del servicio. **(Anexo Nº 4)**[4]

f) 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 Nº 5**)

g) El precio de la oferta en **SOLES**. Adjuntar obligatoriamente el **Anexo Nº 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.*

*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 Nº 27269, Ley de Firmas y Certificados Digitales[5]). 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.***

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.

2.2.2. <u>Documentación de presentación facultativa:</u>

Importante para la Entidad

- *En caso el comité de selección considere evaluar otros factores además del precio, incluir el siguiente literal:*

a) *Incorporar en la oferta los documentos que acreditan los **"Factores de Evaluación"** establecidos en el Capítulo IV de la presente sección de las bases, a efectos de obtener el puntaje previsto en dicho Capítulo para cada factor.*

- *Si durante la fase de actos preparatorios, las Entidades advierten que es posible la participación de proveedores que gozan del beneficio de la exoneración del IGV prevista en la Ley Nº 27037, Ley de Promoción de la Inversión en la Amazonía, consignar el siguiente literal:*

*b) Los postores que apliquen el beneficio de la exoneración del IGV previsto en la Ley Nº 27037, Ley de Promoción de la Inversión en la Amazonía, deben presentar la Declaración Jurada de cumplimiento de condiciones para la aplicación de la exoneración del IGV **(Anexo Nº 7)**.*

- *En el caso de procedimientos por relación de ítems cuando la contratación del servicio en general va a ser prestado fuera de la provincia de Lima y Callao y el monto del valor*

[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.

[5] 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.

estimado de algún ítem no supere los doscientos mil Soles (S/ 200,000.00), consignar el siguiente literal:

c) *En el* [CONSIGNAR EL ÍTEM O ÍTEMS, SEGÚN CORRESPONDA, EN LOS QUE SE PUEDE SOLICITAR LA BONIFICACIÓN] *los postores con domicilio en la provincia donde se prestará el servicio, o en las provincias colindantes, sean o no pertenecientes al mismo departamento o región, pueden presentar la solicitud de bonificación por servicios prestados fuera de la provincia de Lima y Callao, según* ***Anexo Nº 10.***

- *En caso de procedimientos de selección por relación de ítems cuando el monto del valor estimado de algún ítem corresponda al monto de una Adjudicación Simplificada, se incluye el siguiente literal:*

Ítem Nº [...]

d) *Solicitud de bonificación del cinco por ciento (5%) por tener la condición de micro y pequeña empresa* ***(Anexo N°11).***

Incorporar a las bases o eliminar, según corresponda.

Advertencia
El comité de selección no podrá exigir al postor la presentación de documentos que no hayan sido indicados en los acápites "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) Contrato de consorcio con firmas legalizadas ante Notario de cada uno de los integrantes de ser el caso.
c) 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.
d) Copia de la vigencia del poder del representante legal de la empresa que acredite que cuenta con facultades para perfeccionar el contrato, cuando corresponda.
e) 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 – PIDE[6] 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).

f) Domicilio para efectos de la notificación durante la ejecución del contrato.
g) Autorización de notificación de la decisión de la Entidad sobre la solicitud de ampliación de plazo mediante medios electrónicos de comunicación [7] (**Anexo N° 12**).
h) Detalle de los precios unitarios del precio ofertado[8].
i) Estructura de costos[9].

[6] 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/

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

[8] Incluir solo en caso de la contratación bajo el sistema a suma alzada.

[9] Incluir solo cuando resulte necesario para la ejecución contractual, identificar los costos de cada uno de los rubros que

j) Detalle del precio de la oferta de cada uno de los servicios que conforman el paquete[10].

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 Haya[11].*

- *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 el cuarto piso de la Av. Vía Expresa Luis Fernán Bedoya Reyes N° 3245 San Isidro - Lima en el horario de 08:30 hasta las 17:30 horas o a través del canal virtual del PROGRAMA NACIONAL PAIS https://pais.gob.pe/mesadepartes/web/login.

comprenden la oferta.

[10] Incluir solo en caso de contrataciones por paquete.

[11] Según lo previsto en la Opinión N° 009-2016/DTN.

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 forma mensual, previa conformidad de la prestación de servicios emitida por la Unidad de Tecnologías de la Información.

Para efectos del pago de las contraprestaciones ejecutadas por el contratista, la Entidad debe contar con la siguiente documentación:

- Informe del funcionario responsable del Ejecutivo de la Unidad de Tecnologías de la Información, emitiendo la conformidad de la prestación efectuada.
- Comprobante de pago.

Dicha documentación se debe presentar en el cuarto piso de la Av. Vía Expresa Luis Fernán Bedoya Reyes N° 3245 San Isidro - Lima en el horario de 08:30 hasta las 17:30 horas o a través del canal virtual del PROGRAMA NACIONAL PAIS https://pais.gob.pe/mesadepartes/web/login.

Primer Pago:
Comprende la implementación, instalación de toda la solución ofertada la cual se evidenciará con el acta de instalación en un formato designado por el contratista la cual debe tener una letra legible, con la fecha de instalación del servicio, nombre completo y firma del encargado de las Unidades Territoriales y/o sedes lima.

El costo de la instalación será cancelado al término de la totalidad de la implementación y entrega de la totalidad de los servicios, junto con el primer mes de servicio, Previo informe del Ejecutivo de la Unidad de Tecnologías de la Información.

CAPÍTULO III
REQUERIMIENTO

SE ADJUNTAN LOS TDR

3.1. REQUISITOS DE CALIFICACIÓN

A	**CAPACIDAD LEGAL**
	HABILITACIÓN

ITEM 1

Requisitos:

- Contar con autorización del Ministerio de Transportes y Comunicaciones para la prestación del servicio solicitado ó la autorización del Ministerio de Transportes y Comunicaciones para brindar Servicios de Valor Añadido según Ley de las Telecomunicaciones
- Debe ser miembros activos NAP Perú.

ITEM 2

Requisitos:

- El proveedor deberá ser partner y/o distribuidor autorizado del fabricante de la solución ofertada.

Importante
De conformidad con la Opinión N° 186-2016/DTN, la habilitación de un postor, está relacionada con cierta atribución con la cual debe contar el proveedor para poder llevar a cabo la actividad materia de contratación, este es el caso de las actividades reguladas por normas en las cuales se establecen determinados requisitos que las empresas deben cumplir a efectos de estar habilitadas para la ejecución de determinado servicio o estar autorizadas para la comercialización de ciertos bienes en el mercado.

ITEM 1

Acreditación:

Copia del documento de autorizaciones para brindar el servicio de transmisión datos, Internet emitida por el Ministerio de Transporte y Telecomunicaciones.

Se aceptará una impresión de la página Web del NAP Perú, para certificar ser miembro de la Asamblea, incluyendo en la impresión la fecha del mismo.

ITEM 2

Acreditación:

Copia de carta emitida por fabricante o cartas brindadas por el subsidiario local en nombre del fabricante donde se especifique la razón social y el ID o código de partner. Se aceptarán cartas de fabricantes o cartas brindadas por el subsidiario local en nombre del fabricante donde indique que el CONTRATISTA es un canal autorizado

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.

Importante para la Entidad
*Asimismo, la Entidad **puede** adoptar uno o más de los requisitos de calificación siguientes:*

Esta nota deberá ser eliminada una vez culminada la elaboración de las bases, así como los requisitos de calificación que no se incluyan.

B	**CAPACIDAD TÉCNICA Y PROFESIONAL**
B.2	**INFRAESTRUCTURA ESTRATÉGICA**
	ITEM 1 Requisitos: • Los Centros de datos principal y contingencia CONTRATISTA deberá ser propios o alquilados, ubicado en la ciudad de Lima (Perú) y deberán contar con certificación TIER-3 en sostenibilidad operacional y/o diseño otorgado por el UpTime Institute y/o Norma ANSI/TIA-942-B con una vigencia durante el periodo del contrato. Acreditación: Copia de documentos que sustenten la propiedad, la posesión, el compromiso de compra venta o alquiler u otro documento que acredite la disponibilidad de la infraestructura estratégica requerida. **Importante** *En el caso que el postor sea un consorcio los documentos de acreditación de este requisito pueden estar a nombre del consorcio o de uno de sus integrantes.*
B.3	**CALIFICACIONES DEL PERSONAL CLAVE**
B.3.1	**FORMACIÓN ACADÉMICA**
	ITEM 1 Y 2 **GESTOR DEL PROYECTO (01 PERSONA)** Requisitos: Título Profesional y/o Bachiller del personal clave requerido como Ingeniero de Telecomunicaciones y/o Sistemas y/o Ingeniería Electrónica y/o Ingeniería de Computación. Acreditación: El BACHILLER Y/O TITULO PROFESIONAL 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. **Importante para la Entidad** *El postor debe señalar los nombres y apellidos, DNI y profesión del personal clave, así como el nombre de la universidad o institución educativa que expidió el grado o título profesional requerido.* ***Incluir o eliminar, según corresponda. Sólo deberá incluirse esta nota cuando la formación académica sea el único requisito referido a las calificaciones del personal clave que se haya previsto. Ello a fin que la Entidad pueda verificar los grados o títulos requeridos en los portales web respectivos.*** En caso BACHILLER Y/O TITULO PROFESIONAL 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.
B.3.2	**CAPACITACIÓN**
	ITEM 01 **GESTOR DEL PROYECTO (01 PERSONA)** Requisitos: 120 horas lectivas, en gestión de proyectos del personal clave requerido como Gestor de proyecto.

	Acreditación: Se acreditará con copia simple de DIPLOMA. **Importante** *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.*
B.4	**EXPERIENCIA DEL PERSONAL CLAVE**
	ITEM 1 **GESTOR DEL PROYECTO (01 PERSONA)** Requisitos: Dos (02) años en Servicio de Internet y/o Servicio de Enlace de Datos y/o Servicio de hosting o housing o alojamiento de gabinetes y equipos de telecomunicaciones) y/o Servicio de Acceso a Internet y/o Servicio de Acceso Dedicado a Internet y/o Servicio de Transmisión de Datos y/o Servicio de Interconexión de Datos y/o Servicio de telco y/o Servicio de cloud u onpremise y/o Servicio de cableado para fibra óptica o puntos de red y/o Servicio de transmisión de datos e internet satelital del personal clave requerido como GESTOR DE PROYECTO. **ITEM 2** **GESTOR DEL PROYECTO (01 PERSONA)** Dos (02) años en Servicio de correo electrónico y/o Servicio de herramientas colaborativas y/o Servicio de backup de correo y/o Servicio de Migración de plataforma de correos electrónicos del personal clave requerido como GESTOR DE PROYECTOS TI. **ESPECIALISTA DE LA SOLUCIÓN (01 PERSONA)** Un (01) año en Servicio de correo electrónico y/o Servicio de herramientas colaborativas y/o Servicio de backup de correo y/o Servicio de Migración de plataforma de correos electrónicos del personal clave requerido como implementador de soluciones en nube. De presentarse experiencia ejecutada paralelamente (traslape), para el cómputo del tiempo de dicha experiencia sólo se considerará una vez el periodo traslapado. 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**
	ITEM 1 Requisitos: El postor debe acreditar un monto facturado acumulado equivalente a S/ **8'967,999.99 (Ocho millones novecientos sesenta y siete mil novecientos noventa y nueve con 99/100 soles)** por la contratación de servicios iguales o similares al objeto de la convocatoria, durante los ocho (8) 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 similares a los siguientes: • Servicio de Internet • Servicio de Enlace de Datos • Servicio de hosting o housing o alojamiento de gabinetes y equipos de telecomunicaciones) • Servicio de Acceso a Internet • Servicio de Acceso Dedicado a Internet • Servicio de Transmisión de Datos • Servicio de Interconexión de Datos • Servicio de telco • Servicio de cloud u onpremise • Servicio de cableado para fibra óptica o puntos de red • Servicio de transmisión de datos e internet satelital **ITEM 2** Requisitos: El postor debe acreditar un monto facturado acumulado equivalente a **S/ 935,555.40 (Novecientos treinta y cinco mil quinientos cincuenta y cinco con 40/100 soles)** por la contratación de servicios iguales o similares al objeto de la convocatoria, durante los ocho (8) 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 similares a los siguientes:

- Servicio de correo electrónico.
- Servicio de Entornos colaborativos
- Servicio de video conferencia.
- Servicio de backup de correo.
- Servicio de Migración de plataforma de correos electrónicos.

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 pago[12], correspondientes a un 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 Nº 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 Nº 8** referido a la Experiencia del Postor en la Especialidad.

Importante

[12] Cabe precisar que, de acuerdo con la **Resolución N° 0065-2018-TCE-S1 del Tribunal de Contrataciones del Estado**:

> *"… 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".*

	• *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".*

Importante

- *Si como resultado de una consulta u observación corresponde precisarse o ajustarse el requerimiento, se solicita la autorización del área usuaria y se pone de conocimiento de tal hecho a la dependencia que aprobó el expediente de contratación, de conformidad con el numeral 72.3 del artículo 72 del Reglamento.*

- *El cumplimiento de los Términos de Referencia se realiza mediante la presentación de una declaración jurada. De ser el caso, adicionalmente la Entidad puede solicitar documentación que acredite el cumplimiento del algún componente de estos. Para dicho efecto, consignará de manera detallada los documentos que deben presentar los postores en el literal e) del numeral 2.2.1.1 de esta sección de las bases.*

- *Los requisitos de calificación determinan si los postores cuentan con las capacidades necesarias para ejecutar el contrato, lo que debe ser acreditado documentalmente, y no mediante declaración jurada.*

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**	
	Evaluación: Se evaluará considerando el precio ofertado por el postor. Acreditación: 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: $$Pi = \frac{Om \times PMP}{Oi}$$ **i** = Oferta **Pi** = Puntaje de la oferta a evaluar **Oi** = Precio i **Om** = Precio de la oferta más baja **PMP** = Puntaje máximo del precio **100 puntos**

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 INTERNET PARA SEDE CENTRAL – UNIDADES TERRITORIALES, SERVICIOS EN LA NUBE Y ENTORNOS COLABORATIVOS (CORREOS ELECTRÓNICOS) PARA EL PROGRAMA NACIONAL "PLATAFORMAS DE ACCIÓN PARA LA INCLUSIÓN SOCIAL – PAIS, que celebra de una parte [CONSIGNAR EL NOMBRE DE LA ENTIDAD], en adelante LA ENTIDAD, con RUC Nº [……], con domicilio legal en [……], representada por [……], identificado con DNI Nº [……], y de otra parte [……], con RUC Nº [……], 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 Nº 002-2024-MIDIS/PNPAS** para la contratación de SERVICIO DE INTERNET PARA SEDE CENTRAL – UNIDADES TERRITORIALES, SERVICIOS EN LA NUBE Y ENTORNOS COLABORATIVOS (CORREOS ELECTRÓNICOS) PARA EL PROGRAMA NACIONAL "PLATAFORMAS DE ACCIÓN PARA LA INCLUSIÓN SOCIAL – PAIS, 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 SERVICIO DE INTERNET PARA SEDE CENTRAL – UNIDADES TERRITORIALES, SERVICIOS EN LA NUBE Y ENTORNOS COLABORATIVOS (CORREOS ELECTRÓNICOS) PARA EL PROGRAMA NACIONAL "PLATAFORMAS DE ACCIÓN PARA LA INCLUSIÓN SOCIAL – PAIS

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 PAGO[13]

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

[13] En cada caso concreto, dependiendo de la naturaleza del contrato, podrá adicionarse la información que resulte pertinente a efectos de generar el pago.

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.

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 ULTIMO CASO].

Importante para la Entidad

De preverse en los Términos de Referencia la ejecución de actividades de instalación, implementación u otros que deban realizarse de manera previa al inicio del plazo de ejecución, se debe consignar lo siguiente:

"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]*."*

Incorporar a las bases o eliminar, según corresponda.

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."*

En el caso que corresponda, consignar lo siguiente:

- Garantía fiel cumplimiento por prestaciones accesorias: [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], la misma que debe mantenerse vigente hasta el cumplimiento total de las obligaciones garantizadas.

Importante

Al amparo de lo dispuesto en el numeral 151.2 del artículo 151 del Reglamento de la Ley de Contrataciones del Estado, si el postor ganador de la buena pro solicita la retención del diez por ciento (10%) del monto del contrato de la prestación accesoria como garantía de fiel cumplimiento de prestaciones accesorias, debe consignarse lo siguiente:

- *"De fiel cumplimiento por prestaciones accesorias:* [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 cumpliese 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.

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 CONTROVERSIAS[14]

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.

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:

DOMICILIO DE LA ENTIDAD: [.....]

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.

[14] 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).

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 Nº 27269, Ley de Firmas y Certificados Digitales[15].

[15] 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 Nº 1

DECLARACIÓN JURADA DE DATOS DEL POSTOR

Señores
COMITÉ DE SELECCIÓN
CONCURSO PÚBLICO Nº 002-2024-MIDIS/PNPAIS
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 Nº [CONSIGNAR EN CASO DE SER PERSONA JURÍDICA] Asiento Nº [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[16]		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 servicios[17]

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.

[16] 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.

[17] 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 Nº 1

DECLARACIÓN JURADA DE DATOS DEL POSTOR

Señores
COMITÉ DE SELECCIÓN
CONCURSO PÚBLICO Nº 002-2024-MIDIS/PNPAIS
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[18]		Sí		No	
Correo electrónico :					

Datos del consorciado 2					
Nombre, Denominación o Razón Social :					
Domicilio Legal :					
RUC :	Teléfono(s) :				
MYPE[19]		Sí		No	
Correo electrónico :					

Datos del consorciado …					
Nombre, Denominación o Razón Social :					
Domicilio Legal :					
RUC :	Teléfono(s) :				
MYPE[20]		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.

[18] 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.

[19] Ibídem.

[20] Ibídem.

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 servicios[21]

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.

[21] 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 Nº 2

DECLARACIÓN JURADA
(ART. 52 DEL REGLAMENTO DE LA LEY DE CONTRATACIONES DEL ESTADO)

Señores
COMITÉ DE SELECCIÓN
CONCURSO PÚBLICO Nº 002-2024-MIDIS/PNPAIS
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 Nº 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 Nº 3

DECLARACIÓN JURADA DE CUMPLIMIENTO DE LOS TÉRMINOS DE REFERENCIA

Señores
COMITÉ DE SELECCIÓN
CONCURSO PÚBLICO Nº 002-2024-MIDIS/PNPAIS
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 Nº 4

DECLARACIÓN JURADA DE PLAZO DE PRESTACIÓN DEL SERVICIO

Señores
COMITÉ DE SELECCIÓN
CONCURSO PÚBLICO Nº 002-2024-MIDIS/PNPAIS
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 Nº 5

PROMESA DE CONSORCIO
(Sólo para el caso en que un consorcio se presente como postor)

Señores
COMITÉ DE SELECCIÓN
CONCURSO PÚBLICO Nº 002-2024-MIDIS/PNPAIS
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 Nº 002-2024-MIDIS/PNPAIS**

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]	[%] [22]
	[DESCRIBIR LAS OBLIGACIONES DEL CONSORCIADO 1]	
2.	OBLIGACIONES DE [NOMBRE, DENOMINACIÓN O RAZÓN SOCIAL DEL CONSORCIADO 2]	[%] [23]
	[DESCRIBIR LAS OBLIGACIONES DEL CONSORCIADO 2]	
	TOTAL OBLIGACIONES	100%[24]

[CONSIGNAR CIUDAD Y FECHA]

[22] Consignar únicamente el porcentaje total de las obligaciones, el cual debe ser expresado en número entero, sin decimales.

[23] Consignar únicamente el porcentaje total de las obligaciones, el cual debe ser expresado en número entero, sin decimales.

[24] Este porcentaje corresponde a la sumatoria de los porcentajes de las obligaciones de cada uno de los integrantes del consorcio.

.....	.....
Consorciado 1	**Consorciado 2**
Nombres, apellidos y firma del Consorciado 1	**Nombres, apellidos y firma del Consorciado 2**
o de su Representante Legal	**o de su Representante Legal**
Tipo y N° de Documento de Identidad	**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 Nº 6

PRECIO DE LA OFERTA

Señores
COMITÉ DE SELECCIÓN
CONCURSO PÚBLICO Nº 002-2024-MIDIS/PNPAIS
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]".

Importante para la Entidad

- *En caso de procedimientos según relación de ítems, consignar lo siguiente:*
  "El postor puede presentar el precio de su oferta en un solo documento o documentos independientes, en los ítems que se presente".
- *En caso de contrataciones que conllevan la ejecución de prestaciones accesorias, consignar lo siguiente:*
  "El postor debe detallar en el precio de su oferta, el monto correspondiente a la prestación principal y las prestaciones accesorias".

Incluir o eliminar, según corresponda

ANEXO Nº 8

EXPERIENCIA DEL POSTOR EN LA ESPECIALIDAD

Señores
COMITÉ DE SELECCIÓN
CONCURSO PÚBLICO Nº 002-2024-MIDIS/PNPAIS
Presente.-

Mediante el presente, el suscrito detalla la siguiente EXPERIENCIA EN LA ESPECIALIDAD*:*

Nº	CLIENTE	OBJETO DEL CONTRATO	N° CONTRATO / O/S / COMPROBANTE DE PAGO	FECHA DEL CONTRATO O CP [25]	FECHA DE LA CONFORMIDAD DE SER EL CASO[26]	EXPERIENCIA PROVENIENTE[27] DE:	MONEDA	IMPORTE[28]	TIPO DE CAMBIO VENTA[29]	MONTO FACTURADO ACUMULADO [30]
1										
2										
3										
4										

[25] 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.

[26] 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 periodo.

[27] 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"*.

[28] Se refiere al monto del contrato ejecutado incluido adicionales y reducciones, de ser el caso.

[29] 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.

[30] Consignar en la moneda establecida en las bases.

Nº	CLIENTE	OBJETO DEL CONTRATO	N° CONTRATO / O/S / COMPROBANTE DE PAGO	FECHA DEL CONTRATO O CP [25]	FECHA DE LA CONFORMIDAD DE SER EL CASO[26]	EXPERIENCIA PROVENIENTE[27] DE:	MONEDA	IMPORTE[28]	TIPO DE CAMBIO VENTA[29]	MONTO FACTURADO ACUMULADO [30]
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 Nº 9

DECLARACIÓN JURADA
(NUMERAL 49.4 DEL ARTÍCULO 49 DEL REGLAMENTO)

Señores
COMITÉ DE SELECCIÓN
CONCURSO PÚBLICO Nº 002-2024-MIDIS/PNPAIS
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 Nº 002-2024-MIDIS/PNPAIS
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 NÚMERO 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.

SERVICIO DE INTERNET PARA SEDE CENTRAL – UNIDADES TERRITORIALES, SERVICIOS EN LA NUBE Y ENTORNOS COLABORATIVOS (CORREOS ELECTRÓNICOS) PARA EL PROGRAMA NACIONAL "PLATAFORMAS DE ACCIÓN PARA LA INCLUSIÓN SOCIAL – PAIS

1. FINALIDAD PÚBLICA

Contar con un servicio de Internet para Sede Central – Unidades Territoriales, servicios en la nube y entornos colaborativos (correos electrónicos), tiene como finalidad garantizar la continuidad de funciones del Programa Nacional PAIS (PNPAIS) permitiendo contar con una comunicación adecuada (Internet) y el alojamiento de los sistemas de información.

2. ANTECEDENTES

Mediante Decreto Supremo N° 013-2017-MIDIS, se estable el Programa Nacional "Plataformas de Acción para la Inclusión Social – PAIS" sobre la base del Programa Nacional Tambos, creado por Decreto Supremo N° 016-2013-VIVIENDA, el cual tiene por finalidad mejorar la calidad de vida de la población pobre y extremadamente pobre, especialmente la asentada en los centros poblados rurales o rural dispersa, coadyuvando a su desarrollo económico, social y productivo que contribuyan a su inclusión social. Asimismo, tiene como objetivo, permitir el acceso de la población pobre y extremadamente pobre, especialmente la asentada en los centros poblados del área rural y de manera dispersa, a los servicios y actividades, en materias sociales y productivas que brinda el Estado.

Para el desarrollo de su finalidad y objetivo, el Programa Nacional "Plataformas de Acción para la Inclusión Social – PAIS", en adelante el Programa, cuenta con líneas de intervención orientadas, entre otras, a implementar plataformas de servicios que: a) Brinden los servicios y actividades del Sector Desarrollo e Inclusión Social; b) Coordine con los Gobiernos Regionales y Locales en el marco de las políticas y prioridades del Gobierno Nacional; c) Contribuyan, coordinen y faciliten la intervención y la prestación de los servicios y actividades de las entidades de los tres niveles de gobierno, que permitan mejorar la calidad de vida, generar igualdad de oportunidades y desarrollar o fortalecer sus capacidades productivas, individuales y comunitarias; d) Ejecuten, coordinen y faciliten acciones de prevención, atención y mitigación de riesgos frente a desastres naturales, en el marco de sus competencias; y, e) Coordine las intervenciones dirigidas al desarrollo y protección de las poblaciones rural y rural dispersa, a través de las Plataformas Itinerantes de Acción Social (PIAS) u otras.

Actualmente el Programa Nacional "Plataformas de Acción para la Inclusión Social – PAIS" cuenta 490 Tambos operativos, los cuales han sido construidos con material noble y equipados con bienes de última tecnología, en tal sentido, a efectos de garantizar el normal desarrollo de las actividades del Programa Nacional "Plataformas de Acción para la Inclusión Social – PAIS", es necesario contar con el Servicio de certificados de seguridad SSL para los dominios y sub dominios para la seguridad digital del Programa Nacional PAIS. lo cual permitirá asegurar la información en los servicios web, mediante la identificación pública y el cifrado de datos.

3. OBJETIVOS

Contar con un servicio de Internet para Sede Central y Unidades Territoriales del Programa Nacional PAIS, servicio en la nube y entornos colaborativos (correos electrónicos) que permitan la comunicación efectiva dentro y fuera del Programa y el Alojamiento de los sistemas de información.

4. **Pedido siga:** N° 0088314.

5. **Actividad POI: 0088314. -** Gestión de Sistemas y Tecnologías de la información

GESTIONAR LOS RECURSOS TECNOLOGICOS NECESARIOS PARA GARANTIZAR LA SEGURIDAD INFORMATICA Y ASEGURAR LA CONTINUIDAD DE LAS OPERACIONES DE TI

6. ALCANCES Y DESCRIPCIÓN DEL SERVICIO

ITEM	UM	DESCRIPCION
1	Servicio	SERVICIO DE INTERNET, CONECTIVIDAD ENTRE CENTRO DE DATOS, HOSTING DEDICADO DE CENTRO DE DATOS PRINICPAL Y CONTIGENCIAS, SEGURIDAD INFORMATICA, EQUIPAMIENTO DE SERVIDORES Y COMPONENTES DE RESPALDO DE INFORMACION. PARA LA SEDE CENTRAL, UNIDADES TERRITORIALES Y SEDES LIMA.

2	Servicio	SERVICIO DE ENTORNOS COLABORATIVOS (CORREOS ELECTRÓNICOS)

6.1. ITEM N° 01 SERVICIO DE INTERNET, CONECTIVIDAD ENTRE CENTRO DE DATOS, HOUSING DEDICADO DE CENTRO DE DATOS PRINICPAL Y CONTIGENCIAS, SEGURIDAD INFORMATICA, EQUIPAMIENTO DE SERVIDORES Y COMPONENTES DE RESPALDO DE INFORMACION.

A. Componente 01 Acceso a internet al centro de datos principal y contingencia.
B. Componente 03 Conectividad de enlace de datos entre los centros de datos del CONTRATISTA, la sede central, sedes Lima y las Unidades Territoriales del Programa Nacional PAIS (anexo 1).
C. Componente 04 Incluye Hosting Dedicado para el servicio de cómputo en el Centro de Datos Principal y centro de datos de contingencia del CONTRATISTA y equipamiento de servidores dedicados y componentes de respaldo de Información.
D. Componente 05 Seguridad Informática de la red del Programa Nacional PAIS.

ESPECIFICACIONES TECNICAS

A. ACCESO A INTERNET AL CENTRO DE DATOS PRINCIPAL Y CONTINGENCIA. (COMPONENTE 01)

El CONTRATISTA debe ofertar la habilitación de un (01) **enlace dedicado de Internet**, en los Centros de Datos Principal y Centro de Datos de Contingencia. El enlace debe ser de **1Gbps de ancho de banda simétrico (1:1)** por medio fibra óptica. Los equipos para este servicio serán provistos como comodato durante el periodo de contratación.

El servicio Internet a brindar será del tipo empresarial, deberá ser un servicio de pasarela a Internet de forma dedicada y transparente, a través de la misma Red IP ofertada, la cual permitirá establecer comunicación bidireccional con cualquier otro usuario conectado a Internet que no ponga restricciones adicionales a ello.

La Red del Servicio a Internet Empresarial con acceso a Internet de banda ancha como Sistema Autónomo Público, se deberá conectar directamente al backbone de Internet en Lima vía Fibra Óptica, con niveles de redundancia de red en alta disponibilidad para el CONTRATISTA.

- Las características mínimas del Servicio Internet serán como se indica a continuación:

  - Servicio de acceso a Internet con Overbooking 1:1, es decir, el ancho de banda contratado debe ser dedicado y garantizado hacia la salida internacional y hacia el NAP Perú.
  - La Red IP, ofertada deberá estar conectada al NAP Perú, para el intercambio de tráfico bidireccional Internet en el ámbito nacional, con los usuarios de otros CONTRATISTAS nacionales de acceso a Internet.
  - Se requiere asignar al servicio **24 IP Publicas**.
  - El CONTRATISTA deberá ser un miembro formal del NAP – PERÚ.
  - El ancho de banda garantizado al 100%
  - El servicio deberá poseer múltiple redundancia dentro de la red del CONTRATISTA
    a. Redundancia en el Backbone.
    b. Redundancia en los servidores DNS.
    c. Redundancia en los enlaces de salida Internacional.
    d. Equipos de Balanceo de Carga.
  - Deberá soportar aplicaciones de Voz, Datos, Video y almacenamiento sin degradación del servicio de internet.
  - Soporte servicios Multimedia Multicast.
  - Monitoreo, Reporte de Tráfico y Aplicaciones
  - El CONTRATISTA deberá contar como mínimo con 2 CONTRATISTAS TIER 1 y que cuente con las salidas internacionales de al menos de 40 Gbps, asimismo la red del contratista deberá estar en capacidad de soportar IP Multicast.
  - El CONTRATISTA deberá de entregar una herramienta que permita mitigar ataques contra denegación de servicios en el tráfico de Internet el cual deberá estar instalado en el centro de datos del CONTRATISTA.

- **Consola de Monitoreo del Servicio:**

  El CONTRATISTA deberá de entregar una consola con las siguientes características:

  - El proveedor debe con un Centro de Operaciones de red informática la cual deberá de Monitorear todo el equipamiento de su solución ofertada y reportarla de forma mensual al CONTRATISTA, cabe resaltar que ante alguna incidencia el CONTRASTISTA deberá de contactarse con el personal técnico de la Unidad de tecnologías de la información de la ENTIDAD para superar la incidencia
  - Atención de reportes y gestión de cambios de configuración 24x7x365. Debiendo el CONTRATISTA remitir los detalles cada fin de mes.
  - La herramienta de gestión que entregará el CONTRATISTA deberá tener representación del diagrama de equipos mediante un esquema de colores del estado de dicho dispositivo y de cada uno de sus componentes asociados (puertos físicos y lógicos, etc.)
  - Monitoreo y visualización del tráfico cursado por los equipos WAN diferenciándolos por tipo de aplicación, mediante el uso del protocolo de gestión.
  - La solución debe mantener almacenada en su base de datos de largo plazo un histórico de información del reporte de uso de ancho de banda (consumo de tráfico) de máximo de 01 año. La cual podrá ser descargada por la entidad
  - El sistema debe permitir generar reportes en base a la información contenida en el repositorio de largo plazo estableciendo umbrales los cuales sean comparados con los porcentajes, utilización o volumen de cada una de las interfaces monitoreadas para establecer filtros de inclusión de la información en los reportes
  - Monitoreo de configuraciones y generación de alarmas ante la detección de cambios. Todas las problemáticas detectadas a partir de la gestión de configuraciones deben estar incluidas dentro del análisis de causa raíz permitiendo de esta forma que la resultante de dicho análisis pueda haber sido un cambio de configuración.
  - El monitoreo y generación de alarmas deberá de llegar a un correo de la Entidad como informativo, cabe resaltar que el CONTRATISTA tendrá su propia central de monitoreo ante cualquier caída o eventualidad del servicio.
  - La interfaz de usuario será de tipo web sin la necesidad de instalación de componentes clientes propietarios en las estaciones de trabajo de los usuarios.
  - La solución deberá facilitar la realización de planeamiento de los recursos (ej.: ancho de banda IP de un enlace, CPU, memoria física, memoria virtual, etc.)
  - El tiempo de ventana de los reportes generados por la herramienta (sobre el uso de ancho de banda) deberán ser flexibles y configurables, permitiendo reportes diarios, mensuales y anual (1 año), y de valores máximos, mínimos y promedios y evaluación de una o más variables (sobre el uso de ancho de banda).

- **Atención de Averías, Soporte y Mantenimiento**

  - El servicio de averías remoto deberá de tener un tiempo de atención no mayor de 30 minutos.
  - El servicio de averías presencial deberá tener un tiempo de atención no mayor a 24 horas.
  - Ante un problema o incidente comunicado por el PNPAIS, al CONTRATISTA, el tiempo de respuesta para iniciar la atención de la solución de la incidencia será no mayor a 15 minutos inmediatamente después de generado el ticket.
  - Toda actividad o provisión de bienes que tenga que ejecutar el CONTRATISTA para subsanar la avería de un equipo será sin costo alguno para el PNPAIS, siempre y cuando se confirme que sea defecto de fábrica.
  - El CONTRATISTA deberá brindar la disponibilidad del servicio de Internet al 99.95%, como mínimo.
  - El CONTRATISTA deberá contar en su Red con sistemas que cuenten con distintas medidas de seguridad para evitar el rastreo e interceptación de las llamadas telefónicas hacia el exterior y viceversa, garantizando de esta manera la privacidad y la seguridad de las comunicaciones. La privacidad y la seguridad de las comunicaciones, será de acuerdo con lo indicado por el ente regulador OSIPTEL.
  - El CONTRATISTA deberá contar con un Centro de Atención de Averías con un número al que se pueda llamar sin costo desde un teléfono fijo o móvil. El servicio de soporte debe ser permanente 7x24x365 y contar con un sistema de gestión adecuado para reportar fallas y atenciones mediante este centro de atención, así mismo dicha gestión podrá ser realizada médiate correo electrónico designado por el CONTRATISTA.

- El servicio de soporte técnico deberá ser Brindado por el CONTRATISTA y/o FABRICANTE de la solución ofertada.
- Los servicios deberán estar operativos las 24 horas de los 7 días, por 365 días.

B. CONECTIVIDAD DE ENLACE DE DATOS ENTRE LA SEDE CENTRAL, SEDES LIMA Y LAS UNIDADES TERRITORIALES DEL PROGRAMA NACIONAL PAIS (ANEXO 1) (COMPONENTE 03)

- El CONTRATISTA deberá brindar un servicio de enlace de datos entre sus Centros de Datos (Principal y Contingencia) y las sedes del Programa Nacional PAIS (Sede Central y 18 Unidades Territoriales) considerando un enlace dedicado (1:1) por medio fibra óptica o radio enlace en banda licenciada destinando un ancho de banda de 30Mbps a cada Unidad Territorial (a excepción de Iquitos que contará con 15 Mbps), 415 Mbps en la Sede Central, y de 10Gbps para las cabeceras (principal y respaldo) ubicadas en el Centro de Datos Principal y Centro de Datos de Contingencia del CONTRATISTA. Los equipos para las unidades territoriales deberán contar con servicio WiFi como mínimo, en la sede central se deberá considerar la habilitación del servicio WiFi para los 3 pisos (1 equipo por piso) y serán provistos como comodato durante el periodo de contratación. Se debe considerar la provisión de 01 un Gabinete de 04 UR como mínimo para cada sede, donde la seguridad eléctrica de los equipos instalados será de responsabilidad del contratista en todas las unidades territoriales. Las características de las cabeceras en los Centros de Datos Principal y Contingencia se especifican en el anexo 1.
- El CONTRATISTA ofrecerá la habilitación de dos (02) enlaces de Datos, desde EL DATACENTER PRINCIPAL Y CONTIGENCIA del CONTRATISTA.
- La Sede Central y las 18 Unidades Territoriales saldrán al servicio de internet a través de los enlaces cabecera ubicados en los Centros de Datos del CONTRATISTA.
- Deberá considerarse dos hilos de fibra óptica por cada enlace
- El CONTRATISTA deberá incluir todos los equipos y accesorios que permitan el enlace entre la entidad y la sede DC del CONTRATISTA, tales como switches, transceiver, cables entre otros.
- Las interfaces y cantidades en ambos extremos dependerán de la propuesta del CONTRATISTA.
- A través enlace de fibra óptica ultra rápida entre estas dos sedes (virtualmente se trataría de la misma sede (Lan extendida). En caso los enlaces estén bajo la modalidad de activo - pasivo, compartirán el mismo pool público asignado. La cual debera ser de uso exclusivo para la entidad, la velocidad de trasmiscion deberá ser de 10 Gbps.

- **SWITCHES PARA LA SEDE CENTRAL DE PAIS.**
  Se requiere 08 switches de acceso para la Sede Central, el proveedor deberá de realizar la configuración y puesta en marcha de los switches ofertados, la configuración será en coordinación con el área técnica de la ENTIDAD.

  El CONTRATISTA se encargará de realizar la puesta en marcha y configuración de su solución ofertada.

  La administración de toda la solución ofertada será compartida las cuales deberán de ser diferenciadas por usuarios para la entidad y el contratista. La responsabilidad el contratista no comprende las acciones efectuadas por los usuarios asignados a la entidad.

  Todos los swtiches de la solución ofertada deberán estar conectados mediante las Interfaces de GE/10 GE SFP+ a los swtiches core que proporcionara el CONTRATISTA.

  Características Físicas
  - 48 puertos de red con velocidad de 1Gbps
  - 04 interfaces GE/10 GE SFP+
  - 01 puerto de gestión 10/100/1000
  - 01 puerto de consola RJ45 o Serial
  - Deberá ser de tipo non-blocking
  - Deberá contar con un sistema de ventilación Front to back con al menos un ventilador como mínimo
  - Factor de forma de 1 RU como máximo
  - Deberá tener doble fuente redundante de tipo Hot swap, intercambio en caliente sin necesidad de apagar el equipo.

Capacidades

- Capacidad de Switching (duplex): 176 Gbps como mínimo
- Paquetes por Segundo (Duplex): 262 Mpps como mínimo
- Max. direcciones MAC: 32 K como mínimo
- Packet Buffer: 4 MB o superior
- DRAM: 1 GB o superior
- Min. ACLs soportadas: 1 K entradas como mínimo
- Deberá soportar capa 2 y capa 3

- **ATENCIÓN DE AVERÍAS, SOPORTE TECNICO Y MANTENIMIENTO**
  - El servicio de averías remoto deberá de tener un tiempo de atención no mayor de 30 minutos.
  - El servicio de averías presencial deberá tener un tiempo de atención no mayor a 24 horas.
  - Ante un problema o incidente comunicado por el PNPAIS, al CONTRATISTA, el tiempo de respuesta para iniciar la atención de la solución de la incidencia será no mayor a 15 minutos inmediatamente después de generado el ticket.
  - Toda actividad o provisión de bienes que tenga que ejecutar el CONTRATISTA para subsanar la avería de un equipo será sin costo alguno para el PNPAIS, siempre y cuando se confirme que sea defecto de fábrica.
  - El CONTRATISTA deberá brindar la disponibilidad del servicio de Internet al 99.95%, como mínimo.
  - El CONTRATISTA deberá contar en su Red con sistemas que cuenten con distintas medidas de seguridad para evitar el rastreo e interceptación de las llamadas telefónicas hacia el exterior y viceversa, garantizando de esta manera la privacidad y la seguridad de las comunicaciones. La privacidad y la seguridad de las comunicaciones, será de acuerdo con lo indicado por el ente regulador OSIPTEL.
  - El CONTRATISTA deberá contar con un Centro de Atención de Averías con un número al que se pueda llamar sin costo desde un teléfono fijo o móvil. El servicio de soporte debe ser permanente 7x24x365 y contar con un sistema de gestión adecuado para reportar fallas y atenciones mediante este centro de atención, así mismo dicha gestión podrá ser realizada médiate correo electrónico designado por el CONTRATISTA.
  - El servicio de soporte técnico deberá ser Brindado por el CONTRATISTA y/o FABRICANTE de la solución ofertada.
  - Los servicios deberán estar operativos las 24 horas de los 7 días, por 365 días.

a. Incluye Hosting Dedicado del Centro de Datos Principal. (Componente 04).

- Los centros de datos principal y contingencia deberán tener una certificación en Tier III en sostenibilidad operacional y/o diseño y/o Norma ANSI/TIA-942-B.

- El CONTRATISTA mediante una declaración jurada simple deberá indicar la dirección de ambos centros de datos ofertados PRINCIPAL Y CONTIGENCIA, ambiente que debe estar alojado dentro de la ciudad de Lima, con una arquitectura activo – pasivo. El CONTRATISTA se hará responsable de la infraestructura que brindará en su centro de datos principal y contingencia.

- La administración de toda la solución ofertada será compartida las cuales deberán de ser diferenciadas por usuarios para la entidad y el contratista. La responsabilidad el contratista no comprende las acciones efectuadas por los usuarios asignados a la entidad.

- **Centro de datos Principal**
  - El soporte deberá de ser proporcionados por el CONTRATISTA y el fabricante de la solución.
  - El CONTRATISTA será el responsable de la adquisición o provisión, configuración y puesta en marcha de los equipos. El soporte del fabricante deberá ser gestionado a través del CONTRATISTA.
  - El monitoreo de la infraestructura en el centro de datos principal y de contingencia se realizará de manera compartida.

- El CONTRATISTA será el encargado de proporcionar la solución de monitoreo para el equipamiento en el Centro de Datos Principal y de contingencia.
- El CONTRATISTA se hará responsable de la infraestructura que brindará en su centro de datos principal y en el centro de datos de contingencia.
- En el servicio, el CONTRATISTA debe gestionar la instalación todo el equipamiento necesario. El ambiente debe estar certificado en base a los estándares y/o mejores prácticas de la industria para Centros de Datos, por lo tanto, el CONTRATISTA deberá evidenciar fehacientemente, que cuenta con la certificación emitida por Uptime Institute, entidad certificadora de Centro de Datos o Centros de Procesamiento de Datos, con una certificación TIER III y/o deberá cumplir con la Norma ANSI/TIA-942-B para el centro de datos principal y contingencia como mínimo, que permita garantizar la alta disponibilidad y seguridad de los equipos y servicios, así como minimizar los riesgos que afectan la disponibilidad de los servicios y sistemas de tecnologías de información y cuya disponibilidad será de 99.982% como mínimo.
- El CONTRATISTA o CONTRATISTA será responsable de la integridad de todo el equipamiento ofertado en ambos centros de datos principal y contingencia.
- Debe tener ordenado y etiquetado, el cableado eléctrico y de datos dentro de los gabinetes contratados, para lo cual el CONTRATISTA deberá contar con cantidad de espacio disponible (en gabinetes) suficiente para montar el equipamiento necesario.
- Debe monitorear y hacer el seguimiento a la infraestructura, equipamiento (servidores, equipos de comunicación, seguridad) y conectividad (enlaces, fibra óptica), considerando como mínimo.
    - A los enlaces de fibra óptica ultra rápida, entre los centros de datos principal y contingencia, serán configuradas en capa 2, el cual debe tener una interfaz gráfica, en donde PAIS tendrá un acceso de 24x7x365 días durante el tiempo que dure el servicio. Monitoreo de calidad de Servicio (QoS) en ambos extremos de los enlaces. El monitoreo debe considerar el consumo de ancho de banda y la visualización del uso del ancho de banda (consumo del canal de transmisión y recepción) de todos los enlaces.cabe resaltar que el servicio en mención sera para uso exclusivo de la entidad.
    - A la disponibilidad de los enlaces y equipamiento de comunicación (CPU y memoria, ancho de banda, delay, pérdida de paquetes).
    - Al uso de recursos de todo el equipamiento (CPU, RAM, HDD, Uptime, ping).
    - De presentarse alertas, estas deben ser notificadas al correo electrónico que será proporcionado por PAIS.
    - Generar reportes gráficos de manera diaria y mensual del uso de recursos, disponibilidad de equipos y Uptime del servicio ofertado.
    - Debe generar reportes mensuales del monitoreo de la temperatura, humedad, control de acceso y energía, respecto al centro de datos provisto y de las sedes de personalización remotas.
    - El equipamiento electromecánico (grupos electrógenos, UPS, equipos de aire acondicionado de precisión) e instalaciones eléctricas (tableros eléctricos, alumbrado, sistemas de pozo a tierra) que se conectarán al Centro de Datos requerido, debe garantizar el normal funcionamiento del equipamiento Centro de Datos.
    - Para el acceso a los Centros de Datos del CONTRATISTA este debe contar con por lo menos dos (02) medios de autenticación para el ingreso, siendo obligatoriamente uno de ellos del tipo biométrico.
    - Todas las puertas de acceso al Centro de Datos deben contar con cámaras de seguridad.
    - Debe disponer de personal de energía en formato 24x7, los 365 días del año, para la atención inmediata de eventos de energía que puedan afectar los servicios de PAIS.

- Debe disponer de personal de operaciones en TI en formato 24x7, los 365 días del año, para la atención inmediata de manos remotas (servicio a demanda y limitado a un máximo 48 horas mensuales no acumulables.) o TI de equipos de PAIS que puedan afectar los servicios.
- Los grupos electrógenos, salas de energía y tanques de combustible, deben estar ubicados en ambientes separados que disminuyan los riesgos de inundación y/o actividad sísmica.

- **Para la SEGURIDAD AMBIENTAL, ELÉCTRICA Y ELECTROMECÁNICA, del ambiente del Centro de Datos del CONTRATISTA o CONTRATISTA, este debe cumplir con lo siguiente:**
  - Estar localizado en un lugar alejado de amenazas de aniego, incendio, disturbios, entre otros.
  - Contar con equipos de aire acondicionado de precisión para el control de la temperatura y humedad relativa.
  - Contar con un equipo de aire acondicionado de precisión de contingencia que garantice un óptimo control de la temperatura y humedad en caso uno de los aires acondicionados principales se averíe o esté en mantenimiento.
  - Contar con dos circuitos eléctricos de energía estabilizada para cada gabinete y dos PDUs (cada gabinete debe contar con dos circuitos eléctricos alimentados por UPS's diferentes, es decir el total que se debe proporcionar son 4 circuitos eléctricos independientes alimentados por 2 UPS como mínimo.
  - Cada gabinete deberá contar con un equipo STS o ATS de las tomas necesarias para la solución como mínimo IEC C13.
  - Cada gabinete deberá contar con una barra de aterramiento ojada dentro del mismo.
  - Se aceptarán propuestas similares siempre y cuando se demuestre cumple con la certificación TIER III.
  - Contar con la provisión de energía eléctrica de respaldo ante un corte el suministro de energía comercial mediante el uso de grupos electrógenos redundantes propios y con tanques de combustibles para autonomía de funcionamiento de los grupos electrógenos.
  - Contar con equipos de UPS (Uninterruptible Power Suply), deben contar con la autonomía requerida hasta el encendido del grupo electrógeno.
  - Contar con un cableado en fibra y cobre, respetando las normas internacionales de cableado estructurado.
  - Contar con un Sistema de detección y extinción de incendios en la etapa más temprana.
  - Contar con sensores de aniego para la detección temprana de inundaciones en la Sala TI.
  - Contar con tableros de transferencia automática que ante posibles disturbios en la red eléctrica envíe automáticamente a encender el sistema de respaldo de grupos electrógenos.

- **Para la SEGURIDAD DE ACCESO FÍSICO, debe como mínimo:**
  - Contar con un personal de seguridad para el ingreso a las instalaciones del centro de datos ofertado por el CONTRATISTA o CONTRATISTA y además de tener un sistema de control de ingreso a las salas del centro de datos principal del CONTRATISTA o CONTRATISTA mediante tarjeta de proximidad + clave y/o lector biométrico (tarjeta de proximidad + huella + clave).
  - Contar con un control y registro de ingresos al edificio y a la Sala de centro de datos principal u o CONTRATISTA de personas y equipos en forma continua 24x7. El ingreso de personal del cliente a la Sala de centro de datos principal del CONTRATISTA o CONTRATISTA siempre debe ser acompañado por personal del CONTRATISTA o CONTRATISTA.
  - Tener la vigilancia remota por circuito cerrado de televisión sobre la Sala de centro de datos principal del CONTRATISTA o CONTRATISTA 24x7.
  - Grabar continuamente el Circuito Cerrado de Televisión (CCTV) de la Sala de centro de datos principal del CONTRATISTA o CONTRATISTA, con fecha y hora en horario 24x7.

- Tener gestión centralizada en línea del sistema de control de acceso a la Sala de centro de datos principal del CONTRATISTA o CONTRATISTA.
- Restringir el acceso a los gabinetes y/o racks de asignados al Programa PAIS. El acceso solo será permitido al personal (propio o tercero) autorizado por PAIS al CONTRATISTA o CONTRATISTA, a través de los canales de comunicaciones.
- Realizar revisiones periódicas de las áreas de acceso a los equipos con los que se brinda el servicio a Programa Nacional PAIS y de cuya seguridad el CONTRATISTA sea responsable, incluyendo revisiones de los registros de acceso para ver ocurrencias inusuales, y realizar las actividades de seguimiento de conformidad con sus protocolos de seguridad.

- **Con respecto al EQUIPAMIENTO Y ACCESORIOS, debe considerar como mínimo**:
  - EL CONTRATISTA se encargará de La provisión de los gabinetes necesarios para su solución ofertada en cada site los cuales deberán ser de 42 RU de uso y acceso exclusivo para el servicio solicitado por el PROGRAMA NACIONAL PAIS, para colocar los equipos (el layout de equipos será proporcionado al contratista, al inicio del servicio).
  - Los gabinetes deberán ser exclusivos para el alojamiento del equipamiento ofertado.
  - los equipos de comunicaciones del CONTRATISTA deberán ser instalados en un Gabinete propio.
  - Gabinete adecuado para la instalación del equipamiento indicado en el ANEXO 01 y los de comunicaciones, como mínimo.
  - Debe incluir set de tierra con punto central. Puertas, laterales, techos y suelos deben estar conectados a la estructura del gabinete para contar con tierra homogénea.
  - Cada gabinete deberá incluir 01 marco de escobillas para división del pasillo frio y caliente dentro del armario.
  - Cada gabinete deberá incluir 01 módulo de suelo con escobillas altamente estancas para asegurar el orden del cableado y evitar el ingreso de polvo.
  - Cada gabinete deberá incluir ordenadores horizontales según según el despliegue del CONTRATISTA.
  - Cada gabinete deberá incluir ordenadores verticales de cables de la solución ofertada
  - Cada gabinete deberá incluir cintas de velcro de 4 metros para el peinado y ordenamiento del cableado. Permite ordenar el cableado y mejorar el uso del espacio.
  - Cada gabinete deberá incluir la cantidad de PDU necesarias para la instalación en la misma, así como los cables C13, C14 entre otros.
  - Cada gabinete deberá incluir las bandejas necesarias para equipos de comunicaciones que no son rackeables.
  - De contar con falso piso, deberá respetar los estándares de la industria.
  - De contar con falso piso, solo deberá contar con dos tipos de baldosa, baldosa de acero soldado con huecos en el interior para la circulación de aire frio en pasillo frio y baldosa de acero soldado con núcleo de cemento.
  - De contar con falso piso, baldosa sólida deberá tener una altura mínima de 30 cm y 40 cm como máximo (piso terminado) con respecto a la losa. (se puede presentar alternativas equivalentes).
  - El CONTRATISTA deberá de dimensionar la carga eléctrica necesaria para su solución ofertada.
  - Debe proveer e instalar todo el cableado y accesorios necesarios para la conectorización de los gabinetes hacia la red interna y cuarto de comunicaciones del centro de datos.
  - Debe proveer e instalar todo el cableado y accesorios necesarios para energizar los gabinetes en el centro de datos, no se admitirá instalaciones y materiales de uso doméstico.
- **El ambiente donde se alojarán los equipos debe contar con un SISTEMA DE CONTROL DE INCENDIOS de las siguientes características:**
  - El CONTRATISTA debe presentar en su oferta soluciones para el subsistema de detección y extinción de incendios que contemple un

gas de similares o mejores prestaciones al Novec1230 en tanto que estas constituyan soluciones compatibles con la norma NFPA 2001 (puede ser acreditarlo con la presentación de un informe técnico de pruebas preventivas al sistema de detección y alarmas contra incendio) o soluciones similares.
    - Se aceptarán propuestas similares siempre y cuando se demuestre que pertenece a la familia de agentes limpios y sea parte de norma NFPA 2001.Disponer de un extintor de mano de clase C.
    - Tener un sistema de detección de humo temprana basado en láser o pre-alarma de incendios y alerta de incendios y de un sistema automatizado de extinción de incendios empleando agente limpio.
    - El agente limpio (agente extintor), no debe dañar los equipos informáticos y/o electrónicos de PNPAIS, es decir, debe ser un gas no tóxico, que podría usarse sin ningún riesgo para las personas presentes en los ambientes asignados para los equipos de PNPAIS.
    - Debe prevenir y proteger el centro de Datos contra incidentes por incendios o cortos circuitos.
    - Capacidad de detección combinada por zonas.
    - Complementariamente, debe tener dispositivos de descarga manual.
    - Abortadores de descarga, antes de 30 seg.
    - Elementos para extinción manual.
    - Monitoreo centralizado de alarmas con vigilancia 7x24.
    - Brigada de incendios con personal capacitado, disponible 7x24.
    - Para la suscripción del contrato se deberá presentar:
    - Certificado de operatividad-funcionamiento del sistema contra incendios.
    - Certificado y/o registro de los últimos servicios de mantenimiento del sistema contra incendio realizados o un informe técnico de pruebas preventivas al sistema de detección y alarmas contra incendios.
- **El ambiente donde se alojarán los equipos deberá cumplir los siguientes requisitos a NIVEL DE CLIMATIZACIÓN:**
    - Cumplimiento del estándar ASHRAE TC9.9
    - Sistema respaldado en base a múltiples enfriadores de agua.
    - Distribución de aire con pasillo frio y pasillo caliente
    - Control de temperatura.
    - Control de Humedad Relativa.
    - Filtros de aire.
    - Monitoreo de operación centralizado.
    - Registro histórico de temperatura y humedad relativa.
    - Las unidades de climatización deben ser alimentadas tanto por la energía eléctrica pública como por el sistema eléctrico de emergencia (grupos electrógenos). Estas unidades deberán estar siendo constantemente monitoreadas.

- **El ambiente donde se alojarán los equipos debe cumplir los siguientes requisitos a NIVEL DE ENERGÍA:**
    - Provisión de energía eléctrica con disponibilidad en el punto de entrega a los equipos de PN PAIS cómo mínimo 99.982% anual.
    - Tener una subestación Eléctrica propia con respaldo 1+1 y un Grupo Electrógeno (Generador) con respaldo 1+1, con una autonomía de 48 horas a plena carga.
    - La ubicación del Grupo Electrógeno debe ser en un ambiente separado a la Sala de Equipos del Centro de Datos y UPS con respaldo “N+1”, con una autonomía de 20 minutos a plena carga. Estos equipos deben tener configuración redundante con 02 sistemas, cada uno de ellos con sus respectivos tableros eléctricos.
    - Suministro de energía (Monofásica y/o trifásica) (en la Sala de centro de datos).
    - Distribución interna inteligente, mediante regletas de energía PDU monitoreable (se puede presentar alternativas equivalentes).
    - Monitoreo centralizado 7x24 de estado de los sistemas eléctricos (Suministro público, Generación, UPS, Distribución interna).
    - Alimentación de energía eléctrica por vía A y B para 02 fuentes del equipo.
    - Equipo eléctrico STS o ATS, para el respaldo de equipos de 01 fuente de poder.

- Monitoreo centralizado 7x24 de estado de los sistemas eléctricos (Suministro público, Generación, UPS, Distribución interna).
- Registro histórico de eventos que han afectado la disponibilidad de la energía eléctrica.
- Debe tener programaciones de mantenimiento semestrales de los UPS del centro de datos. Se debe medir y probar los equipos, realizar limpieza, reparación o cambio de ser necesario.
- La capacidad de los UPS que forman parte de la solución debe soportar la carga total del equipamiento para toda la solución ofertada y además debe permitir una carga adicional del 30% de la carga actual. Los UPS debe de contar con un bypass estático automático y un bypass externo de mantenimiento manual.
- El sistema a tierra deberá tener una resistencia de no mayor a los 05 ohmios.
- El Grupos Electrógenos, para el sistema de respaldo eléctrico, debe incluir una solución de con las siguientes especificaciones técnicas mínimas:
    - Debe estar dimensionados para soportar el mínimo del 100% de toda la carga del Centro de Datos, incluyendo la capacidad de posibles incrementos de cargas.
    - Autonomía a plena carga de al menos cuarenta y ocho (48) horas, y debe permitir recarga de combustible en línea. Los tanques de combustible de los grupos electrógenos deberán estar conectados en redundancia.
    - Debe contar con un sistema de conmutación automatizada para el ingreso de los Grupos Electrógenos y/o red comercial.
    - Debe contar con por lo menos dos grupos electrógenos (primario y secundario). La transferencia o pase a grupo electrógeno primario, en caso de una interrupción del fluido eléctrico comercial, deberá ser automatizada y la transferencia al grupo electrógeno secundario en caso de que fallara el grupo electrógeno primario, también deberá ser de forma automatizada.
    - Debe tener programado sus mantenimientos preventivos, a fin de garantizar el normal funcionamiento, los mismos que no deben representar una baja del servicio. Asimismo, los componentes del sistema deberán estar respaldados por un servicio de soporte correctivo 24x7 que garantice la operatividad continua de los mismos.

- **Para la GESTIÓN DEL CENTRO DE DATOS: debe considerar como mínimo, las siguientes actividades:**
    - La gestión de los siguientes sistemas ambientales: espacio físico, energía, climatización y servicios de seguridad física.
    - Revisar y controlar los ambientes del Centro de Datos principal del CONTRATISTA o CONTRATISTA.
    - Elaborar informes mensuales de bitácoras de acceso de CONTRATISTA terceros al personal del PNPAIS a las instalaciones del Centro de Datos principal del CONTRATISTA o CONTRATISTA.
    - Mantener actualizadas las bitácoras y registros del mantenimiento a la infraestructura del Centro de Datos principal del CONTRATISTA o CONTRATISTA.
    - Mantener las instalaciones, equipos y suministros en buenas condiciones de operatividad.
    - Supervisar presencialmente las actividades presenciales del programa de mantenimiento preventivo para las instalaciones que se mencionan a continuación: Generación de energía, Sistema UPS, Aire acondicionado de precisión, Mantenimiento de tableros eléctricos, Control y extinción de incendios, Control de acceso, Sistema de alarmas y monitoreo, Pruebas de funcionamiento de grupos electrógenos, además de escoltar y monitorear a terceros y otros CONTRATISTA que PNPAIS designe para el ingreso a las instalaciones del CONTRATISTA, con la finalidad de realizar trabajos de instalación y/o configuración en los equipos.
- **Para las MANOS REMOTAS: debe considerar como mínimo, las siguientes actividades:**

- El CONTRATISTA debe ofrecer un paquete de servicio de manos remotas por 20 (veinte) horas mensuales no acumulables para la atención del servidor y otros a solicitud del cliente. El servicio incluye:
- Revisión y/o modificación de conexiones físicas del equipo
- Troubleshooting a nivel físico de conectividad y energía eléctrica.
- Colocación / retiro de medios ópticos
- Colocación / retiro de unidades de almacenamiento masivo
- Verificación de alertas a nivel de hardware.
- Información de escalamiento por equipos alarmados
- Ciclo de reinicialización, restablecimiento de equipos, que no involucre la pérdida de garantía del equipo.
- Observación, descripción o información sobre indicadores LEDS e información de visualización sobre equipos o consolas.
- Realización y envío de fotografías (únicamente cuando sean requeridas).
- Observación básica e información sobre entornos (clima).
- Conexión, desconexión e intercambio de cableado de red y/o eléctrico previa coordinación.
- Verificación visual para ayudar en la solución remota de problemas por el cliente.
- Intercambio de medios para copias de seguridad (Cintas, CDs, DVDs, etc).
- Montaje y desmontaje de cintas
- Comprobación de estado y tecleado de comandos por solicitud del cliente para eventos críticos que impidan al cliente acceder a los equipos.
- Montaje y desmontaje de cintas
- Apagado y encendido de servidores
- Apagado y encendido forzado del equipo on-site
- Escalamientos por equipos alarmados
- Visualización de equipos y monitoreo continuo del ambiente
- Confirmar al CONTRATISTA el cambio de un equipo o parte mediante la garantía del fabricante

- **Para las VIDEO VIGILANCIA: debe considerar como mínimo, las siguientes actividades:**
  - Dentro del esquema de seguridad física, el CONTRATISTA deberá disponer del uso de cámaras que vigilen el acceso a los equipos y/o gabinetes del Programa Nacional PAIS ubicados en el Centro de Datos principal, con las siguientes consideraciones:
    - El servicio deberá incluir como mínimo la habilitación de cámaras para el control de los gabinetes del Programa Nacional PAIS en formato 24x7x365 de tal manera que se permita identificar correctamente el acceso y manipulación del o los gabinetes asignados para el cumplimiento del servicio.
    - El sistema deberá permitir el acceso a la visualización de las grabaciones obtenidas por un período no menor de 30 días calendario, luego de eso, el sistema podrá borrar las imágenes grabadas.

- **Para las CINTOTECA O CUSTODIA DE CINTAS debe considerar como mínimo, las siguientes actividades.**
    - Se brindará el servicio de custodia de cintas con espacio hasta 120 Cintas. Esta Cintoteca tiene las siguientes características:
    - Las cintotecas podrán estar fuera del centro de datos del CONTRATISTA o CONTRATISTAS, siempre y cuando se cumpla con el envío y retorno de las cintas cuando sea necesario.
    - Al término del contrato el CONTRATISTA deberá entregar las cintas tapes backup a la ENTIDAD conteniendo la información hasta la última hora de servicio.

SERVIDORES PARA EL SERVICIO CLOUD HOSTING DEDICADO.

El equipamiento de la solución debe ser entregada en modelo Hosting Cloud Dedicado para uso del PROGRAMA NACIONAL PAIS: La titularidad del equipamiento para el Centro de Datos Principal y de Contingencia será del CONTRATISTA.

La administración de toda la solución ofertada será compartida las cuales deberán de ser diferenciadas por usuarios para la entidad y el contratista. La responsabilidad el contratista no comprende las acciones efectuadas por los usuarios asignados a la entidad

CARACTERÍSTICAS EN AMBOS DATA CENTERS

La solución en ambos sitios debe incluir además las siguientes características:

SOLUCIÓN DE INFRAESTRUCTURA HIPERCONVERGENTE (HCI)

NODOS DE HIPERCONVERGENCIA

Descripción	Características técnicas mínimas
Cantidad	Cuatro (04) nodos Hiperconvergentes como mínimo por cada site
Factor de forma	Rackeable de máximo una (01) unidad de rack, debe incluir los accesorios de rackeo.
Procesadores	- Un (01) Procesadores de la última generación por nodo, cada procesador de 24 cores como mínimo y con al menos 2.6 GHz y mínimo 30MB de cache L3. - Debe soportar la tecnología Hyper-Threading o Multithreading
Memoria RAM	- **2048 GB en total**, de tecnología DDR5, en módulos de mínimo 64GB 4800MHz. para cada site. - Deberá soportar un crecimiento de al menos 2TB en su máxima configuración, añadiendo módulos de memoria, sin reemplazar los módulos solicitados. - Con características RAS, que incluye mecanismos de tolerancia rápida de fallas que permitan detectar y corregir errores de memoria antes estos impacten disruptivamente en el sistema.
Boot de hipervisor	- Dos (02) discos M.2 SSD NVMe PCIe 4.0 de mínimo 900GB configurados en RAID 1.
Almacenamiento	- Discos Flash SSD NVMe PCIe 4.0. - La solución HCI debe ser configurada para permitir alta disponibilidad ante la caída de un nodo o FTT=1. - La capacidad total de almacenamiento por cada site deberá ser de al menos 100TB SSD NVMe TiB (binario) usable en RAID 5, sin considerar factores de eficiencia como compresión, deduplicación y la capacidad destinada para la reserva de operaciones del HCI. Cabe resaltar que la capacidad en disco solicitada deberá ser efectiva. - Se debe considerar la distribución de discos de acuerdo con las buenas prácticas del fabricante de hiperconvergencia, en lo que respecta a tipo de disco y cantidad, considerando dos agrupaciones para un mejor rendimiento. - En caso se proponga arquitecturas que utilicen discos de acceso inmediato (cache) y de capacidad, estos deben ser de mínimo 800GB 2.5DWPD y 7TB 1DWPD respectivamente.
Conectividad	- Cuatro (04) puertos Ethernet de 10Gb SFP+ (LAN), distribuidos en dos (02) tarjetas, deben incluir sus respectivos transceivers SR y cables de fibra LC-LC MM OM3 de mínimo 5 metros. - Los nodos se conectarán a los switches LAN provisto por el contratista, donde proporcionará los puertos de 10Gb SFP+ requeridos. - En caso de tener puertos de red libres el CONTRATISTA deberá de realizar la configuración de Ethernet Chanel con los puertos sobrando
Fuentes de poder	- Dos (02) fuentes poder redundantes de 200-230VAC de intercambio en caliente, con sus respectivos cables de poder C13-C14.
Seguridad	- Soporte de TPM 2.0. - El servidor debe cumplir con FIPS 140-3 y NIST SP 800-193. - Debe contar con un sistema de arranque (boot) seguro, que garantice que solo se cargue software inmutable y firmado durante el tiempo de arranque, evitando que

	se cargue código malicioso y ayudando a prevenir ataques como la instalación de rootkits. - Debe contar con protección contra actualizaciones de firmware no autorizadas y corrupción, restaurando el firmware a un estado integral y monitoreo del firmware en busca de posibles compromisos de ataques cibernéticos.
Análisis predictivo de fallas	Debe soportar análisis predictivo de fallas de componentes como: procesador, discos, memoria, ventiladores y fuentes de poder; y debe poder solicitarse el cambio por garantía desde el momento que se presenta una alerta de este tipo en algunos de estos componentes.
Puerto de gestión	Deberá incluir un puerto de gestión de 1GbE RJ45 fuera de banda, que proporcionen una interfaz de administración web, desde la cual se podrá supervisar y gestionar todos los componentes internos del servidor, así mismo deberá contar con mecanismos de despliegue o provisionamiento del sistema operativo, estas funciones deberán ser independientes al sistema operativo.
Software de administración	Factor de forma: máquina o appliance virtual. Deberá incluir el software y todas las licencias necesarias que permitan la administración centralizada de la totalidad de los Nodos de Hiperconvergencia requeridos. Este software debe permitir la administración, control, gestión y manejo de toda la infraestructura de cómputo y realizar las siguientes funciones como mínimo. - Descubrir todo el hardware. - Realizar un inventario de la infraestructura de hardware. - Monitoreo de la salud de los componentes. - Actualizaciones de firmware. - Configuración de patrones de los servidores. - Visualización gráfica de los servidores. - El software deberá soportar la administración remota gráfica de cada servidor independientemente del sistema operativo del servidor. - Proveer acceso detallado a problemas de fallas del sistema. - Call Home. - Capacidad de instalación remota de un servidor o grupo de servidores. - Capacidad de actualización del firmware remota de un servidor o grupo de servidores. - Funcionalidad de acceso remoto compartido entre por lo menos tres usuarios concurrentemente, independiente del sistema operativo del servidor. - Los servidores deberán ser capaces de poder monitorear su estado remotamente, componentes de hardware básico como procesadores, fuentes de poder, ventiladores, memoria y discos duros. Deberán mandar alertas sin necesidad de tener cargado un sistema operativo en los servidores. - Permitir una integración con las consolas de administración de la plataforma virtual vCenter, Microsoft System Center. - Integración con herramientas de administración de recursos como basadas en Ansible, Chef y Puppet.
Licencias	- El CONTRATISTA debe entregar las Licencias de Windows Server 2022 edición Data Center deberán entregadas a solicitud de la entidad durante el periodo de vigencia del contrato (La licencia debe cubrir todos los procesadores suministrados de su solución ofertada) tanto del centro de datos principal como el de contingencia. - El CONTRATISTA debe entregar el servicio y/o software que permita la movilidad de las licencias ante caída de desastres. - En caso de que el fabricante actualice la versión de su sistema operativo el CONTRATISTA debe cubrir el licenciamiento a solicitud de la ENTIDAD durante el periodo de vigencia del contrato
Garantía, soporte técnico e implementación	- Garantía y soporte 24x7 con cuatro (04) horas de tiempo de resolución del fabricante por el periodo de tres (03) años. - La propuesta debe incluir el servicio de implementación de la Solución HCI por parte del fabricante.
Fabricación	- Los nodos deben estar certificados en la Solución HCI por los fabricantes del software y hardware.

	- Los nodos deben tener fecha de fabricación a partir del 2023 en adelante.

EQUIPOS DE COMUNICACIÓN LAN - SAN (SWITCHES) PARA LA SOLUCION HIPERCONVERGENTE.

Para este servicio se requiere contar con switches para la parte de comunicación las cuales, las cuales deben contar con las siguientes características.

Administración

- El switch debe contar con interfaz de línea de comandos (CLI) mediante SSH.
- Deberá soportar administración por IPv4 e IPv6.
- Deberá soportar SNMP v1/v2c/v3.
- Deberá poder configurar su reloj mediante un NTP Server.
- Deberá contar con una línea de comandos estándar.
- Deberá soportar actualizaciones de Software por: TFTP/FTP.
- Debe soportar gestión stand-alone o gestión centralizada desde una consola o dispositivo de gestión centralizada local.
- Deberá permitir realizar labores de diagnóstico sobre el equipo.

Gestión Centralizada

- Deben poder ser gestionados una plataforma de gestión centralizada que soporte alta disponibilidad.
- Debe ser provista en appliance físico con fuente redundante o modalidad virtual del mismo fabricante que los switches.
- Gestionar al menos 10 switches con capacidad de crecimiento posterior a las necesidades del Programa Nacional PAIS.
- Debe poder visualizar el estado de salud de los switches gestionados.
- Debe realizar cambios en la configuración desde la WebUI o CLI.
- Debe realizar funciones de diagnóstico y mantenimiento sobre los switches, incluyendo, pero no limitado a: actualización de firmware, reinicio de equipo, verificación de estado de los puertos, evaluación del cableado.
- Debe mostrar una vista topológica de la red donde se vea como se encuentran conectados los equipos entre sí.
- Debe permitir acceso vía CLI a los equipos desde la misma interfaz WebUI del controlador.
- Deberá poder recolectar los logs de todos los switches administrados.
- Detectar, identificar y mostrar los endpoint y dispositivos de red conectados
- Deberá poder bloquear tráfico intra-VLAN
- Deberá poder aplicar cuarentena a los hosts.
- Deberá poder habilitar funcionalidades de Control de Acceso a la Red (NAC), donde se puede asignar una VLAN por puerto en base a MAC Address, Vendor, OS y/o Usuario.
- Deberá poder identificar dispositivos IoT con licenciamiento habilitado.
- Deberá poder aplicar políticas por puertos del switch de manera dinámica.
- Desde la plataforma de gestión se podrán habilitar políticas de seguridad que consideren las siguientes protecciones:
    - Application Control

Funcionalidades de Capa 2 y Capa 3

- Deberá soportar detección y notificación de conflictos de direcciones IP.
- Deberá soportar Link Aggregation estático.
- Deberá soportar LACP.
- Deberá soportar Spanning Tree.
- Deberá soportar Jumbo Frames.
- Deberá soportar Auto-negociación para la velocidad de los puertos y para Duplex.
- Deberá soportar el estándar IEEE 802.1D MAC Bridging/STP.
- Deberá soportar el estándar IEEE 802.1w Rapid Spanning Tree Protocol (RSTP).
- Deberá soportar el estándar IEEE 802.1s Multiple Spanning Tree Protocol (MSTP).
- Deberá soportar la funcionalidad STP Root Guard.
- Deberá soportar STP BPDU Guard.
- Deberá soportar Edge Port / Port Fast.
- Debe soportar VRF o Multi-VPN Instance CE
- Deberá soportar el estandar IEEE 802.1Q VLAN Tagging.
- Deberá soportar Private VLAN
- Soportar PIM-SSM
- Deberá soportar el estándar IEEE 802.3ad Link Ag.gregation con LACP.

- Deberá soportar el estándar IEEE 802.1AX Link Aggregation.
- Deberá soportar el estándar IEEE 802.3x Flow Control con Back-pressure.
- Deberá soportar el estándar IEEE 802.3z 1000Base-SX/LX.
- Deberá contar con la funcionalidad de Control de Tormentas (Storm Control)
- Deberá soportar la creación de VLANs por MAC, IP y Ethertype-based o basado en protocolo.
- Deberá soportar 4094 VLANs simultáneas.
- Deberá soportar IGMP Snooping.
- Deberá soportar IGMP proxy y querier.
- Deberá permitir limitar la cantidad de MACs aprendidas por puerto.
- Deberá permitir un mínimo de 16 instancias de MSTP.
- Deberá permitir controlar tormentas de broadcast independientemente en cada puerto.
- Deberá soportar un mecanismo de detección y prevención de loops.
- Deberá soportar VLAN Stacking (QnQ) IEE 802.1ad.
- Deberá soportar VXLAN
- Protocolo de enrutamiento: PBR, VRRP, OSPFv2, OSPFv3, BGP y BGP4
- Deberá soportar Ethernet OAM (802.1ag): Connectivity Fault management
- Deberá soportar Ethernet Ring Protection v.2 (ERPv2)
- Deberá soportar SVLAN y CVLAN

Seguridad y Visibilidad

- Deberá soportar Port Mirroring
- Deberá soportar Admin Authentication Via RFC 2865 RADIUS.
- Deberá soportar el estándar IEEE 802.1x authentication Port-based.
- Deberá soportar el estándar IEEE 802.1x Authentication MAC-based.
- Deberá soportar el estándar IEEE 802.1x Guest and Fallback VLAN.
- Deberá soportar el estándar IEEE 802.1x Dynamic VLAN Assignment.
- Deberá soportar el estándar IEEE 802.1ab LLDP-MED.
- Deberá soportar Radius CoA (Change of Authority).
- Deberá soportar Radius Accounting.
- Deberá soportar detección de dispositivos. Se aceptará que esta función sea realizada por la consola de gestión centralizada.
- Deberá soportar sFlow.
- Deberá soportar Flow Export.
- Deberá soportar ACLs.
- Deberá soportar DHCP Snooping.
- Deberá permitir Dynamic ARP Inspection (DAI) o ARP Protection.
- Deberá permitir Access VLANs.
- Deberá soportar MACsec – 802.1ae

RFC

- Deberá soportar el RFC 2865 RADIUS.
- Deberá soportar el RFC 2572 SNMP Message Processing and Dispatching.
- Deberá soportar el RFC 1573 SNMP MIB II.
- Deberá soportar el RFC 1157 SNMPv1/v2c.
- Deberá soportar el RFC 2030 SNTP.
- Deberá tener certificación RoHS2 o RoHS, FCC, UL, CE y VCCI

Otras Funcionalidades

- Deberá soportar Syslog y Netflow o sFlow.
- Debe permitir monitorear la temperatura del dispositivo.
- Debe contar con un sensor de temperatura interno.
- Debe tener capacidad de apilamiento de al menos dos switches mediante stacking u otra tecnología o mecanismo provisto por el fabricante a través de un esquema activo - activo. El apilamiento debe permitir que ambos switches sean vistos como uno solo en la red.

SWITCHES PARA LA RED LAN HIPERCONVERGENTE Y CORE.

Se requiere 04 switches por cada site del CONTRATISTA.

Características Físicas

- 48 interfaces GE/10 GE SFP+
- 04 interfaces GE/100 QSFP

- 01 puerto USB
- 01 puerto de consola RJ45 o Serial
- Deberá ser de tipo non-blocking
- Deberá contar con un sistema de ventilación Front to back con al menos cuatro ventiladores
- Factor de forma de 1 RU como máximo
- Deberá tener doble fuente redundante de tipo Hot swap, intercambio en caliente sin necesidad de apagar el equipo.

Capacidades

- Capacidad de Switching (duplex): 2.1 Tbps como mínimo
- Paquetes por Segundo (Duplex): 1.600 Mbps como mínimo
- Max. direcciones MAC: 120 K como mínimo
- Packet Buffer: 30 MB o superior
- DRAM: 8 GB DDR3 o superior
- Min. ACLs soportadas: 1.5 K entradas como mínimo

SOFTWARE DE LA SOLUCIÓN VIRTUALIZACION

Descripción	Características técnicas mínimas
Licencias	- Deberá incluir las licencias de uso, a nivel del hipervisor y de las instancias virtuales por el periodo de tres (03) años, para todos los Nodos de Hiperconvergencia propuestos. - El licenciamiento debe ser del tipo OPEN u OEM.
Características del Software de Hiperconvergencia	- Deberá permitir virtualizar el almacenamiento local de los servidores x86, esto es que pueda entregar una SAN virtual en base a los discos locales de los servidores. - La solución debe de soportar la integración con LUNs de almacenamiento tradicional a través de protocolos NFS 3 y NFS 4.1. - La solución debe de soportar almacenamiento de primer nivel (Tier 1 o cache) del tipo NVMe. - La solución permitirá tener configuraciones de tipo RAID 1 y RAID 5. - La solución deberá soportar funcionalidades de deduplicación y compresión. - La solución soportará escalar hasta 60 nodos por clúster. - La solución permitirá la instalación de software de recuperación de terceros a nivel del hipervisor. - El almacenamiento ofrecido a las máquinas virtuales deberá ser de tipo SSD NVMe PCIe 4.0 para todos los Nodos de Hiperconvergencia. - El datastore presentado se debe componer únicamente con los discos de capacidad integrados dentro de los nodos de la solución HCI. - La interfaz de administración de la solución debe estar basado en una interfaz HTML 5.0 y debe de integrarse a la consola del software de administración de la Plataforma Virtual. - El software de virtualización (hipervisor) y administración del almacenamiento será de un solo fabricante. - La asignación de almacenamiento se debe de realizar mediante políticas como parte del panel de control de la solución de virtualización y centralizado a la máquina virtual. - La interfaz gráfica de administración de la solución se debe integrar con la herramienta de virtualización para la gestión y monitoreo de la asignación de almacenamiento y el comportamiento de este.
Características del Software Virtualización	- Deberá instalarse y ejecutarse directamente sobre los niveles más bajos de hardware de los equipos en modo “baremetal” sin necesidad de un sistema operativo anfitrión. - Deberá soportar sistemas operativos como Windows Server 2012 R2, Windows Server 2016, Windows Server 2019, Windows Server 2022 y Red Hat Enterprise Linux 6.x y 7.x. - Deberá permitir la sobresuscripción de la memoria física disponible a las máquinas virtuales, esto es, que la suma de la memoria asignada a las máquinas virtuales podrá ser mayor a la cantidad de memoria física. - Deberá eliminar páginas de memoria redundantes de manera que dos o más máquinas virtuales compartirán páginas de memoria idénticas entre ellas, evitando la necesidad de mantener copias redundantes.

	- Deberá de poder establecer un mínimo y máximo de recursos para CPU y memoria con la posibilidad de modificar esta asignación de recursos mientras las máquinas virtuales están en ejecución. - Deberá contar con un módulo para la administración e implementación de actualizaciones y parches de seguridad para el hipervisor, de manera que no interrumpa el funcionamiento y disponibilidad de las máquinas virtuales. - Deberá de brindar la posibilidad de integrarse a un agente que habilite transferir las cargas de trabajo del procesador relacionadas con la ejecución de plataformas de seguridad de terceros como antivirus y antispyware a un appliance virtual sin ejecutarse repetidamente dentro de las máquinas virtuales. - Deberá de tener la posibilidad de definir un perfil de referencia para todos los servidores físicos, de forma que se pueda obtener los valores de configuración de los servidores físicos y que los guarde en una plantilla para configurar otros servidores físicos. - Deberá de ofrecer la capacidad de crear grupos y perfiles de almacenamiento de acuerdo con políticas definidas por el usuario, para que la selección del almacenamiento para nuevas máquinas virtuales sea más rápida y eficiente - Deberá permitir el reinicio automatizado de servicios ante la detección de fallas. Esta prestación debe proveer un servicio de monitoreo de signos vitales que comprenda dos ámbitos principales: el primero es el elemento físico de procesamiento (servidores) y el segundo ámbito son los sistemas operativos en ejecución dentro de las máquinas virtuales. El requerimiento es que la infraestructura de virtualización debe detectar fallas en cualquiera de dichos ámbitos y ejecutar una acción correctiva de forma automática. - Deberá permitir balancear las cargas de trabajo de manera automática para conseguir un rendimiento óptimo. - Deberá permitir priorizar el almacenamiento y el acceso a la red mediante el monitoreo continuo de la carga de I/O de un volumen de almacenamiento y a través de la red, y asigna dinámicamente los recursos de I/O disponibles a las máquinas virtuales según sea necesario.
Características del Software de Administración de la Plataforma Virtual	- La Solución HCI debe de contar con un software de administración, a través de una sola consola, debe ofrecer administración centralizada para todos los servidores virtuales creados en los servidores físicos, automatización de las operaciones, optimización de recursos y alta disponibilidad a los entornos de TI. - Deberá incluir las licencias de uso para todos los Nodos de Hiperconvergencia solicitados, sin tener límite de Nodos a administrar. - Administrar y configurar todas las características de escalabilidad, disponibilidad, seguridad y efectuar mantenimiento no disruptivo del entorno virtual de manera centralizada. - Obtener Inventarios del ambiente virtual incluyendo máquinas virtuales, hipervisores, almacenamiento y redes virtuales. - El aprovisionamiento rápido con un asistente de implementación de plantillas de máquinas virtuales para crear e implementar máquinas virtuales. - Monitorización de rendimiento, incluidos gráficos de utilización de la CPU, memoria, I/O de discos y de red, para analizar el rendimiento de las máquinas virtuales que están ejecutando. - El control de acceso seguro, con sólidos mecanismos de permisos que garanticen el acceso autorizado al entorno y a sus máquinas virtuales, para la delegación de responsabilidades con la posibilidad de crear diferentes roles con diferentes derechos de administración, incluso a nivel de máquina virtual. - Debe contar con la capacidad de Single-Sign-On. - Debe contar con la opción de instalar y exportar máquinas virtuales o virtual appliances en Open Virtual Machine Format (OVF). - Definir alarmas para los estados de los diferentes recursos físicos y máquinas virtuales para manejar y prevenir problemas. Las alarmas activadas deben generar notificaciones y alertas automatizadas. - Programar la ejecución automática de tareas de administración del sistema, tales como envío de mensajes SNMP, envío de correos electrónicos, ejecución de scripts de administración, suspensión, apagado y reinicio de las máquinas virtuales.

	- Deberá poder graficar la topología del hardware HCI, mostrar el inventario de hardware y dar visibilidad del sistema para monitorear el estado, la capacidad y el rendimiento de los recursos.
Replicación	- El software de virtualización deberá de replicar las máquinas virtuales de un site a otro sin la necesidad de un software de terceros la cual deberá ser de forma automática y transparente

COMPONENTE DE BACKUP - SOFTWARE DE BACKUP DEL ENTORNO VIRTUAL EN DISCO (ALTERNO).

- La solución deberá incluir funcionalidades de respaldo (backup) y replicaciones integradas en una única solución; incluyendo vuelta atrás (rollback) de réplicas y replicación desde y hacia la infraestructura virtualizada.
- La administración de toda la solución ofertada será compartida las cuales deberán de ser diferenciadas por usuarios para la entidad y el contratista. La responsabilidad el contratista no comprende las acciones efectuadas por los usuarios asignados a la entidad
- La solución no deberá necesitar de la instalación de agentes en el ambiente o máquinas virtuales para poder realizar sus tareas de respaldo, recuperación granular y replicación de máquinas virtuales.
- La solución no debe necesitar agentes para la recuperación granular de aplicaciones y archivos de los sistemas respaldados.
- Deberá poder realizar respaldos sin detener las máquinas virtuales, y sin generar una merma en su performance, facilitando las tareas de respaldo (backup) y migraciones en conjunto.
- Deberá ser capaz de comprender las máquinas virtuales como objetos del entorno virtual y respaldar las configuraciones de estas, al margen de los datos propios de las máquinas.
- Deberá ser capaz de respaldar de forma indistinta una máquina virtual completa o discos virtuales específicos de una máquina virtual.
- Deberá proveer una herramienta de gestión de archivos para los administradores de máquinas virtuales en la consola del operador.
- Deberá ser una solución altamente eficaz y preparada para el futuro integrándose en forma extensiva, con las APIs de los fabricantes de infraestructura virtualizada, para la protección de datos.
- Deberá poder realizar respaldos (backup) incrementales ultra rápidos aprovechando la tecnología de seguimiento de bloques de disco modificados (changed block tracking) reduciendo al mínimo el tiempo de respaldo (backup) y posibilitando un respaldo (backup) y una replicación más frecuente. De este modo logrando lo establecido respecto de la merma de performance.
- La solución deberá ofrecer múltiples estrategias y opciones de transporte de datos para las tareas de respaldo (backup) a saber:
    - Directamente a través de Storage Area Network (SAN).
    - Directamente desde el storage a través del Hypervisor I/O (Virtual Appliance).
    - Mediante el uso de la red local (LAN).
    - Directamente de instantánea, con al menos un fabricante de sistemas de almacenamiento.
    - Directamente desde el repositorio NFS (Datastore NFS)
- Deberá proporcionar un control centralizado del despliegue distribuido, para esto deberá incluir una consola web que provea una vista consolidada de su despliegue distribuido y federación de múltiples servidores de respaldo (backup), informes centralizados, alertas consolidadas y restauración de auto servicio de máquinas virtuales y a nivel de sistema de archivos (granular), con asignación de permisos sobre máquinas virtuales individuales, y detección automática de permisos sobre máquinas virtuales acorde al perfil del usuario en la infraestructura virtual.
- Deberá poder mantener un respaldo (backup) completo sintético eliminando así la necesidad de realizar respaldo (backup) completos (full) periódicos ya que proporcionará un respaldo (backup) incremental permanente con lo que se permita ahorrar tiempo y espacio.
- Deberá contar con la tecnología de deduplicación para lograr un ahorro de espacio de almacenamiento para los respaldos (backup).
- Deberá proporcionar protección casi continúa de datos (near-CDP), que permita la reducción de los puntos objetivos de recuperación (RPO) sean mínimos.
- Deberá proveer una estrategia de recuperación rápida que permita proveer/devolver el servicio a los usuarios casi inmediatamente y en forma sencilla. Dicha estrategia debe consistir en el inicio y encendido de la máquina virtual, que haya fallado, directamente desde el archivo de respaldo (backup) en el almacenamiento habitual del respaldo (backup).

- La recuperación instantánea de las máquinas virtuales deberá permitir más de una máquina virtual y/o punto de restauración en simultáneo para la disponibilidad del punto de recuperación funcional, permitiendo así, tener múltiples puntos en el tiempo de una o más máquinas virtuales funcionando.
- Posterior a una recuperación rápida, se deberá poder realizar una restauración total sin interrupciones del servicio. La herramienta debe asegurar que el trabajo realizado por los usuarios no estará afecto al migrar sus máquinas virtuales desde el respaldo (backup) hasta el almacenamiento de producción, sin imponer una restricción de tiempo en la ejecución de la maquina durante el proceso de recuperación instantánea.
- Se deberá proveer la capacidad realizar restauraciones completas del respaldo (backup) de cualquier máquina virtual dentro de una ventana de mantenimiento mínima, permitiendo completar los procesos de recuperación en interrupciones del servicio más cortas y menos frecuentes. La estrategia deber consistir en replicar o realizar una copia en caliente del respaldo (backup) de la máquina virtual que se encuentra en un almacenamiento deduplicado al almacenamiento en producción donde la máquina virtual ejecuta. Adicionalmente deberá poder transferir desde este estado de recuperación mediante más de un método tecnológico.
- Deberá poseer una opción de recuperación instantánea de archivos que se encuentren dentro de los respaldos (backup) y replicaciones de las máquinas virtuales. Lo que debe permitir acceder a los contenidos de los discos virtuales de dichas máquinas sin necesidad de recuperar el respaldo (backup) completo y reiniciar desde el mismo la máquina virtual.
- Deberá incluir un asistente para la recuperación instantánea a nivel de archivos en los sistemas de archivos más utilizados de Windows, Linux, Solaris, BSD o MacOS (Por lo menos 15 de ellos).
- Deberá poder crear un índice (catálogo) de todos los archivos que sean manejados por el sistema operativo Windows y Linux, sin agente, cuando este sea el sistema operativo que ejecute dentro de una máquina virtual del que se ha realizado un respaldo (backup).
- Deberá poder realizar búsquedas rápidas mediante índices de los archivos que sean manejados por un sistema operativo Windows, cuando este sea el sistema operativo que ejecute dentro de una máquina virtual del que se ha realizado un respaldo (backup).
- Deberá asegurar la consistencia de aplicaciones transaccionales en forma automática por medio de la Integración con Microsoft VSS, dentro de sistemas operativos Windows.
- Deberá poder realizar el truncado y respaldo de las bitácoras transaccionales (Transaction logs) para máquinas virtuales con Microsoft Exchange, SQL Server, Oracle sin el uso de agentes.
- Deberá poder realizar notificaciones por correo, SNMP o a través de los atributos de la máquina virtual del resultado de la ejecución de sus trabajos.
- Se deberá poder recuperar a nivel de objetos de cualquier aplicación virtualizada, en cualquier sistema operativo, utilizando las herramientas de gestión de aplicaciones existentes.
- Deberá incluir herramientas de fácil recuperación guiada, mediante la cual los administradores de servidores de correo, tales como Microsoft Exchange versión 2007, 2010, 2013, 2016 y 2019 puedan recuperar objetos individuales, tales como correos electrónicos y contactos, sin necesidad de recuperar los archivos de la máquina virtual como un todo y reiniciar la misma. Sin requerir infraestructura intermedia (“Staging”)
- Deberá incluir herramientas de fácil recuperación guiada mediante el cual los administradores de servidores de servicio de directorio, tales como, Microsoft Active Directory, pueden utilizar para recuperar objetos individuales, tales como usuarios, grupos, directivas de grupos (GPO), registros de DNS, particiones de configuración. Sin necesidad de recuperar los archivos de la máquina virtual como un todo y reiniciar la misma.
- Deberá incluir herramientas de fácil recuperación guiada mediante el cual los administradores de servidores de bases de datos Microsoft SQL Server, puedan recuperar objetos individuales, tales como tablas y registros. Sin necesidad de recuperar los archivos de la máquina virtual como un todo y reiniciar la misma.
- Deberá incluir herramientas de fácil recuperación guiada mediante el cual los administradores de servidores de bases de datos Oracle, puedan recuperar base de datos. Sin necesidad de recuperar los archivos de la máquina virtual como un todo y reiniciar la misma.
- Deberá ofrecer visibilidad instantánea, capacidades avanzadas de búsqueda y recuperación rápida de elementos individuales para Sharepoint 2010, 2013, 2016 y 2019 sin la utilización de agentes.
- Deberá poder ofrecer confiabilidad en un 100% en el inicio correcto de todas sus máquinas virtuales respaldadas y en el funcionamiento del rol que cumple dichas máquinas virtuales (DNS Server, Domain Controller, Mail Server, SQL Server, Oracle, etc) al momento de la recuperación, al poder realizar pruebas de recuperabilidad automatizadamente de las máquinas respaldadas.

- Deberá poder crear una copia de trabajo del entorno de producción de cualquier estado anterior para la resolución de problemas, pruebas de procedimientos, capacitación, etc. ejecutando una o varias máquinas virtuales desde el archivo de respaldo (backup) en un entorno aislado, sin necesidad de más espacio de almacenamiento y sin modificar el respaldo (backup).
- La solución debe permitir realizar la migración de máquinas virtuales entre clusters y datacenters de VMware vSphere.
- La solución debe monitorear el espacio libre de las LUN's y en caso de no existir el espacio necesario no debe realizar el snapshot en el ambiente virtual.
- Deberá ofrecer capacidad de recuperación granular de aplicaciones Directorio Activo, SQL Server, Exchange Server, Sharepoint, Oracle y de archivos de sistemas operativos desde instantáneas de SAN de los siguientes fabricantes:
    - HPE (HP StoreVirtual VSA, LeftHand/P4000 y StoreServ 3PAR)
    - EMC (VNX, VNX2, VNXe).
    - Netapp (FAS, FlexArray (V-Series), Edge VSA and IBM N Series (NetApp FAS OEM))
- Deberá ofrecer el archivado en cinta, soportando VTL (Virtual Tape Libraries), biblioteca de cintas y drives independientes.
- Deberá ofrecer Trabajos de Copia de Backup con implementación de políticas de retención. Con el objetivo de mantener una copia o replica de los archivos de respaldo en caso de desastre.
- Deberá incluir un Plug-in VMware para vSphere Web Client y poder monitorear la infraestructura de backup directamente desde el vSphere Web Client, con vistas detalladas y generales del estado de los trabajos y recursos de backup.
- La solución debe tener un mecanismo de recuperación de emergencia de los respaldos cifrados por contraseña en caso de pérdida o extravío de la contraseña, pudiendo ser recuperada con una contraseña maestra generada vía Web.
- La solución debe tener un mecanismo de búsqueda global de archivo entre los respaldos
- Deberá soportar las últimas versiones disponibles de los hipervisores más populares de mercado a la fecha: VMWare vSphere y Microsoft Hyper-V en todas las versiones soportadas por el fabricante respectivo.
- No deberá requerir hardware específico para alcanzar la de-duplicación y compresión de la información fuera de los requerimientos estándar de cualquier software, y específicos para el caso.
- No deberá requerir licencias independientes para las actividades de respaldo, recuperación y replicación.
- Deberá permitir la recuperación granular sin necesidad de montar ambientes temporales para:
    - Microsoft Active Directory 2008 R2 en adelante.
    - Microsoft Exchange Server 2010 en adelante.
    - Microsoft SQL Server 2005 en adelante.
    - Oracle Database 11.x y superior para Windows / Linux.
    - Microsoft Sharepoint 2010 en adelante.
- Deberá ofrecer aceleración de enlaces WAN para la réplica de máquinas virtuales en alguna de sus versiones.
- Deberá ser capaz de realizar replicas en otros sitios o infraestructuras desde los respaldos realizados.
- Deberá presentar un método fácil de recuperación hacia ambientes de contingencia, con las acciones pre-configuradas para evitar acciones manuales en caso de desastre, similar a un botón de emergencia.
- Deberá ofrecer la posibilidad de almacenar los respaldos de forma cifrada, así como asegurar el tránsito de la información bajo este esquema desde el archivo de respaldo, sin requerir cifrado desde el sistema de almacenamiento.
- Deberá disponer de funcionalidades integradas que permitan la selección de un destino de almacenamiento de respaldos que pueda estar alojado en un CONTRATISTA de servicios en la nube (BaaS).
- Deberá disponer de funcionalidades integradas que permitan la selección de un destino de replica que pueda estar alojado en un CONTRATISTA de servicios en la nube (DRaaS).
- Deberá disponer la funcionalidad de generar un almacenamiento de backup global, el cual puede incluir varios y distintos tipos de Storage, y apuntar los trabajos de backup al mismo como si fuese uno, permitiendo también el crecimiento a gran escala del mismo sin impacto sobre el ambiente de backup ya configurado.
- Integración con hardware de deduplicación EMC Data Domain, HP StoreOnce, Quantum DXi y ExaGrid, así como optimizaciones para el uso de cualquier sistema de almacenamiento deduplicado.

- Integración con plataformas de deduplicación en origen EMC DataDomain Boost y HP StoreOnce Catalyst y Quantum Accent.
- Poseer un único número de parte, según la versión o edición, provisto por el fabricante para la adquisición del paquete de software que incluya todas las funcionalidades arriba mencionadas.
- Capacidad de definir grupos de cintas magnéticas para ser utilizadas en una misma sesión de almacenamiento a cinta (Media Pool) para maximizar el rendimiento y velocidad de transferencia.
- La solución debe respaldar los archivos en cinta deduplicados, consiguiendo mayor eficiencia del espacio en cintas.
- Capacidad de procesar el envío de datos en múltiples unidades de cinta en paralelo para maximizar el ancho de banda y minimizar el tiempo de transferencia.
- Capacidad de procesar múltiples trabajos de envío a cinta en paralelo hacia múltiples unidades de cinta.
- Capacidad de desacoplar el rol del servidor de la infraestructura de solución que permita el acceso a las unidades de cinta, evitando la necesidad que este rol se solape con otros roles de la solución.
- Capacidad de lectura directa desde el sistema central de almacenamiento, cuando en un entorno de infraestructura VMWare, este se encuentre presentado a través de protocolo NFS, evitando así, el paso de la información a través de las interfaces de control del hipervisor.
- Poder diferenciar, en máquinas virtuales Windows, aquellos bloques de disco que contengan datos irrelevantes (Dirty Blocks), y evitar su transferencia hacia los respaldos, así como la exclusión arbitraria de archivos dentro de máquinas virtuales Windows.
- La solución debe proveer mecanismos de protección para prevenir la sobre-exigencia sobre los sistemas de almacenamientos de la plataforma virtual, mediante el monitoreo proactivo de la latencia de los datastores, permitiendo la auto-regulación del sistema de respaldos y replicación en función de dichos umbrales definidos.
- Capacidad de diferenciar por unidad lógica o LUN y definir umbrales diferenciados para cada uno de ellos.
- Capacidad de migrar máquinas virtuales entre hipervisores que no estén conectados entre sí por un mismo clúster o controlador de gestión de entorno virtual (vCenter o SCVMM).
- Capacidad de aprovechar el subsistema Changed Block Tracking en el ambiente virtual, también para operaciones de vuelta atrás (failback) acelerando la transferencia de datos al centro de datos productivo.
- Soporte para respaldos nativos (integrados) en VMWare Cloud on AWS.
- Integración con almacenamiento de objetos como Amazon S3, Azure Blob Storage, IBM Cloud Object Storage como también con números CONTRATISTAS de servicios compatibles con el protocolo S3 y almacenamiento local compatible con protocolo S3.
- Realizar archiving de respaldos más antiguos hacia almacenamiento de objeto.
- Eficiencia en la utilización del ancho de banda al integrarse con almacenamiento en nube publica permitiendo recuperar de forma granular datos desde los bloques del archivo de respaldo, ahorrando significativamente el costo de la operación en ancho de banda.
- Al integrarse con almacenamiento en nube publica (Punto 81) debe ser autosuficiente y no dependiente de cualquier catalogo externo, permitiendo en caso de desastre la recuperación completa desde los archivos almacenados en nube pública.
- La solución debe permitir en el futuro realizar recuperaciones en cualquier punto del tiempo sin requerir una licencia pagada. Es decir, puede usar la versión gratuita del producto para esos fines.
- La solución debe permitir el cumplimiento de estándares como GDPR para la eliminación de datos o registros de forma automatizada utilizando scripts (realizados por el cliente) dentro de los archivos de respaldo antes de restaurar una máquina virtual al ambiente productivo. Como también, permitir a los administradores realizar cambios en el sistema operativo, instalación o remoción de aplicaciones para cumplir con el cumplimiento corporativo cuando se restaure una máquina virtual.
- La solución debe integrarse con distintos Antivirus para realizar análisis de antivirus sobre los respaldos existentes en la plataforma, por ejemplo, respaldos anteriores de la misma solución, análisis antes de realizar una recuperación instantánea o completa de la máquina virtual. Como también integrarse en el mecanismo de prueba automatizado de las máquinas virtuales y/o del contenido de la máquina virtual, para realizar proactivamente análisis de antivirus.
- La solución debe identificar y excluir automáticamente las máquinas virtuales que cuenten con la característica “Multi-Writer” habilitada.
- Soporte para las plataformas de servidores Microsoft Windows Server 2019.
- La solución debe permitir publicar las bases de datos de servidores SQL soportados por la plataforma de forma granular directo hacia una instancia.

- Capacidad de recuperación de VMs y Respaldos de máquinas físicas con agentes de la plataforma (realizando la conversión automática de UEFI a BIOS en AWS) de forma directa a Amazon o Azure.
- La solución debe permitir cambiar los tipos de discos (Thin a Thick por ejemplo) cuando se requiera realizar replica de máquinas virtuales.
- La solución también debe permitir recuperar solo los bloques de discos de la máquina virtual que hayan cambiado utilizando CBT.

AGENTES PARA LINUX

- Permitir la integración de agentes para entornos de nube o entornos físicos de plataformas Windows o Linux, para consolidar la visualización de ejecución de trabajos de respaldo desde la consola centralizada.
- Instalación, configuración y gestión de agentes de respaldo para equipos físicos Linux o Windows de forma centralizada.
- Instalación remota de agentes, sin necesidad de realizar ingreso interactivo en los equipos a instalar.
- Debe permitir la protección de datos en ambientes físicos o cloud basados en Sistema Operativo Linux. Deberá tener la capacidad de realizar respaldo, como mínimo, para las siguientes plataformas 32 y 64 bits:
  a. Debian 6 – 9.4.
  b. Ubuntu 10.04 – 18.04.
  c. CentOS / RHEL 6.0 – 7.6.
  d. Oracle Linux 6 (desde UEK R1) – Oracle Linux (desde UEK R4 U7).
  e. Oracle 6 – 7.6 (RHCK).
  f. Fedora 23 – 29, 42.0 – 42.1, Tumbleweed.
  g. open SUSE 11.3 – 13.2
  h. open SUSE Leap 42.2 – 42.3, Leap 15
  i. SLES 11 SP4 – 15 (SP0)
  j. SLES for SAP 11 SP4 – 15 (SP0)
- Deberá permitir los siguientes tipos de respaldo:
  a. Computador/servidor completo
  b. A nivel de volumen específicos (volúmenes simples o LVM)
  c. A nivel de archivos o carpetas.
- Deberá permitir la ejecución de scripts previos al inicio del trabajo de respaldo y posterior a la finalización del trabajo.
- Deberá permitir la ejecución de scripts previos a la generación del snapshot correspondiente al trabajo de respaldo y posterior a la generación del snapshot.
- Deberá permitir la realización de respaldo sin snapshot del sistema operativo con la finalidad de respaldar archivos desde cualquier sistema de archivos montado en el servidor.
- Deberá permitir la creación de índice de archivos y carpetas durante el respaldo, permitiendo la búsqueda de archivos en la imagen de respaldo.
- Deberá ofrecer los siguientes tipos de repositorios de respaldo:
  - Discos locales.
  - DAS (“Direct Attached Storage”)
  - NAS (“Network Attached Storage”)
  - Repositorios manejados por Servidor de Backup Centralizado.
  - Repositorios de CONTRATISTAS de servicio de nube.
- Deberá ofrecer soporte para respaldo y recuperación de los siguientes tipos de Sistema de Archivos: Btrfs (para S.O que usan kernel 3.16 o superior), Ext 2/3/4, F2FS, FAT16, FAT32, HFS, HFS+, HFSP, JFS, NILFS2, NTFS, ReiserFS, XFS.
- Deberá permitir la programación de los trabajos de respaldos a través de una única consola, incluyendo:
  - Permitir la ejecución de procesos de respaldos según políticas a ser definidas (frecuencia, retención, tipo de respaldo full o incremental).
  - Permitir definir la periocidad de los trabajos.
  - Permitir programar los trabajos para una ejecución de forma automatizada.
- Deberá proveer consola de monitoreo via interfaz gráfica con visibilidad a los trabajos en tiempo real a su ejecución.
- Deberá proveer archivos de logs para la verificación/análisis de los trabajos.
- Deberá poseer el manejo centralizado de trabajos de respaldo y recuperación via interfaz gráfica (GUI) y por la línea de comando (CLI).
- Deberá permitir realizar recuperaciones a nivel de volumen para su ubicación original o hacia una nueva ubicación.
- Deberá permitir realizar recuperaciones a nivel de archivos o carpetas.
- Deberá permitir realizar una recuperación completa ante desastres desde el backup hacia mismo hardware o similares, también llamado “Bare-Metal Restore”.

- Deberá permitir la creación de una Imagen de Recuperación, tanto para la recuperación de datos desde el respaldo, como para la ejecución de herramientas Linux de diagnóstico de problemas y corrección de errores.
- Deberá permitir la replicación de los respaldos desde Repositorio Primario hacia Repositorio Secundario.
- Deberá permitir el archivado de respaldos en Dispositivos de cinta Independientes, Librerías Virtuales o Librerías Físicas, LTO3 o superiores a través de la consola centralizada
- Deberá ofrecer la posibilidad de convertir discos en el respaldo hacia formatos de discos virtuales vmdk, vhd o vhdx.
- Deberá tener la capacidad de cifrar los respaldos, utilizando algoritmos más comunes del mercado, soportando utilización de llaves de por lo menos 256 bits.
- Deberá permitir la posibilidad de realizar el cifrado en el procesamiento de los datos, en el tráfico via red o en el repositorio de respaldo.
- Deberá ofrecer la recuperación desde el respaldo del computador/servidor físico, iniciando el computador/servidor en el repositorio, y publicando el mismo directamente en el hypervisor de Hyper-V, permitiendo luego la migración al Hyper-V en línea y sin parada en el servicio.
- Deberá ofrecer la opción de recuperación de archivos, carpetas, etc directamente desde el respaldo sin la necesidad de recuperar completamente el respaldo en AES256 o Blowfish.
- El agente deberá soportar procesamiento Oracle para realizar respaldos consistentes de la base de datos y archive logs de soluciones no clusterizadas como RAC, ASM y soportando las últimas versiones oficiales de Oracle.
- Soporte para respaldos Full en el día deseado de la maquina física Linux.
- Deberá permitir la recuperación a la nube de Microsoft Azure y Amazon a través de la consola centralizada.

AGENTES PARA WINDOWS

- La plataforma debe permitir la protección de datos en computadoras/servidores basados en Sistema Operativo Microsoft Windows. Deberá dar la capacidad de realizar respaldo, como mínimo, para las siguientes plataformas x86-64 bits:
    - Microsoft Windows 7 SP1.
    - Microsoft Windows 8.x.
    - Microsoft Windows 10.
    - Microsoft Windows 10 Actualización de Octubre.
    - Microsoft Windows Server 2008 R2 SP1.
    - Microsoft Windows Server 2012.
    - Microsoft Windows Server 2012 R2.
    - Microsoft Windows Server 2016 y Windows Server version 1803.
    - Microsoft Windows Server 2019
- Deberá ofrecer soporte para Microsoft Bitlocker, para el respaldo y recuperación.
- Deberá ofrecer la posibilidad de respaldar el computador/servidor completo, volúmenes individuales o archivos/carpetas específicas.
- La solución debe tener un controlador CBT (Changed Block tracking) para los ambientes físicos con el objetivo de realizar respaldos incrementales de manera eficiente y rápida.
- Deberá permitir el manejo centralizado de los respaldos y recuperaciones vía interfaz gráfica (GUI) y línea de comando (CLI).
- Permitir el respaldo de archivos abiertos, garantizando la integridad del respaldo.
- Deberá ofrecer mecanismo propio de seguimiento de bloques modificados para una detección rápida de bloques a respaldar.
- Deberá permitir como destino de los respaldos:
    - Disco local.
    - Carpeta compartida de red.
    - Repositorio de disco centralizado de la plataforma de respaldo.
    - Repositorio de disco de CONTRATISTA de servicio certificado.
    - Microsoft OneDrive
- Deberá permitir el uso de discos rotativos como destino de los respaldos.
- Deberá poseer mecanismo de caché que permita continuar con el respaldo aún si el computador/servidor remoto se encuentra temporalmente sin conectividad contra el servidor central de respaldo.
- Deberá poseer integración con Microsoft VSS con el fin de respaldar y asegurar la consistencia transaccional de aplicaciones en el respaldo.
- Deberá permitir la ejecución de scripts previos a la generación del “VSS snapshot” y la ejecución de scripts posterior a generación del “VSS snapshot”.
- Deberá permitir la creación de una Imagen de Recuperación permitiendo:
    - La restauración de la computadora/servidor de forma completa ante evento de desastre hacia hardware similar u original, también llamado “Bare-metal restore”.

    - Ejecutar tareas de diagnóstico de memoria.
    - Ejecutar reparaciones de inicialización.
    - Blanquear contraseña de Administrador local para computadores/servidores fuera del dominio.
- Deberá tener la capacidad de cifrar los respaldos, utilizando los algoritmos más comunes en el mercado, soportando la utilización de llave de, por lo menos, 256 bits.
- Debe permitir elegir si el encriptado será realizado en el proceso de los datos, en el tráfico de datos via red o en el repositorio de respaldo.
- Deberá poder inicializar el computador/servidor completo desde el repositorio de backup (sin transferencia de datos) publicando directamente hacia el Hypervisor Hyper-V como máquina virtual, permitiendo proveer el servicio de forma rápida.
- Deberá permitir transferir el computador/servidor inicializado desde el repositorio de backup hasta el almacenamiento productivo, sin afectar la disponibilidad y el acceso de los usuarios.
- Deberá permitir la recuperación granular de archivos, carpetas, etc; directamente desde el repositorio de respaldo sin necesidad de recuperar el respaldo completo.
- Deberá permitir la recuperación a la nube de Microsoft Azure y Amazon a través de la consola centralizada.
- Deberá permitir la recuperación a nivel de volúmenes.
- Deberá permitir redimensionar volúmenes durante recuperación a nivel de volúmenes.
- Deberá permitir la conversión de respaldos a nivel de volúmenes como discos virtuales de los siguientes formatos: vmdk, vhd y vhdx.
- Deberá permitir el manejo centralizado de los respaldos y recuperaciones via interfaz gráfica (GUI) y línea de comando (CLI).
- Deberá permitir la programación agendada de los respaldos de computadores/servidores a través de interfaz única ofreciendo:
    - La ejecución de procesos de respaldo según políticas a ser definidas (frecuencia, retención, tipo de respaldo).
    - La definición de prioridad de ejecución de los respaldos.
    - La Programación de los trabajos de respaldos automatizadas.
- Permitir el monitoreo via interfaz gráfica y en tiempo real de los trabajos, generando archivo de logs.
- Deberá hacer uso de Base de Datos para el guardado del catálogo de los trabajos, archivos y dispositivos de respaldo.
- Deberá incluir herramientas de recuperación granular para Microsoft Exchange 2010 SP1 y superiores, de forma tal que sea posible recuperar objetos individuales como contactos, mensajes, ítems de agenda, adjuntos, etc directo a producción. Sin necesidad de recuperar la base de datos de MS Exchange.
- Deberá incluir herramientas de recuperación granular para Microsoft Active Directory 2008 R2 SP1 y superior, de forma tal que sea posible recuperar objetos individuales como usuarios, grupos, contenedores, cuentas, objetos de Política de Grupo (GPOs), registros MS DNS, etc directo a producción. Sin la necesidad de recuperar la base de AD.
- Deberá incluir herramientas de recuperación granular para MS SQL Server 2005 SP4 y superior, de forma tal que sea posible recuperar objetos individuales tal como Bases de Datos, Tablas, Registros, Store Procedure, Vistas, Funciones, etc directo a producción. Sin necesidad de recuperar la base de SQL.
- Deberá ofrecer el soporte para Microsoft Failover Cluster, incluyendo SQL Server failover clúster y SQL Server AlwaysOn Availability Groups.
- Deberá incluir herramientas de recuperación granular para MS SharePoint 2010 y superiores, de forma tal que sea posible recuperar sites, documentos, adjuntos, etc. directo a producción. Sin necesidad de recuperar la base de SharePoint.
- Deberá incluir herramienta de recuperación de Base de Datos Oracle 11.x y 12.x directo a producción.
- Deberá permitir realizar el truncado de logs transaccionales para MS Exchange, SQL y truncado de archive log para el caso de Oracle 11.x y 12.x.
- Deberá permitir realizar el respaldo de logs transaccionales para MS SQL y de archive log para el caso de Oracle 11.x y 12.x.
- Deberá permitir la réplica de los respaldos desde repositorio principal hacia repositorio secundario administrado desde interfaz gráfica central.
- Deberá permitir la copia de respaldos a dispositivos de cinta administrado desde interfaz gráfica central.
- Deberá permitir la importación de respaldos realizados por la solución.
- Deberá poseer herramienta que provea interface por línea de comando para realizar tareas de protección de datos y operaciones administrativas, crear scripts o integrar con terceras soluciones.
- Soporte de múltiples tareas de respaldo.
- Respaldo de Discos (HDD o SSD) USB.

- La solución debe tener la capacidad de configurar el ancho de banda a utilizar para la realización de los respaldos.
- La solución debe también restringir las vías de comunicación del agente de respaldo, es decir, restringir por conexión VPN, Restringir por conexión WIFI y/o por redes con mediciones.
- El agente para Windows debe soportar Microsoft Exchange DAG incluyendo IPless DAG, como también las últimas versiones de Exchange Server y Sharepoint.
- Los agentes deben soportar la administración centralizada desde la consola de la plataforma de respaldo como también sin administración.
- La plataforma debe soportar la recuperación de archivos granulares a través de un portal de autoservicio via web.

SERVIDOR DE COPIAS DE SEGURIDAD

Se requiere un (01) servidor de copias de seguridad, éste deberá tener como mínimo:

- 02 procesadores de 24 cores c/u.
- 128 GB de RAM
- 02 discos SSD de 800 GB como mínimo para sistema operativo.
- 50 TB como efectivos en raid 5
- 01 interface SAS o F.O. para interconectar con librería de backup
- Deberá tener una altura máxima de 2RU (Unidad de rack)
- Deberá ser de montado en rack (raqueable).
- La conexión de red deberá ser redundante a 10GbE
- Las fuentes de poder deberán ser a 220V/60Hz y redundantes.
- Deberá incluir todos los cables, elementos de conectividad y red y accesorios necesarios para conectarse a la solución propuesta, incluyendo PDU. Y todo lo necesario para conectarse a la infraestructura de red existente.

DOS LICENCIAS DE BASE DE DATOS ESTÁNDAR PARA LAS INSTANCIAS VIRTUALES.

El tipo de Licenciamiento requerido será por núcleo, donde esta licencia permite a una cantidad ilimitada de usuarios acceder al software del servidor instalado en el servidor con un determinado número de núcleos físicos para productos con licencia a través del modelo por núcleo.
La edición requerida es para el licenciamiento estándar la cual debe tener las siguientes características:

- Compatibilidad con Server Core
- Trasvase de registros
- Creación de reflejo de la base de datos
- Compresión de copia de seguridad
- Instantáneas de base de datos
- Instancias de clúster de conmutación por error de AlwaysOn
- Grupos de disponibilidad Always
- Grupos de disponibilidad básica
- Grupos de disponibilidad contenidos
- Grupos de disponibilidad distribuidos
- Reenrutamiento de la conexión de lectura y escritura automática
- Restauración de archivos y páginas en línea
- Creación y recompilación del índice en línea
- Recompilaciones de índices en línea reanudables
- ADD CONSTRAINT en línea reanudable
- Cambio de esquema en línea
- Recuperación rápida y acelerada de bases de datos
- Copias de seguridad reflejadas
- Agregar memoria y CPU sin interrupción
- Asistente para la recuperación de base de datos
- Copia de seguridad cifrada
- Copia de seguridad y restauración en el almacenamiento de objetos compatible con S3 a través de la API REST
- Copia de seguridad de instantáneas
- Grupo de disponibilidad sin clúster
- Conmutación por error para recuperación ante desastres
- Conmutación por error para alta disponibilidad.
- Deberá admitir hasta 524 petabytes, pero también puede soportar la cantidad máxima de RAM y el número de procesadores de núcleo que ofrece el sistema anfitrión.

- El CONTRATISTA deberá de brindar cinco 05 horas de configuración por mes no acumulables para la administración del software de Base de datos.

- El CONTRATISTA deberá de entregar un software para el monitoreo de la base de datos ante cualquier eventualidad, cabe resaltar que tanto El CONTRATISTA como LA ENTIDAD tendrá usuarios diferentes para acceder al software solicitado.
- El CONTRATISTA deberá de encargarse de la migración de las bases de datos con la que cuenta la ENTIDAD.
- El CONTRATISTA deberá de encargarse de instalar y configurar los servidores para las bases de datos solicitadas por la ENTIDAD.

LIBRERÍA DE BACKUP PARA EL ENTORNO VIRTUAL EN CINTA.

DESCRIPCIÓN	REQUERIMIENTO
Tecnología	Tape Autoloader
Drives	LTO-9 Ultrium SAS Drive Upgrade Kit como mínimo.
Capacidad	18 TB Capacidad Nativa. (2.5:1 ratio)
Transferencia	3.6 TB/hr (1x LTO-9)
Numero de slot para cartuchos	8 como mínimo
Máximo de driver	2
Encriptación	AES 256-bit: LTO-8, LTO-7, LTO-6, LTO-5
Factor de forma	1 U
Dimensiones	4.4 x 48.2 x 80.9 cm
Instalación	Instalación y puesta en marcha realizada por el fabricante del equipo o su representante autorizado.
Garantía y Soporte	(03) años 24x7 con 4 horas de tiempo de respuesta
Cintas tape backup	Todas las cintas tapes backup deberán ser suministradas y almacenadas por el CONTRATISTA durante el periodo de contratación. Cabe resaltar que al finalizar el contrato las cintas tape backup deben ser entregadas a la ENTIDAD

- **ATENCIÓN DE AVERÍAS, SOPORTE TECNICO Y MANTENIMIENTO**
  - El servicio de averías remoto deberá de tener un tiempo de atención no mayor de 30 minutos.
  - El servicio de averías presencial deberá tener un tiempo de atención no mayor a 24 horas.
  - Ante un problema o incidente comunicado por el PNPAIS, al CONTRATISTA, el tiempo de respuesta para iniciar la atención de la solución de la incidencia será no mayor a 15 minutos inmediatamente después de generado el ticket.
  - Toda actividad o provisión de bienes que tenga que ejecutar el CONTRATISTA para subsanar la avería de un equipo será sin costo alguno para el PNPAIS, siempre y cuando se confirme que sea defecto de fábrica.
  - El CONTRATISTA deberá brindar la disponibilidad del servicio de Internet al 99.95%, como mínimo.
  - El CONTRATISTA deberá contar con un Centro de Atención de Averías con un número al que se pueda llamar sin costo desde un teléfono fijo o móvil. El servicio de soporte debe ser permanente 7x24x365 y contar con un sistema de gestión adecuado para reportar fallas y atenciones mediante este centro de atención, así mismo dicha gestión podrá ser realizada médiate correo electrónico designado por el CONTRATISTA.
  - El servicio de soporte técnico deberá ser Brindado por el CONTRATISTA y/o FABRICANTE de la solución ofertada.
  - Los servicios deberán estar operativos las 24 horas de los 7 días, por 365 días.

b. Seguridad Informática de la red del Programa Nacional PAIS. (Componente 05)

- El proveedor debe con un Centro de Operaciones de Seguridad informática la cual deberá de Monitorear todo el equipamiento de su solución ofertada y reportarla de forma mensual al CONTRATISTA, cabe resaltar que ante alguna incidencia el CONTRASTISTA deberá de contactarse

con el personal técnico de la Unidad de tecnologías de la información de la ENTIDAD para superar la incidencia.

- El CONTRATISTA deberá realizar TRES (03) Ethical hacking (caja gris) a la infraestructura y servicios desplegados que se encuentren alojados en su solución ofertada a los 15 días, a los 18 meses y a los 30 meses de iniciado el servicio o firma del acta de instalación. El CONTRATISTA deberá de entregar un Informe técnico final detallado con los resultados del estado del sistema de seguridad de la infraestructura tecnológica priorizando las recomendaciones para mitigar y/o eliminar las debilidades detectadas. El CONTRATISTA deberá de coadyuvar a levantar las observaciones del informe enviado sin costo alguno para la entidad.
- El servicio de Ethical hacking deberá ser del tipo caja gris.
- El CONTRATISTA deberá realizar un auditoria a nivel de código de todos los sistemas de información publicados por LA ENTIDAD a los 15 días, a los 18 meses y a los 30 meses de iniciado el servicio o firma del acta de instalación. El CONTRATISTA deberá de entregar un Informe técnico final detallado con los resultados de la auditoria a nivel de código de todos los sistemas de información desarrolladas por LA ENTIDAD priorizando las recomendaciones a corregir, mitigar y/o eliminar las debilidades detectadas. Cabe resaltar que la ENTIDAD deberá levantar dichas recomendaciones con la finalidad de que el CONTRATISTA realice una segunda auditoria enfocado solo en las recomendaciones indicadas.
- El CONTRATISTA deberá realizar SEIS (06) Pruebas de alta disponibilidad a toda la infraestructura y servicios desplegados que se encuentren alojados en su solución ofertada a los 6 meses, a los 12 meses, a los 18 meses, a los 24 meses, a los 30 meses y a los 36 meses de iniciado el servicio o firma del acta de instalación. El CONTRATISTA deberá de entregar un Informe técnico final detallado con los resultados del estado del sistema de seguridad de la infraestructura tecnológica priorizando las recomendaciones para mitigar y/o eliminar las debilidades detectadas. El CONTRATISTA deberá de coadyuvar a levantar las observaciones del informe enviado sin costo alguno para la entidad. cabe resaltar que los servicios deberán de estar alojados 4 horas en el site de contingencia como mínimo y luego deberá de pasar al site principal
- la configuración y puesta en marcha de toda la solución ofertada estará a cargo del CONTRATISTA
- La administración de toda la solución ofertada será compartida las cuales deberán de ser diferenciadas por usuarios para la entidad y el contratista. La responsabilidad el contratista no comprende las acciones efectuadas por los usuarios asignados a la entidad

SOLUCION NGFW (FIREWALL CONFIGURADO EN HA)

La solución debe considerar equipamiento nuevo y de primer uso, que no estén listados como End of Sales y End of Live, con las siguientes características y capacidades:

Solución NGFW

- Throughput 70 Gbps con la funcionalidad de firewall habilitada para tráfico IPv4 y IPv6, independiente del tamaño del paquete
- Soporte a por lo menos 7.2M conexiones simultaneas.
- Soporte a por lo menos 500K nuevas conexiones por segundo.
- Throughput de al menos 50 Gbps de VPN IPSec.
- Debe incluir capacidad activa de usar 2000 túneles de VPN IPSec site-to-site simultáneos.
- Debe incluir capacidad activa de usar 2000 túneles de clientes VPN IPSec simultáneos
- Throughput de al menos 4 Gbps de VPN SSL
- Soportar al menos 5000 usuarios VPN SSL simultáneos como mínimo.
- Soportar al menos 12.5 Gbps de throughput de IPS
- Soportar al menos 8 Gbps de throughput de Inspección SSL
- Throughput de al menos 10 Gbps con las siguientes funcionalidades habilitadas simultáneamente para todas las firmas que la solución de seguridad tenga debidamente activadas y operativas: control de aplicaciones, IPS, Antivirus/Antispyware. En caso el fabricante tenga publicado múltiples números de desempeño para cualquiera de las funcionalidades, solamente el de valor más pequeño será aceptado.
- Tener al menos
  - 10 interfaces 1Gbps Base-T sin contar las interfaces de gestión y HA
  - 4 interfaces de 10Gbps SFP+
  - Incluir los transceivers necesarios.
- Debe contar con fuente de poder redundante con capacidad de cambio en caliente.
- Estar licenciado y/o tener incluido sin costo adicional, al menos 10 sistemas virtuales lógicos (Contextos) por appliance.

Requisitos Mínimos de Funcionalidad

Características Generales

- La solución debe consistir en una plataforma de protección de Red, basada en un dispositivo con funcionalidades de Firewall de Próxima Generación (NGFW).

- Estar licenciado y habilitado con las funcionalidades de: Firewall, IPS, Antivirus de red, Filtrado URL, Control de aplicaciones, identificación de usuarios a través de directorio activo, prevención de Bots y Sandboxing cloud.
- Las interfaces de red de su solución ofertada deberán de configurarse mediante ethernet channel en caso se disponga de interfaces no utilizadas
- El Contratista deberá desplegar el certificado digital de su solución ofertada mediante una GPO mediante el directorio activo de la entidad con la finalidad de que el equipo de seguridad digital pueda tener activa la opción de firewall de nueva generación (desencriptado del trafico HTTPS).
- El fabricante del equipamiento de seguridad debe haber obtenido una efectividad de seguridad con calificación mínima de "A" en el último reporte de CyberRatings ENTERPRISE FIREWALL.
- Las funcionalidades de protección de red que conforman la plataforma de seguridad, puede ejecutarse en múltiples dispositivos siempre que cumplan todos los requisitos de esta especificación;
- La plataforma debe estar optimizada para análisis de contenido de aplicaciones en capa 7;
- Todo el equipo proporcionado debe ser adecuado para montaje en rack de 19 ", incluyendo un rail kit (si sea necesario) y los cables de alimentación;
- La gestión de los equipos debe ser compatible a través de la interfaz de administración Web en el mismo dispositivo de protección de la red;
- Los dispositivos de protección de red deben soportar 4094 VLANs Tags 802.1q, agregación de enlaces 802.3ad y LACP;
- Los dispositivos de protección de red deben soportar Policy based routing y policy based forwarding;
- Los dispositivos de protección de red deben soportar encaminamiento de multicast (PIM-SM y PIM-DM);
- Los dispositivos de protección de red deben soportar DHCP Relay y DHCP Server
- Los dispositivos de protección de red deben soportar sFlow;
- Los dispositivos de protección de red deben soportar Jumbo Frames;
- Debe ser compatible con NAT dinámica (varios-a-1), (muchos-a-muchos);
- Debe soportar NAT estática (1-a-1), (muchos-a-muchos);
- Debe ser compatible con NAT estático bidireccional 1-a-1;
- Debe ser compatible con la traducción de puertos (PAT);
- Debe soportar NAT de origen y NAT de destino de forma simultánea;
- Debe soportar NAT de origen y NAT de destino en la misma política
- Debe soportar Traducción de Prefijos de Red (NPTv6) o NAT66, para evitar problemas de enrutamiento asimétrico;
- Debe ser compatible con NAT64 y NAT46;
- Debe implementar el protocolo ECMP y balanceo de enlace hash por IP de origen y destino;
- Debe soportar balanceo de enlace por peso. En esta opción debe ser posible definir el porcentaje de tráfico que fluirá a través de cada uno de los enlaces. Debe ser compatible con el balanceo en al menos tres enlaces;
- La solución debe incluir capacidades de SD-WAN durante la vigencia del contrato, permitiendo mejorar la conectividad con las sedes remotas.
- Debe permitir el monitoreo por SNMP de fallas de hardware, uso de recursos por gran número de sesiones, conexiones por segundo, cantidad de túneles establecidos en la VPN, CPU, memoria, estado del clúster, ataques y estadísticas de uso de las interfaces de red;
- Enviar logs a sistemas de gestión externos simultáneamente;
- Debe tener la opción de enviar logs a los sistemas de control externo a través de TCP y SSL;
- Debe soportar protección contra la suplantación de identidad (anti-spoofing);
- Para IPv4, soportar enrutamiento estático y dinámico (RIPv2, OSPFv2 y BGP);
- Para IPv6, soportar enrutamiento estático y dinámico (OSPFv3);
- Debe contar con la certificación USGv6-r1 como mínimo en FW e IPS, para garantizar que estén integrados con IPv6 y permitan utilizar las capacidades de Firewall e IPS también en IPv6.
- Soportar OSPF graceful restart;
- 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 sin necesidad de tener que hacer uso de contextos o dominios virtuales.
- Soportar la configuración de alta disponibilidad activo / pasivo y activo / activo: En modo transparente, en capa 3 y con al menos 3 dispositivos en el cluster
- La configuración de alta disponibilidad debe sincronizar: Sesiones, políticas de firewall, NAT, QoS, objetos de red, asociaciones VPN.
- En modo HA (Modo de alta disponibilidad) debe permitir la supervisión de fallos de enlace;
- Debe permitir la creación de administradores independientes para cada uno de los sistemas virtuales existentes, con el fin de permitir la creación de contextos virtuales que se pueden administrar por diferentes áreas funcionales;
- La solución de gestión debe ser compatible con el acceso a través de SSH y la interfaz web (HTTPS), incluyendo, pero no limitado a, la exportación de configuración de sistemas virtuales (contextos) por ambos tipos de acceso;

- Control, inspección y descifrado de SSL para tráfico entrante (Inbound) y saliente (Outbound), debe soportar el control de los certificados individualmente dentro de cada sistema virtual, o sea, aislamiento de las operaciones de adición, eliminación y utilización de los certificados directamente en los sistemas virtuales (contextos);
- Debe identificar potenciales vulnerabilidades y destacar las mejores prácticas que podrían ser usadas para mejorar la seguridad general y el rendimiento de la red;

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.
- El servicio del fabricante deberá incluir soporte para asistir a la Entidad en las investigaciones de ciberseguridad originadas por alguna sospecha de ataque y debe ofrecer bolsas de horas adicionales de acuerdo al soporte requerido para la detección, análisis, contención, reducción del impacto del incidente y recuperación de las operaciones.
- El servicio del fabricante deberá incluir la investigación avanzada de logs e indicadores de compromiso (IOC) y estar alineado a estrategias de cacería de amenazas (threat hunting).
- El servicio del fabricante deberá incluir el asesoramiento a la Entidad para superar el incidente y dar recomendaciones personalizadas para el afinamiento de la plataforma.
- En conjunto con la entidad se debe desarrollar al menos dos manuales de estrategias de respuesta a Incidentes (playbooks) y deben ser probados (ejercicios de simulación) con la entidad al menos dos de dichos manuales de estrategias de respuesta a incidentes, a fin de que la entidad cuente con un plan de acción de respuesta a incidentes definido.
- El servicio debe realizar una evaluación inicial del plan de respuesta a incidentes de la entidad y proporcionar un informe del nivel de madurez, los resultados de la evaluación y un conjunto de recomendaciones.
- Estos alcances deben ser brindados directamente por al área especializada de respuesta a incidentes del fabricante. No se aceptará que sea ejecutado por un partner o ingenieros comerciales del fabricante.

Control por Politica de Firewall
- Debe soportar controles de zona de seguridad y políticas de control por puerto y protocolo;
- Contar con políticas por aplicación, grupos estáticos de aplicaciones, grupos dinámicos de aplicaciones (en base a las características y comportamiento de las aplicaciones) y categorías de aplicaciones;
- Control de políticas por usuarios, grupos de usuarios, direcciones IP, redes y zonas de seguridad;
- Debe poder aplicar la inspección de control de aplicaciones y filtrado web como mínimo.
- Debe contar con objetos que incluyan servicios comunes de Internet y que permita agregarlos directamente a las políticas de firewall;
- Debe incluir el almacenamiento de bitácoras (logs) en tiempo real en un appliance dedicado local (on-premise) del mismo fabricante independiente del firewall, que permita al menos 06 meses de información para vistas y reportes. Debe incluir por los menos 8 TB luego de aplicar RAID 1 o superior.
- Debe soportar el protocolo de la industria 'syslog' para el almacenamiento usando formato Common Event Format (CEF);
- Debe soportar el protocolo estándar de la industria VXLAN;

Control de Aplicación
- Los dispositivos de protección de red deben tener la capacidad de reconocer las aplicaciones, independientemente del puerto y protocolo;
- Debe ser posible liberar y bloquear aplicaciones sin necesidad de abrir o cerrar puertos y protocolos;
- Reconocer al menos 1.700 aplicaciones diferentes, incluyendo, pero no limitado a: El tráfico relacionado peer-to-peer, redes sociales, acceso remoto, actualización de software, protocolos de red, VoIP, audio, vídeo, Proxy, mensajería instantánea, compartición de archivos, correo electrónico;
- Debe inspeccionar el payload del paquete de datos con el fin de detectar las firmas de las aplicaciones conocidas por el fabricante independiente de puerto y protocolo;
- Debe detectar aplicaciones a través del análisis del comportamiento del tráfico observado, incluyendo, pero no limitado a las aplicaciones de VoIP que utilizan cifrado propietario y BitTorrent;
- Identificar el uso de tácticas evasivas, es decir, debe tener la capacidad de ver y controlar las aplicaciones y los ataques con tácticas evasivas a través de las comunicaciones cifradas, como la utilización de la red Tor;
- Para tráfico cifrado SSL, debe poder descifrarlo a fin de posibilitar la lectura de payload para permitir la identificación de firmas de la aplicación conocidas por el fabricante;
- Identificar el uso de tácticas evasivas a través de las comunicaciones cifradas;
- Actualización de la base de firmas de la aplicación de forma automática;
- Limitar el ancho de banda (carga / descarga) utilizado por las aplicaciones (traffic shaping), basado en IP de origen, usuarios y grupos;
- Los dispositivos de protección de red deben tener la capacidad de identificar al usuario de la red con la integración de Microsoft Active Directory sin necesidad de instalación del agente en el controlador de dominio, o en estaciones de trabajo de usuario;

- Debe ser posible añadir múltiples reglas de control de aplicaciones;
- Debe ser compatible con múltiples métodos de identificación y clasificación de las aplicaciones, al menos verificar firmas y protocolos de decodificación;
- Para mantener la seguridad de red eficiente debe soportar el control de las aplicaciones desconocidas y no sólo en aplicaciones conocidas;
- Permitir la creación de forma nativa de firmas personalizadas para el reconocimiento de aplicaciones propietarias en su propia interfaz gráfica, sin la necesidad de la acción del fabricante;
- La creación de firmas personalizadas debe permitir el uso de expresiones regulares, el contexto (sesiones o transacciones), utilizando la posición en el payload de paquetes TCP y UDP, y el uso de decodificadores de al menos los siguientes protocolos: HTTP, FTP, NBSS, DCE RPC, SMTP, Telnet, SSH, MS-SQL, IMAP, DNS, LDAP, SSL y RTSP;
- El fabricante debe permitir solicitar la inclusión de aplicaciones en su base de datos;
- Debe alertar al usuario cuando sea bloqueada una aplicación;
- Debe permitir la diferenciación de tráfico Peer2Peer (Bittorrent, eMule, etc) permitiendo granularidad de control/reglas para el mismo;
- Debe permitir la diferenciación de tráfico de mensajería instantánea (AIM, Hangouts, Facebook Chat, etc.) permitiendo granularidad de control/reglas para el mismo;
- Debe permitir la diferenciación y manejo de las aplicaciones de chat; por ejemplo permitir el chat pero impedir la llamada de video;
- Debe permitir la diferenciación de aplicaciones Proxies, permitiendo granularidad de control/reglas para el mismo;
- Debe ser posible la creación de grupos dinámicos de aplicaciones, basado en las características de las mismas;
- Debe ser posible configurar Application Override seleccionando las aplicaciones individualmente

Prevención de Amenazas

- La tecnología adquirida debe ser parte de la agrupación internacional Cyber Threat Alliance (CTA) para compartir indicadores de compromiso (IoC) con otros fabricantes líderes de ciberseguridad en base al framework de MITRE ATT&CK, con el fin de mejorar la protección de los clientes a través de la detección de contenido malicioso como: archivos, nombres de dominio, direcciones IP y URI's.
- Para proteger el entorno contra los ataques, deben tener módulo IPS, antivirus y anti-spyware integrado en el propio equipo;
- Debe incluir firmas de prevención de intrusiones (IPS) y el bloqueo de archivos maliciosos (antivirus y anti-spyware);
- Las características de IPS, antivirus y anti-spyware deben funcionar de forma permanente, pudiendo utilizarlas de forma indefinida, aunque no exista el derecho a recibir actualizaciones o no exista un contrato de garantía del software con el fabricante;
- Todos los miembros del cluster deben contar con las firmas de IPS, antivirus, anti-spyware cuando se implementa en alta disponibilidad;
- Debe implementar los siguientes tipos de acciones a las amenazas detectadas por IPS: Permitir, permitir y generar registro, bloquear, bloquear IP del atacante durante un tiempo y enviar tcp-reset;
- Las firmas deben ser capaces de ser activadas o desactivadas, o activadas sólo en el modo de monitoreo;
- Debe ser posible crear políticas para usuarios, grupos de usuarios, IP, redes o zonas de seguridad;
- Excepciones por IP de origen o destino deben ser posibles en las reglas o en cada una de las firmas;
- Debe soportar granularidad en las políticas de IPS, Antivirus y Anti-Spyware, permitiendo la creación de diferentes políticas por zona de seguridad, dirección de origen, dirección de destino, servicio y la combinación de todos estos elementos;
- Debe permitir el bloqueo de exploits conocidos;
- Debe incluir la protección contra ataques de denegación de servicio;
- Debe tener los siguientes mecanismos de inspección IPS: Análisis de decodificación de protocolo, análisis para detectar anomalías de protocolo, desfragmentación IP, reensamblado de paquetes TCP y bloqueo de paquetes con formato incorrecto (malformed packets)
- Debe ser capaz de prevenir los ataques básicos, tales como inundaciones (flood) de SYN, ICMP , UDP, etc;
- Detectar y bloquear los escaneos de puertos de origen;
- Bloquear ataques realizados por gusanos (worms) conocidos;
- Contar con firmas específicas para la mitigación de ataques DoS y DDoS;
- Contar con firmas para bloquear ataques de desbordamiento de memoria intermedia (buffer overflow);
- Debe poder crear firmas personalizadas en la interfaz gráfica del producto;
- Debe permitir utilizar operadores de negación en la creación de firmas personalizadas de IPS o anti-spyware, permitiendo la creación de excepciones con granularidad en la configuración;
- Permitir bloqueo de virus y software espía en por lo menos los siguientes protocolos: HTTP, FTP, SMB, SMTP y POP3;
- Soportar el bloqueo de archivos por tipo;

- Identificar y bloquear la comunicación con redes de botnet;
- Registrar en la consola de supervisión la siguiente información sobre amenazas concretas: El nombre de la firma o el ataque, la aplicación, el usuario, el origen y destino de las comunicaciones, además de las medidas adoptadas por el dispositivo;
- Debe permitir la captura de paquetes (PCAP), mediante la firma de IPS o control de aplicación, así como la cuarentena de malware mediante la protección antivirus/antimalware, facilitando el análisis forense y la identificación de falsos positivos.
- Debe incluir capacidad de filtro DNS alimentada por un servicio de inteligencia de amenazas de la propia marca.
- Soportar Threat Feeds mediante cualquier de los siguientes métodos: STIX, servicios web, archivos o texto.
- Los eventos deben identificar el país que origino la amenaza;
- Debe incluir protección contra virus en contenido HTML y Javascript, software espía (spyware) y gusanos (worms);
- Debe permitir la configuración de diferentes políticas de control de amenazas y ataques basados en políticas de firewall considerando usuarios, grupos de usuarios, origen, destino, zonas de seguridad, etc., es decir, cada política de firewall podrá tener una configuración diferente de IPS basada en usuario, grupos de usuarios, origen, destino, zonas de seguridad;
- Soportar proteger contra ataques de día cero y malware desconocido a través de un servicio de sandboxing del fabricante con análisis en Windows como mínimo.

Filtrado de URL

- Debe permitir especificar la política por tiempo, es decir, la definición de reglas para un tiempo o período determinado (día, mes, año, día de la semana y hora);
- Debe ser posible crear políticas para usuarios, IPs, redes, o zonas de seguridad;
- Debe tener la capacidad de crear políticas basadas en la visibilidad y el control de quién está usando las URL que mediante la integración con los servicios de directorio Active Directory y la base de datos local, en modo de proxy transparente y explícito;
- Debe soportar la capacidad de crear políticas basadas en control por URL y categorías de URL del servicio de inteligencia del fabricante
- Debe tener la base de datos de URLs en caché en el equipo o en la nube del fabricante, evitando retrasos de comunicación / validación de direcciones URL;
- Tener por lo menos 60 categorías de URL;
- Debe tener la funcionalidad de exclusión de URLs por categoría;
- Permitir página de bloqueo personalizada;
- Permitir bloqueo y continuación (/que permita al usuario acceder a un sitio potencialmente bloqueado, informándole en pantalla del bloqueo y permitiendo el uso de un botón Continuar para que el usuario pueda seguir teniendo acceso al sitio);

Identificación de Usuarios y dispositivos

- Se debe incluir la capacidad de crear políticas basadas en la visibilidad y el control de quién está usando dichas aplicaciones a través de la integración con los servicios de directorio, a través de la autenticación LDAP, Active Directory, E-directorio y base de datos local;
- Debe tener integración con Microsoft Active Directory para identificar a los usuarios y grupos, permitiendo granularidad a las políticas / control basado en usuarios y grupos de usuarios;
- Debe tener integración y soporte para Microsoft Active Directory para los siguientes sistemas operativos: Windows Server 2003 R2, Windows Server 2008, Windows Server 2008 R2, Windows Server 2012 y Windows Server 2012 R2;
- Debe tener integración con Microsoft Active Directory para identificar a los usuarios y grupos que permita tener granularidad en las políticas/control basado en usuarios y grupos de usuarios, soporte a single-sign-on. Esta funcionalidad no debe tener límites licenciados de usuarios o cualquier restricción de uso como, pero no limitado a, utilización de sistemas virtuales, segmentos de red, etc;
- Debe tener integración con RADIUS para identificar a los usuarios y grupos que permiten las políticas de granularidad / control basado en usuarios y grupos de usuarios;
- Debe tener la integración LDAP para la identificación de los usuarios y grupos que permiten granularidad en las políticas/control basado en usuarios y grupos de usuarios;
- Debe permitir el control sin necesidad de instalación de software de cliente, el equipo que solicita salida a Internet, antes de iniciar la navegación, entre a un portal de autentificación residente en el equipo de seguridad (portal cautivo);
- Debe soportar la identificación de varios usuarios conectados a la misma dirección IP en entornos Citrix y Microsoft Terminal Server, lo que permite una visibilidad y un control granular por usuario en el uso de las aplicaciones que se encuentran en estos servicios;
- Debe de implementar la creación de grupos de usuarios en el firewall, basada atributos de LDAP / AD;
- Permitir la integración con tokens para la autenticación de usuarios, incluyendo, pero no limitado a, acceso a Internet y gestión de la plataforma;

- Proporcionar al menos un token de forma nativa, lo que permite la autenticación de dos factores para la administración segura de la plataforma.
- Debe brindar visibilidad de parámetros de los dispositivos que generan tráfico, como mínimo: tipo de dispositivo, fabricante del hardware, hostname, MAC, versión de sistema operativo.

QoS Traffic Shaping
- Con el fin de controlar el tráfico y aplicaciones cuyo consumo puede ser excesivo (como YouTube, Ustream, etc.) y que tienen un alto consumo de ancho de banda, se requiere de la solución que, además de permitir o denegar dichas solicitudes, debe tener la capacidad de controlar el ancho de banda máximo cuando son solicitados por los diferentes usuarios o aplicaciones, tanto de audio como de video streaming;
- Soportar la creación de políticas de QoS y Traffic Shaping por dirección de origen, dirección de destino, por usuario y grupo.
- Soportar la creación de políticas de calidad de servicio y Traffic Shaping por puerto;
- En QoS debe permitir la definición de tráfico con ancho de banda garantizado, con máximo ancho de banda y colas de prioridad.
- Soportar la priorización de protocolo en tiempo real de voz (VoIP) como H.323, SIP, SCCP, MGCP.
- Soportar marcación de paquetes DiffServ, incluso por aplicación;
- Soportar la modificación de los valores de DSCP para Diffserv;
- Soportar priorización de tráfico utilizando información de Tipo de Servicio (Type of Service);
- Proporcionar estadísticas en tiempo real para clases de QoS y Traffic Shaping;
- Debe soportar QoS (traffic-shapping) en las interfaces agregadas o redundantes;

Filtro de Datos
- Permite la creación de filtros para archivos y datos predefinidos, realizando la detección y bloqueo de archivos por su extensión
- Los archivos deben ser identificados por tamaño y tipo;
- Permitir identificar y opcionalmente prevenir la transferencia de varios tipos de archivo (MS Office, PDF, etc.) identificados en las aplicaciones (HTTP, FTP, SMTP, etc.);
- Soportar la identificación de archivos comprimidos o la aplicación de políticas sobre el contenido de este tipo de archivos;
- Soportar la identificación de archivos cifrados y la aplicación de políticas sobre el contenido de este tipo de archivos;

Geolocalización
- Soportar la creación de políticas por geolocalización, permitiendo bloquear el tráfico de cierto País/Países;
- Debe permitir la visualización de los países de origen y destino en los registros de acceso;
- Debe permitir la creación de zonas geográficas por medio de la interfaz gráfica de usuario y la creación de políticas usando las mismas;

VPN
- Soporte VPN de sitio-a-sitio y cliente-a-sitio;
- Soportar VPN IPSec y VPN SSL, desde dispositivos endpoint y móviles usando agente e incluir también modos sin agente.
- El agente de VPN SSL o IPSEC cliente-a-sitio debe permitir ser instalado al menos en Windows, Mac OS, Linux, Android e IOS. De ser requerido, se debe incluir el licenciamiento necesario para permitir esta capacidad.
- La VPN IPSec debe ser compatible con 3DES, AES de 128, 192 y 256 (Advanced Encryption Standard), así como MD5 y SHA-1
- La VPN IPSec debe ser compatible con Diffie-Hellman Grupo 1, Grupo 2, Grupo 5 y Grupo 14;
- La VPN IPSec debe ser compatible con Internet Key Exchange (IKEv1 y v2);
- La VPN IPSec debe ser compatible con la autenticación a través de certificados IKE PKI;
- Soportar VPN para IPv4 e IPv6, así como el tráfico IPv4 dentro de túneles IPv6 IPSec;
- Debe permitir activar y desactivar túneles IPSec VPN desde la interfaz gráfica de la solución, lo que facilita el proceso troubleshooting;
- Debe permitir que todo el tráfico de los usuarios VPN remotos fluya hacia el túnel VPN, previniendo la comunicación directa con dispositivos locales como un proxy;
- Asignación de DNS en la VPN de cliente remoto;
- Debe permitir la creación de políticas de control de aplicaciones, IPS, antivirus, filtrado de URL y AntiSpyware para el tráfico de clientes remotos conectados a la VPN SSL;
- Soportar autenticación vía AD/LDAP, token, certificado y base de usuarios local;
- Soportar lectura y revisión de CRL (lista de revocación de certificados);
- Permitir la aplicación de políticas de seguridad y visibilidad para las aplicaciones que circulan dentro de túneles SSL;

- El agente de VPN debe validar la configuración del dispositivo cliente antes de otorgar el acceso a la red. Debe soportar como mínimo los siguientes criterios de evaluación antes de brindar el acceso a la red: detectar un proceso específico en ejecución, detectar un registro específico, protección activa del antivirus, firewall de host y versión de sistema operativo, así como una combinación de estos criterios.
- El agente de VPN SSL o IPSEC cliente-a-sitio debe ser compatible con al menos Windows 7 (32 y 64 bits), Windows 8 (32 y 64 bits), Windows 10 (32 y 64 bits) y Mac OS X (v10.10 o superior);
- El proveedor deberá de entregar 300 licencias de VPN SSL para conectarse a la red de la ENTIDAD, así mismo deberan tener cargado el certificado de SSL para contar con una conexión segura

SOLUCION FIREWAL DE APLICACIONES WEB
El solucion puede ser, appliance físico, virtual, o como servicio en la nube del proveedor
Características de la solución:
- Throughput mínimo para HTTP de 1 Gbps
- Mínimo de 2 interfaces de 1Gbps RJ-45 (todas BYPASS)
- Mínimo de 4 interfaces de 1Gbps SFP
- Almacenamiento de 450GB SSD con 2 unidades físicas y/o virtuales de almacenamiento como mínimo.

Funcionalidades de Red:
- La solución debe de ser capaz de ser implementada en modo Proxy (Transparente y Reverso), Pasivo y Transparente en línea (Bridge)
- La solución debe de ser capaz de ser implementada con protocolo WCCP
- Soportar VLANs del estándar IEEE 802.1q.
- Debe de implementar el protocolo Link Aggregation Control Protocol (LACP) - IEEE 802.3ad
- Soportar direccionamiento IPv4 y IPv6 en las interfaces físicas y virtuales (VLANs).
- La solución debe de soportar y brindar cluster de alta disponibilidad entre dos equipos en modo Activo-Pasivo y Activo-Activo, de forma que el tráfico siga siendo procesado en caso de fallo del equipo principal.
- La solución debe de soportar la sincronización de configuración entre dos appliances del mismo tipo, con el objetivo de operar en modo activo-activo, con la distribución de tráfico siendo realizada por balanceador de tráfico externo o por la propia solución.
- La solución debe de soportar enrutamiento por políticas.

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.

Funcionalidades de Gestión
- Sistema operacional / firmware debe soportar interfaz gráfica web para la configuración de las funciones del sistema, utilizando navegadores disponibles gratuitamente y protocolo HTTPS, y también por CLI (interface de línea de comando), accediendo localmente por puerto de console, o remotamente vía SSH
- Debe de soportar administración basada en interface web HTTP
- Debe de soportar administración basada en interface de línea de comando vía SSH
- Tener auto complementación de comandos en la CLI y ayuda contextual en la CLI
- La solución debe de tener un Dashboard con información sobre el sistema (información del cluster, hostname, número de serie, modo de operación, tiempo en servicio, versión de firmware)
- Debe de ser posible visualizar a través de la interfaz gráfica de gestión la información de licencia, firmas y contrato de soporte
- La solución ofertada deberá de tener acceso a la línea de comando CLI vía la interfaz gráfica de gestión
- Debe de proveer, en la interfaz de gestión, las siguientes informaciones del sistema para cada equipo: consumo de CPU y estadísticas de conexión
- Debe de ser posible visualizar en la interfaz de gestión la información de consumo de memoria
- Debe de ser posible visualizar en la interfaz de gestión la información de uso de los discos de log
- Debe de incluir herramienta dentro de la interfaz gráfica de gestión (dashboard) que permita visualizar los últimos logs de ataques detectados/bloqueados
- Debe proveer la siguiente información en la interfaz gráfica de gestión: estadísticas de throughput HTTP en tiempo real, estadísticas de eventos de ataques detectados/bloqueados, estadísticas de requisición HTTP en tiempo real y los últimos logs de eventos del sistema
- Tener en la interfaz gráfica estadísticas de conexión concurrente y por segundo, de políticas de seguridad del sistema
- Tener un dashboard de visualización con información de las interfaces de red del sistema
- La configuración de administración de la solución debe permitir la utilización de perfiles
- Debe de ser posible ejecutar y recuperar backup por la interfaz Web (GUI) o utilizando FTP o SFTP o TFTP

- Debe ser posible instalar un firmware alternativo en disco y arrancarlo en caso de fallo del firmware principal
- Debe soportar los protocolos de monitoreo SNMP v1, SNMP v2c e SNMP v3
- Debe ser capaz de realizar notificación de eventos de seguridad a través de e-mail, traps SNMP y Syslog
- La solución deberá de soportar almacenar logs localmente en disco y en servidor externo vía protocolo SYSLOG
- Debe tener la capacidad de almacenar los logs en appliance remoto
- La solución debe tener la capacidad de enviar alertas por email de los eventos basado en severidad y/o categorías
- La solución debe tener datos analíticos conteniendo la localización geográfica de los clientes web
- La solución debe tener datos analíticos, siendo posible visualizar el total de ataques y porcentaje de cada país de origen, el volumen total de tráfico en bytes y porcentaje de cada país de origen, y el total de accesos (hits) y porcentaje de cada país de origen
- Debe tener la capacidad de generar reportes detallados basados en tráfico/acceso/actividades del usuario
- Debe soportar RESTful API para gestión de la configuración

Funcionalidades de Autenticación
- Los usuarios deben de ser capaces de autenticarse a través del encabezado de autorización HTTP / HTTPS
- Los usuarios deben de ser capaces de autenticarse a través de formularios HTML embebidos
- La solución debe de ser capaz de autenticar los usuarios a través de certificados digitales personales
- Debe tener base local para almacenamiento y autenticación de los usuarios
- La solución debe tener la capacidad de autenticar usuarios en bases externas remotas LDAP y RADIUS
- La solución debe de ser capaz de autenticar los usuarios en base remota vía NTLM
- La solución debe de soportar el modelo de seguridad positiva definido por OWASP, por lo menos lo que está en el TOP 10

Funcionalidades de Web Application Firewall
- Debe de ser capaz de identificar y bloquear ataques a través de una base de datos de firmas de virus y reputación IP, actualizado de forma automática
- La solución debe permitir elegir entre utilizar la base de datos completa o solamente la base de datos que contiene los últimos y más peligrosos virus
- Debe permitir analizar archivos en un servicio de sandboxing del mismo fabricante, que utilice Windows como mínimo.
- Tener mecanismo de aprendizaje automático capaz de identificar todos los contenidos de la aplicación, incluyendo URLs, parámetros de URLs, campos de formulários y lo que se espera de cada campo
- El perfil aprendido de forma automática debe de poder ser ajustado
- La solución debe tener generación de reportes con la información obtenida en auto aprendizaje, con las estadísticas y las políticas de tráfico obtenido, los reportes de ataques, eventos y reportes de chequeo de vulnerabilidades para fines de cumplimiento de reglamentación
- Tener la capacidad de creación de firmas personalizadas de ataques
- Tener la capacidad de protección contra ataques del tipo Adobe Flash binary (AMF) protocol
- Tener la capacidad de protección contra ataques del tipo Botnet
- Tener la capacidad de protección contra ataques del tipo Browser Exploit Against SSL/TLS (BEAST)
- La solución debe tener funcionalidad de proteción contra ataques como acceso por fuerza bruta
- Debe soportar detección de ataques de Clickjacking
- Debe soportar detección de ataques de cambios de cookie
- Identificar y proteger contra ataques del tipo Cross Site Request Forgery (CSRF)
- La solución debe tener funcionalidad de protección contra ataques como cross site scripting (XSS)
- Debe tener protección contra ataques de Denial of Service (DoS);
- Tener la capacidad de protección contra ataques del tipo HTTP header overflow
- Tener la capacidad de protección contra ataques del tipo Local File inclusion (FLI)
- Tener la capacidad de protección contra ataques del tipo Man-in-the0middle (MITM)
- Tener la capacidad de protección contra ataques del tipo Remote File Inclusion (RFI)
- Tener la capacidad de protección contra ataques del tipo Server Information Leakage
- Protección contra envíos de comandos SQL ocultos en las requisiciones enviadas a la base de datos (SQL Injection);
- Tener la capacidad de protección contra ataques del tipo Malformados XML
- Identificar y prevenir ataques del tipo Low-rate DoS
- Prevention contra Slow POST attack
- Proteger contra ataques Slowloris
- Tener la capacidad de protección contra ataques del tipo SYN flood
- Tener la capacidad de protección contra ataques del tipo Forms Tampering

- La solución debe tener funcionalidad de protección contra ataques de manipulación de campos ocultos
- Tener la capacidad de proteción contra ataques del tipo Directory Traversal
- Tener la capacidad de proteción del tipo Access Rate Control
- Identificar y proteger contra Zero Day Attacks
- Tener la capacidad de configurar proteción del tipo TCP SYN flood-style para prevención de DoS para cualquier política, a través de Syn Cookie y Half Open Threshold
- Permitir configurar reglas de bloqueo a métodos HTTP no deseados
- Permitir que se configuren reglas de límite de upload por tamaño del archivo
- Debe permitir que el administrador bloquee el tráfico de entrada o salida en base a países, sin la necesidad de gestionar manualmente los rangos de dirección IP correspondientes a cada país
- Debe soportar crear políticas de geo-localización, permitiendo que el tráfico de determinado país sea bloqueado
- Permitir configurar listas negras de bloqueo y listas blancas de confianza, basadas en dirección IP de origen
- Permitir la liberación temporal o definitiva (white-list) de direciones IP bloqueadas por tener originado ataques detectados por la solución.
- Debe permitir añadir, automáticamente o manualmente, en una lista de bloqueo, las direcciones IP de origen, según la base de IP Reputation.
- Tener la capacidad de prevención contra pérdida de información (DLP), bloqueando la pérdida de información del encabezado HTTP
- Tener la funcionalidad de proteger el website contra modificaciones no autorizadas, brindando recuperación automática del website en caso de ocurrencia.
- Tener la funcionalidad de antivirus integrada para inspección de tráfico y archivos, sin la necesidad de instalación de otro equipo
- Tener la capacidad de investigar y analizar todo el tráfico HTTP para validar si está en conformidad con la respectiva RFC, bloqueando ataques y tráfico no conformes
- Debe de ser capaz de hacer aceleración de SSL a nivel de hardware, donde se instalan los certificados digitales en la solución y las requisiciones HTTP sean enviadas a los servidores sin criptografía
- La solución debe de ser capaz de funcionar como terminador de sesión SSL para aceleración de tráfico
- Para SSL/TLS offload soportar al menos TLS 1.0, 1.1, 1.2 y 1.3
- La solución debe tener la capacidad de almacenar certificados digitales de CA's
- La solución debe de ser capaz de generar CSR para ser firmado por una CA
- La solución debe de ser capaz de chequear los certificados válidos y que no fueron revocados por una lista CRL
- La solución debe contener las firmas de robos conocidos como link checkers, indexadores de web, search engines, spiders y web crawlers que puedan ser añadidos a los perfiles de control de acceso, así como resetear dichas conexiones
- La solución debe de tener un sistema de reputación de direcciones IP públicas conocidas como origen de ataques de DDoS, botnets, spammers, etc. Esto sistema debe de ser actualizado automáticamente.
- La solución debe de ser capaz de limitar el total de conexiones permitidas hacia cada servidor real de un pool de servidores
- La solución debe permitir la personalización o reenvío de solicitudes y respuestas HTTP en el HTTP Host, Request URL HTTP, HTTP Referer, HTTP Body y HTTP Location
- La solución debe permitir crear reglas definiendo el orden con que las páginas deben de ser accedidas para prevenir ataques como cross-site request forgery (CSRF).
- La solución debe de tener la capacidad de definir restricción a determinados métodos HTTP
- La solución debe tener la capacidad de proteger contra detección de campos ocultos
- La solución debe tener la capacidad de actuar como un scanner de vulnerabilidades para diagnóstico e identificación de amenazas en los servidores web, software no actualizado y posibles buffers overflows
- Debe generar perfil de protección automáticamente a partir de reporte en formato XML generado por scanner de vulnerabilidades de terceros
- Debe permitir programar la verificación de vulnerabilidades
- La solución debe generar un reporte de análisis de vulnerabilidades en formato HTML
- La solución debe permitir exclusión de URLs en el análisis de vulnerabilidades.
- Debe de ser capaz de hacer compresión del contenido HTTP, para reducir la cantidad de información enviada al cliente
- Soportar redirección y reescritura de request y response HTTP
- Permitir redirección de request HTTP hacia HTTPS
- Permitir reescribir la línea URL del encabezado de un request HTTP, el campo HOST, REFERER del encabezado de un request HTTP
- Permitir redirigir request para otro website
- Permitir enviar response HTTP 403 Forbidden para request HTTP
- Permitir reescribir el parámetro LOCATION en el encabezado HTTP del response de redirección HTTP de un servidor web

- Permitir reescribir el cuerpo ("body") de una respuesta HTTP de un servidor web
- Permitir añadir el campo X-Forwarded-For para identificación de la dirección IP real del cliente cuando en modo proxy reverso
- La solución debe de soportar reglas para definir si las requisiciones HTTP serán aceptadas en función de la URL y origen de la petición y, si necesario, aplicar una tasa específica de velocidad (rate limit).
- La solución debe de soportar combinación de control de acceso y autenticación utilizando mecanismos como HTML Form, Basic y soporte a SSO, métodos como LDAP y RADIUS para consultas e integración de los usuarios de la aplicación
- Tener capacidad de caching para aceleración web
- Debe permitir al administrador crear nuevas firmas y/o cambiar las firmas pre existentes

Funcionalidades de Balanceo de Carga

- La solución debe incluir la funcionalidad de balanceo de carga entre servidores web
- Debe soportar configurar puertos no estándar para aplicación web HTTP y HTTPS
- Soportar balanceo / distribución de tráfico y enrutar el contenido hacia distintos servidores web
- La solución debe permitir crear grupos de servidores (Server Farm / Pool) para distribuir las conexiones de los usuarios.
- Soportar como mínimo el algoritmo Round Robin, Weighted Round y Least Connection para balanceo de carga entre servidores
- La solución debe de soportar creación de servidores virtuales que definan la interfaz de red/bridge y dirección IP por donde el tráfico con destino al Server Pool es recibido
- Los servidores virtuales deben de entregar el tráfico hacia un único servidor web y también incluir la opción de distribuir las sesiones/conexiones entre los servidores web del Server Pool
- Debe de ser posible definir el número máximo de conexiones TCP simultáneas hacia un determinado servidor miembro del Server Pool
- Permitir prueba de disponibilidad del servidor web a través del método TCP
- Permitir prueba de disponibilidad del servidor web a través del método ICMP ECHO_REQUEST (ping), TCP Half Open, TCP SSL, HTTP, HTTPS
- En las pruebas de disponibilidad HTTP y HTTPS, permitir indicar la URL exacta a ser probada, permitir elegir entre los métodos HEAD, GET y POST, permitir elegir el nombre del campo HTTP "host" a ser probado
- Soportar ruteo de los request de los clientes web basado en contenido HTTP a través de “Host", “URL", “Parámetro HTTP", “Referer", “Dirección IP de Origen", “Encabezado, “Cookie", “Valor del campo del Certificado X509"
- Implementar Cache de Contenido para HTTP, permitiendo que objetos sean almacenados y request HTTP sean contestadas directamente por la solución
- La solución debe de ser capaz de balancear las nuevas sesiones, pero manteniendo sesiones existentes en un mismo servidor, implementando persistencia como mínimo por: análisis de cualquier parámetro del header HTTP, URL accedida, por cookie (método cookie insert, cookie rewrite y cookie original), Session ID
  (ASP, PHP y JSP), sesión SSL

SOLUCIÓN DE PROTECCIÓN, DETECCIÓN Y RESPUESTA AUTOMATIZADA PARA ENDPOINTS (EDR)

La solución propuesta debe estar licenciado para 350 endpoints. El cual podrá ser appliance físico, virtual, o como servcicio en la nube del proveedor, esta solución debe incluir las siguientes características:

Requerimiento del Agente

- La solución propuesta debe ser compatible mínimo con los siguientes sistemas operativos: Windows (32-bit & 64-bit versiones) XP SP2/SP3, 7, 8, 8.1, 10 y 11.
- La solución propuesta debe ser compatible mínimo con los siguientes sistemas operativos: Windows Server 2003 R2 SP2, 2008 R1 SP2, 2008 R2, 2012, 2012 R2, 2016 y 2019
- La solución propuesta debe ser compatible mínimo con los siguientes sistemas operativos: macOS Versiones: Yosemite (10.10), El Capitan (10.11), Sierra (10.12), High Sierra (10.13), Mojave (10.14) y Catalina (10.15)
- La solución propuesta debe ser compatible mínimo con los siguientes sistemas operativos: Linux Versiones: RedHat Enterprise Linux y CentOS 6.8, 6.9, 6.10, 7.2, 7.3, 7.4, 7.5, 7.6 y 7.7 y Ubuntu LTS 16.04.5, 16.04.6, 18.04.1 y 18.04.2 server, 64-bit
- La solución propuesta debe tener la habilidad de actualizar el agente sin interacción por parte del usuario y sin necesidad de reinicio.
- La solución propuesta debe trabajar sin depender de firmas hash locales conocidas para la detección de archivos maliciosos.
- La solución propuesta debe poder registrar en tiempo real información del proceso y datos adicionales como conocer el usuario asociado con los eventos.

Requerimientos de soporte

- Debe incluir la asesoría de Servicios Profesionales del fabricante durante la implementación inicial.
- Estos alcances deben ser brindados directamente por al área especializada de Servicios Profesionales del fabricante. Así mismo también se aceptará que sea ejecutado por un partner o ingenieros comerciales del fabricante.

Detección de Malware

- La solución debe incluir la capacidad de compartir inteligencia de amenazas de endpoints con soluciones NGFW, además de generar acciones de respuesta mejoradas en el NGFW, como suspender o bloquear una dirección IP luego de un ataque de infiltración.
- La solución propuesta debe poder funcionar en caso el agente no se encuentre conectado a la red empresarial.
- La solución propuesta debe poder detectar, eliminar y volver a su valor inicial cambios realizado por procesos maliciosos en el registro de las PC.
- La solución propuesta debe poder detectar conexiones de red desde el dispositivo.
- La solución propuesta debe identificar actividad maliciosa conocida.
- La solución propuesta debe tener la capacidad de categorizar los eventos detectados en diferentes categorías según la criticidad del evento.
- La solución propuesta debe incorporar las técnicas de MITRE ATT&CK en el esquema de detección y mostrar cuáles de estas técnicas fueron utilizadas en los eventos maliciosos.
- La solución propuesta debe haber sido capaz de bloquear todas las técnicas probadas en al menos una evaluación de ATT&CK de MITRE.

Prevención de Malware

- La solución propuesta debe tener la capacidad de prevención de ejecución de archivos maliciosos.
- La solución propuesta debe incorporar un motor de antivirus de última generación (NGAV) basado en el kernel con capacidad de "Machine Learning".
- La solución propuesta debe tener capacidad de controlar dispositivos USB y crear excepciones a los dispositivos USB basado en: nombre del dispositivo o vendor o número serial.
- La solución propuesta debe poder bloquear tráfico malicioso de exfiltración de datos y comunicación hacia C&C (Command & Control)
- La solución propuesta debe evitar cifrados de disco causado por ransomware y modificación de archivos o registro de los dispositivos.
- La solución propuesta debe poder ser configurada en modo de monitoreo, donde no se realice ningún bloqueo, pero toda actividad maliciosa sea registrada.
- La solución propuesta debe poder permitir la realización de escaneos periódicos de los archivos contenidos en los dispositivos con el Agente instalado.

Post-Infección

- La solución propuesta debe permitir el aislamiento automático del tráfico de red de un dispositivo donde se ha encontrado una actividad causada por malware.
- La solución propuesta debe permitir el bloqueo de las actividades realizadas por parte de archivos maliciosos.
- La solución propuesta debe tener la capacidad de crear excepciones para los falsos positivos de forma manual para marcar la actividad como falso positivo y evitar que ocurran bloqueos futuros.
- La solución propuesta debe tener la capacidad de recalificar automáticamente la actividad como falso positivo y evitar que ocurran detecciones similares, ya sea a través de un servicio automatizado de la solución o por el servicio de Managed Detection and Response (MDR) del fabricante.

Respuesta a Incidentes

- La solución propuesta debe almacenar meta-data generada por los dispositivos para que la misma sea usada en investigaciones forenses.
- La solución propuesta debe permitir la integración con plataformas de correlación de eventos vía Syslog.
- La solución propuesta debe tener la capacidad de obtener capturas instantáneas de memoria o "dumps" de memoria que permitan la realización de procesos forenses.
- La solución propuesta debe permitir la integración a través de API donde el mismo tenga la capacidad de entregar información generada en un evento tales como: Dirección IP, nombre de host, usuario, fecha / hora ocurrida, actividad sospechosa, etc.) para permitir la integración vía API.
- La solución propuesta debe tener la capacidad para terminar un proceso, eliminar un archivo y aislar dispositivos infectados basado en la clasificación del mismo.
- La solución propuesta debe obtener visibilidad completa de la cadena de ataque y cambios maliciosos.
- La solución propuesta debe permitir la limpieza automática de los dispositivos y revertir los cambios maliciosos manteniendo la disponibilidad del dispositivo.

- La solución propuesta debe permitir el envío de ejecutables para su análisis a un sandbox, con la finalidad de determinar si son maliciosos o inofensivos.

Control de Vulnerabilidades y Comunicación
- La solución debe prevenir la comunicación de aplicaciones riesgosas y no autorizadas, que se estén comunicando a través de la red.
- La solución propuesta debe poder visualizar y entregar información sobre el uso de aplicaciones en red mostrando información como los IP destinos del tráfico generado por la aplicación.
- La solución propuesta debe permitir utilizar políticas proactivas de bloqueo de comunicación basadas en el riesgo de acuerdo a CVE y la calificación o reputación que puede tener una aplicación.
- La solución debe permitir bloquear la ejecución de aplicaciones a fin de evitar el uso de aplicaciones no deseadas en la organización.

Consola de Administración
- La consola de administración de la solución propuesta debe permitir el uso de roles granulares para los administradores.
- La consola de administración de la solución propuesta debe permitir la gestión a través de Full Restful API.
- La solución propuesta debe poder ser gestionada completamente en nube.
- La solución propuesta debe soportar la integración con el servicio de inteligencia en nube del mismo fabricante para actualización de inteligencia de malware y amenazas.
- La consola de administración de la solución propuesta debe permitir la visualización de salud de los agentes instalados.
- La consola de administración de la solución propuesta debe permitir la desactivación/activación remota del agente instalado en los dispositivos.
- La consola de administración de la solución propuesta debe permitir la actualización remota del agente instalado en los dispositivos.
- La consola de administración de la solución propuesta debe permitir la creación de reportes ejecutivo conteniendo un resumen que describe los eventos de seguridad y el estado del sistema.
- La consola de administración de la solución propuesta debe permitir la creación de grupos organizativos de dispositivos en los cuales cada grupo podrá tener reglas de protección independiente de los demás.
- La consola de administración de la solución propuesta debe permitir la exportación de bitácoras locales generadas por los agentes desde la misma consola.
- La consola de administración de la solución propuesta debe permitir la visibilidad de eventos generados por los dispositivos o eventos de acuerdo al proceso ejecutado.
- La consola de administración de la solución propuesta debe el envío de alertas a través de correo electrónico.
- La solución propuesta debe permitir agregar automáticamente direcciones IP maliciosas detectadas en uno o más firewalls remotos integrados, ya sea a través de API u otro método de integración.
- La solución propuesta debe permitir que los servicios de inteligencia en nube recategoricen la clasificación de un evento automáticamente, ya sea a través de un servicio automatizado de la solución o por el servicio de Managed Detection and Response (MDR) del fabricante.
- La solución debe tener la capacidad de creación de playbooks o plantillas de flujo de trabajo con el objetivo de automatizar las capacidades de detección y respuesta.

SOLUCIÓN DE CONTROL DE ACCESO A LA RED (NAC)
La solución propuesta debe estar licenciado para 350 endpoints. Esta solución podrá de brindarse en appliance físico, virtual, o como servicio en la nube del proveedor, el cual debe incluir las siguientes características:

Características Generales
- Debe basarse en Appliance físico o máquinas virtuales (VMs), desplegables sobre arquitecturas VMware, Hyper-V, AWS o Azure
- Debe ser desplegada en alta disponibilidad, para asegurar la continuidad del servicio.
- La solución debe soportar, al menos 400 dispositivos conectados simultáneamente y deberá poder escalar a 1000 dispositivos concurrentes.

Visibilidad de red
- La solución debe permitir un despliegue centralizado, en una arquitectura fuera de banda, y brindar control de acceso en Capa 2 y Capa 3 sobre una infraestructura cableada e inalámbrica.
- Debe permitir crear una estructura jerárquica que permita ordenar los dispositivos de infraestructura de la red de manera lógica y/o geográfica.
- Debe permitir crear, modificar y borrar dispositivos y sus características.
- Debe permitir el registro manual de dispositivos no SNMP.
- Debe contar con un proceso continuo de detección y categorización de dispositivos de infraestructura de red, que permita detectar y controlar los switches, routers y otros dispositivos de la red.

- Debe permitir mover fácilmente los dispositivos dentro de la estructura jerárquica generada
- Debe permitir realizar consulta a nivel Capa 2 y Capa 3 (polling) de los dispositivos que se encuentren conectados a los equipos de red controlados, para poder utilizar esta información en la fase de control de acceso.
- La solución debe poder ser registrada como un dispositivo independiente dentro de la topología física en la consola de gestión unificada del firewall del mismo fabricante de la solución de control de acceso a la red ofertada
- La solución debe operar indistintamente para entornos cableados o inalámbricos, locales o remotos.
- Debe permitir la detección de hosts desconocidos (rogue).

Visibilidad de endpoint

- Debe permitir la identificación de hosts mediante Portal Cautivo
- Debe permitir la categorización automática de hosts y dispositivos IoT.
- Debe permitir la recategorización periódica de los hosts desconocidos
- Debe recordar el perfil asignado a cada host, y verificar que sigue siendo válido en cada nueva conexión del host. Si el perfil variara, deberá impedir su conexión y notificar inmediatamente sobre el evento.
- Debe permitir la fijación de períodos de tiempo en los que el host está autorizado a conectarse, y evaluarlos periódicamente.
- Debe permitir la importación de un archivo .CSV conteniendo información sobre los hosts a registrar.
- Debe permitir la integración con plataformas MDM.
- La solución no debe requerir el uso de 802.1x para permitir el descubrimiento de hosts o usuarios, o brindar control de acceso a nivel de Puerto en la infraestructura cableada.
- Debe permitir determinar el perfil de los hosts descubiertos mediante métodos que no requieran la instalación de agentes incluyendo, al menos, los siguientes:
    - DHCP Fingerprinting, Ubicación, Rangos IP, SNMP
    - HTTP/HTTPS, SSH, Telnet, TCP, UDP
    - OUI
    - WMI, WinRM
    - Activo con NMAP o pasivo
    - Agente
    - ONVIF, Network traffic
    - Script usando Perl
- Debe permitir determinar el perfil de los dispositivos IoT mediante una URL hacia una base de datos de Servicios de IoT del mismo fabricante de la solución de control de acceso a la red ofertada
- La solución debe poder reconocer los siguientes sistemas operativos sin necesidad de agentes:
    - Android, Apple iOS, Chrome OS, Windows Phone/CE/RT
    - Free BSD, Linux, Solaris, Symbian
    - Mac OS X
    - Windows

Visibilidad de usuarios

- Debe permitir el uso de Agentes Persistentes para el perfilamiento de hosts
- Debe permitir la identificación de usuarios mediante Active Directory
- Debe permitir la identificación de usuarios mediante Portal Cautivo
- La solución debe incluir opciones de análisis flexibles para plataformas Windows, MacOS y Linux. La tecnología de agentes desvanecibles no debe requerir la instalación de software de terceros, tales como Java.
- Debe permitir la designación de un Sponsor que autorice el acceso de un invitado.
- Debe permitir la designación de un Sponsor que autorice la categorización de un host.
- Debe permitir el ingreso de credenciales mediante 802.1x o Portal Cautivo

Automatización y control

- Debe soportar la validación de credenciales:
    - Con Google Account
    - Con un servidor RADIUS externo
    - Con un servidor LDAP
- Debe actuar como servidor de Radius local embebido dentro de la misma solución de control de acceso a la red
- Debe permitir modo de autenticación de Radius Local con los siguientes modos de EAP 802.1X:
    - TTLS/PAP
    - TTLS/MSCHAPv2
    - PEAP/MSCHAPv2
    - TLS
- Debe soportar la validación automática de credenciales mediante agentes persistentes o volátiles
- La solución debe tener la capacidad de aprovechar la combinación de informaciones sobre la identidad del usuario y el tipo de dispositivo para aprovisionar dinámicamente permisos de acceso basados en roles y distintos niveles de acceso.

- Debe permitir la generación de políticas de control, agrupadas jerárquicamente, y determinar la política a aplicar a cada dispositivo en función de una serie de reglas de asignación.
- Debe soportar, al menos, los siguientes tipos de información para determinar la política a aplicar:
    - Ubicación
    - Grupo de Pertenencia
    - Atributo
    - Fecha y Hora
- La solución debe incluir funcionalidades de Guest Management, permitiendo la creación de perfiles de Invitados y Contratistas.
- Debe permitir la creación de plantillas que agrupen a los invitados o contratistas en grupos que tengan distintos permisos de acceso, o períodos de tiempo de acceso permitido.
- Debe contar con herramientas que permitan la generación y mantenimiento de este tipo de usuarios y sus claves de acceso.
- Debe permitir la creación de Portales de Auto-Registro.
- Debe soportar el envío de claves de acceso mediante SMS.
- Debe permitir la existencia de Sponsors que aprueben el ingreso de Invitados o Contratistas a la red, o que eleven los permisos de acceso de ciertos individuos.
- La solución debe incluir funcionalidades de IoT Onboarding con autorización de Sponsors
- La solución debe incluir funcionalidades de detección y contención de dispositivos desconocidos (rogues)
- La solución debe incluir funcionalidades de Endpoint Compliance. Antes de permitir el acceso de los dispositivos a la red, debe asegurarse de que estos cumplen con una serie de requisitos de seguridad, integridad y configuración, que hagan seguro su acceso a la red.
- Debe permitir el uso de agentes persistentes, evanescentes (desaparecen luego de realizado en análisis) o pasivos.
- Debe permitir el control de acceso a la red basado en políticas de acceso que determinen el tipo de segmentación de red para los dispositivos y usuarios registrados. Estas políticas deben asignar un tag de firewall que será recibido automáticamente por el firewall del mismo fabricante de la solución ofertada.
- Si un dispositivo no pasa los tests de Compliance, debe ser posible:
    - No forzar la remediación
    - Forzar la remediación inmediatamente, enviando al dispositivo a una red de cuarentena
    - Permitir la remediación retardada, dando un período de tiempo desde la detección inicial de problemas, para la solución de estos. Pasado el período de tolerancia, de persistir los problemas, el dispositivo debe ser puesto en cuarentena inmediatamente.
- Debe permitir el control de acceso a la red de los usuarios remotos autenticados a través de VPN IPSec y/o SSL utilizando como terminador VPN el mismo fabricante de la solución de control de acceso a la red ofertada
- Debe permitir determinar la postura de Seguridad de los usuarios conectados remotamente a través de VPN IPSec y/o SSL utilizando agente disolvente descargado a través de un portal para las redes de contratistas y agente persistente para la red corporativa

Integraciones

- La solución debe incluir una REST API que permita:
    - Obtener información detallada sobre un elemento en particular, tal como un usuario o un host.
    - Interrogar a la base de datos para obtener información sobre un conjunto de dispositivos
    - Actualizar los registros de usuarios o dispositivos
    - Bloquear o desbloquear el acceso de un usuario o dispositivo a la red.
- La solución debe integrarse con la plataforma actual de seguridad perimetral que tiene la institución permitiendo alcanzar un control de acceso granular y respuesta automatizada ante cualquier evento de seguridad presentado utilizando etiquetas de firewall y conectores.
- La información enviada por la solución de control de acceso a la red a la plataforma de seguridad perimetral que tiene la institución debe contener IP, usuario, Grupo o etiqueta personalizados que permiten ser asignados de manera automática a grupos de usuarios de firewall utilizados en políticas de IPV4 para aplicar segmentación de acceso a la red
- Control de usuarios conectados por VPN, con el fin de validar su postura antes que éstos ingresen a los recursos de Red. Esta funcionalidad debe estar integrada como mínimo a plataformas Fortigate y Cisco de severidad de los mensajes de syslog de múltiples

Administración

- La solución debe permitir distintos roles administrativos, incluyendo la capacidad de limitar y controlar la cantidad de acceso permitido a las funcionalidades disponibles, dependiendo del grupo administrativo de la organización al que pertenezca el usuario. Por ej., Help Desk, Operaciones de Red, Operaciones de Seguridad.
- La solución debe proveer información de auditoría de todas las conexiones de la red, tanto cableadas como inalámbricas. Esto debe incluir una interfaz amigable, que permita buscar y generar consultas en la información almacenada.

- La solución debe incluir información de auditoría de todas las acciones y cambios realizados al sistema por los usuarios administradores, incluyendo qué se cambió, cuándo se cambió y quién lo cambió.

Reportes

- La Debe contar con un Tablero de Control que presente información relevante de manera resumida.
- El Tablero de Control debe poder ser modificable para permitir el despliegue de la información que el Administrador considere más relevante.
- Debe contar con reportes predefinidos que incluyan resultados sobre:
    - Registro de Invitados
    - Registro de dispositivos
    - Escaneo de Dispositivos
- Debe permitir la generación de reportes a medida sobre:
    - Registro de usuarios y Dispositivos
    - Falla en los Registros
    - Logs de Conexión
- Debe permitir la generación y archivado de reportes periódicos
- Debe permitir el envío automatizado de reportes mediante correo electrónico
- El log de alarmas debe poder ser ordenado por severidad.
- Debe permitir la aceptación y eliminación de alarmas del log de forma manual.
- Debe permitir la aceptación y eliminación de alarmas del log de forma automática.
- Debe permitir la definición de alarmas en función de la ocurrencia de determinados eventos.

SOLUCIÓN DE DOBLE FACTOR DE AUTENTICACIÓN CON TOKEN

La solución propuesta debe estar licenciado para 350 usuarios. Esta solución podrá de brindarse en appliance físico, virtual, o como servcicio en la nube del proveedor, el cual debe incluir las siguientes características:

Características Generales

- Debe basarse en Appliance físico o máquinas virtuales (VMs), desplegables sobre arquitecturas VMware o Hyper-V
- La solución debe soportar, al menos 400 usuarios.
- La solución debe soportar administración vía interface gráfica (GUI) por HTTP / HTTPS
- Permite definir perfiles de administradores para una solución, de modo que puede segmentar la responsabilidad de los administradores por tareas operativas
- La solución debe ser brindada en configuración de alta disponibilidad (HA) activo-pasivo o activo-activo, minimizando el tiempo de inactividad
- Debe incluir el envío de mensajes SMS a los usuarios a través de gateway SMS de terceros
- La solución debe soportar el registro de todos los eventos que los usuarios de su base de datos local realizan con sus cuentas, como crear un usuario, cambiar la contraseña de un usuario y cambiar la información general

Autenticación

- La solución debe realizar la autenticación para la gestión de identidad de los usuarios de la red, siendo un punto central de control de autenticación, donde se pueden consolidar múltiples métodos de autenticación
- La solución debe brindar autenticación de dos factores (two-factor authentication) con el código token enviado por SMS para 350 usuarios.
- La solución debe permitir la definición de un nivel de complejidad mínima para las contraseñas de todos los usuarios registrados en la base de datos local, permitiendo la definición de un número mínimo de letras minúsculas, mayúsculas, caracteres numéricos, caracteres especiales, etc.
- La solución debe permitir la creación de una política de bloqueo automático de usuarios después de una serie de fallas de autenticación, evitando así los ataques de fuerza bruta
- La solución debe soportar la creación de usuarios a nivel local, que se puede utilizar para autenticar dispositivos según sea necesario.
- La solución debe permitir la creación de nuevos usuarios en la base de datos local y que el equipo genere una contraseña aleatoria y la envíe automáticamente al usuario.
- La solución debe permitir la creación de nuevos usuarios en la base de datos local sin la definición de una contraseña, requiriendo que use el token como el único factor de autenticación
- Permite asociar tokens a usuarios creados localmente en la base de datos
- Eliminación automática masiva de usuarios inactivos, según criterios definidos
- Los tokens deben generar códigos con un mínimo de 6 dígitos e intervalos que no excedan los 60 segundos
- La solución debe soportar autenticación de dos factores por aplicación móvil (iPhone y Android)
- La solución debe soportar autenticación de dos factores mediante el envío de correo electrónico.
- Permite desactivar un token cuando es robado o perdido, permitiendo su reactivación posterior cuando / si se recupera

- Permite la disociación de un token a un usuario y asociarlo con otro usuario cuando sea necesario, permitiendo así su reutilización
- Permite la autenticación de doble factor en clientes Windows, incluso con la máquina fuera de línea
- Debe proporcionar un portal web para que los usuarios se registren automáticamente, de modo que puedan acceder, completar sus datos y enviar el registro. Después de que el usuario inicia sesión, el administrador debe ser notificado automáticamente para aprobar o denegar el registro del usuario antes de que el usuario sea activado.
- La solución La solución debe soportar la integración con el servidor RADIUS
- La solución debe soportar la integración con un servidor LDAP remoto (como Microsoft Active Directory)
- La solución debe permitir a los usuarios que no tienen una cuenta local o de redes sociales autenticarse a través de un registro rápido, que garantice una trazabilidad mínima, a través de la validación de direcciones de correo electrónico o números de teléfono.
- La solución debe soportar el lenguaje de marcado de aserción de seguridad (SAML), que actúa como un CONTRATISTA de identidad (IDP), estableciendo una relación de confianza para la autenticación segura de los usuarios que intentan acceder a un CONTRATISTA de Servicios (SP)
- La solución debe actuar como una Autoridad de Certificación (CA)
- Permite la administración de certificados digitales, con emisión y revocación.
- Debe proporcionar un repositorio para la autenticación VPN site-to-site a través de certificados
- Debe crear y firmar certificados X.509 para usar en servidores https y ssh, así como clientes de servicios HTTPS, SSH, VPNs IPSec.
- Permite que el administrador del sistema genere, firme y revoque certificados digitales para los usuarios.

GESTIÓN CENTRALIZADA DE EQUIPOS DE SEGURIDAD
Un equipo para cada site, esta solución podrá de brindarse en appliance físico, virtual, o como servcicio en la nube del proveedor, el cual debe incluir las siguientes características:

Capacidades:
- Si la solución es virtualizada, debe ser compatible con Citrix XenServer 7.2, Google Cloud Platform, Linux KVM Redhat 7.1, Microsoft Azure, Microsoft Hyper-V Server 2012/2016/2019, Nutanix AHV (AOS 5.10.5), OpenSource XenServer 4.2.5, Oracle Private Cloud y VMware ESXi versions 6.5 y posterior.
- No debe haber límites a la cantidad de múltiples vCPU si el aparato es virtual.
- No debe haber límites a la expansión de memoria RAM si el aparto es virtual.
- Si la solución es virtualizada, debe tener capacidades de Alta disponibilidad (HA).
- Debe tener la capacidad de automatizar flujos de trabajo y configuraciones para los dispositivos gestionados desde una sola consola.
- La solución debe tener la capacidad Multi-Tenancy para separar los datos de gestión de infraestructura de manera lógica o geográfica y permitir despliegue Zero-Touch para un aprovisionamiento masivo rápido.
- La solución debe ser capaz de realizar respaldos automáticos de configuración hasta en 5 nodos, conteniendo updates de todos los dispositivos gestionados.
- Debe tener la capacidad de permitir provisionar comunidades VPN y monitorear conexiones VPN de todos los dispositivos gestionados desde una sola consola y mostrar su geolocalización en un mapa.
- La solución debe permitir utilización de API RESTful para permitir interacción con portales personalizados en la configuración de objetos y políticas de seguridad.
- En la fecha de la propuesta, ninguno de los modelos de la oferta puede estar en el sítio del fabricante en listados de end-of-life o end-of-sales.
- La gestión de la solución debe soportar acceso por SSH, cliente o WEB (HTTPS) y API abierta.
- Debe permitir accesos concurrentes de administradores.
- Debe tener interfaz basada en línea de comando para administración de la solución de gestión.
- Debe tener un mecanismo de búsqueda por comandos en la gestión por SSH, facilitando la ubicación de comandos.
- Bloquear cambios, en el caso de acceso simultaneo de dos o más administradores.
- Definición de perfiles de acceso a la consola con permiso granular como: acceso a escrita, acceso de lectura, creación de usuarios, cambio de configuraciones.
- Generar alertas automáticas por Email, SNMP y Syslog.
- Debe soportar backup/restore de todas las configuraciones de la solución de gestión, permitiendo al administrador agendar backups de configuración en un determinado día y horario.
- Debe ser permitido al administrador transferir los backups a un servidor FTP, SCP y SFTP.
- Los cambios realizados en un servidor de gestión deben ser automáticamente replicados al servidor redundante;
- Debe ser permitido a los administradores autenticarse en los servidores de gestión a través de cuentas de usuarios LOCALES, TACACS+, LDAP y RADIUS.
- Debe soportar sincronización de reloj interno por protocolo NTP.
- Debe registrar las acciones efectuadas por cualquier usuario;

- Debe soportar SNMP versión 2 y la versión 3 en los equipos de gestión.
- Debe permitir habilitar o deshabilitar, para cada interfaz de red de la solución de gestión, permisos de acceso HTTP, HTTPS, SSH, SNMP y Web Services (API).
- Debe permitir virtualizar la solución de gestión, de manera que cada administrador pueda gerenciar, visualizar y editar solo los dispositivos autorizados y registrados en su ambiente virtualizado.
- La solución de gestión debe permitir crear administradores que tengan acceso a todas las instancias de virtualización.
- La gestión debe permitir la creación y administración de políticas de firewall y control de aplicación.
- La gestión debe permitir la creación y administración de políticas de IPS, Antivírus y Anti-Spyware.
- La gestión debe permitir la creación y administración de políticas de Filtro de URL.
- Permitir buscar cuáles reglas un objeto está siendo utilizado.
- Permitir la creación de reglas que permanezcan activas en horario definido.
- La solución debe permitir ser repositorio de firmas de antivirus, IPS, Web Filtering, email filtering, para optimizar la velocidad y descarga centralizada a los dispositivos gestionados.
- Debe tener capacidad de desplegar los resultados de auditoría de seguridad de los dispositivos gestionados.
- Permitir backup de las configuraciones y rollback de configuración para la última configuración salva;
- Debe tener mecanismos de validación de políticas avisando cuando haya reglas que ofusquen o conflictúen con otras (shadowing).
- Debe permitir la visualización y comparación de configuraciones actuales, configuraciones previas y configuraciones antiguas.
- Debe posibilitar que todos los firewalls sean controlados de manera centralizada utilizando solo un servidor de gestión.
- La solución debe incluir una herramienta para gestionar centralmente las licencias de todos los aparatos controlados por estaciones de gestión, permitiendo al administrador actualizar licencias en los aparatos a través de esta herramienta.
- La solución debe permitir la distribución y instalación remota, de manera centralizada, de nuevas versiones de software de los aparatos.
- Debe ser capaz de generar reportes o presentar comparativos entre dos secciones distintas, resumiendo todos los cambios efectuados.
- Debe permitir crear flujos de aprobación en la solución de gestión, donde un administrador pueda crear todas las reglas, pero estas mismas solamente sean aplicadas después de la aprobación de otro administrador.
- Tener "wizard" en la solución de gestión para agregar los dispositivos por interfaz gráfica utilizando IP, login y clave de estos.
- Permitir que las políticas y los objetos ya presentes en los dispositivos sean importados a la solución de gestión cuando se agregan.
- Permitir la visualización, a partir de la estación de gestión centralizada, informaciones detalladas de los dispositivos gerenciados, tales como hostname, serial, IP de gestión, licencias, horario de lo sistema y firmware.
- Permitir crear en la solución de gestión templates de configuración de los dispositivos con informaciones de DNS, SNMP, configuraciones de LOG y administración.
- Permitir crear scripts customizados, que sean ejecutados de forma centralizada en un o más dispositivos gestionados con comandos de CLI de los mismos.
- Tener histórico de los scripts ejecutados en los dispositivos gestionados pela solución de gestión.
- Permitir crear varios paquetes de políticas que serán aplicados/asociados a los dispositivos o grupos de dispositivos.
- Debe permitir crear reglas de NAT64 y NAT46 de forma centralizada.
- Permitir la creación de reglas anti DoS de forma centralizada.
- Debe permitir la creación de objetos que serán utilizados en las políticas de forma centralizada.
- Debe permitir crear a partir de la solución de gestión, VPNs entre los dispositivos gestionados de forma centralizada, incluyendo topologia (hub, spoke, dial-up) autenticaciones, claves y métodos de criptografía.
- Debe permitir el uso de DDNS en VPNs de manera centralizada.
- Debe permitir la gestión de Access Points propietarios de manera centralizada.
- Debe permitir la gestión de Switches propietarios de manera centralizada.
- Debe permitir la gestión de perfiles de seguridad de software endpoint propietario de manera centralizada.

SOLUCIÓN DE ALMACENAMIENTO DE LOG Y REPORTERÍA en entorno virtual
Capacidades:

- Si la solución es virtualizada, debe ser compatible con el ambiente VMware ESXi 5.0/5.1/5.5/6.0/6.5/6.7;
- Si la solución es virtualizada, debe ser compatible con el ambiente Microsoft Hyper-V 2008 R2 / 2012 / 2012 R2/2016

- Si la solución es virtualizada, debe ser compatible con el ambiente Citrix XenServer 6.0+
- Si la solución es virtualizada, debe ser compatible con el ambiente Open Source Xen 4.1+
- Si la solución es virtualizada, debe ser compatible con el ambiente KVM on Redhat 6.5+ and Ubuntu 17.04
- Si la solución es virtualizada, debe ser compatible con el ambiente Nutanix AHV (AOS 5.10.5)
- Si la solución es virtualizada, debe ser compatible con el ambiente Amazon Web Services (AWS)
- Si la solución es virtualizada, debe ser compatible con el ambiente Microsoft Azure.
- Si la solución es virtualizada, debe ser compatible con el ambiente Google Cloud (GCP)
- Si la solución es virtualizada, debe ser compatible con el ambiente Oracle Cloud Infrastructure (OCI)
- Si la solución es virtualizada, debe ser compatible con el ambiente Alibaba Coud (AliCloud)
- Si la solución es virtualizada, no debe haber límites a la cantidad de múltiples vCPU
- Si la solución es virtualizada, no debe haber límites a la expansión de memoria RAM
- Debe soportar acceso vía SSH, WEB (HTTPS) para la gestion de la solución
- Contar con comunicación cifrada y autenticación con usuario y contraseña para la obtención de reportes, tanto en interface gráfica (GUI) como vía linea de comandos en consola de gestión.
- Permitir acceso simultáneo de administración, así como permitir crear por lo menos 2 (dos) perfiles para administración y monitoreo.
- Soporte SNMP versión 2 y 3
- Permitir virtualizar la gestión y administración de los dispositivos, donde cada administrador solo tenga acceso a los equipos autorizados.
- Debe permitir la creación de administrador general, que tenga acceso general a todas las instancias de virtualización de la solución.
- Debe permitir activar y desactivar para cada interface de la plataforma, los permisos de acceso HTTP, HTTPS, SSH
- Autenticación de usuarios de acceso a la plataforma via LDAP
- Autenticación de usuarios de acceso a la plataforma via Radius
- Autenticación de usuarios de acceso a la plataforma via TACACS+
- Generación de informes en tiempo real de tráfico, en formato de gráfica de mapas geográficos
- Generación de informes en tiempo real de tráfico, en formato de gráfica de burbuja.
- Generación de informes en tiempo real de tráfico, en formato de gráfica tabla
- Definición de perfiles de acceso a consola con permiso granulares, tales como: acceso de escritura, de lectura, de creación de nuevos usuarios y cambios en configuraciones generales.
- Debe contar con un asistente gráfico para agregar nuevos dispositivos, usando la dirección IP, usuario y contraseña del mismo.
- Debe ser posible ver la cantidad de logs enviados desde cada dispositivo supervisado
- Contar con mecanismos de borrado automático de logs antiguos.
- Permitir la importación y exportación de reportes
- Debe contar con la capacidad de crear informes en formato HTML
- Debe contar con la capacidad de crear informes en formato PDF
- Debe contar con la capacidad de crear informes en formato XML
- Debe contar con la capacidad de crear informes en formato CSV
- Debe permitir exportar los logs en formato CSV
- Generación de logs de auditoría, con detalle de la configuración realizada, el administrador que realizó el cambio y hora del mismo.
- Los logs generados por los dispositivos administrados deben ser centralizados en los servidores de la plataforma, pero la solución debe ofrecer también la posibilidad de utilizar un servidor externo de Syslog o similar.
- La solución debe contar con reportes predefinidos
- Debe poder enviar automáticamente los logs a un servidor FTP externo a la solución
- Debe ser posible la duplicación de reportes existentes para su posterior edición.
- Debe tener la capacidad de personalizar la portada de los reportes obtenidos.
- Permitir centralmente la visualización de logs recibidos por uno o más dispositivos, incluido la capacidad de uso de filtros para facilitar la búsqueda dentro de los mismos logs.
- Los logs de auditoría de cambios de configuración de reglas y objetos deben ser visualizados en una lista distinta a la de los logs relacionados a tráfico de datos.
- Tener la capacidad de personalización de gráficas en los reportes, tales como barras, líneas y tablas
- Debe poseer mecanismo de “Drill-Down” para navegar en los reportes de tiempo real.
- Debe permitir descargar de la plataforma los archivos de logs para uso externo.
- Tener la capacidad de generar y enviar reportes periódicos automáticamente.
- Permitir la personalización de cualquier reporte preestablecido por la solución, exclusivamente por el Administrador, para adoptarlo a sus necesidades.
- Permitir el envío por email de manera automática de reportes.
- Debe permitir que el reporte a enviar por email sea al destinatario específico.

- Permitir la programación de la generación de reportes, conforme a un calendario definido por el administrador.
- Debe ser posible visualizar gráficamente en tiempo real la tasa de generación de logs por cada dispositivo gestionado.
- Debe permitir el uso de filtros en los reportes.
- Debe permitir definir el diseño de los reportes, incluir gráfico, añadir texto e imágenes, alineación, saltos de página, fuentes, colores, entre otros.
- Permitir especificar el idioma de los reportes creados
- Generar alertas automáticas vía email, SNMP y Syslog, basado en eventos especiales en logs, severidad del evento, entre otros.
- Debe permitir el envío automático de reportes a un servidor externo SFTP o FTP.
- Debe ser capaz de crear consultas SQL o similar dentro de las bases de datos de logs, para uso en gráficas y tablas en reportes.
- Tener la capacidad de visualizar en GUI de reportes de información del Sistema, como licencias, memoria, disco duro, uso de CPU, tasa de logs por segundo recibidos, total de logs diarios recibidos, alertas del sistema, entre otros.
- Debe contar con una herramienta que permita analizar el rendimiento en la generación de reportes, con el objetivo de detectar y arreglar problemas en generación de los mismos.
- Que la solución sea capaz de importar archivos con logs de dispositivos compatibles conocido y no conocidos por la plataforma, para posterior generación de reportes.
- Debe ser posible poder definir el espacio que cada instancia de virtualización puede utilizar para almacenamiento de logs.
- Debe proporcionar la información de cantidad de logs almacenados y la estadística de tiempo restante de almacenado.
- Debe ser compatible con autenticación de doble factor (token) para usuarios administradores de la plataforma.
- Debe permitir aplicar políticas para el uso de contraseñas para los administradores de la plataforma, como tamaño mínimo y caracteres permitidos
- Debe permitir visualizar en tiempo real los logs recibidos.
- Debe permitir el reenvío de logs en formato syslog.
- Debe permitir el reenvío de logs en formato CEF (Common Event Format).
- Debe incluir dashboard para operaciones SOC que monitorea las principales amenazas de seguridad para su red
- Debe incluir dashboard para operaciones SOC que monitorea comprometimiento de usuarios y uso sospechoso de la web en su red.
- Debe incluir dashboard para operaciones SOC que monitorea el tráfico en su red.
- Debe incluir dashboard para operaciones SOC que monitorea el tráfico de aplicaciones y sitios web en su red
- Debe incluir dashboard para operaciones SOC que monitorea detecciones de amenazas de día cero en su red (sandboxing).
- Debe incluir dashboard para operaciones SOC que monitorea actividad de endpoints en su red.
- Debe incluir dashboard para operaciones SOC que monitorea actividad VPN ren su red.
- Debe incluir dashboard para operaciones SOC que monitorea puntos de acceso WiFi y SSIDs
- Debe incluir dashboard para operaciones SOC que monitorea rendimiento de recursos local de la solución (CPU, Memoria)
- Debe permitir crear dashboards personalizados para monitoreo de operaciones SOC
- Debe soportar configuración de alta disponibilidad Master/Slave en la capa 3
- Debe permitir generar alertas de eventos a partir de logs recibidos
- Debe permitir crear incidentes a partir de alertas de eventos para endpoint
- Debe permitir la integración al sistema de tickets ServiceNow
- Debe soportar servicio de Indicadores de Compromiso (IoC) del mismo fabricante, que muestre las sospechas de comprometimiento de usuarios finales en la web, debiendo informar por lo menos: dirección IP de usuario, hostname, sistema operativo, veredicto (clasificación general de la amenaza), el número de amenazas detectadas.
- Debe permitir respaldar logs en nube publica de Amazon S3
- Debe permitir respaldar logs en nube publica de Microsoft Azure
- Debe permitir respaldar logs en nube publica de Gooogle Cloud
- Debe soportar el estándar SAML para autenticación de usuarios administradores
- Debe contar con reporte de cumplimiento de PCI DSS
- Debe contar con reporte de utilización de aplicaciones SaaS
- Debe contar con reporte de prevención de perdida de datos (DLP)
- Debe contar con reporte de VPN
- Debe contar con reporte de Sistema de prevención de intrusos (IPS)
- Debe contar con reporte de reputación de cliente
- Debe contar con reporte de análisis de seguridad de usuario

- Debe contar con reporte de análisis de amenaza cibernética
- Debe contar con reporte de breve resumen diario de eventos e incidentes de seguridad
- Debe contar con reporte de tráfico DNS
- Debe contar con reporte tráfico de correo electrónico
- Debe contar con reporte de Top 10 de Aplicaciones utilizadas en la red
- Debe contar con reporte de Top 10 de Websites utilizadas en la red
- Debe contar con reporte de uso de redes sociales
- Debe contar con reporte de evaluación de riesgo para correo electrónico
- Debe contar con reporte de cumplimiento PCI de Wireless.
- Debe contar con reporte de AP´s y SSID´s autorizados, así como clientes WIFi
- Debe contar con reporte de vulnerabilidades de solución gestionada de seguridad de equipo terminal.
- Debe contar con reporte de aplicaciones web, si se cuenta con plataforma de seguridad web.

SOLUCIÓN DE PROTECCIÓN ANTE AMENAZAS PERSISTENTES AVANZADAS Y AMENAZAS DE DÍA CERO en entorno virtual

Esta solución podrá de brindarse en appliance físico, virtual, o como servcicio en la nube del proveedor, el cual debe incluir las siguientes características:

GENERAL

- Mínimo de 4 interfaces de GE RJ45
- Tener espacio en disco mínimo de 1TB
- Soportar análisis de al menos 120 archivos en el Sandbox por hora
- Debe soportar hasta 6 máquinas virtuales simultaneas.
- Soportar hasta 5000 correos por hora trabajando como MTA
- Soportar hasta 500 Mbps trabajando como sniffer

FUNCIONALIDADES

- La solución debe proporcionar la funcionalidad de inspección del tráfico entrante en busca de malware desconocido (APT: amenazas persistentes avanzadas y amenazas de día cero), ransomware con filtro de amenazas avanzado y análisis de ejecución en tiempo real, e inspección del tráfico saliente de callbacks.
- Poseer la capacidad de prevenir amenazas desconocidas
- Debido a que el malware es muy dinámico y un Antivirus reactivo común no puede detectarlos con la misma velocidad que se crean sus variaciones, la solución que se ofrece debe tener características para la prevención de malware desconocido incluidas en la propia herramienta (día cero)
- El dispositivo de protección debe poder enviar automáticamente los archivos transferidos para su análisis en la solución instalada localmente (on premise), donde el archivo será ejecutado y simulado en un ambiente controlado.
- La solución debe contar con la nube de inteligencia propia del fabricante que se encarga de actualizar toda la base de seguridad a través de firmas.
- Debe ser capaz de monitorear y analizar el tráfico generado por archivos maliciosos y así determinar la naturaleza del tráfico y sus conexiones.
- La solución debe poder inspeccionar el tráfico cifrado SSL.
- Compatibilidad con el análisis de archivos de paquetes de Office (.doc, .docx, .xls, .xlsx, .ppt, .pptx), archivos java (.jar y class), APK de Android, MacOS y Linux en un entorno sandbox.
- Debe soportar los siguientes tipos de archivos: 7z, .ace, .apk, .app, .arj, .bat, .bz2, .cab, .cmd, .dll, .dmg, .doc, .docm, .docx, .dot, .dotm, .dotx, .eml, .elf, .exe, .gz, .htm, html, .iqy, .iso, .jar, .js, .kgb, .lnk, .lzh, Mach-O, .msi, .pdf, .pot, .potm, .potx, .ppam, .pps, .ppsm, .ppsx, .ppt, .pptm, .pptx, .ps1, .rar, .rtf, .sldm, .sldx, .swf, .tar, .tgz, .upx, .rl, .vbs, WEBLink, .wsf, .xlam, .xls, .xlsb, .xlsm, .xlsx, .xlt, .xltm, .xltx, .xz, .z, .zip
- Debe ser capaz de diferenciar los archivos analizados en al menos dos categorías: las que se identificaron como virus maliciosos y/o malignos y archivos sospechosos por tener comportamiento no esperado o características indeseables
- Debe ser capaz de clasificar los archivos sospechosos de acuerdo con el riesgo que suponen.
- Debe ser capaz de exportar los resultados del análisis de archivos maliciosos y sospechosos a PDF desde su propia interfaz de gestión
- Debe tener la capacidad de analizar en sandbox enlaces (HTTP y HTTPS) presentes en el cuerpo de los mensajes del correo electrónico SMTP. Debe generarse un informe si la apertura del enlace por el sandbox lo identifica como malicioso.
- Debe soportar el monitoreo de archivos transferidos en internet (HTTPs, FTP, HTTP, SMTP) así como archivos transferidos internamente entre servidores de archivos usando SMB en todos los modos de implementación: sniffer, transparente y L3.
- La solución debe admitir topologías de implementación

    - con adaptadores para la integración con soluciones de terceros a través del protocolo ICAP o BCC
    - a través del uso compartido de archivo
    - a través de la API JSON

- La solución debe tener un mecanismo para identificar hosts infectados que intentan acceder a direcciones DNS de dominios maliciosos.
- Seleccionar mediante política qué tipos de expedientes serán objeto de este análisis y prevención.
- Implementar e identificar malware en archivos adjuntos de correo electrónico y URL conocidos.
- Implementar detección y bloqueo inmediatos de malware que utilice un mecanismo de explotación en archivos PDF.
- El sistema de análisis debe proporcionar información sobre las actividades de los archivos maliciosos y sospechosos en las máquinas virtuales infectadas, información tal como qué procesos se inicializan por el archivo, los archivos creados, los archivos eliminados, los cambios realizados en el registro, el comportamiento de la red, como direcciones URL utilizadas por los programas maliciosos (seguros y no seguros) cambios de registros proporcionando información sobre el usuario infectado (al menos su dirección IP).
- Debe permitir la descarga de malware identificados a partir de la interfaz de gestión propia
- Se debe tener mecanismo de integración para proporcionar corrección automática. Una vez que se detecta el código malicioso, un paquete de firmas de antivirus basado en amenazas detectadas debe ser desarrollado y enviado a los dispositivos registrados como firewalls, y estaciones de trabajo de usuarios para ayudar en la mitigación.
- En caso de un veredicto positivo, debe presentar un desglose del comportamiento de la máquina comprometida, que contenga al menos información para fines de auditoría.:
    - sobre el Tipo de archivo
    - IP de origen del malware
    - IP de destino (cliente que descargó el malware)
    - virus Link to Reference Total
    - Resumen del comportamiento del malware

- La solución local debe permitir la gestión a través de la interfaz de línea de comandos (CLI).
- La solución debe soportar las reglas YARA como estándar para la creación de reglas para la detección de malware
- La solución local va a crear cuentas de administrador con al menos dos perfiles distintos: la lectura y escritura y solamente lectura.
- La solución local debe permitir la creación de cuentas de administrador con autenticación local o remota a través de servidores RADIUS.
- La solución local debe permitir la configuración del servicio de envío de correo electrónico de notificaciones cuando se detectan archivos maliciosos y reportes automáticos frecuentes.
- La solución local es instalar los paquetes de actualización de los módulos de seguridad tan pronto como estén disponibles.
- Deben soportar el análisis de los archivos maliciosos en un ambiente controlado con al menos los sistemas operativos Windows 10, Windows 8.1, Windows 7, macOS, Linux, Android, and ICS systems
- La solución local debe ser compatible con la compra, descarga e instalación de máquinas virtuales adicionales.
- La solución sandbox debe permitir la carga de máquinas virtuales personalizadas
- La solución local debe permitir al usuario cambiar la distribución de las máquinas virtuales de su entorno.
- El sistema de análisis debe trabajar en forma que permita que otros dispositivos de red tales como firewall, WAF (Web Application Firewall), AntiSpam o software de seguridad de estación de trabajo envíen archivos para su análisis de forma automática.
- Permitir a los usuarios introducir una lista de contraseñas predeterminada para los archivos para analizar bajo demanda
- El sistema debe permitir el envío de archivos bajo demanda para su análisis en ambiente controlado (sandbox) a través de la API y vía interface gráfica (GUI).
- Al realizar el análisis bajo demanda debe permitir la grabación de un video de todo el proceso.
- Deberá permitir la interacción con las máquinas virtuales mientras se realiza el análisis bajo demanda.
- Todo análisis y bloqueo de malware y/o código malicioso debe ocurrir en tiempo real y el bloqueo debe ser inmediato, no se aceptarán soluciones que solo detecten malware y/o código malicioso.

CERTIFICADOS DE SEGURIDAD SSL PARA LOS DOMINIOS Y SUB-DOMINIOS

Certificado de Seguridad SSL para los dominios y subdominios del Programa Nacional PAIS.

- Los portales y aplicaciones web del Programa Nacional PAIS se alojan en servidores virtuales que pertenecen a la entidad.
- Compatibilidad con el 99.9% de navegadores presentes en el mercado.
- El CONTRATISTA deberá brinda una consola administrativa para SSL para uso del personal de la entidad.
- El CONTRATISTA deberá de encargarse de implementar el certificado SSL en todos los servidores del Programa Nacional PAIS. cabe resaltar que la instalación de los certificados sin costo adicional para la entidad.
- El CONTRATISTA deberá de realizar que toda la configuración necesaria en los servidores del Programa Nacional PAIS en caso sea necesario.
- El CONTRATISTA deberá brinda una consola administrativa para SSL para uso del personal de la entidad.
- El soporte debe ser 365X7X24 durante la vigencia del servicio.
- Debe incluir soporte on line con base de conocimiento y documentos de soporte
- Debe incluir soporte vía telefonía y/o remota, de ser necesario la generación de archivos CSR o instalación de los certificados in situ.

Características	Requerido
Cantidad	1
Tipo	WildCard
Nivel de validación	OV - Validación de la Organización
Duración	1 años
Estándar	x.509 v3
Algoritmo de firma	SHA256 como mínimo
Nivel de cifrado	256 bits
Protocolos criptográficos	TLS/SSL
Criptografía	RSA, ECC
Longitud de la clave	Soportar 2048bits, 3072bits o 4096 bits
Cantidad de Subdominios	Deberá proteger un dominio y todos los subdominios de primer nivel de forma ilimitada (*.pais.gob.pe)
Licencias para servidores	Licencias ilimitadas para servidores.
Gerenciador web	SI, debe permitir crear y reemitir certificados sin costo alguno durante todo el periodo del servicio, además de permitir la opción de importar certificados de otras entidades certificadoras en modo lectura.
Protocolo de verificación	• Soporte de IDN (International Domain Ñames) y OSCP (Online Certifícate Status Protocol). • Emitido por un Root Certifícate Authority - CA Raíz reconocido. • Re-emisiones gratuitas ilimitadas durante el periodo de validez del certificado.
Compatibilidad mínima navegadores	99,9% de los navegadores y 99.5% para dispositivos móviles (smartphones)
Compatible con servidores WEB	99.9%
Carta de fabricante	SI
Soporte técnico	El soporte Tecnico deberá ser mediante: • Teléfono • Remoto • Correo

SOLUCION NGINX (EN AMBOS SITE)

El CONTRATISTA debe de entregar una solución de NGINX en versión de máquina virtual para desplegar los siguientes servicios.

- NGINX PARA DOCKERS.
- NGINX PARA CONTENEDEORES.
- NGINX PARA PAGINAS WEB.

El servicio de NGINX deberá se desplegado por EL CONTRATISTA de acuerdo a los servicios web con los que cuenta LA ENTIDAD.

La administración de toda la solución ofertada será compartida las cuales deberán de ser diferenciadas por usuarios para la entidad y el contratista. La responsabilidad el contratista no comprende las acciones efectuadas por los usuarios asignados a la entidad.
La instalación configuración y puesta en marcha del servicio el cual deberá de ser realizado por EL CONTRATISTA.

- **ATENCIÓN DE AVERÍAS, SOPORTE Y MANTENIMIENTO**
  - El servicio de averías remoto deberá de tener un tiempo de atención no mayor de 30 minutos.
  - El servicio de averías presencial deberá tener un tiempo de atención no mayor a 24 horas.
  - Ante un problema o incidente comunicado por el PNPAIS, al CONTRATISTA, el tiempo de respuesta para iniciar la atención de la solución de la incidencia será no mayor a 15 minutos inmediatamente después de generado el ticket.
  - Toda actividad o provisión de bienes que tenga que ejecutar el CONTRATISTA para subsanar la avería de un equipo será sin costo alguno para el PNPAIS, siempre y cuando se confirme que sea defecto de fábrica.
  - El CONTRATISTA deberá brindar la disponibilidad del servicio de Internet al 99.95%, como mínimo.
  - El CONTRATISTA deberá contar en su Red con sistemas que cuenten con distintas medidas de seguridad para evitar el rastreo e interceptación de las llamadas telefónicas hacia el exterior y viceversa, garantizando de esta manera la privacidad y la seguridad de las comunicaciones. La privacidad y la seguridad de las comunicaciones, será de acuerdo con lo indicado por el ente regulador OSIPTEL.
  - El CONTRATISTA deberá contar con un Centro de Atención de Averías con un número al que se pueda llamar sin costo desde un teléfono fijo o móvil. El servicio de soporte debe ser permanente 7x24x365 y contar con un sistema de gestión adecuado para reportar fallas y atenciones mediante este centro de atención, así mismo dicha gestión podrá ser realizada médiate correo electrónico designado por el CONTRATISTA.
  - Los servicios deberán estar operativos las 24 horas de los 7 días, por 365 días.

SOBRE LA IMPLEMENTACION Y LA MIGRACION DE LOS SERVICIOS:

- La implementación del servicio debe considerar:
- En el Centro de Datos Principal del CONTRATISTA, los servicios de despliegue de los nodos de hiperconvergencia, instalación de solución de virtualización con parametrización, puesta a punto y migración de hasta 39 servidores virtuales (considerar la conversión de algunos servidores físicos a virtuales), desde el entorno de virtualización actual (VMware) al nuevo entorno. El PROGRAMA NACIONAL PAIS proporcionará el listado de las máquinas virtuales. Esta migración se debe hacer a nivel de máquinas virtuales, sin tener que realizar reinstalación de sistemas operativos, ni entornos de base de datos, ni aplicaciones, ni parametrización de usuarios desde cero. Así mismo, el CONTRATISTA debe configurar las políticas de backup y reglas para 39 máquinas virtuales acorde a lo especificado por PROGRAMA NACIONAL PAIS.
- Para la topología y nodos se tiene solo dos segmentos de red (LAN y DMZ). La migración solo se realizará a nivel de Máquinas virtuales las capacidades necesarias de procesamiento, memoria y almacenamiento estarán en función a su equipamiento ofertado. Cinco servidores se encuentran en el sistema virtualización propio de la ENTIDAD la cual están en el centro de datos del PNPAIS ubicado en Av. Vía Expresa Luis Fernán Bedoya Reyes N° 3245 - Piso 4 (Ex.Paseo de la República), San Isidro – Lima y los treinta y nueve (39) servidores virtuales se encuentran bajo una plataforma Hipervisor VMware están ubicados en el site del principal del CONTRATISTA actual. De existir servicios complementarios que impliquen la operación de la post migración, estas deberán ser previstos y asumidos por el CONTRATISTA. De existir servicios o softwares complementarios que impliquen la operación de la migración, estas deberán ser previstos y asumidos por el CONTRATISTA.
- En el Centro de Datos de Contingencia, el CONTRATISTA deberá proveer una solución integrada a la plataforma de hiperconvergencia para automatizar el proceso de failover y de failback o failover reverso que provea soporte a 3 años y que automatice el proceso para la replicación de hasta 39 máquinas virtuales. El CONTRATISTA debe configurar que el gestor de toda la solución
- Los servicios de despliegue de los nodos de hiperconvergencia, instalación de solución de virtualización con parametrización y puesta a punto y configuración de Jobs de backup / replicación de hasta 39 máquinas virtuales desde el datacenter virtual de producción al datacenter virtual de contingencia. El PROGRAMA NACIONAL PAIS proporcionará el listado de las máquinas virtuales a replicar. Esta replicación / backup se debe hacer a nivel de máquinas virtuales, sin tener que realizar reinstalación de sistemas operativos, ni entornos de base de datos ni aplicaciones, ni parametrización de usuarios desde cero. El CONTRATISTA debe proveer los servicios asociados a la configuración de las políticas y las reglas de backup requeridas por PROGRAMA NACIONAL PAIS y de la replicación entre datacenters virtuales para el número de servicios y en las condiciones que PROGRAMA NACIONAL PAIS lo requiera (no incluye en este aspecto la configuración de backups a cinta ni configuración de procesos de entrega de medios o cintoteca).

- Sobre la solución de hiperconvergencia, se debe incluir y considerar:

#	REQUERIMIENTO
1	Realizar, durante los **30** primeros días del contrato, la planeación de las actividades para el diseño e implementación de la solución
2	Asegurar la continuidad y disponibilidad de todos los servidores antes, durante y después de la ejecución del plan de implementación.
3	Incluir los servicios necesarios para la instalación, configuración e implementación de la solución, a fin de dejar en funcionamiento los sistemas de información con los componentes suministrados.
4	Realizar la entrega, instalación, configuración y puesta en funcionamiento del hardware, software, dispositivos y servicios contratados, de acuerdo con las especificaciones incluidas en el presente documento.
5	Realizar transferencia de conocimientos para 5 personas, en la Administración y Operación de la solución adquirida, dichas capacitaciones serán por un periodo de 40 horas y serán coordinadas con el Personal designado por el PROGRAMA NACIONAL PAIS
6	Ejecutar el plan de diseño e implementación de la solución
7	Realizar seguimiento a la implementación del equipamiento de hiperconvergencia por parte del fabricante de la solución propuesta por 2 semanas.

Se deben entregar los equipos incluidos y disponer su implementación a satisfacción del PROGRAMA NACIONAL PAIS en ambos centros de datos. La garantía, soporte y mantenimiento por sobre los componentes incluidos serán por un plazo máximo de 36 meses contados a partir de la fecha de entrega del fabricante de la solución. Para efectos de los servicios de soporte, se debe considerar:

#	REQUERIMIENTO
1	Dotar al **PROGRAMA NACIONAL PAIS** del acceso al Portal de Soporte Web
2	Informar líneas telefónicas de atención de soporte
3	Entregar la documentación mediante la cual el fabricante especifica el procedimiento y los pormenores de la atención para Soporte, Garantía y Mantenimiento

Asimismo:

#	REQUERIMIENTO
1	Acceso telefónico las 24 horas, todos los días, incluidos los festivos, al centro de recepción de llamadas del fabricante, para soporte (o su equivalente).
2	Envíos a sitio de técnicos o piezas de repuesto a las instalaciones del
3	Asistencia para la solución remota de problemas comunes de soporte
4	Solución de problemas en el sitio disponible cuando el caso de soporte se haya evaluado y determinado que es necesario en el apoyo de campo para un diagnóstico adicional
5	Acceso de foros de soporte en línea las 24 horas
6	Se debe considerar un mantenimiento preventivo de software y hardware anual.

Sobre la migración, se requiere la asesoría, el diseño, la dirección del proceso y la transferencia de conocimiento para realizar las labores de migración y replicación desde la plataforma actual descrita a continuación, teniendo en cuenta los siguientes aspectos:

Infraestructura actual de PNPAIS a migrar a Solución de Hiperconvergencia:

Infraestructura actual de PNPAIS a migrar a Solución de Hiperconvergencia: La solución que busca PROGRAMA NACIONAL PAIS es para reemplazar la infraestructura actual existente, basada en tecnología x86, así como actualizar los SO de los directorios activos de la entidad sin verse afectado a la disponibilidad de su servicio.

N°	VM	CPUs	MEMORIA RAM	DISCO DURO CAPACIDAD EN GB	DIRECCION IP	SISTEMA OPERATIVO	UBICACIÓN
1	Asclepio	2	16	4349.95	192.168.10.52	Microsoft Windows Server 2016 or later (64-bit)	CENTRO DE DATOS PAIS
2	Helios	2	16	11821.63	192.168.10.51	Microsoft Windows Server 2016 or later (64-bit)	CENTRO DE DATOS PAIS
3	Isis	4	64	2355.2	172.168.1.39	Microsoft Windows Server 2016 or later (64-bit)	CENTRO DE DATOS PAIS
4	Ra	8	16	512	172.168.1.42	CentOS 7 (64-bit)	CENTRO DE DATOS PAIS
5	Sigmund	8	16	520	172.168.1.40	Ubuntu Linux (64-bit)	CENTRO DE DATOS PAIS
6	Amon	6	64	2252.8	172.168.1.31	Microsoft Windows Server 2019 (64-bit)	CENTRO DE DATOS CONTRATISTA ACTUAL
7	Anubis	16	64	4399.1	172.168.1.33	Microsoft Windows Server 2019 (64-bit)	CENTRO DE DATOS CONTRATISTA ACTUAL
8	apu	6	32	152	172.168.1.17	Microsoft Windows Server 2012 (64-bit)	CENTRO DE DATOS CONTRATISTA ACTUAL
9	Artemis	50	24	400	172.168.1.24	CentOS 7 (64-bit)	CENTRO DE DATOS CONTRATISTA ACTUAL
10	Astrea	50	125	4992	172.168.1.37	Microsoft Windows Server 2019 (64-bit)	CENTRO DE DATOS CONTRATISTA ACTUAL
11	Atahualpa	1	2	40	192.168.10.20	Microsoft Windows Server 2012 (64-bit)	CENTRO DE DATOS CONTRATISTA ACTUAL
12	Atlas	8	16	204	172.168.1.41	Ubuntu Linux (64-bit)	CENTRO DE DATOS CONTRATISTA ACTUAL
13	Balder	2	8	100	192.168.10.26	Microsoft Windows Server 2016 (64-bit)	CENTRO DE DATOS CONTRATISTA ACTUAL
14	Bragi	2	16	204	172.168.1.23	CentOS 7 (64-bit)	CENTRO DE DATOS CONTRATISTA ACTUAL
15	Cronos	1	8	100	172.168.1.18	CentOS 6 (64-bit)	CENTRO DE DATOS CONTRATISTA ACTUAL
16	Dioniso	1	8	512	192.168.10.21	CentOS 6 (64-bit)	CENTRO DE DATOS CONTRATISTA ACTUAL
17	EOS	6	16	400	192.168.10.42	Microsoft Windows Server 2016 (64-bit)	CENTRO DE DATOS CONTRATISTA ACTUAL
18	Forseti	4	8	480	192.168.10.25	Microsoft Windows Server 2012 (64-bit)	CENTRO DE DATOS CONTRATISTA ACTUAL
19	Freya	32	16	400	172.168.1.29	Ubuntu Linux (64-bit)	CENTRO DE DATOS CONTRATISTA ACTUAL
20	Hebe	2	16	100	192.168.10.27	CentOS 6 (64-bit)	CENTRO DE DATOS CONTRATISTA ACTUAL
21	Hefesto	4	16	100	192.168.10.22	CentOS 6 (64-bit)	CENTRO DE DATOS CONTRATISTA ACTUAL
22	Hel	32	16	400	172.168.1.30	Ubuntu Linux (64-bit)	CENTRO DE DATOS CONTRATISTA ACTUAL
23	Hela	32	132	520	172.168.1.38	Microsoft Windows Server 2019 (64-bit)	CENTRO DE DATOS CONTRATISTA ACTUAL
24	Helius	4	16	800	192.168.10.43	Microsoft Windows Server 2019 (64-bit)	CENTRO DE DATOS CONTRATISTA ACTUAL
25	hera1	8	16	256	172.168.1.14	Microsoft Windows Server 2016 (64-bit)	CENTRO DE DATOS CONTRATISTA ACTUAL
26	Heron	3	8	100	192.168.10.29	CentOS 6 (64-bit)	CENTRO DE DATOS CONTRATISTA ACTUAL

27	Hestia	8	12	122	172.168.1.20	CentOS 7 (64-bit)	CENTRO DE DATOS CONTRATISTA ACTUAL
28	Honos	2	16	300	192.168.10.28	Microsoft Windows Server 2012 (64-bit)	CENTRO DE DATOS CONTRATISTA ACTUAL
29	illapa	8	10	130	192.168.10.31	Microsoft Windows Server 2016 (64-bit)	CENTRO DE DATOS CONTRATISTA ACTUAL
30	Inti	2	8	153	192.168.10.10	Microsoft Windows Server 2012 (64-bit)	CENTRO DE DATOS CONTRATISTA ACTUAL
31	Neptuno	2	8	200	172.168.1.200	Microsoft Windows Server 2019 (64-bit)	CENTRO DE DATOS CONTRATISTA ACTUAL
32	Osiris	4	16	300	192.168.10.156	Microsoft Windows Server 2019 (64-bit)	CENTRO DE DATOS CONTRATISTA ACTUAL
33	Seth	8	16	665	172.168.1.21	Microsoft Windows Server 2019 (64-bit)	CENTRO DE DATOS CONTRATISTA ACTUAL
34	Teseo	8	16	150	172.168.1.15	Microsoft Windows Server 2019 (64-bit)	CENTRO DE DATOS CONTRATISTA ACTUAL
35	Thanos	2	8	122	192.168.10.19	Microsoft Windows Server 2019 (64-bit)	CENTRO DE DATOS CONTRATISTA ACTUAL
36	Tlaloc	2	4	150	172.168.1.16	Microsoft Windows Server 2019 (64-bit)	CENTRO DE DATOS CONTRATISTA ACTUAL
37	Urano	1	8	102	192.168.10.24	CentOS 6 (64-bit)	CENTRO DE DATOS CONTRATISTA ACTUAL
38	Vulcano	3	8	153	192.168.10.23	CentOS 6 (64-bit)	CENTRO DE DATOS CONTRATISTA ACTUAL
39	Hathor	4	8	100	172.168.1.43	Ubuntu Linux (64-bit)	CENTRO DE DATOS PAIS
	TOTAL	348	893	39117.68			

Sobre la capacitación de la solución ofertada, el CONTRATISTA deberá de considerar la siguiente capacitación:

- Se deberá incluir un curso por parte del CONTRATISTA de la solución de Virtualización para 03 personas (mínimo 40 horas).
- Taller de transferencia de conocimientos sobre la instalación y puesta en marcha.
- La realización de estos eventos de capacitación será en fechas coordinadas con PNPAIS, y se realizarán en un plazo de 60 días calendario contados a partir de la conformidad en la entrega y funcionamiento de la solución ofertada.

Sobre la solución de seguridad, se debe considerar la siguiente capacitación:

- Se deberá incluir un curso por parte del CONTRATISTA de la solución de seguridad para 03 personas (mínimo 40 horas).
- Taller de transferencia de conocimientos sobre la instalación y puesta en marcha podrá ser de manera virtual y/o presencial.
- La realización de estos eventos de capacitación será en fechas coordinadas con PNPAIS, y se realizarán en un plazo de 60 días calendario contados a partir de la conformidad en la entrega y funcionamiento de este componente de solución.

Sobre la solución de base de datos de la solución ofertada, se debe considerar la siguiente capacitación:

- Se deberá incluir un curso por parte del CONTRATISTA de base de datos para 02 personas (mínimo 20 horas).
- Taller de transferencia de conocimientos sobre la instalación y puesta en marcha podrá ser de manera virtual y/o presencial.
- La realización de estos eventos de capacitación será en fechas coordinadas con PNPAIS, y se realizarán en un plazo de 60 días calendario contados a partir de la conformidad en la entrega y funcionamiento de este componente de solución.

Sobre la solución de powerbi, se debe considerar la siguiente capacitación:

- Se deberá incluir un curso por parte del CONTRATISTA de power bi para 02 personas (mínimo 20 horas).
- La realización de estos eventos de capacitación será en fechas coordinadas con PNPAIS, y se realizarán en un plazo de 60 días calendario contados a partir de la conformidad en la entrega y funcionamiento de este componente de solución.

6.2. ITEM N° 2: SERVICIO DE ENTORNOS COLABORATIVOS (CORREO ELECTRONICO)

a) LA PLATAFORMA DE PRODUCTIVIDAD Y COLABORACIÓN EN LA NUBE

La herramienta colaborativa debe ser una solución que posibilite a los usuarios la capacidad de trabajar en cualquier momento y desde cualquier lugar, comunicarse con cualquier persona, compartir su trabajo en tiempo real y con total seguridad, utilizar el correo electrónico, el calendario y la información de los contactos desde prácticamente todo tipo de dispositivos, disponer de una intranet de colaboración para todos los empleados y controlar toda la información de la empresa con robustos controles de seguridad y privacidad.

b) CARACTERÍSTICAS DE LA SOLUCIÓN:

SEGURIDAD

La solución debe almacenar los datos en una red propia de centros de datos, ubicadas estratégicamente en todo el mundo y debe ofrecer características de seguridad integrada a todos los clientes y controles opcionales para que estos puedan personalizar las preferencias de seguridad.

Características de seguridad integrada disponibles

- Centros de datos físicos supervisados las 24 horas del día.
- Aislamiento lógico de datos entre distintos clientes.
- Acceso administrativo controlado por un proceso basado en roles.
- Separación de la red interna de centros de datos y la red externa, así como cifrado de los datos transmitidos a través de las redes.
- Cifrado de los datos de correo con el cifrado de BitLocker de 256 bits, así como cifrado SSL/TLS de los datos en tránsito.
- Aplicaciones diseñadas siguiendo el ciclo de vida de desarrollo de seguridad, garantizando la seguridad y privacidad desde el desarrollo del software hasta la puesta en marcha del servicio.

Características de seguridad personalizadas:

- Cifrado avanzado con Rights Management Service que permite a los administradores cifrar elementos de forma selectiva.
- Control de acceso de usuarios, a través de servicios de identidad como Active Directory, Azure Active Directory y los servicios de federación de Active Directory.
- Posibilidad de habilitar características de cumplimiento tales como la prevención de pérdida de datos para impedir que la información confidencial salga de la organización.
- Características de retención legal, gobierno y archivado que permiten retener datos confidenciales con fines legales y de archivado.
- Facilidad para encontrar rápidamente elementos en Sharepoint Online, Exchange Online y Skype empresarial con fines de auditoría y seguridad.
- Los administradores pueden personalizar fácilmente las características de antimalware y de protección contra correo no deseado.

PRIVACIDAD

La solución debe contemplar tecnologías que mejoran y respetan la privacidad de sus servicios. Se debe considerar que en todo momento los datos pertenecen a los usuarios del Programa Nacional PAIS y que:

- No se examinan los correos ni los documentos para elaborar análisis, extraer datos o mejorar el servicio.
- Los datos no se mezclan: La herramienta colaborativa permite mantener los datos separados.

COMPROMISO

La herramienta colaborativa debe estar provista de capacidades que ayudan a adecuarse a las regulaciones externas de la industria y a cumplir los requisitos internos de seguridad.

CONTROL DE CALIDAD

La herramienta colaborativa debe adherirse a normas mundiales del sector, incluidas la norma ISO 27001, las Cláusulas modelo de la UE, el acuerdo HIPAA BAA y la ley FISMA. Asimismo, se somete a auditorías de terceros por parte de auditores de reconocido prestigio internacional con el fin de obtener un testimonio independiente del cumplimiento de las directivas y los procedimientos de seguridad, privacidad, continuidad y normativas.

TRANSPARENCIA

El PNPAIS puede identificar en todo momento dónde se encuentran sus datos, qué usuarios de la institución pueden acceder a ellos y qué hacen con la información.
Además, los administradores de TI designados por PNPAIS pueden elegir recibir actualizaciones relacionadas con los cambios de ubicación de los centros de datos, así como información de seguridad, privacidad y auditoría.

c) PLANES REQUERIDOS DEL SERVICIO.

Los planes requeridos son según el perfil de los usuarios:

550 usuarios usarán el plan básico (solo buzón de correo) o equivalente.

CORREO Y CALENDARIO.

- Hospedaje de correo con un buzón de 50 GB y enviar mensajes de hasta 150MB.
- Usa tu propio nombre de dominio personalizado (por ejemplo, tunombre@tuempresa.com)
- La Bandeja de entrada deberán facilitar el seguimiento de los mensajes de correo más importantes. El buzón deberá incluir dos pestañas: Prioritarios, para los mensajes de correo que necesitan una acción inmediata, y Otros, para todos lo demás. Puedes cambiar las pestañas en cualquier momento y ver siempre cómo el correo pasa a Otros.
- Los calendarios deberán permitir programar reuniones y accede a las características de colaboración, como el uso compartido de calendarios, grupos, la lista global de direcciones, los contactos externos, las tareas, las salas de conferencias y las funciones de delegación.

300 usuarios usarán el plan básico que tenga ofimática en las versiones web y móviles o equivalente.

- La solución ofertada debe proveer como mínimo las siguientes herramientas de colaboración en la nube:
  - Procesador de Texto.
  - Hojas de Cálculo.
  - Presentaciones.
  - Calendario.
  - Bloc de Notas.
  - Alojamiento Web.
  - Almacenamiento en nube.
  - Videoconferencia.
  - Mensajería instantánea, chat para grupos
- Permitir el acceso a las funcionalidades de la plataforma desde dispositivos iOS y Android que cuenten con acceso a internet.
- Coautoría en tiempo real para que varios usuarios puedan trabajar en el mismo documento de forma simultánea
- Hospedaje de correo con un buzón principal de 50 GB y enviar mensajes de hasta 150MB, opcionalmente habilitar buzón de “ARCHIVO” en la nube de 50 Gb.
- Usa tu propio nombre de dominio personalizado (por ejemplo, tunombre@tuempresa.com)
- Correo de categoría empresarial en dispositivos móviles, tabletas, escritorios y la Web
- Administrar el calendario, compartir tu disponibilidad, programar reuniones y recibir avisos
- Programa reuniones y responde a invitaciones con facilidad mediante calendarios compartidos
- Configurar nuevos correos de usuario, restaurar cuentas eliminadas recientemente, crear scripts personalizados y mucho más, desde cualquier lugar
- Permite acceder desde la web para realizar trabajo en equipo y comunicación
- La herramienta debe Hospedar las reuniones online y videollamadas para hasta 250 asistentes

- La herramienta debe de poder comunicar a través de texto con cualquier usuario desde cualquier lugar
- La herramienta debe de unir todas las aplicaciones, los archivos, las reuniones y los mensajes de texto de los usuarios del PN PAIS para que puedas comunicarte y colaborar fácilmente desde cualquier lugar
- La Herramienta debe de crea sitios de equipo para compartir información, contenido y archivos a través de tu intranet.

ALMACENAMIENTO Y USO COMPARTIDO DE ARCHIVOS

- la herramienta debe de tener un 1 TB de almacenamiento en la nube para almacenamiento y uso compartido de archivos por usuarios.
- la herramienta debe poder tener la capacidad de trabajar un archivo y guárdalo directamente al almacenamiento en la nube (los cambios se actualizarán en todos los dispositivos sincronizados)
- la herramienta debe de compartir archivos con contactos externos proporcionándoles acceso o vínculos de invitado.
- la herramienta debe de compartir documentos de forma segura y enviar correos para que solo aquellos con los permisos adecuados puedan obtener acceso a la información
- la herramienta debe de poder de tener acceso a archivos y sincronizarlos en equipos Windows o Mac o en dispositivos móviles

SEGURIDAD Y CUMPLIMIENTO

- la herramienta debe de Proteger el correo ante software malintencionado, correo no deseado y amenazas conocidas.
- la herramienta debe de Controlar quién tiene acceso a la información del PNPAIS y grupos de seguridad y permisos personalizados
- la herramienta debe permitir crear directivas de contraseña que requieran que los usuarios restablezcan sus contraseñas después de un número de días especificado.

30 usuarios usarán el plan E3 o equivalente que tenga ofimática en las versiones web y móviles

- La solución ofertada debe proveer como mínimo las siguientes herramientas de colaboración en la nube:
  - Procesador de Texto.
  - Hojas de Cálculo.
  - Presentaciones.
  - Calendario.
  - Bloc de Notas.
  - Alojamiento Web.
  - Almacenamiento en nube.
  - Videoconferencia.
  - Mensajería instantánea, chat para grupos.
- Permitir el acceso a las funcionalidades de la plataforma desde dispositivos iOS y Android que cuenten con acceso a internet.
- Coautoría en tiempo real para que varios usuarios puedan trabajar en el mismo documento de forma simultánea
- Hospedaje de correo con un buzón principal de 50 GB y enviar mensajes de hasta 150MB, opcionalmente habilitar buzón de “ARCHIVO” en la nube de 50 Gb.
- Usa tu propio nombre de dominio personalizado (por ejemplo, tunombre@tuempresa.com)
- Correo de categoría empresarial en dispositivos móviles, tabletas, escritorios y la Web
- Administrar el calendario, compartir tu disponibilidad, programar reuniones y recibir avisos
- Programa reuniones y responde a invitaciones con facilidad mediante calendarios compartidos
- Configurar nuevos correos de usuario, restaurar cuentas eliminadas recientemente, crear scripts personalizados y mucho más, desde cualquier lugar
- Permite acceder desde la web para realizar trabajo en equipo y comunicación
- La herramienta debe Hospedar las reuniones online y videollamadas para hasta 250 personas
- La herramienta debe de poder comunicar a través de texto con cualquier usuario desde cualquier lugar
- la herramienta debe de unir todas las aplicaciones, los archivos, las reuniones y los mensajes de texto de los usuarios del PN PAIS para que puedas comunicarte y colaborar fácilmente desde cualquier lugar

- La Herramienta debe de crea sitios de equipo para compartir información, contenido y archivos a través de tu intranet.
- La herramienta debe permitir crear aplicaciones que necesitas y realizarlas de forma personalizable
- La herramienta debe permitir la creación de flujos de trabajo para la automatización de tareas repetitivas
- La herramienta debe permitir la programación de citas programadas por clientes internos y externos a la organización

ALMACENAMIENTO Y USO COMPARTIDO DE ARCHIVOS

- la herramienta debe de tener un 1 TB de almacenamiento en la nube para almacenamiento y uso compartido de archivos por usuarios.
- la herramienta debe poder tener la capacidad de trabajar un archivo y guárdalo directamente al almacenamiento en la nube (los cambios se actualizarán en todos los dispositivos sincronizados)
- la herramienta debe de compartir archivos con contactos externos proporcionándoles acceso o vínculos de invitado.
- la herramienta debe de compartir documentos de forma segura y enviar correos para que solo aquellos con los permisos adecuados puedan obtener acceso a la información
- la herramienta debe de poder de tener acceso a archivos y sincronizarlos en equipos Windows o Mac o en dispositivos móviles

20 usuarios usarán el plan E5 o equivalente que tenga ofimática en las versiones web y móviles

- Además de cumplir todo lo anterior, debe cumplir con:
- Versiones de escritorio de aplicaciones de Ofimática para equipos PC y Mac
- la herramienta debe de cumplir con las Versiones completamente instaladas y actualizadas de herramientas ofimáticas.
- la herramienta debe de cumplir con que cada usuario puede instalar las aplicaciones de Ofimática hasta en cinco equipos PC o Mac.

PROTECCIÓN CONTRA AMENAZAS AVANZADA

- la herramienta debe de Ayudar a proteger contra amenazas sofisticadas ocultas en datos adjuntos y vínculos de correo, y proporciona defensas de última tecnología contra amenazas de día cero, ransomware y otros intentos de malware avanzado con Protección contra amenazas avanzada.
- la herramienta debe de Eliminar de forma remota los datos de la empresa de dispositivos robados o perdidos con Borrado selectivo de Intune
- la herramienta debe de Restringir el copiado o guardado de información de la empresa por parte de aplicaciones no autorizadas y ubicaciones con Protección de aplicaciones para Aplicaciones móviles.
- la herramienta debe de permitir controlar quién tiene acceso a la información de la empresa aplicando restricciones como No copiar y No reenviar con Information Rights Management.
- la herramienta debe de permitir Aplicar directivas que proporcionan resistencia contra amenazas de prevulneración
- la herramienta debe de permitir reforzar la protección contra malware para mantener tus dispositivos con Windows 10 libres de virus, spyware y otro software malicioso.
- la herramienta debe permitir Habilitar el almacenamiento en la nube y las directivas de conservación a largo plazo para asegurarte de que nunca pierdes un correo con Archivado

ADMINISTRACIÓN DE PC Y DISPOSITIVOS MÓVILES

- la herramienta debe de permitir Configurar las características de seguridad y la configuración en PC con Windows 10 y dispositivos móviles con iOS o Android® con un asistente de configuración fácil de usar la herramienta debe permitir Usar controles simplificados para administrar directivas aplicadas a PC con Windows 10.
- La herramienta debe de permitir Implementar automáticamente las aplicaciones de Ofimática en equipos PC con Windows 10.
- El CONTRATISTA deberá encargase de la migración de las 600 casillas de correo, configuración de dominio, migración de datos, habilitación de la consola de administración, sincronización con el dominio local del programa y todo lo que resulte necesario para operativizar el servicio.
- Se precisa la migración hace referencia a las 600 cuentas de correo electrónicos que la entidad cuenta.
- Se precisa que el CONTRATISTA podrá utilizar las capacidades de la plataforma de hiperconvergencia o el servidor de dominio de la entidad para la sincronización con el dominio local.

- la herramienta debe de permitir Configurar los equipos del PN PAIS para que instalen automáticamente las actualizaciones.
- la herramienta debe de permitir Aplicar directivas de seguridad para proteger los datos de la empresa en todos tus dispositivos, incluidos los dispositivos iOS, Android® y PC Windows con la Administración de dispositivos móviles de Intune

- Para ambos planes, considerar como soporte técnico e implementación
  - Soporte técnico telefónico y en línea ininterrumpido.
- El soporte técnico se realizará únicamente en modalidad remota, es decir vía telefónica o en línea. De ser requerido, ante una situación de complejidad, se podrá coordinar un soporte presencial.
  - 99.99 por ciento de tiempo de actividad garantizada
  - Podrá realizar backup de manera segura en las instalaciones de PN PAIS a través de agentes hasta un límite máximo de 20 cuentas correo electrónico en simultaneo la cual será alojada en la solución de hiperconvergencia.

d) SOFTWARE DE BACKUP PARA TODAS LAS CUENTAS DE CORREO DE LA SOLUCIÓN OFERTADA.

- Se deberá asignar un único espacio en nube para ejecutar, administrar y almacenar los respaldos generados. El tamaño de almacenamiento de toda la información de copias de seguridad y respaldo deberá tener como mínimo 30TB, esto incluye los respaldos generados por el servicio de correo y entornos colaborativos.
- Protección integral de datos: La solución debe permitir realizar copias de seguridad de la solución de correo ofertada, incluyendo buzones de correos electrónicos, calendarios, contactos.
- El respaldo para los buzones será de forma ilimitada.
- Para el servicio de backup se deberá contemplar que los respaldos se realicen de manera automática hasta 02 backups diarios.
- El espacio de almacenamiento en la nube para los respaldos deberá almacenarse en el misma plataforma de la solución de respaldo ofertada o en un espacio en la nube que cumpla con los estándares de seguridad de información tal como certificado ISO 27001 y reporte Soc2.
- Copias de seguridad automáticas y programadas: Se podrá programar copias de seguridad automáticas según las necesidades, permitiendo la protección continua de los datos. Con opciones flexibles para definir las políticas de retención y versionado de los respaldos.
- Recuperación granular: La solución debe permitir restaurar elementos individuales, como correos electrónicos, contactos, archivos y elementos de las aplicaciones de la solución ofertada, sin tener que restaurar todo el respaldo. Esto para agilizar el proceso de recuperación y minimizar el tiempo de inactividad.
- Búsqueda y recuperación avanzada: La solución debe ofrecer potentes capacidades de búsqueda para ayudarte a encontrar rápidamente los datos que necesitas recuperar. Puedes buscar y recuperar elementos específicos según palabras clave, filtros de fecha, remitentes, receptores, etc.
- Cumplimiento normativo y protección contra pérdida de datos: La solución debe garantizar el cumplimiento normativo y ayudar a prevenir la pérdida accidental o intencional de datos críticos. Poder realizar copias de seguridad fuera de la plataforma y mantener los datos respaldados en un entorno seguro y controlado.
- Informes y supervisión: La solución debe proporcionar informes detallados sobre las actividades de copia de seguridad y recuperación, lo que te permitirá evaluar y auditar fácilmente el estado de los datos respaldados. También ofrecer alertas y notificaciones para mantenerse informado sobre el estado de las copias de seguridad.

e) SERVICIO DE ANTISPAM AVANZADO EN LA NUBE PARA TODAS LAS CUENTAS DE CORREO Y HERRAMIENTAS COLABORATIVAS DE LA SOLUCIÓN OFERTADA

- Deberá brindar un 99,9% de disponibilidad en el servicio.
- Deberá tener características antispam, antivirus, anti-spyware y anti-phishing.
- Deberá ser capaz de realizar la inspección de malware del correo entrante y saliente.
- La solución se deberá conectar en tiempo real con la base de datos del fabricante propuesto para descargar actualizaciones de Anti-Spam.
- Deberá proporcionar protección contra ataques de denegación de servicio, tales como mail bomb.
- Deberá permitir la implementación de listas negras y listas blancas.
- Deberá ser capaz de ejecutar el análisis antivirus / antispyware en archivos comprimidos como ZIP, PKZIP, LHA, ARJ y RAR.
- Deberá detectar firmas de spam y archivos adjuntos.
- Deberá detectar URL de spam, malware y phishing.

- Los motores de análisis antivirus/antimalware y antispam deberán ser provistos por el mismo fabricante del antispam propuesto.
- Deberá ser capaz de filtrar y analizar los archivos adjuntos y el contenido del e-mail.
- Deberá ser capaz de realizar una inspección minuciosa de los encabezados de correo electrónico.
- Deberá ser capaz de realizar análisis bayesiano para determinar si un correo es spam.
- Deberá ser capaz de filtrar mensajes de correo electrónico basados en los URI (Uniform Resource Identifier) contenidas en el cuerpo del mensaje.
- Deberá ser compatible con Sender Policy Framework (SPF).
- Deberá ser compatible con Domain Keys Identified Mail (DKIM).
- Deberá ser compatible con Domain Based Message Authentication (DMARC).
- Permitir que se informe de la actividad, el análisis de los archivos de eventos (logs) y presentarlos en formato de tabla o gráfica.
- Generar informes por demanda o programados a intervalos de tiempo específicos.
- Generar y enviar informes en formato PDF o HTML.

f) 01 licencia para almacenamiento de archivos

- Almacenamiento de 25TB para archivos, fotos y vídeos.
- Debe tener prevención de perdida de datos avanzada de tal forma que ayude a proteger la información confidencial de amenazas como el malware, el ransomware y el phishing. Debe usar aprendizaje automático para identificar y bloquear archivos potencialmente maliciosos.
- Debe permitir la copia de seguridad automática de dispositivos
- Debe permitir el acceso a archivos desde cualquier dispositivo
- Debe permitir compartir archivos fácilmente con otros
- Debe permitir la sincronización de archivos entre dispositivos

CAPACITACIÓN Y/O ENTRENAMIENTO

- El postor adjudicado realizará capacitaciones dirigidas tanto al personal técnico responsable de la administración del servicio como a los usuarios finales del mismo.
- La capacitación será virtual y serán tres (03) durante el tiempo de vigencia del contrato, según se detalla a continuación:
- La capacitación dirigida a los usuarios finales deberá tener una explicación de las funcionalidades a nivel usuario básicas hasta funcionalidades avanzadas de la herramienta de correo electrónico, almacenamiento y mensajería instantánea. Estas capacitaciones serán a usuarios finales internos del PNPAIS y tendrán una duración de seis (06) horas, las cuales serán distribuidas entre las Unidades Organicas y Territoriales del Programa Nacional PAIS.
- La capacitación a nivel de administrador incluirá las funcionalidades básicas hasta funcionalidades avanzadas de administración de las herramientas de correo electrónico, anti spam, y el proceso de respaldo de correos tanto nivel Cliente corno a nivel Servidor. También deberá incluir conceptos importantes, como descripción del alcance de suscripción, beneficios, ingreso a la plataforma, y otros temas de gestión y operación relevantes para la administración del servicio. Esta capacitación deberá contemplar un número de seis (06) usuarios con una duración total de doce (12) horas.
- Las capacitaciones serán virtuales e incluirán manuales y videos tutoriales en formato digital para todos los participantes. El horario será coordinado con el responsable de la Unidad de Tecnologías de la Información.
- El postor deberá incluir la certificación no oficial para cada uno de los participantes.
- Se debe de realizar un chat bot virtual para soporte en mediante una plataforma de chat y videollamadas

GESTIÓN DEL SERVICIO

- Monitoreo
  El servicio de monitoreo realizará la supervisión de la disponibilidad, el estado de salud y rendimiento. Además de los siguientes;
  - Monitoreo de los servicios de sincronización de identidades locales a nube.
  - Monitoreo del servicio Antispam, anti-phishing, anti-malware, Identificación de remitentes de spam frecuentes.
  - Monitoreo de las Alertas configuradas, tales como DLP, log de servidor de correo.
  - Monitoreo y seguimiento de los casos abiertos y su escalamiento.
- Información de uso
  - Utilización de suscripciones adquiridas
  - Próxima expiración de suscripciones
  - Utilización de los Servicios en nube como (Correo electrónico, Sharepoint y Teams)
  - Envío del listado de la cantidad de usuarios activos en los servicios de nube

    - Información de Usuarios y la última fecha de interacción con el servicio de correo electrónico.
- Información de acceso
    - Acceso satisfactorio o fallido
    - Estado de usuarios (Altas, bajas)
    - Usuarios con contraseñas próximas a expirar
- Actividades de Operación.
    - Gestión de acceso para usuarios con roles administrativos, operativa, de auditoria o de visualización de informes. La retención de los logs deber ser no menor de 60 días.
    - Creación de grupos con fines de asignación de licencias
    - Activación / desactivación de reglas
    - Cambios en Antispam
    - Realizar la gestión de los respaldos de los buzones de correo.
- Gestión de Incidencias
    - Atención 24x7x365, atención de incidentes y escalamiento al fabricante de la solución en nube (en caso ser necesario).
    - El proveedor deberá de brindar un Asistente Virtual (Bot) para poder responder las consultas frecuentes de los usuarios de la entidad. Esto con la finalidad de reducir las atenciones de soporte de la OTI antes consultas de la solución de productividad que tengan los usuarios de la entidad durante la duración de vigencia de las licencias. Esto es muy independiente a las incidencias que la OTI pueda reportar y deban ser atendidas por el proveedor.
    - El servicio de soporte remoto deberá de tener un tiempo de solución no mayor de 2 horas para incidentes y/o problemas en el servicio ofertado; y un tiempo de solución no mayor a 48 horas para temas de requerimiento y/o consultas.
- Herramientas de gestión avanzada
    - Para la correcta gestión del servicio se deberá de contar con un Panel de visualización de los servicios contratados, así como la consulta al estado de salud del mismo.
    - Portal de gestión de incidencias/requerimientos.

6.3. CONTRATISTA TODOS LOS ITEMS

Condiciones Generales:

- Tener Registro Único de Contribuyente habilitado.
- Tener Código de Cuenta Interbancario registrado.
- Tener Registro Nacional de CONTRATISTA.

Condiciones Particulares PARA ITEM 1:

- El CONTRATISTA debe contar con experiencia en la contratación de servicios iguales o similares al objeto de la contratación.
- Deberá contar con soporte técnico en castellano, vía telefónica, remota o presencial.
- No estar impedido para contratar con el Estado.
- El CONTRATISTA debe acreditar un monto facturado acumulado equivalente a no mayor a una vez el valor estimado del ítem, por la contratación de servicios iguales o similares al objeto de la convocatoria, durante los ocho (8) 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.
- El CONTRATISTA debe contar con experiencia en la contratación de servicios iguales o similares al objeto de la contratación con lo siguiente:
    - Servicio de Internet
    - Servicio de Enlace de Datos
    - Servicio de hosting o housing o alojamiento de gabinetes y equipos de telecomunicaciones)
    - Servicio de Acceso a Internet
    - Servicio de Acceso Dedicado a Internet
    - Servicio de Transmisión de Datos
    - Servicio de Interconexión de Datos
    - Servicio de telco
    - Servicio de cloud u onpremise
    - Servicio de cableado para fibra óptica o puntos de red
    - Servicio de transmisión de datos e internet satelital

Condiciones Particulares PARA ITEM 2:

- El CONTRATISTA debe contar con experiencia en la contratación de servicios iguales o similares al objeto de la contratación.
- Deberá contar con soporte técnico en castellano, vía telefónica, remota o presencial.
- No estar impedido para contratar con el Estado.

- El CONTRATISTA debe acreditar un monto facturado acumulado equivalente a no mayor a una vez el valor estimado del ítem, por la contratación de servicios iguales o similares al objeto de la convocatoria, durante los ocho (8) 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.
- El CONTRATISTA debe contar con experiencia en la contratación de servicios iguales o similares al objeto de la contratación con lo siguiente:
    - Se consideran servicios similares a los siguientes:
    - Servicio de entornos colaborativos.
    - Servicio de correo electrónico.
    - Videoconferencia
    - Telefonía

Acreditación:
La experiencia del CONTRATISTA se acreditará con copia simple de (i) contratos u órdenes de compra, 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 pago[1].

6.4. LUGAR DE LA PRESTACION DEL SERVICIO TODOS LOS ITEMS:
La prestación se realizará donde la naturaleza del servicio lo exija, teniendo como punto de coordinación la Sede Central del Programa Nacional PAIS, sito en Av. Vía Expresa Luis Fernán Bedoya Reyes N° 3245 - Piso 6 (Ex. Paseo de la República), San Isidro.

6.5. SISTEMA DE CONTRATACIÓN TODOS LOS ITEMS
La presente contratación será a Suma alzada.

6.6. PLAZO DE ENTREGA DEL SERVICIO TODOS LOS ITEMS
El plazo de vigencia del servicio será de mil noventa y cinco (1095) días calendarios.

- **PLAZO DE IMPLEMENTACION PARA ITEM 1**
  el plazo de implementación del servicio será de ciento veinte (120) días calendarios contado a partir de firmado el contrato.

- **PLAZO DE IMPLEMENTACION PARA ITEM 2**
  el plazo de implementación del servicio será de cinco (05) días calendarios contado a partir de firmado el contrato.

6.7. CONDICIONES Y MODALIDADES DE PAGO TODOS LOS ITEMS
Primer Pago:
Comprende la implementación, instalación de toda la solución ofertada la cual se evidenciará con el acta de instalación en un formato designado por el contratista la cual debe tener una letra legible, con la fecha de instalación del servicio, nombre completo y firma del encargado de las Unidades Territoriales y/o sedes lima.
El costo de la instalación será cancelado al término de la totalidad de la implementación y entrega de la totalidad de los servicios, junto con el primer mes de servicio, Previo informe del jefe de la Unidad de Tecnologías de la Información.

El pago se efectuará de forma mensual con abono en cuenta, en moneda nacional, posterior a la conformidad de servicios.

---

[1] Cabe precisar que, de acuerdo con la **Resolución N° 0065-2018-TCE-S1 del Tribunal de Contrataciones del Estado**:

"… el solo sello de cancelado en el comprobante, cuando ha sido colocado por el propio CONTRATISTA, 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 CONTRATISTA afirmando que el comprobante de pago ha sido cancelado"
(…)
"Situación diferente se suscita ante el sello colocado por el cliente del CONTRATISTA [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 conformidad deberá ser emitida dentro del plazo máximo de 07 días de presentado el entregable y/o producto
- El pago deberá efectuarse dentro de un plazo máximo de diez (10) días de emitida la conformidad.

7. CONFORMIDAD DE LA PRESTACION TODOS LOS ITEMS

La conformidad de servicios será otorgada por el Jefe y/o Coordinador de la Unidad de Tecnologías de la Información, previo informe del personal designado.
De existir observaciones, el PNPAIS comunicará al CONTRATISTA del servicio, indicando claramente el sentido de estas, otorgándole un plazo para subsanar no menor de dos (02) ni mayor de ocho (08) días, dependiendo de la complejidad o sofisticación de la contratación. Si pese al plazo otorgado, el CONTRATISTA del servicio no cumpliese a cabalidad con la subsanación, el PNPAIS puede otorgarle periodos adicionales para las correcciones pertinentes. En este supuesto corresponde aplicar la penalidad por mora desde el vencimiento del plazo para subsanar.
Conformidad de la prestación del servicio acompañado de los entregables detallados en el numeral 8.

Para el primer pago el proveedor deberá presentar el acta de instalación y activación de todos los servicios.

8. PRODUCTOS O ENTREGABLES PARA TODOS LOS ITEMS
Entregable de instalación: Informes de Instalación de los servicios:

EL CONTRATISTA DEBERA DE ENTREGAR LAS ACTAS DE INSTALACION DE TODOS LOS COMPONENTES DE LA SOLUCION OFERTADA QUE SE DETALLAN A CONTINUACION PARA ITEM 1

- Acta de Instalación del servicio de Conectividad de enlace de datos de las Unidades Territoriales, Sedes Lima y sede Central del Programa Nacional PAIS.
- Acta de Instalación del servicio de internet del ancho de banda contratado de los centros de datos principal y contingencia.
- Acta de instalación de la Fibra óptica ultra rápida entre centro de datos principal y contingencia.
- Acta de Instalación de los componentes de la solución ofertada en los centros de datos principal y contingencia del CONTRATISTA.

EL CONTRATISTA DEBERA DE ENTREGAR LAS ACTAS DE INSTALACION DE TODOS LOS COMPONENTES DE LA SOLUCION OFERTADA QUE SE DETALLAN A CONTINUACION PARA ITEM 2

- Acta de inicio y/o implementación del servicio del servicio

Entregable mensual: Informes Mensuales (PARA EL ITEM1):

- Reporte de la Conectividad de enlace de datos de las Unidades Territoriales, Sedes Lima y sede Central del Programa Nacional PAIS.
- Reporte del servicio de internet del ancho de banda contratado de los centros de datos principal y contingencia.
- Reporte de la conexión de la Fibra óptica ultra rapida entre el centro de datos principal y contingencia.
- Reporte del consumo de tráfico, aplicaciones, servicios web entre otros de los equipos de seguridad Informática de la red del Programa Nacional PAIS en comodato.

El plazo para los informes mensuales podrá ser presentados dentro de los quince (15) días calendarios posteriores al termino de casa mes posterior al inicio del servicio. Este informe será presentado por mesa de partes de la entidad.

9. SEGURIDAD DE LA INFORMACION TODOS LOS ITEMS

- El CONTRATISTA se compromete a mantener en reserva y no revelar a tercero alguno, sin previa conformidad escrita del PN PAIS, 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 y subcontratistas, sobre la base de "necesidad de conocer".

- El CONTRATISTA se compromete (excepto que la Ley dispusiera lo contrario o resultare necesario para obtener consejo profesional en relación con este Contrato) a no revelar ni permitir la revelación de cualquier detalle a los medios de prensa o a terceros, y a no usar el nombre del PN PAIS en cualquier promoción, publicidad o anuncio, sin previa autorización escrita.

- El CONTRATISTA deberá adoptar las medidas de índole técnica y organizativas necesarias para que el contenido de dicha información no se divulgue a terceros sin autorización expresa de la PN PAIS, para garantizar la seguridad de los datos de carácter personal y evitar su alteración.

10. PENALIDADES TODOS LOS ITEMS

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 con 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 ciento veinte (120) 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.

Cuando se llegue a cubrir el monto máximo de la penalidad, equivalente al diez por ciento (10%) del monto del contrato vigente, la Entidad podrá resolver el contrato a través de carta simple sin requerir previamente el cumplimiento al contratista.

11. OTRAS PENALIDADES TODOS LOS ITEMS

Se define el nivel de acuerdo del servicio como el compromiso por parte del CONTRATISTA para ofrecer servicios de calidad, en función a la calidad de atención ante averías.

Penalidad por caída del servicio

SUPUESTO DE APLICACIÓN DE PENALIDAD	FORMA DE CALCULO	PROCEDIMIENTO DE VERIFICACIÓN
Por un tiempo entre 8 minutos y 30 minutos al mes	05% del pago mensual del componente averiado.	Informe del área usuaria.
Por un tiempo entre 30 minutos y 100 minutos al mes	08% del pago mensual del componente averiado.	Informe del área usuaria.
Por un tiempo mayor a 100 minutos al mes	10% del pago mensual del componente averiado.	Informe del área usuaria.

Se detecta la caída del servicio, el área usuaria solicita atención al proveedor a través de llamada telefónica, ticket o correo electrónico a su centro de atención con copia a la Unidad de Administración y otros correos que proporcione el proveedor, y se contabilizará desde ese instante el tiempo de interrupción del servicio.

Para el cálculo de estas penalidades el CONTRATISTA debe entregar una estructura de costos detallada por componentes.

Incumplimiento en la entrega de la documentación solicitada.

- Se aplicará una penalidad del 10% de la UIT vigente a la fecha de ocurrido el incumplimiento, por cada día calendario de retraso en la entrega.
- Según lo indicado en el informe de la Unidad de Tecnologías de la Información.

- 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.

12. PROPIEDAD INTELECTUAL TODOS LOS ITEMS

De acuerdo con la materia de contratación, hay que precisar que la entidad tendrá todos los derechos de propiedad intelectual (sin limitación, patentes, derechos de autor, nombres comerciales y marcas registradas respecto a los productos u otros materiales relacionados a la contratación).

13. ANTICORRUPCION TODOS LOS ITEMS

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 con el 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. 12. RESPONSABILIDAD POR VICIOS OCULTOS Indicar el plazo máximo de responsabilidad que tendrá el contratista por la calidad ofrecida y por los vicios ocultos de los servicios efectuados, cuyo plazo no podrá ser menor a un (01) año contado a partir de emitida la conformidad.

14. OTRAS CONDICIONES TODOS LOS ITEMS

En esta sección se debe adjuntar la información adicional que se considere relevante para el cumplimiento del servicio.

15. SOLUCIÓN DE CONTROVERSIAS TODOS LOS ITEMS

Los conflictos que se deriven de la ejecución e interpretación de la presente contratación son resueltos mediante trato directo, conciliación y/o acción judicial.

16. REQUISITOS DE CALIFICACIÓN

CAPACIDAD LEGAL
HABILITACIÓN
<u>ITEM N° 01</u> Requisitos: • Contar con autorización del Ministerio de Transportes y Comunicaciones para la prestación del servicio solicitado ó la autorización del Ministerio de Transportes y Comunicaciones para brindar Servicios de Valor Añadido según Ley de las Telecomunicaciones • Debe ser miembros activos NAP Perú. Acreditación: • Copia del documento de autorizaciones para brindar el servicio de transmisión datos, Internet emitida por el Ministerio de Transporte y Telecomunicaciones. • Se aceptará una impresión de la página Web del NAP Perú, para certificar ser miembro de la Asamblea, incluyendo en la impresión la fecha del mismo. **<u>ITEM N° 02</u>** Requisitos: • El proveedor deberá ser partner y/o distribuidor autorizado del fabricante de la solución

ofertada.

Acreditación:

- Copia de carta emitida por fabricante o cartas brindadas por el subsidiario local en nombre del fabricante donde se especifique la razón social y el ID o código de partner. Se aceptarán cartas de fabricantes o cartas brindadas por el subsidiario local en nombre del fabricante donde indique que el CONTRATISTA es un canal autorizado.

CAPACIDAD TÉCNICA Y PROFESIONAL

INFRAESTRUCTURA ESTRATÉGICA

ITEM N° 01

Requisitos:

- Los Centros de datos principal y contingencia CONTRATISTA deberá ser propios o alquilados, ubicado en la ciudad de Lima (Perú) y deberán contar con certificación TIER-3 en sostenibilidad operacional y/o diseño otorgado por el UpTime Institute y/o Norma ANSI/TIA-942-B con una vigencia durante el periodo del contrato.
- Los proveedores podrán participar en consorcio para cumplir este requerimiento pudiendo cada socio brindar un servicio diferente.

Acreditación:

- Copia de documentos que sustenten la propiedad, la posesión, el compromiso de compraventa o alquiler u otro documento que acredite la disponibilidad de la infraestructura estratégica.
- Las características de TIER-III se deberán acreditar mediante el certificado emitido por el Uptime Institute y/o Norma ANSI/TIA-942-B el cual deberá mantenerse vigente durante la prestación del servicio.

CALIFICACIONES DEL PERSONAL CLAVE

FORMACIÓN ACADÉMICA

ITEM N° 01 y 02

GESTOR DEL PROYECTO (01 PERSONA)

Requisitos:

Titulado profesional o Bachiller en Ingeniería de Telecomunicaciones y/o Sistemas y/o Ingeniería electrónica y/o Ingeniería de Computación

Nota:

Se precisa que la colegiatura y habilitación profesional se debe presentar para el inicio de su participación efectiva en el servicio.

Acreditación:

El título profesional o grado de bachiller en Ingeniería de Telecomunicación y/o Sistemas requerido 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 : http://www.titulosinstitutos.pe/, según corresponda. En caso de que el título o grado requerido no se encuentre inscrito en el referido registro, el CONTRATISTA debe presentar la copia del diploma respectivo a fin de acreditar la formación académica requerida.

CAPACITACIÓN

ITEM N° 01

Requisitos:

GESTOR DEL PROYECTO (01 PERSONA)

- Diplomado en gestión de proyectos con duración mínima de 120 horas lectivas
  Adicionalmente, deberá contar con la certificación PMP vigente emitido por organismo autorizado a nombre del PMI donde se indique el número de registro.
  Para el programa en gestión de tecnologías de información se aceptará los certificados emitidos por una entidad educativa autorizada indicando la cantidad de horas lectivas.

  Acreditación:

- Se acreditará con copia simple de constancia o certificado correspondiente

ITEM N° 02

Requisitos:

GESTOR DEL PROYECTO (01 PERSONA)

- Deberá contar con la certificación PMP vigente emitido por organismo autorizado a nombre del PMI donde se indique el número de registro.

- Deberá contar con certificación ITIL vigente.
- Contar con certificado oficial en la solución de correo ofertada.
- Contar con certificado oficial a nivel Professional en la solución de respaldo (backup) ofertada.

ESPECIALISTA DE LA SOLUCIÓN (01 PERSONA)

- Deberá contar con curso y/o certificado en gestión de proyectos y/o PMP.
- Deberá contar con curso y/o certificado en ITIL.
- Contar con certificado oficial de seguridad en la solución de correo ofertada a nivel Associate o Intermedio.
- Contar con certificado oficial en la solución de correo ofertada.
- Contar con certificado oficial a nivel Professional en la solución de respaldo ofertada.

EXPERIENCIA DEL PERSONAL CLAVE

ITEM N° 01

Requisitos:

GESTOR DEL PROYECTO (01 PERSONA)

Experiencia específica mínima de dos (02) años en gestión de proyectos similares a los ofertados tales como:

- Servicio de Internet
- Servicio de Enlace de Datos
- Servicio de hosting o housing o alojamiento de gabinetes y equipos de telecomunicaciones)
- Servicio de Acceso a Internet
- Servicio de Acceso Dedicado a Internet
- Servicio de Transmisión de Datos
- Servicio de Interconexión de Datos
- Servicio de telco
- Servicio de cloud u onpremise
- Servicio de cableado para fibra óptica o puntos de red
- Servicio de transmisión de datos e internet satelital

ITEM N° 02

Requisitos:

GESTOR DEL PROYECTO (01 PERSONA)

- Experiencia específica mínima de dos (02) años en gestión de proyectos TI similares a los ofertados tales como:
  - Servicio de correo electrónico.
  - Servicio de herramientas colaborativas.
  - Servicio de backup de correo.
  - Servicio de Migración de plataforma de correos electrónicos.

ESPECIALISTA DE LA SOLUCIÓN (01 PERSONA)

- Experiencia específica mínima de dos (01) años en implementación de soluciones en nube similares a los ofertados tales como:
  - Servicio de correo electrónico.
  - Servicio de herramientas colaborativas.
  - Servicio de backup de correo.
  - Servicio de Migración de plataforma de correos electrónicos.

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

EXPERIENCIA DEL CONTRATISTA EN LA ESPECIALIDAD

Requisitos:

ITEM N° 01

El CONTRATISTA debe acreditar un monto facturado acumulado equivalente a no mayor a una vez el valor estimado del ítem, por la contratación de servicios iguales o similares al objeto de la convocatoria, durante los ocho (8) 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 similares a los siguientes:

- Servicio de Internet
- Servicio de Enlace de Datos
- Servicio de hosting o housing o alojamiento de gabinetes y equipos de telecomunicaciones)
- Servicio de Acceso a Internet
- Servicio de Acceso Dedicado a Internet
- Servicio de Transmisión de Datos
- Servicio de Interconexión de Datos
- Servicio de telco
- Servicio de cloud u onpremise
- Servicio de cableado para fibra óptica o puntos de red
- Servicio de transmisión de datos e internet satelital

ITEM Nº 02

El CONTRATISTA debe acreditar un monto facturado acumulado equivalente no menor a una vez el valor estimado del ítem, por la contratación de servicios iguales o similares al objeto de la convocatoria, durante los ocho (8) 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 similares a los siguientes:

- Servicio de correo electrónico.
- Servicio de Entornos colaborativos
- Servicio de video conferencia.
- Servicio de backup de correo.
- Servicio de Migración de plataforma de correos electrónicos.

Acreditación:

La experiencia del CONTRATISTA 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 pago, correspondientes a un máximo de veinte (20) contrataciones.

ANEXO 1: Relación de Unidades Territoriales que contaran con enlace de datos para acceso a Internet.

	Uso predominante Oficinas / Almacén / Archivo / Otro (precisar)	**Dirección del Local (Calle, Jirón, Avenida, Nro., Distrito, Provincia, Departamento)**
01	oficina-AMAZONAS	CHACHAPOYAS - CHACHAPOYAS Jr. Bolivia Nº 708- del Barrio Santo Domingo del distrito de Chachapoyas, provincia Chachapoyas.
02	oficina-ANCASH	HUARAZ - HUARAZ - Pje. Jacinto Palacios N° 879 Urb. Belen Mz. 152 lote 2B
03	oficinas-APURIMAC	ABANCAY - ABANCAY - Jr. Arequipa Nº 824
04	oficina-AREQUIPA	AREQUIPA - AREQUIPA - Urbanización Francisco Mostajo F2-2, Cercado Arequipa – Distrito de Arequipa
05	oficina-AYACUCHO NORTE	HUAMANGA - AYACUCHO - Urb. Cáceres Mz. 4 Lt. 34
06	oficina-AYACUCHO SUR	LUCANAS - PUQUIO - Jr. saisa n° 275, mz. 8, lote 17
07	oficina-CAJAMARCA	CAJAMARCA - CAJAMARCA - Jr. El Bosque N° 135
08	oficina-CUSCO	CUSCO - WANCHAQ - Jr,. Cajamarca I-11 (Mz.I, lote 11) Urb. San Borja
09	oficina-HUANCAVELICA	HANCAVELICA - ASCENSION - Mz P Lote 20 Centro Poblado Ascensión (Ernesto Morales N° 548)

10	oficina-HUANUCO – San Martin	HUANUCO - HUANUCO - Jr. Damaso Beraún N° 857 Sección B (2do piso)
11	oficina-JUNIN	HUANCAYO / JUNÍN – Pasaje San Antonio Nro. 152 Urb. San Carlos (Altura Jr. Francisco Solano- Parque Tupac -Clinica Salazar) Distrito y Provincia de Huancayo
12	oficina-LORETO	MAYNAS - IQUITOS - Calle Rufino Echenique N° 793 o Pueblo Joven Asentamiento Bermúdez Mz 8 lote 24 etapa primera
13	oficina-LA LIBERTAD – Lambayeque	TRUJILLO - LA LIBERTAD – Calle los pétalos N°130 – urb. Los Rosales de San Andrés
14	oficina-PASCO – Lima	PASCO - YANACANCHA - Av. Proceres N° 075, Barrio Yanacancha
15	oficina-PIURA	PIURA - CASTILLA - Calle las Begonias Mz R lote 16 Urb. Miraflores
16	oficina-PUNO	PUNO - PUNO - Jr. Ejército N° 256 - Tercer Piso
17	oficina-TACNA Moquegua	TACNA - TACNA - Calle Deustua N° 335 2do piso
18	Oficina – Sucursal Lima	Av. Brasil 2694 departamento 106, 206 y 306
19	Oficina – Canaval y Moreyra	Av. Canaval Y Moreyra 654 Piso 07
20	Oficina – Sede Central	Av. Vía Expresa Luis Fernán Bedoya Reyes N° 3245 - Piso 4 (Ex.Paseo de la República), San Isidro - Lima
21	Almacén Central	Jr Napo 361 Breña