

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

CONCURSO PÚBLICO N° 001-2023-APN

**CONTRATACIÓN DE SERVICIO DE INTERNET, SEGURIDAD
PERIMETRAL, Y TELEFONIA FIJA PARA LA SEDE
CENTRAL DE LA AUTORIDAD PORTUARIA NACIONAL
(APN) Y SERVICIO DE ENLACE DE DATOS ENTRE EL
CENTRO DE CONTROL DE COMUNICACIONES Y
RESPUESTA A EMERGENCIAS (CCCRE) DEL CALLAO Y
LA SEDE CENTRAL**

BASES INTEGRADAS

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 N° 27269, Ley de Firmas y Certificados Digitales¹). Los demás documentos deben ser visados por el postor. En el caso de persona jurídica, por su representante legal, apoderado o mandatario designado para dicho fin y, en el caso de persona natural, por este o su apoderado. No se acepta el pegado de la imagen de una firma o visto. Las ofertas se presentan foliadas.

Importante

- *Los formularios electrónicos que se encuentran en el SEACE y que los proveedores deben llenar para presentar sus ofertas, tienen carácter de declaración jurada.*
- *En caso la información contenida en los documentos escaneados que conforman la oferta no*

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 accesorio, la misma que debe ser renovada periódicamente hasta el cumplimiento total de las obligaciones garantizadas.

Importante

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

3.2.3. GARANTÍA POR ADELANTO

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

3.3. REQUISITOS DE LAS GARANTÍAS

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

Importante

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

Advertencia

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

1. La clasificadora de riesgo que asigna la clasificación a la empresa que emite la garantía debe encontrarse listada en el portal web de la SBS (<http://www.sbs.gob.pe/sistema-financiero/clasificadoras-de-riesgo>).

2. Se debe identificar en la página web de la clasificadora de riesgo respectiva, cuál es la clasificación vigente de la empresa que emite la garantía, considerando la vigencia a la fecha de emisión de la garantía.

3. Para fines de lo establecido en el artículo 148 del Reglamento, la clasificación de riesgo B, incluye las clasificaciones B+ y B.

4. Si la empresa que otorga la garantía cuenta con más de una clasificación de riesgo emitida por distintas empresas listadas en el portal web de la SBS, bastará que en una de ellas cumpla con la clasificación mínima establecida en el Reglamento.

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

De otro lado, además de cumplir con el requisito referido a la clasificación de riesgo, a efectos de verificar si la empresa emisora se encuentra autorizada por la SBS para emitir garantías, debe revisarse el portal web de dicha Entidad (<http://www.sbs.gob.pe/sistema-financiero/relacion-de-empresas-que-se-encuentran-autorizadas-a-emitar-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 : Autoridad Portuaria Nacional - APN
RUC N° : 20509645150
Domicilio legal : Av. Santa Rosa N° 135 - La Perla - Callao
Teléfono: : 630-9600 anexo 1321
Correo electrónico: : tespinoza@apn.gob.pe

1.2. OBJETO DE LA CONVOCATORIA

El presente procedimiento de selección tiene por objeto la contratación del servicio de internet, seguridad perimetral, y telefonía fija para la sede central de la Autoridad Portuaria Nacional (APN) y servicio de enlace de datos entre el Centro de Control de Comunicaciones y Respuesta a Emergencias (CCCRE) del Callao y la Sede Central.

El mismo que comprende:

Ítem	Componentes
contratación del servicio de internet, seguridad perimetral, y telefonía fija para la sede central de la Autoridad Portuaria Nacional (APN) y servicio de enlace de datos entre el Centro de Control de Comunicaciones y Respuesta a Emergencias (CCCRE) del Callao y la Sede Central	Servicio de Internet
	Seguridad Perimetral
	Servicio de Enlace de datos
	Servicio de telefonía fija digital
	Servicio de Central Telefónica

1.3. EXPEDIENTE DE CONTRATACIÓN

El expediente de contratación fue aprobado mediante proveído al Memorando N° 1083-2023-APN-OGA el 31.08.2023.

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 A 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

La implementación, instalación y puesta en producción de todos los servicios y sus componentes como parte del contrato no deberá exceder de los ciento treinta y seis (136) días calendario contados a partir del día siguiente de firmado el acta de inicio de implementación del servicio, dicha acta se firmará al día siguiente de la confirmación de recepción de la comunicación formal de la APN, para el inicio del servicio.

La ejecución de todos los servicios contratados será por un plazo de treinta y seis (36) meses contados a partir del día siguiente de la firma del acta de activación del servicio mensual.

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 S/ 5.00 (Cinco y 00/100 soles) en la caja (Tesorería) ubicada en la sede central de la APN, sito en Av. Santa Rosa N° 135 – La Perla, Callao.

Importante

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

1.10. BASE LEGAL

- Ley N° 31638 Ley de Presupuesto del Sector Público para el Año Fiscal 2023.
- Ley N° 31639 Ley de Equilibrio Financiero del Presupuesto del Sector Público del año fiscal 2023.
- Texto Único Ordenado de la Ley N° 30225 Ley de Contrataciones del Estado, aprobado por D.S N° 082-2019-EF, en adelante la Ley.
- D.S N° 344-2018-EF Reglamento de la Ley de Contrataciones del Estado en adelante el Reglamento
- Ley N° 27806, Ley de Transparencia y acceso a la información pública
- D.S N° 006-2017-JUS Texto Único Ordenado de la Ley N° 27444 Ley del Procedimiento Administrativo General.
- Código Civil
- Directivas del OSCE

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

CAPÍTULO II DEL PROCEDIMIENTO DE SELECCIÓN

2.1. CALENDARIO DEL PROCEDIMIENTO DE SELECCIÓN

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

Importante

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

2.2. CONTENIDO DE LAS OFERTAS

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

2.2.1. Documentación de presentación obligatoria

2.2.1.1. Documentos para la admisión de la oferta

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

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

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

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

Advertencia

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

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

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

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

- e) Declaración jurada de plazo de prestación del servicio. **(Anexo N° 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 N° 5)**
- g) El precio de la oferta en Soles. Adjuntar obligatoriamente el **Anexo N° 6**.

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

Importante

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

2.2.1.2. Documentos para acreditar los requisitos de calificación

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

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 – PIDE⁵ y

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

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 ⁶ (**Anexo N° 10**).
- h) Detalle de los precios unitarios del precio ofertado⁷.
- i) Detalle del precio de la oferta de cada uno de los servicios que conforman el paquete⁸.
- j) **Formatos de Cumplimiento de acuerdo a los Anexos A, B, C, D, E, F, G y H** según modelos, los mismos que se ubican al final de los Términos de Referencia, cada uno sustentado evidenciados en los documentos emitidos por el fabricante (folletos, catálogos brochures u otros documentos, entendiéndose como otros los siguientes: guías prácticas, hojas técnicas, website o manuales o carta del fabricante⁹) indicando el folio en la referencia técnica correspondiente. Además de la carta del fabricante también pueden presentar carta de una filial del fabricante o carta de una empresa autorizada por el fabricante o carta del representante del fabricante o carta del distribuidor autorizado por el fabricante. Estos documentos deberán estar acompañados de la carta del fabricante que valide que son filiales o entes autorizados o representantes de la marca o distribuidor autorizado¹⁰.

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.*

Importante

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

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

⁸ Incluir solo en caso de contrataciones por paquete.

⁹ La carta del fabricante se podrá presentar solo para las características específicas que no se encuentren en la documentación pública o interna del fabricante y no para todas las características de los Anexos A,B,C,D,E,F,G y H (según corresponda). Asimismo, en caso de presentar carta del fabricante ésta deberá tener una antigüedad máxima de la fecha de la integración de bases.

¹⁰ Absolución Pliego N° 168, 171 participante AMERICATEL PERU S.A

- *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 Haya¹¹.*
- *La Entidad no puede exigir documentación o información adicional a la consignada en el presente numeral para el perfeccionamiento del contrato.*

2.4. PERFECCIONAMIENTO DEL CONTRATO

El contrato se perfecciona con la suscripción del documento que lo contiene. Para dicho efecto el postor ganador de la buena pro, dentro del plazo previsto en el artículo 141 del Reglamento, debe presentar la documentación requerida en Mesa de Partes (tramite documentario) ubicado en la sede central de la APN; sito en la Av. Santa Rosa N° 135 La Perla, Callao, [en el horario de lunes a viernes 8.30am a 5.30 pm](#)¹².

2.5. FORMA DE PAGO

La Entidad realizará el pago de la contraprestación pactada a favor del contratista en Pagos Periódicos de acuerdo a lo indicado en el numeral 6 Forma y Condiciones de Pago de los Términos de Referencia.

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

- Informe mensual presentado por el contratista
- Informe del funcionario responsable de la Oficina de Tecnologías de la Información – OTI, emitiendo la conformidad de la prestación efectuada.
- Comprobante de pago.

Dicha documentación se debe presentar en Mesa de Partes (Trámite Documentario) ubicada en la Sede Central de la APN, sito en Av. Santa Rosa N° 135 La Perla, Callao o a través de la ventanilla virtual de la Entidad¹³.

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

¹² Absolución Pliego N° 40 participante VIETTEL PERU S.A.C N° 73 participante AMERICA MOVIL PERU S.A.C N° 169 participante AMERICATEL PERU S.A

¹³ <https://ventanillavirtual.apn.gob.pe/login>

CAPÍTULO III REQUERIMIENTO

Importante

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

3.1. TERMINOS DE REFERENCIA

GUTARRA RAMOS
Martha FAU
20509645150
hard
Firmado digitalmente
por GUTARRA RAMOS
Martha FAU
20509645150 hard
Fecha: 2023.08.04
12:44:48 -05'00'



PERÚ

Ministerio
de Transportes
y Comunicaciones

Autoridad Portuaria
Nacional

"Decenio de la Igualdad de Oportunidades para Mujeres y Hombres"
"Año de la unidad, la paz y el desarrollo"

OCAÑA
MOSTACERO
Miguel Angel FAU
20509645150 hard
Firmado digitalmente
por OCAÑA
MOSTACERO Miguel
Angel FAU
20509645150 hard
Fecha: 2023.08.04
12:42:59 -05'00'

REQUERIMIENTO DE SERVICIOS EN GENERAL

TÉRMINOS DE REFERENCIA

A. INFORMACIÓN GENERAL

1) DENOMINACIÓN DE LA CONTRATACIÓN

Contratación del Servicio de Internet, Seguridad Perimetral, y Telefonía Fija para la Sede Central de la Autoridad Portuaria Nacional (APN) y Servicio de Enlace de Datos entre el Centro de Control de Comunicaciones y Respuesta a Emergencias (CCCRE) del Callao y la Sede Central.

2) FINALIDAD PÚBLICA

El presente requerimiento tiene como finalidad publica, mantener a la APN interconectado digitalmente dentro de la comunidad portuaria para coadyuvar a la ejecución de sus actividades y funciones, así como al cumplimiento de sus metas organizacionales.

Asimismo, permite que la APN cumpla con la actividad operativa del Plan Operativo Institucional – POI referente a Mantener y asegurar los servicios tecnológicos para optimizar las actividades en la APN, la misma que está alineada a la Acción Estratégica de Sistemas y servicios informáticos implementados para optimizar la operatividad de la entidad del Plan Estratégico Institucional – PEI APN

3) OBJETIVOS DE LA CONTRATACIÓN

La APN, requiere contratar los servicios de telecomunicaciones como la línea dedicada para el acceso a Internet, la interconexión de datos con la Oficina de Centro de Control de Comunicaciones y Respuesta a Emergencias, la telefonía fija y el Internet Móvil a nivel nacional, además de los servicios de central telefónica y Seguridad perimetral para la APN, con cobertura las 24 horas del día, de manera ininterrumpida durante el plazo de ejecución contractual.

4) ÁREA O UNIDAD ORGÁNICA

Oficina de Tecnologías de la Información.

5) ACTIVIDAD DEL POI

Maximizar la disponibilidad de los servicios de TI

6) MES PROBABLE DE CONVOCATORIA

Julio

B. INFORMACION ESPECÍFICA

1) DESCRIPCIÓN DEL SERVICIO

A continuación, se detalla las características de cada componente que se requiere contratar por el periodo de treinta y seis (36) meses:

• **COMPONENTES DEL SERVICIO**

COMPONENTES	DESCRIPCIÓN
1: Servicio de Internet	100 Mbps - Overbooking 1:1 Enlace de Contingencia de 100 Mbps. Última milla de Fibra Óptica.
	02 equipos router en calidad de alquiler (un equipo para el enlace principal y otro para el de contingencia), que soporte un ancho de banda mínimo de 100 Mbps.
	02 equipos Switches de 08 puertos 10/100/1000BaseT, en calidad de alquiler, estos Switches son para la conexión WAN en contingencia.
	64 módems USB o Router Portátiles o Hotspots 3G y/o 4G y/o 4.5G¹⁴ con servicio de internet móvil. Capacidad de descarga de 20GB por mes Velocidad de hasta 5000Kbps o superior.
2: Seguridad Perimetral	02 equipos Firewalls perimetrales en calidad de alquiler, configurados en redundancia. (activo/pasivo).
	01 equipo Administrador de Ancho de Banda, en calidad de alquiler.
	Servicio de Protección avanzada de puesto de trabajo y servidores
	Servicio de Ciberdefensa
	Servicio de Gestion de Vulnerabilidades
	Servicio de DDoS
	Soporte de LAN gestionada.
3: Servicio de Enlace de Datos	35 Mbps – 100% garantizado en ambos extremos. Enlace de datos entre dos sedes (Sede Central de la APNy el CCCRE del puerto del Callao). El enlace de datos será configurado para la transmisión de:voz, datos y video. Última milla de Fibra Óptica.
	02 equipos Router (uno para la sede principal y otro para el CCCRE del Puerto del Callao), que soporte un ancho de banda mínimo de 50 Mbps.
4: Servicio de Telefonía Fija Digital	Primario E1 o SIP TRUNK o Troncal SIP con 30 canales de voz y 100 DIDs como mínimo. Llamadas a Fijo y Móvil, Local, Nacional, Internacional Primario E1 o SIP TRUNK o Troncal SIP de contingencia con 30 canales de voz y 100 DIDs como mínimo. Última milla de Fibra Óptica.
5: Servicio de Central Telefónica	Appliance Central telefónica <ul style="list-style-type: none"> El equipo debe contemplar 02 puertos para 2enlaces primarios. El equipo debe contemplar 60 puertos parateléfonos analógicos, como mínimo. 86 licencias para telefonía IP como mínimo.

¹⁴ Según Absolución Pliego N° 12 participante VIETTEL PERU S.A.C



Ministerio
de Transportes
y Comunicaciones

Autoridad Portuaria
Nacional

"Decenio de la Igualdad de Oportunidades para Mujeres y Hombres"
"Año de la unidad, la paz y el desarrollo"

	<ul style="list-style-type: none">• Debe permitir asignar hasta 300 códigos para la realización de llamadas por cada usuario como mínimo.
	86 teléfonos IP
	Incluir: Instalación, Configuración y puesta en producción.
	Incluir: Software de Tarificación.

Se precisa que para el caso del servicio de "LAN Gestionada" del componente de Seguridad Perimetral, el CONTRATISTA deberá considerar que la gestión de un Switch y de 05 teléfonos IP que se encuentra en el CCCRE del puerto de Iquitos, donde tendrán que acceder de manera remota a fin de poder gestionarlo y en caso de falla física deberá desplazar a un personal para respectiva reparación (los tiempos de respuesta se detallan en punto 07 de los términos de referencia.

Asimismo, se precisa que todos los equipos que serán entregados en alquiler a la entidad y que serán nuevos y sin uso, serán devueltos al finalizar el contrato y cuando se haya entregado toda la información y configuraciones que se almacenen en dichos equipos.

A continuación, se detalla las características de cada componente de los servicios de Internet y Telefonía Fija:

1.1 SERVICIO DE ACCESO A INTERNET DEDICADO

a) Características del servicio de acceso a internet dedicado

- ✓ Uno de los dos enlaces será configurado en modo activo/standby, el medio físico de transporte de ambos enlaces deberá ser fibra óptica canalizada o área en todo su recorrido desde el punto de presencia del proveedor hasta el local central de la APN, garantizando de esta forma la calidad y continuidad del servicio. El enlace de respaldo deberá provenir de un nodo diferente al enlace principal, así como deberá utilizar una ruta distinta. El CONTRATISTA deberá entregar junto con el plan de trabajo indicado en la Fase I del Numeral 1.6 de los presentes términos de referencia los planos de la topología de las rutas de los nodos de tal forma que se evidencie que estos vienen de rutas diferentes (los planos podrán ser entregados en formato AutoCAD o mediante un plano en formato KML (imágenes de Google Earth))¹⁵.

Cabe indicar que al referirse al modo Activo-Standby, se refiere a que uno de los enlaces contratados (100 Mbps) estará en modo activo, mientras que el segundo enlace (100 Mbps) será configurado en modo standby, entendiéndose que la entidad está solicitando solo 02 enlaces en el presente servicio. (*suprimido*)¹⁶

¹⁵ Según Absolución Pliego N° 222 participante AMERICATEL PERU S.A

¹⁶ Según Absolución Pliego N° 78, 104 participante AMERICA MOVIL PERU S.A.C N° 223,224,225 participante AMERICATEL PERU S.A N° 247 participante WIN EMPRESAS S.A.C



Ministerio
de Transportes
y Comunicaciones

Autoridad Portuaria
Nacional

"Decenio de la Igualdad de Oportunidades para Mujeres y Hombres"
"Año de la unidad, la paz y el desarrollo"

- ✓ La disponibilidad del servicio debe ser del 99.90% como mínimo caso contrario se ha de considerar como caída del servicio y estará sujeto a las penalidades indicadas en el punto 9) Penalidades del presente documento. El CONTRATISTA presentará un procedimiento para la atención de averías, al momento de firmarse el acta de activación del servicio, el cual tener una previa aprobación de la Oficina de Tecnologías de la Información – OTI para su uso.
- ✓ El servicio de acceso a Internet debe estar disponible las veinticuatro (24) horas del día, los siete (07) días de la semana los trescientos sesenta y cinco (365) días del año, durante el periodo de contrato.

Debe poseer un ancho de banda hacia el Internet Internacional de 10 Gbps como mínimo por cada interconexión y debe contar con sistemas de redundancia en la salida internacional como mínimo dos operadores TIER1 internacionales distintos con rutas físicas diferentes con los que deberá tener conexión directa a través de enlaces de Fibra Óptica. Con ello se busca garantizar la velocidad, seguridad y disponibilidad mensual del acceso a Internet requerido. Debe garantizar la conexión internacional para ambas rutas y por distintos proveedores internacionales.

De manera opcional el POSTOR podrá ser miembro formal y activo del NAP Perú así como también podrá poseer conexión propia a este. Asimismo, también de manera opcional podrá contar con una capacidad mínima de 2x100Gbps¹⁷.

- ✓ Entregará como mínimo 75 direcciones IP públicas (59 IPs públicas IPv4 y 16 IPs públicas IPv6), con la capacidad de aumentar de acuerdo con los requerimientos de la APN, siguiendo las normas de ARIN (American Registry for Internet Numbers), o LACNIC, así mismo, registro DNS, es decir inscripción de nuestros dominios en los servidores del CONTRATISTA. Asimismo, deberá considerar que, durante el periodo de contrato, la APN podrá solicitar el cambio del pool de IP públicas de IPv4 a IPv6, así como la configuración en los equipos de comunicaciones en calidad de alquiler y los equipos de comunicaciones de propiedad de la APN (los cuales cuentan con soporte para IPv6), para que se configure el protocolo IPv6 en la red LAN, dicha configuración no tendrá costo para la institución. El CONTRATISTA, deberá entregar las IP públicas asignadas, a través de un correo electrónico en un archivo excel (opcionalmente se podrá encriptar el archivo o configurando una clave para acceder a dicho archivo), esto deberá realizarse en la fase 02 de la implementación del servicio¹⁸.
- ✓ Se precisa que el pool de 59 direcciones IP públicas IP versión 4, serán las direcciones efectivas y no están incluidas las IP de red, las IP del Gateway, IP virtual e IP Broadcast.
- ✓ El Contratista debe entregar los accesos para que la entidad pueda realizar de manera automática el registro o modificación de los DNS, (los accesos deberán ser entregados en la fase 02 de la implementación, mediante correo electrónico) en un portal autogestionable, como parte de la administración compartida. En caso la entidad requiera el apoyo del CONTRATISTA, este podrá realizarlo durante las 24 horas de los 07 días de la semana durante

¹⁷ Absolución Pliego N° 13,14, 15 participante VIETTEL PERU S.A.C

¹⁸ Absolución Pliego N° 105 participante AMERICA MÓVIL PERU S.A.C



Ministerio
de Transportes
y Comunicaciones

Autoridad Portuaria
Nacional

"Decenio de la Igualdad de Oportunidades para Mujeres y Hombres"
"Año de la unidad, la paz y el desarrollo"

el tiempo del contrato o también será aceptado que la entidad solicite el registro de DNS mediante correo electrónico tomando en cuenta que estas solicitudes deberán ser atendidas en un máximo de 01 hora, contado desde que la entidad haya recepcionado el ticket de atención mediante correo electrónico. Para el caso de solicitudes de creación o eliminación o modificaciones de registros DNS, se deberán tener en cuenta los siguientes tiempos de respuesta y atención:

Tiempo de Respuesta: Será Máximo de hasta 01 hora, contados desde que la entidad haya realizado la solicitud mediante correo electrónico hasta que se reciba el número de ticket de atención¹⁹.

Tiempo de Atención: Será máximo de hasta una hora, contados desde que la entidad haya recibido mediante correo electrónico el número de ticket de atención.

- ✓ Garantizará que el ancho de banda contratado para el enlace será de uso exclusivo para la APN desde la puerta WAN del Router en el local de la entidad hasta el Router de borde del proveedor del servicio de Internet.
- ✓ Debe brindar un portal web o sistema donde el personal autorizado de la APN pueda visualizar reportes del tráfico en forma gráfica y para un periodo determinado, en línea (tiempo real) con un rango de actualización de 05 minutos, almacenando como mínimo 06 meses de información de tráfico de red, para fines comparativos. Dicho acceso se deberá brindar en la fase 02 de la implementación del servicio y se firmará un acta de recepción de los accesos a dicho portal.
- ✓ La APN brindará los ambientes adecuados con la infraestructura necesaria (pozo a tierra, UPS, aire acondicionado, energía estabilizada) para la instalación del equipamiento relacionado al servicio a contratar.
- ✓ Debe brindar la posibilidad técnica de un traslado de local por mudanza de la institución previa coordinación con la APN. En caso se presente este escenario, se realizará a través de una adenda por prestación adicional, previa validación de su factibilidad técnica.

b) Equipos de enrutamiento – Router

Debe, entregar en calidad de alquiler 02 Router, de los cuales 01 se usará como el enlace principal y el otro para la contingencia del servicio de internet. Para garantizar un óptimo servicio, se deberá proveer equipos de enrutamiento que tengan la vigencia tecnológica de parte de la marca a proponer. Las características mínimas de los equipos enrutadores, deberá ser la siguiente:

¹⁹ Según absolución Pliego N° 17 participante VIETTEL PERU S.A.C

- ✓ Interfaces: como mínimo cuatro (04) puertos 10/100/1000BaseT + 2SFP, 1 puerto USB²⁰.
- ✓ Para efectos de la propuesta, ninguno de los modelos ofertados podrá estar listados ni anunciado en el sitio web del fabricante como end-of-life o end-of-sale o end-of-support. Se deberá adjuntar para el perfeccionamiento del contrato el enlace público del fabricante o catálogos o brochures o guías prácticas o hojas técnicas, website o manuales o carta de fabricante que verifique que los modelos propuestos no están en ese listado - Ver Anexo A.
- ✓ Routing: BGP, OSPF, RIP v1/v2, Rutas estáticas, ECMP (opcional), RPF y enrutamiento basado en rutas y/o políticas.
- ✓ Multicast: IGMP v1/v2, PIM-SM, PIM-DM, SSM.
- ✓ Alta disponibilidad: Activo/Activo, Activo/Pasivo, VRRP.
- ✓ Switching L2 (Opcional): LACP, autenticación de puerto basada en 802.1x.
- ✓ Opcionalmente la capacidad mínima de memoria RAM/FLASH de 4GB.
- ✓ Para efectos de performance de manera opcional el enrutador podrá soportar al menos 450 Mbps de tráfico IMIX y 60,000 sesiones concurrentes, pero deberá poder soportar los 100 Mbps solicitados.
- ✓ Los equipos opcionalmente deben soportar (no instalado) sin cambio de hardware:
 - Antivirus
 - Antispam
 - Filtro Web
 - IPS
- ✓ Opcionalmente, el equipo router podrá permitir almacenar un mínimo de dos sistemas operativos para mantener la alta disponibilidad y opcionalmente almacenar de forma local un mínimo de dos archivos de configuración realizadas.
- ✓ Si el equipo instalado falla, el CONTRATISTA debe cambiarlo por otro similar o superior, en caso de tener que cambiar el equipo por uno superior se debe cambiar también el segundo router por modelo y marca del equipo reemplazado, a fin de garantizar un óptimo funcionamiento de la solución. Se precisa que el cambio de equipos sin costo cuando se deba a una falla de fabrica o cuando el servicio se vea afectado por rendimiento o capacidad del equipo.
- ✓ Para la interconexión entre los enrutadores y la solución de seguridad perimetral, se deberá considerar dos (02) Switches de al menos 08 puertos 10/100/1000BaseT en alta disponibilidad, los cuales se describen en el literal c).
- ✓ A fin de validar las características técnicas mínimas ofertadas de los router, el postor ganador deberá presentar para el perfeccionamiento del contrato el formato de cumplimiento del Anexo A debidamente sustentado, indicando las referencias técnicas (número de folio) evidenciadas en los documentos emitidos por el fabricante (folletos catálogos, brochures u otros documentos entendiéndose como otros documentos los siguientes: guías prácticas o hojas técnicas o website del fabricante o manuales o carta del fabricante). La

²⁰ Absolución Pliego N° 109 participante AMERICA MOVIL PERU S.A.C



PERÚ

Ministerio
de Transportes
y Comunicaciones

Autoridad Portuaria
Nacional

"Decenio de la Igualdad de Oportunidades para Mujeres y Hombres"
"Año de la unidad, la paz y el desarrollo"

carta del fabricante se podrá presentar solo para las características específicas que no se encuentren en la documentación pública o interna del fabricante y no para todas las características que se debe acreditar en el Anexo A. Asimismo, que en caso de presentar carta del fabricante esta deberá tener fecha actualizada a la fecha de la presentación de la documentación para el perfeccionamiento del contrato.

c) Switch de 08 Puertos

El CONTRATISTA debe entregar en calidad de alquiler 02 Switch de al menos 08 puertos de 10/100/1000 BaseT, cada uno, para la conexión WAN en activo y en stanby. Para garantizar un óptimo servicio, se deberá proveer equipos de tecnología vigente de parte de la marca a proponer. Dichos switches deben contar con las siguientes características:

- ✓ Se requiere de un conmutador modular administrable de interfaces GigaEthernet que permita la operación en capa 2, capa 3 del modelo OSI.
- ✓ Deberá disponer de al menos 08 puertos 10/100/1000BaseT. Las interfaces deberán permitir la auto negociación de la velocidad del puerto y del modo dúplex de la comunicación.
- ✓ Para efectos de la propuesta, ninguno de los modelos ofertados podrá estar listados ni anunciado en el sitio web del fabricante como end-of-life o end-of-sale o end-of-support. Se deberá adjuntar para el perfeccionamiento del contrato el enlace público del fabricante o catálogos o brochures o guías prácticas o hojas técnicas, website o manuales o carta de fabricante que verifique que los modelos propuestos no están en ese listado – Ver Anexo B.
- ✓ Para la administración local se deberá considerar de al menos un (01) puerto de Consola RS232 o un (01) puerto RJ45 o un (01) puerto USB.
- ✓ La capacidad de tráfico mínimo que deberá procesar el equipo será no menor de 25Gbps de switch fabric y una tasa de envío de paquetes no menor a 20Mpps.
- ✓ Entre las funcionalidades básicas de administración, operación y mantenimiento se deberá considerar: SSHv2, HTTPS, Puerto Espejo (Port Mirroring), RMON, SNMP v2/v3, Netflow o Sflow, SNTP, TACACS+, IEEE 802.1Q – VLAN trunking y tagging, IEEE 802.3ad - LACP, IEEE 802.3x – control de flujo de los puertos 10/100/1000BaseT, IEEE 802.1d – Spanning Tree Protocol, IEEE 802.1w – Rapid Spanning Tree Protocol, IEEE 802.1s – Múltiple Spanning Tree Protocol, IEEE 802.1ag – Ethernet OAM Connectivity Fault Management.
- ✓ Debe incluir el soporte de enrutamiento estático entre VLAN y las siguientes funcionalidades sin la necesidad de cambio de hardware: BFD – Bidirectional Forwarding Detection, OSPFv2, Routing Information Protocol versión 1 y versión 2, enrutamiento estático, VRF – Virtual Routing and Forwarding.



PERÚ

Ministerio
de Transportes
y Comunicaciones

Autoridad Portuaria
Nacional

"Decenio de la Igualdad de Oportunidades para Mujeres y Hombres"
"Año de la unidad, la paz y el desarrollo"

- ✓ Debe permitir la asignación dinámica de IP de forma estática o vía DHCP Server local, DHCP Relay con opción 82 tanto para VLAN como para puertos en Capa 3.
- ✓ Soporte los siguientes protocolos multicast sin cambio de hardware o a través de upgrade de software: IGMP v1/v2/v3, IGMP snooping con puertos RVIs o IRB, PIM DM/SM/SSM, MVR.
- ✓ Debe soportar cuatro (04) colas por puerto o más, para diferenciar o priorizar el tráfico, QoS capa 2-3, Clase de Servicio sobre interfaces agregadas (LAGs).
- ✓ De manera opcional el sistema operativo del equipo podrá evitar o reducir los errores humanos durante su operación, para ello el sistema operativo debe considerar las siguientes características:
 - El usuario administrador del equipo es quien decide en qué momento se aplicarán los cambios realizados en la configuración del equipo. Los comandos ingresados no deberán ser ejecutados de forma inmediata por el sistema, sino por el contrario solo cuando el usuario administrador lo autorice.
 - El equipo deberá evitar errores lógicos e inestabilidad del sistema cuando los comandos de configuración introducidos no guarden un orden secuencial entre sí. Por lo tanto, el resultado de la configuración será el mismo independientemente del orden de como hayan sido ingresados los comandos.
 - En caso haya dos o más usuarios administradores realizando configuraciones de manera simultánea, los cambios realizados serán independientes entre ellos. Por lo tanto, cuando un usuario administrador autorice el cambio, el sistema no considerará la información ingresada por los otros administradores.
 - Cuando el usuario administrador autorice ejecutar al sistema, la configuración realizada por este, el sistema deberá validarla. En caso de encontrar algún error sobre la configuración, ésta no será ejecutada y el sistema adicionalmente deberá indicar claramente cuál es el error o errores encontrados para su posterior corrección.
- ✓ A fin de validar las características técnicas mínimas ofertadas se, el postor ganador deberá presentar para el perfeccionamiento del contrato el formato de cumplimiento del Anexo B debidamente sustentado, indicando las referencias técnicas (número de folio) evidenciadas en los documentos emitidos por el fabricante (folletos catálogos, brochures u otros documentos entendiéndose como otros documentos los siguientes: guías prácticas o hojas técnicas o website del fabricante o manuales o carta del fabricante). La carta del fabricante se podrá presentar solo para las características específicas que no se encuentren en la documentación publica o interna del fabricante y no para todas las características que se debe acreditar en el Anexo B. Asimismo, que en caso de presentar carta del fabricante esta



Ministerio
de Transportes
y Comunicaciones

Autoridad Portuaria
Nacional

"Decenio de la Igualdad de Oportunidades para Mujeres y Hombres"
"Año de la unidad, la paz y el desarrollo"

deberá tener fecha actualizada a la fecha de la presentación de la documentación para el perfeccionamiento del contrato.

d) Módems o Routers Portátiles - para Internet Móvil.

- ✓ Los Modems o Routers Portátiles deberán tener las siguientes medidas como máximo: 12x8x2cm.
- ✓ El CONTRATISTA debe brindar en calidad de alquiler sesenta y cuatro (64) módems portátiles 4G o 4.5G con servicio de internet móvil y con plan de datos como mínimo de 20 GB por mes a una velocidad de bajada de hasta 5000Kbps, en cobertura 4G.
- ✓ Se deberá realizar la entrega de dichos módems (los equipos deberán ser nuevos y de primer uso) con el servicio activo mediante un acta de entrega, firmada por el jefe de proyecto por parte de la APN. La entrega de los Módems y la firma del acta de entrega será antes de culminar la fase 02 de la implementación del servicio. **El Servicio de Internet Móvil con los MODEMS o Routers Portátiles se activará a partir del día siguiente de la firma del acta de activación del Servicio a contratar.**
- ✓ El CONTRATISTA, deberá garantizar la cobertura según lo publicado por OSIPTEL, pero tomando como referencia las siguientes ubicaciones a nivel nacional:

Ítem	Descripción	Ubicación
1	CALLAO	Av. Santa Rosa N.º 135 La Perla – Callao
2	CCCRE del Puerto del Callao	Av. Manco Cápac S/N - Callao
3	PAITA	Jr. Zepita 368 Paita
4	Terminal Portuario Euroandinos (TPE) de Paita	Jr. Ferrocarril 127 – Paita - Piura
5	ANEXO DE LA OD. PAITA EN TALARA	Av. Bolognesi s/n edificio Semor Oficina 303 – 304
6	SALAVERRY	Mz. Q, Lote 26 A, Urb. Covicorti- Distrito de Trujillo, provincia de Trujillo, Departamento de la Libertad
7	Terminal Portuario Multipropósito de Salaverry	El puerto está ubicado a 8° 13' 27" de latitud sur y 78° 59' 52" de longitud oeste, a una distancia aproximadamente a 14 kilómetros del centro de la ciudad de Trujillo y está muy cerca de la Carretera Panamericana.
8	PISCO	Av. Las Américas 925 Urb Los Bancarios Distrito Pisco Playa, Provincia de Pisco, Departamento de Ica
9	Terminal Portuario General San Martín – Pisco	Carretera Punta Pejerrey Km 39, Paracas - Pisco
10	SAN NICOLÁS	Marcona Zona M23 - D - Distrito de Marcona, Provincia de Nazca, Departamento de Ica
11	MATARANI	Urb. Centenario Mz: A Lote 14 - Distrito de Mollendo, Provincia de Islay, Departamento de Arequipa



Ministerio
de Transportes
y Comunicaciones

Autoridad Portuaria
Nacional

"Decenio de la Igualdad de Oportunidades para Mujeres y Hombres"
"Año de la unidad, la paz y el desarrollo"

12	Terminal Portuario de Matarani	El puerto está ubicado a Latitud 16° 59' 42.5" Sur y Longitud 72° 06' 13.2" Oeste
13	ILO	Urb. Enapu B2, Lote 2 - Distrito de Ilo, Provincia de Ilo, Departamento de Moquegua
14	IQUITOS	Av. De la Marina N° 1338- Interior Terminal Portuario ENAPU- Distrito de Villa Punchana, Provincia de Maynas, Departamento de Loreto.
15	ANEXO DE LA OD. IQUITOS EN NAUTA	Calle Junín Mz-C Lt-2 - Distrito de Nauta, Provincia de Loreto, Departamento de Loreto
16	PUCALLPA	Prolongación Jr. Ucayali S/ Amazonas N° 207 Mz. 189 Lote 15-B Calleria
17	YURIMAGUAS	Calle Libertad 1301 a Calle Jose Galvez 302- Distrito de Yurimaguas, Provincia de Alto Amazonas, Departamento de Loreto
18	Terminal Portuario de Yurimaguas de Nueva Reforma	Carretera a Nuevo Puerto - 16500

1.2 SEGURIDAD PERIMETRAL

a) Equipo Firewall – Seguridad Perimetral.

El servicio deberá contar con una solución de seguridad perimetral, para ello el CONTRATISTA instalará en calidad de alquiler dos (02) equipos Next Generation Firewall, en modalidad activo/standby, de propósito dedicado, para garantizar un óptimo servicio; asimismo, se deberá proveer equipos de seguridad que sean de tecnología vigente de parte de la marca a proponer. Los equipos de seguridad deberán contar con las siguientes características mínimas:

GENERALES

- ✓ La solución debe consistir en dos appliances de seguridad con funcionalidades de Next Generation Firewall (NGFW).
- ✓ La solución tiene que ser ofrecida en alta disponibilidad, es decir por lo menos 2 (dos) appliances con las mismas características mínimas mencionadas en estas especificaciones.
- ✓ La plataforma propuesta debe contar con certificación USGv6 para trabajar IPv6 tanto en Firewall como en IPS.
- ✓ La plataforma debe ser optimizada para análisis de contenido de aplicaciones en capa 7.
- ✓ Para efectos de la propuesta, ninguno de los modelos ofertados podrá estar listados ni anunciado en el sitio web del fabricante como end-of-life o end-of-sale o end-of-support. Se deberá adjuntar para el perfeccionamiento del contrato el enlace público del fabricante o catálogos o brochures o guías prácticas o hojas técnicas,



PERÚ

Ministerio
de Transportes
y Comunicaciones

Autoridad Portuaria
Nacional

"Decenio de la Igualdad de Oportunidades para Mujeres y Hombres"
"Año de la unidad, la paz y el desarrollo"

website o manuales o carta de fabricante que verifique que los modelos propuestos no están en ese listado – Ver Anexo C

- ✓ Los equipos NGFW deberán tener soporte vigente de fábrica durante la fecha de contrato del servicio, el soporte del fabricante deberá incluir atención de incidentes de software o hardware de la plataforma, reposición de partes o equipo de reemplazo en caso de falla de hardware.
- ✓ De manera opcional el CONTRATISTA podrá proporcionar una cuenta de acceso al portal oficial de soporte del fabricante, donde la Entidad tendrá la potestad de dar seguimiento a los casos abiertos por el CONTRATISTA. **En este caso, hará entrega de los antes indicado en la fase 02 de la implementación, mediante correo electrónico.**
- ✓ Como parte de la propuesta, se debe proporcionar el acceso a una herramienta que permita evaluar el nivel de adopción de buenas prácticas de configuración en el Next Generation Firewall implementado, con la finalidad de mejorar la postura de seguridad de red proporcionada por la solución. **Esto deberá ser entregado en la fase 02 de la implementación, mediante correo electrónico.**
- ✓ Dicha herramienta mínimamente debe contemplar la adopción de buenas prácticas en materia de configuración de los diferentes módulos de seguridad de la solución, como mínimo estos: Control de Aplicaciones, Antivirus/Antimalware, Antispyware/Antibot, IPS, Sandboxing, Filtro Web, Gestión de Logs. De manera opcional el CONTRATISTA, podrá incluir en su propuesta la documentación pública sobre dicha herramienta explicando su alcance.
- ✓ La herramienta de evaluación de buenas prácticas deberá ser específica para la configuración de Next Generation Firewall implementado, no se aceptarán portales con guías de usuarios genéricas.
- ✓ La Entidad deberá poder realizar la evaluación de buenas prácticas a libre demanda y de manera autónoma.
- ✓ Si se identifica actividad sospechosa y/o maliciosa en la red, o sufra una brecha de seguridad luego de implementar las buenas prácticas de seguridad sugeridas por la herramienta de evaluación, la Entidad tendrá la potestad de contar con un servicio directo con el Fabricante, el cual incluye:
 - Expertos, herramientas especializadas de inteligencia de amenazas y prácticas de cacería de amenazas.
 - Análisis de logs e indicadores de compromiso
 - Evaluación de la configuración del NGFW que incluya recomendaciones personalizadas
 - Recomendaciones de pasos siguientes a realizar

CAPACIDAD

- ✓ Throughput de Next Generation Firewall de 3 Gbps medido con tráfico productivo real (transacciones usando una mixtura de aplicaciones de capa 7, transacciones medidas en condiciones empresariales o transacciones HTTP 64KB de tamaño). No se aceptarán mediciones hechas con tráfico UDP o RFCs 3511, 2544, 2647 o 1242 o mixes de tráfico que no especifiquen tamaño de transacciones o paquetes.



PERÚ

Ministerio
de Transportes
y Comunicaciones

Autoridad Portuaria
Nacional

"Decenio de la Igualdad de Oportunidades para Mujeres y Hombres"
"Año de la unidad, la paz y el desarrollo"

- ✓ Throughput de Prevención de Amenazas de 1.5 Gbps medido con tráfico productivo real (transacciones usando una mixtura de aplicaciones de capa 7, transacciones medidas en condiciones empresariales o transacciones HTTP 64KB de tamaño), con las siguientes funcionalidades habilitadas simultáneamente: Control de aplicaciones, Sistema de Prevención de Intrusos (IPS), Antivirus/Antimalware de red, Antispyware/AntiBot, control de amenazas avanzadas de día cero (Sandboxing), Filtro de Archivos, y Logging activo. Si el fabricante tuviese diferentes niveles o modos de inspección de seguridad, el equipo ofertado deberá soportar el throughput requerido con el nivel o modo más alto de inspección. Se debe garantizar que el equipo no degrade su performance por debajo de lo requerido por la Entidad cuando se vayan habilitando los módulos de seguridad indicados en el modo más alto de inspección. No se aceptarán mediciones hechas con tráfico UDP o RFCs 3511, 2544, 2647 o 1242 o mixes de tráfico que no especifiquen tamaño de transacciones o paquetes.
- ✓ El equipo debe soportar como mínimo 290.000 sesiones simultáneas y 50.000 nuevas sesiones por segundo, medidos con paquetes HTTP de 1 byte.
- ✓ Disco de estado sólido interno de 120 GB o superior.
- ✓ Mínimo ocho (08) interfaces de red 10/100/1000 en cobre, formato RJ45 para tráfico de datos de la red
- ✓ Mínimo una (01) interfaz de consola RJ45,

CARACTERÍSTICAS GENERALES

- ✓ El dispositivo de seguridad debe soportar VLAN Tags 802.1q, agregación de links 802.3ad, policy based routing o policy based forwarding, ruteo multicast, jumbo frames, sub-interfaces ethernet lógicas, NAT de origen y destino.
- ✓ Debe soportar enrutamiento estático y dinámico (RIPv2, BGP y OSPFv2).
- ✓ Soportar como mínimo las siguientes funcionalidades en IPv6: SLAAC (address auto configuration), NAT64, Identificación de usuarios a partir de LDAP/AD, Captive Portal, IPv6 over IPv4 IPSec, Reglas de seguridad contra DoS (Denial of Service), Descifrado SSL/TLS y SSH, PBR (Policy Base Routing) o PBF (Policy Based Forwarding), OSPFv3, QoS, DHCPv6 Relay, SNMP, NTP, NTP autenticado, SYSLOG, DNS y control de aplicaciones.
- ✓ Permitir configurar el tiempo de almacenamiento en caché de la Tabla ARP.
- ✓ Permitir NAT de destino basado en dominio en lugar de IP. El equipo deberá ser capaz de balancear el tráfico entrante por esa regla de NAT de destino.
- ✓ Soportar DNS Dinámico en las interfaces de red del equipo de seguridad.
- ✓ Soportar túneles GRE como punto inicio o finalización del túnel.
- ✓ Capacidad de inspeccionar el contenido en túneles GRE, GPRS, VXLAN e IPSec no cifrado, sin necesidad de que el equipo de seguridad sea el punto final del túnel.
- ✓ Soportar IPv6 en modos de alta disponibilidad, tanto Activo/Activo como Activo/Pasivo.



PERÚ

Ministerio
de Transportes
y Comunicaciones

Autoridad Portuaria
Nacional

"Decenio de la Igualdad de Oportunidades para Mujeres y Hombres"
"Año de la unidad, la paz y el desarrollo"

- ✓ 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.

ALTA DISPONIBILIDAD

- ✓ Soporte a configuración de alta disponibilidad Activo/Pasivo y Activo/Activo, con despliegues de los equipos tanto en modo transparente como en modo capa 3 (L3).
- ✓ La configuración en alta disponibilidad debe sincronizar: Sesiones; Certificados de descifrado, Configuraciones, incluyendo, más no limitado a políticas de Firewall, NAT, QoS y objetos de red.
- ✓ Debe ser posible el monitoreo de fallo de enlaces, ya sea ante la caída de al menos una de las interfaces del equipo, una conexión física adyacente o pérdida de conectividad hacia una IP desde una de las interfaces.
- ✓ Debe permitir cifrar la comunicación entre dos Firewall de HA durante la sincronización de las configuraciones.

FUNCIONALIDADES DE FIREWALL

- ✓ Control de políticas por zonas, puertos, direcciones IP, segmentos y/o rangos de red, región geográfica, usuarios y grupos de usuarios, aplicaciones grupos estáticos de aplicaciones, grupos dinámicos de aplicaciones (basados en sus atributos) y categorías de aplicaciones.
- ✓ Deberá ser posible la identificación de la aplicación y la inspección de malware, spyware y exploits dentro del tráfico cifrado por los protocolos en mención.
- ✓ Permitir el agendamiento de las políticas de seguridad.
- ✓ Debe ser posible especificar en las reglas de seguridad un grupo de objetos basados en IP y/o URL que se alimenten dinámicamente de una fuente externa.
- ✓ Permitir agrupar las políticas de seguridad utilizando etiquetas u otro método.
- ✓ Permitir añadir un comentario de auditoría cada vez que se cree o se edite la política de seguridad. Cada comentario deberá estar asociado a la versión de la política editada. Esto con el fin de garantizar buenas prácticas de documentación, organización y auditoría.
- ✓ Debe permitir realizar validaciones de la configuración antes de ser aplicada o instalada, esto implica, entre otras cosas, identificar y notificar cuando existan reglas generales superpuestas sobre otras específicas (shadowed rules).
- ✓ Debe mostrar la primera y última vez que se utilizó una regla de seguridad.
- ✓ Debe mostrar la fecha de creación y última fecha de modificación de la regla de seguridad.
- ✓ Debe mostrar a través de un filtro, las reglas de seguridad que no han tenido uso en la red desde el último encendido del dispositivo firewall.



Ministerio
de Transportes
y Comunicaciones

Autoridad Portuaria
Nacional

"Decenio de la Igualdad de Oportunidades para Mujeres y Hombres"
"Año de la unidad, la paz y el desarrollo"

DESCIFRADO DE TRÁFICO SSL/TLS

- ✓ Debe permitir descifrar el tráfico de navegación de usuarios a internet mediante la instalación de un certificado digital en los equipos.
- ✓ Debe permitir descifrar el tráfico entrante hacia servidores HTTPS publicados en internet importando el certificado del servidor en el Firewall.
- ✓ Debe ser capaz de inspección el tráfico cifrado, incluyendo el protocolo TLS 1.3.
- ✓ Debe tener la capacidad de bloquear la conexión hacia sitios web cifrados con protocolos obsoletos e inseguros.
- ✓ Debe identificar y notificar al cliente si está visitando una página web con certificado digital no válido o emisor no confiable, a pesar de no aplicar descifrado al tráfico SSL/TLS
- ✓ Debe soportar certificados que utilice Subject Alternative Name (SAN) y Server Name Indication (SNI).
- ✓ Debe permitir excluir sitios a los cuales no se les aplicará la política de descifrado, identificados por dominios y wildcards.
- ✓ Para los certificados almacenados localmente en el firewall, tiene que ser posible bloquear la posibilidad de exportar las claves privadas, para evitar un uso indebido por parte de los administradores.
- ✓ Debe contar con un dashboard de reportes y logs dedicados a monitorear el tráfico de descifrado SSL/TLS, este dashboard deberá estar disponible en la interfaz gráfica, con el objetivo de identificar rápidamente problemas relacionados con las técnicas de descifrado de tráfico, el mismo debe tener varios estados de troubleshooting y proveer de las herramientas a los administradores para encontrar rápidamente las causas por las cuales se puede producir una falla en la descifrado del tráfico (por ejemplo, informar sobre certificados expirados, claves de cifrado débiles, certificados revocados, cierre de la conexión por parte del cliente, entre otros).

CONTROL DE APLICACIONES

- ✓ Reconocer por lo menos 3000 aplicaciones diferentes, incluyendo, más no limitando: el tráfico relacionado a peer-to-peer, redes sociales, acceso remoto, update de software, protocolos de red, voip, audio, vídeo, proxy, mensajería instantánea, email.
- ✓ Debe procesar e inspeccionar aplicaciones que utilicen HTTP/2
- ✓ Para tráfico cifrado (SSL/TLS), debe permitir el descifrado de paquetes con el fin de permitir la lectura del payload de la aplicación cifrada.
- ✓ Debe inspeccionar el payload del paquete de datos con el objetivo de detectar las aplicaciones en capa 7, a través de expresiones regulares, firmas u otro mecanismo. El chequeo de firmas también debe determinar si una aplicación está utilizando su puerto default o no, por ejemplo, RDP en el puerto 80 en vez del 3389.
- ✓ Las políticas de seguridad deberán poder definirse 100% en base a aplicaciones pudiendo aplicar reglas específicas a cada aplicación, ejemplo si 2 aplicaciones utilizan el mismo puerto y protocolo, se tienen que poder crear 2 políticas de seguridad en las cuales se apliquen controles diferentes a cada aplicación.



Ministerio
de Transportes
y Comunicaciones

Autoridad Portuaria
Nacional

"Decenio de la Igualdad de Oportunidades para Mujeres y Hombres"
"Año de la unidad, la paz y el desarrollo"

- ✓ Debe poder identificar y crear políticas de seguridad basadas en aplicaciones de Sistemas de Infraestructura Crítica (ICS) como addp, bacnet, modbus, dnp3, coap, dlms, iccp, iec-60870-5-104, mms-ics, rockwell, siemens, entre otros.
- ✓ Debe aplicar análisis heurístico a fin de detectar aplicaciones a través de análisis de comportamiento del tráfico observado.
- ✓ Con el objetivo de identificar aplicaciones propietarias a nivel de capa 7, la solución debe permitir nativamente la creación de aplicaciones personalizadas desde la interfaz de gestión, sin la necesidad de acción por parte del fabricante.
- ✓ Debe ser posible la creación de grupos estáticos de aplicaciones y grupos dinámicos de aplicaciones basados en sus atributos.
- ✓ Al crear políticas basadas en aplicaciones, si las mismas dependen de otras aplicaciones, la interfaz gráfica debe sugerir y permitir agregar las aplicaciones dependientes de la seleccionada, para poder permitir el uso correcto de la política de seguridad en capa 7.
- ✓ Debe contar con un módulo de optimización de políticas, que identifique las aplicaciones que han pasado sobre políticas basadas en puertos o de Capa 4, indicando consumo en Bytes, Hits y Fechas de visualización. Este módulo deberá facilitar la migración de la política de Capa 4 a una política de Capa 7 a través de un wizard.

PREVENCION DE AMENAZAS CONOCIDAS

- ✓ Para seguridad del ambiente contra ataques, los dispositivos de seguridad deben poseer módulo de IPS (Intrusion Prevention System), Antivirus/Antimalware, Antispyware/Antibot.
- ✓ Capacidad de realizar DNS Sinkhole para la identificación de equipos comprometidos por spyware en entornos corporativos
- ✓ Las funcionalidades de IPS, Antivirus y Antispyware/Antibot deben operar en carácter permanente, pudiendo ser utilizadas por tiempo indeterminado, incluso si no existe el derecho de recibir actualizaciones debido a caducidad de soporte con el fabricante.
- ✓ El equipo deberá soportar el throughput solicitado operando en el máximo nivel o modo de seguridad de inspección de IPS, Antivirus y Antispyware/Antibot.
- ✓ Las firmas deberán estar basadas en patrones del malware y no únicamente en hashes, con el objetivo de detectar malware polimórfico que pertenezca a una misma familia.
- ✓ Debe sincronizar las firmas de seguridad cuando el Firewall se implementa en alta disponibilidad.
- ✓ Debe soportar granularidad en las políticas de IPS, Antivirus y Antispyware/Antibot, permitiendo la creación de diferentes políticas por zona de seguridad, dirección de origen, dirección de destino, servicio, usuario y grupo de usuarios y la combinación de todos esos ítems.
- ✓ Debe permitir capturar el paquete de red (en formato PCAP) asociada a la alerta de seguridad.
- ✓ Debe identificar las consultas que realizan los hosts infectados hacia dominios maliciosos, de tal forma que el Firewall pueda bloquear dichas consultas DNS.
- ✓ Los eventos deben identificar el país que origino la amenaza.



PERÚ

Ministerio
de Transportes
y Comunicaciones

Autoridad Portuaria
Nacional

"Decenio de la Igualdad de Oportunidades para Mujeres y Hombres"
"Año de la unidad, la paz y el desarrollo"

- ✓ Deberá posibilitar la creación de firmas customizadas por la interfaz gráfica del producto.
- ✓ Debe ser capaz de detectar y bloquear el virus y malware en general que se propague en, al menos, los siguientes protocolos: HTTP, HTTPS, HTTP/2, FTP, SMB (versiones 1, 2 y 3), SMTP, IMAP y POP3; tanto en IPv4 como en IPv6, para todos los protocolos en mención.
- ✓ Debe soportar la creación de firmas de IPS basadas en el formato de Snort.

ANÁLISIS DE MALWARE DE DÍA CERO

- ✓ La solución propuesta debe incluir mecanismos de detección de amenazas de día cero, incluyendo una plataforma Sandboxing.
- ✓ La plataforma de Sandboxing deberá ser ofrecido en Nube (Cloud). Como mínimo se requiere que el Sandbox propuesto pueda detectar el malware de día cero en un tiempo no mayor a 5 minutos utilizando la emulación completa de malware en entornos Windows, Linux, Android y Mac (este tiempo de análisis se debe cumplir de manera paralela para todos los archivos enviados al Sandbox, considerando análisis dinámico completo, es decir, no incluye Firmas o Prefiltros).
- ✓ Deberá tener una disponibilidad del servicio de al menos 99.9% contabilizados mensualmente.
- ✓ Deberá ser un servicio propio del fabricante, no se aceptarán plataformas que tercericen el servicio de Sandboxing con entidades terceras.
- ✓ El Next Generation Firewall deberá ser capaz de actualizar las firmas de malware en tiempo real, con el objetivo de tener información de malware detectado a nivel global por el fabricante.
- ✓ Deberá garantizar la privacidad y confidencialidad del contenido de los archivos analizados, para lo cual se requiere que el servicio cuente como mínimo con certificaciones SOC2 Tipo II de AICPA, FedRAMP.
- ✓ El malware de día cero deberá poder ser identificado dentro de la infraestructura de la Entidad, sin necesidad de enviar el archivo a ser analizado fuera de la red.
- ✓ Debe analizar Links/URLs para determinar si es o no malicioso, a pesar de no estar categorizada dentro de la Base de Datos del fabricante.
- ✓ Debe proveer información forense sobre las acciones realizadas por el malware y generar automáticamente las firmas de malware y bloquear el acceso a las URLs maliciosas utilizadas por el malware.
- ✓ El Next Generation Firewall debe ser capaz de enviar al sandbox de manera automática los archivos sospechosos que se propaguen por los protocolos HTTP, HTTPS, HTTP/2, FTP, SMTP, POP3, IMAP y SMB, tanto en IPv4 como en IPv6.
- ✓ Debe permitir al administrador la descarga del archivo original analizado por el Sandbox.
- ✓ Debe permitir reportar al fabricante eventos que son falso-positivo y falso-negativo en el análisis de malware de día cero a partir de la propia consola de administración.
- ✓ Deberá soportar el análisis de archivos ejecutables (EXE), DLLs, ELF (Linux), archivos comprimidos (ZIP, 7ZIP, RAR) archivos office (.doc, .docx, .xls, .xlsx, .ppt, .pptx), archivos java (.jar e class), archivos de



PERÚ

Ministerio
de Transportes
y Comunicaciones

Autoridad Portuaria
Nacional

"Decenio de la Igualdad de Oportunidades para Mujeres y Hombres"
"Año de la unidad, la paz y el desarrollo"

tipos script (.vbs, .ps1, .js), email link, flash, archivos de MacOS (mach-o, dmg, pkg) y Android APKs en el ambiente controlado.

- ✓ Permitir la subida de archivos al sandbox de forma manual y vía API.
- ✓ Debe detectar técnicas usadas para evadir herramientas de sandboxing como detección de hypervisor (no debe usar hypervisores comerciales), inyección de código a procesos permitidos y deshabilitación de funcionalidades de seguridad del host.
- ✓ La solución debe realizar el análisis en un ambiente de hardware real, deshabilitando totalmente la habilidad de la amenaza de evadir sandboxing en máquinas virtuales.

FILTRO DE CONTENIDO WEB

- ✓ Permite especificar la política por tiempo, horario o determinado período (día, mes, año, día de la semana y hora)
- ✓ Deberá incluir la capacidad de creación de políticas basadas en la visibilidad e identificar el usuario que accede a una URL a través de la integración con servicios de directorio, autenticación vía Active Directory, LDAP en general y base de datos local.
- ✓ Debe soportar un cache local de URLs en el appliance, evitando el delay de comunicación/validación de las URLs
- ✓ Debe poseer al menos 70 categorías de URLs, incluyendo las de malware y phishing.
- ✓ Debe permitir la creación de categorías personalizadas.
- ✓ Debe contar con multi categorías de URL, que permita que un sitio web pertenezca a dos categorías distintas.
- ✓ Debe identificar y categorizar los dominios nuevos, menores a 30 días de antigüedad.
- ✓ Debe permitir la customización de la página de bloqueo.
- ✓ Permitir la inserción o modificación de valores en la cabecera HTTP del tráfico de aplicaciones SaaS que pasen por el equipo de seguridad.
- ✓ Debe permitir notificar al usuario, mostrándole solo una página de alerta, pero permitiéndole continuar la navegación al site.
- ✓ Debe identificar cuando un usuario envía credenciales corporativas de red a sitios no autorizados y debe poder bloquear dicho envío, previniendo así ataques de phishing.

PROTECCION AVANZADA DE DNS

- ✓ La solución debe ser alimentada por un servicio de inteligencia global capaz de identificar decenas de millones de dominios maliciosos con análisis en tiempo real sin depender de firmas estáticas.
- ✓ El servicio de protección de DNS debe alimentarse de telemetría provista por clientes a nivel mundial y más de 30 fuentes de inteligencia de amenazas de terceros.
- ✓ La solución debe ser capaz de predecir y detener dominios maliciosos de malware basados en algoritmos de generación de dominio (DGA).
- ✓ Debe utilizar machine learning y/o inteligencia artificial para detectar nuevos dominios nunca vistos autogenerados por algoritmos DGA
- ✓ Debe poseer políticas para bloquear dominios DGA o interrumpir las consultas de DNS a dichos dominios.



Ministerio
de Transportes
y Comunicaciones

Autoridad Portuaria
Nacional

"Decenio de la Igualdad de Oportunidades para Mujeres y Hombres"
"Año de la unidad, la paz y el desarrollo"

- ✓ Debe ayudar a contener ataques emergentes basados en DNS, que utilicen técnicas de tunelización lenta sobre tráfico DNS, técnicas de entradas de DNS pendientes y adquisición de subdominios
- ✓ Debe ser capaz de predecir nuevos dominios maliciosos inmediatamente luego de su registro, antes de que puedan ser utilizados en ataques
- ✓ Debe detectar e interrumpir robo de datos ocultos o tunelizados en tráfico DNS
- ✓ Debe analizar las consultas de DNS, incluyendo las tasas de consultas y patrones, entropía y frecuencia de n-grams para detectar posibles intentos de tunelización.
- ✓ Debe bloquear resoluciones de DNS que usen técnicas de SNI Spoofing utilizadas para eludir los controles de descifrado.

IDENTIFICACION DE USUARIOS

- ✓ Debe incluir a capacidad de creación de políticas basadas en la visibilidad y control de usuarios y/o grupos de usuarios a través de la integración de servicios de autenticación vía LDAP, Active Directory, E- Novell Directory, Exchange y base de datos local.
- ✓ Debe poseer integración con Microsoft AD Domain Controller para la identificación de direcciones IP y usuarios. Esta integración se podrá realizar con o sin software agente.
- ✓ Debe poder identificar la IP y el usuario de Dominio en base a Event Viewer y WMI.
- ✓ Debe poder monitorear eventos de login y logout del Active Directory utilizando el protocolo WinRM.
- ✓ Debe soportar la recepción de eventos de autenticación de Controladores Wireless con 802.1x, Soluciones NAC y Proxy, vía Syslog, XFF (X-forward-for) en la cabecera HTTP y/o XML API para la identificación de direcciones IP y usuarios.
- ✓ Debe permitir el control, sin instalación de cliente de software, en equipamientos que soliciten salida a internet para que antes de iniciar la navegación, se muestre un portal de autenticación residente en el firewall (Captive Portal). Adicionalmente se podrá añadir un segundo factor de autenticación.
- ✓ Debe permitir la definición de grupos dinámicos de usuarios.

FILTRO DE DATOS

- ✓ Los archivos deben ser identificados por extensión y firmas.
- ✓ Permite identificar y opcionalmente prevenir la transferencia (subida o bajada) de varios tipos de archivos (incluidos MS Office, PDF, PE, APK, Flash, DLL, BAT, CAB, PIF, REG, archivos comprimidos en RAR, ZIP u otro) identificados sobre aplicaciones.
- ✓ Permitir identificar y opcionalmente prevenir la transferencia de información sensible basados en el contenido del archivo, incluyendo, más no limitando al número de tarjetas de crédito; y permitiendo la creación de nuevos tipos de datos vía expresión regular.



PERÚ

Ministerio
de Transportes
y Comunicaciones

Autoridad Portuaria
Nacional

"Decenio de la Igualdad de Oportunidades para Mujeres y Hombres"
"Año de la unidad, la paz y el desarrollo"

VPN

- ✓ Soportar VPN Site-to-Site y Cliente-To-Site en protocolos IPsec o SSL.
- ✓ La VPN IPsec debe soportar como mínimo:
 - DES y 3DES; AES 128, 192 e 256 (Advanced Encryption Standard)
 - Autenticación MD5, SHA-1, SHA-2;
 - Diffie-Hellman Group 1, Group 2, Group 5 y Group 14;
 - Algoritmo Internet Key Exchange (IKEv1 & IKEv2);
- ✓ Permitir la aplicación de políticas de seguridad y visibilidad para las aplicaciones que circulan dentro de los túneles VPN.
- ✓ Las VPN client-to-site deben poder operar usando el protocolo IPsec o SSL y permitir la conexión por medio de agente instalado en el sistema operativo.
- ✓ Soportar autenticación vía AD/LDAP, Kerberos, TACACS+, SAML, Certificados Digitales y RADIUS, incluyendo Doble Factor de Autenticación (2FA).
- ✓ Debe permitir definir segmentos de red para ser agregadas de forma automática en la tabla de rutas de la interfaz túnel del equipo que tenga instalado el agente de VPN.
- ✓ Debe soportar Split Tunnel para elegir los segmentos de red que serán enrutados por la VPN.
- ✓ Debe permitir los siguientes tipos de conexión del cliente al túnel VPN:
 - Antes del usuario se autentique en la estación;
 - Después de la autenticación del usuario en la estación usando Single Sign On (SSO);
 - Bajo demanda del usuario;
- ✓ El agente de VPN client-to-site debe ser compatible al menos con: Windows 7, Windows 8, Windows 10, MacOS X.
- ✓ Debe contar con un dashboard gráfico que permita monitorear a los usuarios conectados por VPN.
- ✓ Debe permitir al menos 300 usuarios concurrentes, el CONTRATISTA, debe considerar el licenciamiento necesario para cumplir con la cantidad de usuarios requeridos como mínimo.

CONSOLA DE ADMINISTRACION Y MONITOREO

- ✓ Con la finalidad de no degradar el performance de procesamiento de red y seguridad del Next Generation Firewall, la administración del equipo, gestión de reportes y gestión de logs deben contar con recursos dedicados de CPU, Memoria RAM y Disco Duro, ya sea integrado dentro del mismo appliance u otro appliance independiente del mismo fabricante
- ✓ Permitir exportar las reglas de seguridad en formato CSV y PDF
- ✓ Debe contar con un dashboard interactivo y gráfico que permita monitorear el uso de las aplicaciones en capa 7, sitios web visitados, actividad de los usuarios, actividad por IP (origen y destino), países origen y destino del tráfico, uso de las reglas de seguridad, actividad del tráfico malicioso, actividad de los usuarios VPN. Esta información podrá ser vista en base a Bytes y Sesiones, y ser filtrado en base a un rango de tiempo, IP, usuario, país y regla de seguridad.



PERÚ

Ministerio
de Transportes
y Comunicaciones

Autoridad Portuaria
Nacional

"Decenio de la Igualdad de Oportunidades para Mujeres y Hombres"
"Año de la unidad, la paz y el desarrollo"

- ✓ Debe permitir el control de acceso a la gestión del equipo a través de roles personalizables.
- ✓ Debe permitir la captura de paquetes en formato PCAP para poder ser leídos por una herramienta tercera. La captura de paquetes deberá poder ser filtrada antes del proceso de ejecución en base a la interfaz, IP y Puerto (origen y destino)
- ✓ Ante escenarios donde existan dos o más administradores del Next Generation Firewall logueados y realizando cambios en simultáneo en la consola de gestión, la solución deberá de ser capaz de solo aplicar los cambios realizados por cada administrador individual, sin afectar o sobrescribir los cambios del otro administrador.
- ✓ Contar con un módulo que permita comparar y que indique específicamente que cambio se hizo a una política de seguridad respecto a una versión anterior de dicha política.
- ✓ Debe ser capaz de detectar errores humanos de configuración de reglas de seguridad donde se sobrepongan reglas generales sobre reglas específicas (shadowing rules).
- ✓ Debe permitir el almacenamiento de diferentes versiones de archivos de respaldo de configuración (backup).
- ✓ Debe poder realizar una copia de seguridad (backup) automática de las configuraciones y rollback de configuración a la última configuración salvada.
- ✓ Debe permitir el monitoreo de eventos basados en SNMP, integración con SIEM a través de Syslog, y envío de alertas por correo electrónico (integrándose a un servidor SMTP).
- ✓ Debe permitir la generación de logs de auditoría detallados, informando de la configuración realizada, el administrador que la realizó, su IP y el horario de la alteración;
- ✓ Debe permitir la asignación de una cuota de uso de disco para definir una capacidad máxima de almacenamiento de logs de tráfico de datos, amenazas, auditoría de configuraciones, eventos de sistema.
- ✓ Debe soportar la personalización de reportes, permitiendo mostrar información de eventos de antivirus, antispyware, IPS, navegación a internet, aplicaciones, malware de día cero, debe permitir seleccionar las columnas a mostrar, filtrar la información en base a usuarios, grupos de usuarios, direcciones IP, el rango de fechas de los datos, deben poder ser exportados en PDF y enviados automáticamente vía correo electrónico.
- ✓ La plataforma de seguridad debe permitir realizar tareas de gestión a través del API basado en XML.
- ✓ A fin de validar las características técnicas mínimas ofertadas para los equipos firewall, se el postor ganador deberá presentar para el perfeccionamiento del contrato el formato de cumplimiento del Anexo C debidamente sustentado, indicando las referencias técnicas (número de folio) evidenciadas en los documentos emitidos por el fabricante (folletos catálogos, brochures u otros documentos entendiéndose como otros documentos los siguientes: guías prácticas o hojas técnicas o website del fabricante o manuales o carta del fabricante). La carta del fabricante se podrá presentar solo para las características específicas que no se encuentren en la documentación pública o interna del fabricante y no para todas las características que se



PERÚ

Ministerio
de Transportes
y Comunicaciones

Autoridad Portuaria
Nacional

"Decenio de la Igualdad de Oportunidades para Mujeres y Hombres"
"Año de la unidad, la paz y el desarrollo"

debe acreditar en el Anexo C. Asimismo, que en caso de presentar carta del fabricante esta deberá tener fecha actualizada a la fecha de la presentación de la documentación para el perfeccionamiento del contrato.

b) Servicio de Protección avanzada de puesto de trabajo y servidores

El CONTRATISTA, debe entregar un servicio gestionado de detección y respuesta avanzada a través de algún software con las siguientes características mínimas:

- ✓ Deberá estar integrada al servicio de ciberdefensa (visualización de investigaciones).
- ✓ Protección para 50 máquinas servidores y/o estaciones de trabajo compatible con los siguientes sistemas operativos:
 - Windows 7 SP1 hasta Windows 10
 - Windows Server 2008 R2 SP1 hasta Server/Core 2019
 - MacOS Big Sur (opcional), Catalina (opcional), Mojave (opcional).
 - Ubuntu, Redhat (RHEL), CentOS, Oracle.
 - Opcionalmente podrá ser compatible con Amazon AMI, SUSE Linux Enterprise Server, Fedora, Debian, Virtuozzo, Scientific Linux²¹.
- ✓ La solución estará basada en una administración On-Premise o SaaS multitenant de fácil uso y gestión flexible. El servicio debe incluir protección, detección y respuesta ante amenazas de los endpoint²².
- ✓ Protección contra ransomware con tecnología AI basado en comportamiento.
- ✓ Protección automática ante una amenaza.
- ✓ Prevención de ataques basada en archivos mediante inteligencia artificial estática y el servicio de inteligencia en nube del fabricante
- ✓ Detección de ataques fileless mediante IA de análisis de comportamiento
- ✓ Respuesta autónoma frente a amenazas/eliminación, cuarentena
- ✓ Respuesta de remediación/rollback autónoma, mediante una sola instrucción.
- ✓ Dispositivo en cuarentena de la red.
- ✓ Inventario de aplicaciones del dispositivo final.
- ✓ Detección de dispositivos no autorizados
- ✓ Vulnerabilidad de la aplicación del dispositivo final (opcional)²³.
- ✓ Reglas de detección personalizadas con respuesta activa de acuerdo con el contexto.
- ✓ El portal de administración de la solución EDR debe contar con las siguientes características:
 - Deberá ser una plataforma ampliada de detección y respuesta (XDR)
 - Capacidad de administrar la autenticación y autorización mediante SSO, MFA, RBAC.
 - Integración con la inteligencia de amenazas del propio fabricante y con los indicadores de amenaza de MITRE ATT&CK.

²¹ Absolución Pliego N° 49 participante VIETTEL PERU S.A.C

²² Absolución Pliego N° 50,53 participante VIETTEL PERU S.A.C

²³ Absolución Pliego N° 56 participante VIETTEL PERU S.A.C

- Dashboard que permita el análisis de seguridad de los datos.
- Notificaciones configurables por email o Syslog²⁴.
- ✓ La protección del dispositivo final deberá considerar: Inteligencia Artificial (AI) estática, IA basado en el análisis de comportamiento, protección frente a documentos, malware que se ejecuta en memoria, exploits. movimiento lateral de malware
- ✓ No se requiere una conexión central o consola de administración, para proteger el dispositivo final, ante la desconexión a Internet se mantendrá la protección de manera autónoma²⁵.
- ✓ Respuesta automática a Ransomware, con capacidad de reversión a una sola intrusión.
- ✓ Detección, prevención y respuesta a nivel organizacional
- ✓ Como respuesta del evento de ciberseguridad sobre el dispositivo final, la solución de EDR deberá realizar remediación y reversión a su estado original, cuarentena del dispositivo afectado, y protección con o sin acceso a Internet.
- ✓ Entre las características más importantes del EDR se deberá considerar: la detección de dispositivos sin el agente o no autorizados, inventario y vulnerabilidad de aplicaciones instaladas en el dispositivo final, control de dispositivo bluetooth, USB, control de Firewall OS con reconocimiento de ubicación.
- ✓ El servicio de EDR debe considerar un argumento de ataque, brindar visibilidad a bajo nivel, profunda del incidente, y permitir la caza de amenaza.
- ✓ La solución de EDR debe permitir determinar la causa raíz detrás de los actores de amenazas y responder de forma autónoma, sin depender de los recursos de la nube.
- ✓ La solución de EDR debe permitir determinar la causa raíz detrás de los actores de amenazas y responder de forma autónoma, sin depender de los recursos de la nube.
- ✓ A fin de validar las características técnicas mínimas ofertadas la protección avanzada de puesto de trabajo y servidores el postor ganador deberá presentar para el perfeccionamiento del contrato el formato de cumplimiento del Anexo D debidamente sustentado, indicando las referencias técnicas (número de folio) evidenciadas en los documentos emitidos por el fabricante (folletos catálogos, brochures u otros documentos entendiéndose como otros documentos los siguientes: guías prácticas o hojas técnicas o website del fabricante o manuales o carta del fabricante). La carta del fabricante se podrá presentar solo para las características específicas que no se encuentren en la documentación pública o interna del fabricante y no para todas las características que se debe acreditar en el Anexo D. Asimismo, que en caso de presentar carta del fabricante esta deberá tener fecha actualizada a la fecha de la presentación de la documentación para el perfeccionamiento del contrato.

c) Equipo de Administración de Ancho de Banda.

El CONTRATISTA, debe entregar en calidad de alquiler una solución de administración de ancho de banda, para ello deberá instalar un (01)

²⁴ Absolución Pliego N° 55 participante VIETTEL PERU S.A.C

²⁵ Absolución Pliego N° 51 participante VIETTEL PERU S.A.C



Ministerio
de Transportes
y Comunicaciones

Autoridad Portuaria
Nacional

"Decenio de la Igualdad de Oportunidades para Mujeres y Hombres"
"Año de la unidad, la paz y el desarrollo"

equipo (appliance) de propósito dedicado, para garantizar el óptimo servicio éste debe ser de tecnología vigente. Dicho equipo deberá contar con las siguientes características mínimas:

- ✓ Un equipo dedicado a la funcionalidad de gestionar ancho de banda, este componente o función no deberá estar embebida sobre enrutadores, firewalls, NGFW, UTM entre otras.
- ✓ Para efectos de la propuesta, ninguno de los modelos ofertados podrá estar listados ni anunciado en el sitio web del fabricante como end-of-life o end-of-sale o end-of-support. Se deberá adjuntar para el perfeccionamiento del contrato el enlace público del fabricante o catálogos o brochures o guías prácticas o hojas técnicas, website o manuales o carta de fabricante que verifique que los modelos propuestos no están en ese listado – Ver Anexo E.
- ✓ Debe estar licenciado para poder gestionar 100 Mbps de throughput full duplex (100 Mbps entrante y 100 Mbps saliente) y deberá tener capacidad de poder incrementar (con licenciamiento adicional) a 2 Gbps (sin cambiar de hardware).
- ✓ Capacidad de clasificar el tráfico según: Aplicación, Protocolo, Puerto, Rango de puertos, IP, Rango de IPs, Subred y VLAN
- ✓ Las reglas de clasificación se podrán configurar en múltiples niveles, mínimo 10, de forma que una regla pueda tener diferentes reglas hijo, y así sucesivamente.
- ✓ La configuración de políticas ha de realizarse mediante una aplicación con interfaz web
- ✓ La construcción de políticas ha de realizarse de forma visual, representándose el árbol con los diferentes niveles de forma gráfica y no en modo tabla.
- ✓ Cada nodo del árbol de políticas ha de ser capaz de contraerse para facilitar la visibilidad de todas las reglas, o poder visualizar un único nodo y sus políticas hijas.
- ✓ Se debe disponer de un buscador que, al escribir una aplicación, puerto, IP, dibuje el camino que recorre en el árbol para saber rápidamente qué política se le está asignando.
- ✓ Aplicar reglas de QoS que contengan las siguientes opciones:
 - Asignación de un mínimo de ancho de banda
 - Limitación a un máximo ancho de banda
 - Definición de diferentes prioridades
 - Descartar aquellos paquetes no deseados (drop)
 - Mantener el QoS original
 - Eliminar el QoS para que sea más proclive a descartarse si hay saturación
- ✓ Los catálogos de clasificación y control deben ser válidos para aplicar a cualquier nivel del árbol de clasificación (sin necesidad de definir a qué nivel corresponde la regla)
- ✓ Se debe disponer de capacidad de tener plantillas para poder clonar políticas.
- ✓ Se debe poder tener algoritmos de QoS para priorización y limitación de tráfico basado en % en vez de en valores estáticos o fijos.
- ✓ El elemento es transparente a nivel de transporte, sin cambios en las direcciones IP y puestos de origen destino.



PERÚ

Ministerio
de Transportes
y Comunicaciones

Autoridad Portuaria
Nacional

"Decenio de la Igualdad de Oportunidades para Mujeres y Hombres"
"Año de la unidad, la paz y el desarrollo"

- ✓ La solución de QoS ha de ser integrable dentro de una herramienta de analítica avanzada que permita todas las funcionalidades descritas en el módulo de reporting.
- ✓ El sistema de políticas debe tener autoprotección y detección de incongruencias en políticas impidiendo la creación de una política errónea y quedando marcado en el árbol de políticas en algún color aquella política que no es válida impidiendo ser guardada.
- ✓ El equipo para ofertar debe disponer de un bypass externo y pasivo simultaneo de interfaces de cobre y/o de fibra óptica, dicho bypass deberá garantizar que en caso de falla eléctrica o de procesamiento de este equipo, el tráfico no se vea interrumpido y se garantice la continuidad de la conectividad de las interfaces en funcionamiento.
- ✓ El dispositivo de gestión de ancho de banda deberá poder soportar la optimización TCP de tráfico dentro de la misma caja, deberá poder hacer las siguientes funcionalidades de aceleración:
 - La solución de optimización deberá ir en línea y cumplir con los siguientes requisitos:
 - Optimización de tráfico encriptado por protocolo TLS (versiones 1.0, 1.1, 1.2 y 1.3) sin romper la encriptación extremo a extremo.
 - Optimización de tráfico encriptado por protocolo SSL (versiones 2.0, 3.0) sin romper la encriptación extremo a extremo.
 - Optimización de tráfico de Internet (tráfico no proveniente del centro de datos/WAN).
 - Optimización de tráfico de aplicaciones albergadas en la nube.
 - Despliegue en un solo punto en el camino del tráfico. No deberá ser necesario desplegar parejas de elementos en cada extremo del tráfico a optimizar.
 - Despliegue en la nube no necesaria para optimizar aplicaciones albergadas.
 - Despliegue tanto en appliances de fabricante como modo software en entorno virtual.
 - Los parámetros de optimización se autoajustarán con algoritmos de aprendizaje.
 - El elemento actuará como un enlace físico (bump-in-the-wire) que manda el tráfico entre dos puertos físicos sin necesitar de direcciones IP asignadas y sin cambiar las MACs de los paquetes que lo atraviesan.
 - El elemento soporta agregación de enlaces.
 - El elemento soporta VLANs
 - El elemento es compatible con los siguientes mecanismos de respaldo (failover): OSPF (opcional), BGP (opcional), 802.3ad.
 - El elemento es transparente a nivel de transporte, sin cambios en las direcciones IP y puestos de origen destino.
- ✓ Capilaridad a nivel de Aplicaciones y reporting del gestor de ancho de banda



Ministerio
de Transportes
y Comunicaciones

Autoridad Portuaria
Nacional

"Decenio de la Igualdad de Oportunidades para Mujeres y Hombres"
"Año de la unidad, la paz y el desarrollo"

- ✓ La consola de analítica y reportería debe ser poder montada dentro del gestor de ancho de banda sin que esto afecte al rendimiento. No se admitirán soluciones cuya gestión vaya fuera del appliance de gestión de tráfico o en la nube.
- ✓ Dicha parte de reportería deberá tener las siguientes capacidades de monitorización y analítica avanzada:
 - Creación de cuadros de mando personalizados a las necesidades del cliente.
 - Capacidad de hacer filtros en las diferentes tablas de la base de datos y de las distintas fuentes de datos.
 - Capacidad de hacer ZOOM o "Drill Down" desde una vista superior a otra vista más particular.
 - Capacidad de crear cuadros de mando con leyendas personalizadas, incrustar vídeos, o fotos explicativas en la página web del cuadro de mando. Capacidad de incrustar Logos o cualquier otra información.
 - Posibilidad de crear botones de búsqueda, cuadros de mando de búsquedas, posibilidad de hacer búsquedas múltiples por diversos criterios, etc.
 - Interfaz gráfica multilenguaje.
 - Interfaz gráfica debe soportar "modo claro" y "modo oscuro".
 - La interfaz gráfica debe auto-adaptarse a la resolución y/o al tipo de terminal: laptop, tableta, móvil, etc.
 - Posibilidad de hacer filtros de todo tipo de los datos y de las vistas de los datos.
 - Capacidad multitenant de acceso a las vistas de datos y a los datos. Dicha funcionalidad no puede ser de coste adicional.
 - Capacidad de multiplexar diferentes fuentes de datos en un único cuadro de mando.
 - Capacidad de creación de alarmas y eventos y planificación de eventos.
 - Notificación de alarmas en múltiples formatos tipo email, Slack, o similares.
 - Capacidad de visualizar umbrales de tres niveles, pudiendo seleccionar los colores, tanto para series temporales como agregadas y acelerómetros.
 - Capacidad de generación de informes e informes automatizados que se puedan programar y generar automáticamente en formato PDF y otros, tipo JPG o CSV.
 - Capacidad de creación mapas de "carreteras" que permitan visualizar por donde va un flujo, servicio o aplicación. Capacidad de autodescubrimiento de nodos de red.
 - Capacidad de generar múltiples vistas de datos en formato tabla, series temporales, diagramas, gráficos de barras, gráficos de agregación como por ejemplo tipo "pie" y otros muchos tipos.
 - Se podrán sacar informes y gráficas en función del tiempo, seleccionando mediante un calendario el periodo a visualizar.
 - Se podrá definir la resolución de los datos a visualizar, por ejemplo: cada minuto, cada 5 minutos, etc. Incluso se podrá ir



PERÚ

Ministerio
de Transportes
y Comunicaciones

Autoridad Portuaria
Nacional

"Decenio de la Igualdad de Oportunidades para Mujeres y Hombres"
"Año de la unidad, la paz y el desarrollo"

a resoluciones inferiores siempre y cuando se tengan datos con una resolución inferior.

- Se podrán crear cuantos "dashboards" o cuadros de mando se desea y la forma de construirlos será mediante tarjetas (cards) que se pueden definir de cualquier tamaño, se podrán asignar colores, leyendas y en definitiva personalizar.
 - Dichas tarjetas estarán accesibles para los usuarios en función de sus privilegios y podrán ser particulares de un usuario o generales para ser utilizadas por muchos usuarios.
 - Las tarjetas deben permitir suscribirse a eventos creados en otras tarjetas. Es decir, haciendo click en un campo de una tarjeta, debe permitir que se aplique el filtro del valor seleccionado en otra u otras tarjetas.
 - Una tarjeta puede ser definida como filtro, de modo que permita crear una entrada de texto, una lista desplegable, botones de selección, etc. Dichos filtros han de aplicarse a las tarjetas predefinidas.
 - Las tarjetas pueden configurarse para aparecer invisibles en el cuadro de mando y aparecer sólo cuando se aplique un evento determinado.
- ✓ Métricas, KPIs y tipos de aplicaciones necesarias de la herramienta:
- Reconocimiento de aplicaciones a nivel 7.
 - Capacidad de generar firmas para reconocimiento de aplicaciones corporativas.
 - Deben disponer de reportes relativos a: Aplicaciones, Conversaciones, URLs, Puertos, Grupo de aplicaciones, Nombre de host, IP origen, IP destino, Puerto origen, Puerto destino
 - Calcular las siguientes métricas:
 - QoE
 - RTT
 - TCP duplicate ACK
 - TCP Packet lost
 - TCP Retransmission
 - TCP RTT Client site
 - TCP RTT Server site
 - Network
 - Number of flows
 - Total throughput
 - Total volume
 - Downstream
 - Upstream
 - Packets transmit
 - Packets received
 - Activity duration
 - Max peak throughput
 - HTTP/HTTPS
 - Service Setup time
 - Mean data
 - Peak data



PERÚ

Ministerio
de Transportes
y Comunicaciones

Autoridad Portuaria
Nacional

"Decenio de la Igualdad de Oportunidades para Mujeres y Hombres"
"Año de la unidad, la paz y el desarrollo"

- Service non accessibility
 - Session failure ratio
 - Session time
 - Set up time
 - Transactions
 - Data transfer cut off
 - Service access failure
 - Usuario
 - Duration Usage
 - Total activity
 - Start time
 - Stop time
 - VoIP
 - RTT
 - TCP duplicate ACK
 - TCP Packet lost
 - TCP Retransmission
 - TCP RTT Client site
 - TCP RTT Server site
 - Caller ID
 - Session Time o Duration time
- ✓ La sonda de red debe ser capaz de realizar capturas de tráfico para poder generar PCAPs tanto para IPs concretas como para rangos de IPs. Dichas capturas se podrán truncar para de la carga útil del paquete. Se podrá seleccionar las IPs o VLANs desde donde se realiza la captura.
 - ✓ Se podrá almacenar en la base de datos gran cantidad de datos (días, incluso semanas) para realizar las capturas siempre en función del almacenamiento necesario para las mismas.
 - ✓ Se podrá identificar el tráfico de un mismo flujo que pueda estar duplicado, tanto para la captura de paquetes como para la propia monitorización de la sonda DPI.
 - ✓ Se puede recibir información segmentada por VLANs.
 - ✓ Se podrá identificar un flujo o conexión independientemente de que pudiera haber en la red un Proxy, NAT o un cambio en la cabecera de los paquetes de dicha conexión.
 - ✓ El sistema gestor de tráfico debe poder soportar, no licenciado de inicio, en el mismo equipo y sin HW adicional la capacidad de monitorizar todos los equipos externos al gestor que forman parte de la comunicación del enlace a Internet (FW, SW, Routers, Servidores u otros).
 - ✓ A fin de validar las características técnicas mínimas ofertadas del equipo administrador de ancho de banda se el postor ganador deberá presentar para el perfeccionamiento del contrato el formato de cumplimiento del Anexo E debidamente sustentado, indicando las referencias técnicas (número de folio) evidenciadas en los documentos emitidos por el fabricante (folletos catálogos, brochures u otros documentos entendiéndose como otros documentos los siguientes: guías prácticas o hojas técnicas o website del fabricante o manuales



PERÚ

Ministerio
de Transportes
y Comunicaciones

Autoridad Portuaria
Nacional

"Decenio de la Igualdad de Oportunidades para Mujeres y Hombres"
"Año de la unidad, la paz y el desarrollo"

o carta del fabricante). La carta del fabricante se podrá presentar solo para las características específicas que no se encuentren en la documentación pública o interna del fabricante y no para todas las características que se debe acreditar en el Anexo E. Asimismo, que en caso de presentar carta del fabricante esta deberá tener fecha actualizada a la fecha de la presentación de la documentación para el perfeccionamiento del contrato.

d) Servicio de Ciberdefensa

El CONTRATISTA, deberá entregar un servicio de ciberdefensa propio o de un tercero, este servicio de manera opcional podrá contar con certificación ISO27001 e ISO22301. Este servicio deberá permitir mediante el análisis de logs de la solución de seguridad perimetral (Firewall) y solución EDR, permita realizar investigaciones y escalar incidentes con las siguientes características:

- ✓ Capas adicionales como analítica de comportamiento de usuarios (UBA), orquestación, automatización y respuesta de seguridad (SOAR), para procesar múltiples eventos de seguridad y mecanismos de detección propietarios basados en Inteligencia artificial totalmente integrados al servicio.
- ✓ Con el objetivo de validar y dar seguimiento a las investigaciones de ciberseguridad, el CONTRATISTA deberá entregar un Portal web seguro con doble factor de autenticación para revisar las investigaciones. Esto se deberá entregar en la fase 02 de la implementación del servicio, a través de un correo electrónico.
- ✓ El portal debe actuar como una interfaz gráfica de usuario (GUI) que muestre investigaciones que fueron realizadas por los componentes (SIEM, UBA, SOAR, I.A.).
- ✓ El portal deberá mostrar investigaciones por el periodo de contrato para efectos de historial y permitir consultas como: en cualquier rango de tiempo, fuentes datos, estados, por lo menos 3 niveles de condición de defensa o DEFCON (normal, intermedio y crítica) asociado a las investigaciones y misiones pendientes de revisar
- ✓ Capas adicionales al SIEM como analítica de comportamiento de usuarios (UBA), orquestación, automatización y respuesta de seguridad (SOAR), para procesar múltiples eventos de seguridad y mecanismos de detección propietarios basados en Inteligencia artificial totalmente integrados al servicio.
- ✓ Monitoreo 24x7 identificando amenazas cibernéticas que puedan afectar la operación.
- ✓ Inteligencia de amenazas mediante actualizaciones de indicadores de compromiso (IOC) de múltiples fuentes que incluyen indicadores internos extraídos de eventos, comunidades de código abierto, redes sociales, inteligencia técnica e inteligencia procedente de la Deep and Dark Web. Las fuentes de inteligencia de amenazas deberán ser enviadas al gestor de eventos de la seguridad de la información para correlacionar y generar detecciones.



PERÚ

Ministerio
de Transportes
y Comunicaciones

Autoridad Portuaria
Nacional

"Decenio de la Igualdad de Oportunidades para Mujeres y Hombres"
"Año de la unidad, la paz y el desarrollo"

- ✓ Caza de amenazas sobre el gestor de eventos de seguridad, identificando, evaluando y mejorando la capacidad de detección mediante búsqueda exhaustiva de ciber-amenazas y actividades maliciosas.
- ✓ Respuesta y mitigación de incidentes en tiempo real ante ciber-amenazas.
- ✓ Optimización de procesos consistentes de desarrollo y aprendizaje que incluyan optimización de reglas, actualizaciones y sugerencias de implementación de nuevas tecnologías de detección de amenazas cibernéticas.
- ✓ Investigación forense de procesos en curso de presuntas actividades maliciosas y amenazas cibernéticas incluyendo el análisis post mortem de incidentes verificados. Mínimo de 4 horas mensuales de ser requerido.
- ✓ *El servicio deberá tener la capacidad de integrarse a los componentes de seguridad ofertados en el presente proceso y sus fuentes de registro y Endpoint²⁶*
- ✓ *Configuración personalizable de notificaciones vía email (notificaciones, recomendaciones, acciones pendientes, nuevas investigaciones, escalamiento de una investigación en curso, modificación del estado de una investigación en curso)*
- ✓ *De manera opcional este servicio podrá ser retroalimentado por un emisor externo de incidentes para que de esta manera no sea juez ni parte en la emisión de investigaciones, a fin de asegurar la imparcialidad y permitir que la entidad pueda dar seguimiento de los tiempos de resolución y atención del postor²⁷.*
- ✓ Monitoreo de credenciales y direcciones IP en Web Oscura
 - Monitoreo 24x7x365 de credenciales de correo del dominio apn.gob.pe (ilimitadas), 10 direcciones de correo personal (gmail,outlok,etc) y de 49 direcciones Ipv4 públicas
 - Entregar visibilidad de los passwords comprometidos, si el hallazgo lo permite
 - Incluir información personal, si el hallazgo lo permite, como fecha de nacimiento, nombres, apellidos, números de identificación personal y/o fiscal
 - *Se deberá enviar un informe mensual en el caso de detectarse una brecha esta deberá ser detallada en dichos informes con los hallazgos correspondientes²⁸.*
- ✓ Gestión continua de vulnerabilidades y monitoreo de superficie de ataque para el dominio apn.gob.pe y hasta 30 subdominios por el periodo de contrato.
- ✓ Visibilidad desde el punto de vista de un ciberdelincuente mediante visualización de recursos y/o aplicaciones expuestas. Se deberá restringir todo lo que no sea necesario estar publicado. Se deberá poder visualizar:
 - Direcciones ip
 - Hostnames
 - Puertos
 - Protocolos
 - Servicios
 - Información de servicios
 - Expiración de certificados SSL

²⁶ Absolución Pliego N°60 participante VIETTEL PERU S.A.C

²⁷ Absolución Pliego N°61 participante VIETTEL PERU S.A.C

²⁸ Absolución Pliego N°82 participante AMERICA MOVIL PERU S.A.C



PERÚ

Ministerio
de Transportes
y Comunicaciones

Autoridad Portuaria
Nacional

"Decenio de la Igualdad de Oportunidades para Mujeres y Hombres"
"Año de la unidad, la paz y el desarrollo"

- ✓ La gestión continua de vulnerabilidades deberá ejecutarse de forma semanal, por el periodo de contrato y cada vez que se registre una amenaza emergente indicando los CVE asociados.
- ✓ La solución deberá ejecutar como mínimo 11,000 controles infosec. El contratista deberá adjuntar el listado de controles con la siguiente información:
 - Nombre del control
 - CVE
 - Data de publicación
 - Clasificación CVSS
 - Factor de riesgo (alto, mediano, bajo).
- ✓ Los controles de seguridad deben ser del tipo:
 - Software y hardware vulnerable
 - Vulnerabilidades de aplicaciones Web
 - OWASP10
 - SQL Injection
 - XSS
 - XXE
 - Fuga de información
 - Información local de directorio
 - Dirección IP interna
 - Reducción de superficie de ataque
 - Base de datos expuestas
 - Interfaces administrativas
 - Servicios sensibles (SMB)
 - Software de monitoreo de red
 - Debilidad SSL/TLS
 - Heartbleed, Crime, Beast, Robot
 - Protocolos de bajo cifrado
 - Configuraciones erróneas de certificados SSL
 - Servicios sin encriptación
- ✓ Los informes deberán presentar las vulnerabilidades encontradas con el siguiente contexto
 - Descripción
 - Ocurrencia
 - Evidencia
 - Remediación
 - Nuevas vulnerabilidades versus análisis anterior

e) Servicio de Gestión de Vulnerabilidades

El CONTRATISTA, deberá entregar un servicio de gestión de vulnerabilidades que contemple lo siguiente:

- ✓ Una solución de gestión de vulnerabilidades y auditoría de configuraciones de infraestructura que está basada en cloud, en modalidad software como servicio, licenciada para 65 activos de infraestructura y 20 aplicaciones web.
- ✓ Realizar escaneos de vulnerabilidades y evaluación de configuraciones (políticas) en forma programada y automática. Los resultados de estos deberán estar consolidados en un único sistema de gestión.



PERÚ

Ministerio
de Transportes
y Comunicaciones

Autoridad Portuaria
Nacional

"Decenio de la Igualdad de Oportunidades para Mujeres y Hombres"
"Año de la unidad, la paz y el desarrollo"

- ✓ Colectar datos mediante escáneres activos, escáneres pasivos (análisis de tráfico de red) y agentes. No deberá haber límites en la cantidad de escáneres a desplegar en forma distribuida. Además, deberá contar con motores de escaneo públicos para escanear ambientes publicados a Internet.
- ✓ Estar basado en un catálogo propio de vulnerabilidades que incluyan más de 160 mil evaluaciones diferentes y al menos 64 mil vulnerabilidades conocidas por un período no menor a 15 años.
- ✓ Proveer un mecanismo de priorización de vulnerabilidades automático basado en la probabilidad de explotación y que ofrezca información alternativa al CVSS (Common Vulnerability Scoring System) basada en Inteligencia de amenazas reales recabada de diversas fuentes como Deep Web, Dark Web, redes sociales, sitios de divulgación y otros centros de investigación.
- ✓ Ser capaz de evaluar, no solo vulnerabilidades, sino auditar configuraciones y compararlas contra las mejores prácticas y frameworks de seguridad tales como CIS, CERT, CISA STIG, PCI y otros para la totalidad de activos licenciados, incluidos equipos de red, infraestructura de virtualización, Windows, Linux, Bases de Datos, Aplicaciones y otros sistemas. Estas auditorías podrán ser personalizables por la organización. Esta funcionalidad es también conocida como Policy Compliance. Se requiere esta capacidad sin límites de licenciamiento.
- ✓ Deberá contar con una API completa para integración mediante scripting automatizado y exportación de datos mediante llamados. Esta API debe estar liberada y documentada y no deberá tener limitaciones de licencias en cantidad de llamados o sistemas que la consultan. Si no existe una licencia ilimitada, considerar la de mayor capacidad disponible.
- ✓ Los escáneres deben ser desplegables en modalidad software y virtual appliance con soporte de VMware y Hyper-V.
- ✓ Deben permitir la configuración y almacenamiento seguro de credenciales de usuario para escanear mediante cuentas locales y de dominio Windows, cuentas ssh para sistemas Unix/Linux y dispositivos de red. Deberá permitir elevar privilegios mediante "su" y "sudo" y no deberá tener limitaciones en cantidad de credenciales. Además, el sistema deberá integrarse con soluciones de bóvedas digitales como Cyberark, Centrify, Beyondtrust y otras.
- ✓ Deberá ser capaz de obtener vulnerabilidades de estaciones de trabajo en Internet (teletrabajo) y otros ambientes no conectados a la red del organismo, e inalcanzables por un escáner, mediante agente Windows, Linux y MacOS.
- ✓ Deberá contar con escaneos que solo auditen la existencia o inexistencia de parches de todo tipo de sistemas (Windows Desktop, Unix/Linux, equipos de red, aplicaciones y otras plataformas).
- ✓ Deberá mantener registro de estado de vulnerabilidades por activo, de modo de identificar vulnerabilidades que, habiendo sido remediadas, volvieron a surgir en nuevos escaneos.



PERÚ

Ministerio
de Transportes
y Comunicaciones

Autoridad Portuaria
Nacional

"Decenio de la Igualdad de Oportunidades para Mujeres y Hombres"
"Año de la unidad, la paz y el desarrollo"

Deberán registrarse las fechas de primera aparición, última aparición y reaparición. Además, se deberá contar con una vista de vulnerabilidades remediadas.

- ✓ La solución debe ser capaz de identificar sistemas comprometidos por malware y otros códigos maliciosos. También deberá ser capaz de identificar la ejecución y nivel de firmas del sistema de Antimalware presente en el dispositivo.
- ✓ Permitir auto-clasificar activos mediante reglas que asignen clases o etiquetas de acuerdo a diversos criterios como Ubicación, Criticidad, Unidad de negocio, tipo de tecnología, dueño del activo, y otros.
- ✓ Debe reportar vulnerabilidades que sean explotables, establecer el nivel de madurez del código de exploit (si aplica), documentar de que forma se explota (malware, acceso remoto, con o sin credenciales), si el exploit está presente en frameworks reconocidos tales como Metasploit, Canvas, Core y otras.
- ✓ Proporcionar un modelo de licencia dinámico, para garantizar que la recopilación de datos (escaneos activos o detección pasiva) no se interrumpa cuando se rebase temporalmente las licencias contratadas. Además, la solución deberá contar con la posibilidad de informar el conteo de licencias utilizado y licenciado y las fechas de expiración.
- ✓ Proporcionar control de acceso basado en roles y perfiles con suficiente granularidad para controlar a los usuarios el acceso a determinados conjuntos de datos y la funcionalidad que está disponible para los usuarios tales como ejecutar escaneos, cambiar configuraciones, acceder a los resultados, generar reportes, aceptar riesgos y otros casos de uso. Debe contar con roles predefinidos y permitir crear nuevos roles.
- ✓ Permitir configurar características de performance de red para impedir que produzca excesos de tráfico en redes de bajo ancho de banda disponible. También deberá permitir configurar la simultaneidad de sistemas escaneados y la cantidad de chequeos por escaneo. Aun teniendo estas medidas el sistema deberá incluir la capacidad de programar ventanas horarias que automáticamente detengan la ejecución de todos los escaneos y luego los reanuden.
- ✓ Presentar paneles de control predefinidos y personalizables que contengan datos estadísticos, gráficos de tendencias, información relevante mediante filtros, índices de riesgos y otros datos importantes.
- ✓ Deberá ser capaz de identificar activos mediante escaneos de descubrimiento y escaneos pasivos. Además, deberá detectar el sistema operativo, los servicios que se ejecutan, el software instalado y datos que permitan identificarlo tales como IP, MAC Address, hostname/DNS Name. Deberá permitir aplicar etiquetas que designen criterios de clasificación tales como criticidad, área o departamento, dueño, ubicación física, ambiente. Estas etiquetas deberán ser completamente personalizables y permitir crear reglas que las apliquen automáticamente. También deberá registrar el día y hora que



PERÚ

Ministerio
de Transportes
y Comunicaciones

Autoridad Portuaria
Nacional

"Decenio de la Igualdad de Oportunidades para Mujeres y Hombres"
"Año de la unidad, la paz y el desarrollo"

se vio al activo por primera y última vez y la última vez que fue escaneado con credenciales.

- ✓ Contar de forma nativa e incluida en su licenciamiento, la capacidad de conectarse a las API de Google Cloud Platform, AWS y Azure para el descubrimiento de nuevas instancias en entornos de nube. Además, deberá contar con escáneres pre-autorizados y disponibles en esos servicios de nube.
- ✓ Permitir realizar escaneos del tipo auditoría de configuración para determinar el cumplimiento de los controles de seguridad y mejores prácticas contra estándares de industria (CIS, NIST, etc), recomendaciones de fabricantes y políticas internas personalizadas. Estas auditorías deberán alcanzar a sistemas operativos, incluyendo los de los dispositivos de red, aplicaciones, motores de bases de datos, hipervisores, cuentas cloud (AWS, Azure, Google Cloud Platform) y otros componentes de infraestructura y deberá permitir ser ejecutado con escáner de red o con agente.
- ✓ Contar además con mecanismos para detectar información sensible y ser capaz de auditar la ejecución y estado de actualización de los paquetes antivirus instalados.

Para la gestión de vulnerabilidades sobre Aplicaciones Web, se contemplará las siguientes características:

- ✓ Contar con un módulo que automatice el descubrimiento de problemas de seguridad comunes tales como Cross-Site Scripting, SQL Injection, Directory Traversal,
- ✓ Configuraciones inseguras y otras vulnerabilidades y debilidades en aplicaciones Web.
- ✓ Deberá estar orientado al descubrimiento de vulnerabilidades indicadas en el TOP 10 de OWASP <https://owasp.org/www-project-top-ten/>
- ✓ Debe utilizar motores de escaneo propios. No se aceptarán soluciones que utilicen motores de otros fabricantes o tecnologías open-source.
- ✓ Debe contar con motores de escaneo públicos, listos para ser usados sin necesidad de despliegue para aplicaciones publicadas a Internet.
- ✓ Contar con diferentes opciones de escáneres distribuidos globalmente y tener libertad de elegir cual utilizar.
- ✓ Deberá informar los rangos de IP utilizados por cada grupo de escáneres.
- ✓ Los escáneres deberán auto escalar de manera de no producir mayores retrasos ni colas de espera en la ejecución.
- ✓ Contar con una opción de despliegue local para motores de análisis que permitan escanear aplicaciones internas no publicadas a Internet.
- ✓ Definir y administrar grupos de usuarios, incluida la limitación de las funciones de escaneo y el acceso a informes.
- ✓ Contar con la opción de configurar métodos de autenticación de múltiples factores.
- ✓ Contar con ilimitados motores de escaneo sin que la licencia limite su uso.



Ministerio
de Transportes
y Comunicaciones

Autoridad Portuaria
Nacional

"Decenio de la Igualdad de Oportunidades para Mujeres y Hombres"
"Año de la unidad, la paz y el desarrollo"

- ✓ Se debe permitir la definición de secciones críticas de la aplicación que sean seguras para escanear y de otras partes que nunca deberían escanearse, para evitar latencias de rendimiento e interrupciones.
- ✓ Debe soportar todas las versiones de protocolos de transporte utilizados comúnmente en los sitios web actuales, incluyendo http v.1.1, http v.1.0, SSL/TLS, http compression, http User Agent Configuration.
- ✓ debe estar basada en escaneos activos mediante tests remotos. No se tendrán en cuenta herramientas que analicen tráfico ni requieran la implementación de piezas de software o código en la aplicación o requiera la instalación de un gateway para su análisis.
- ✓ Debe contar con plantillas de scan que permitan escanear las vulnerabilidades de una aplicación y otros que permitan solo entender la estructura del sitio. Deberá también haber plantillas para auditar la versión de SSL/TLS implementada en la aplicación.
- ✓ Contar con una plantilla que permita auditar la configuración de la aplicación.
- ✓ Contar con un repositorio de credenciales para ser utilizadas en los escaneos.
- ✓ Contar con la posibilidad de ingresar credenciales de usuarios válidos de la aplicación y soportar los siguientes esquemas:
 - Usuario/Password usando esquema Basic/Digest o NTLM.
 - Formulario de Login de la aplicación indicando url y con la opción de configurar una Regex o una página específica que permita verificar el login exitoso.
 - Cookie con verificación de login exitoso.
 - Selenium mediante la generación de un script automatizado mediante el registro de ingreso de una sesión válida
- ✓ El escáner debe mantener una sesión válida activa durante todo el escaneo, tanto para descubrir los elementos del sitio (parámetros, cookies, formularios, enlaces, etc.) como para el testeo de vulnerabilidades.
- ✓ Deberá permitir configurar una programación para ejecutar un escaneo en forma recurrente, programando la frecuencia o definiendo día y hora precisa de inicio.
- ✓ Permitir configurar permisos de acceso y visibilidad a los resultados y de control y configuración de los parámetros del escaneo.
- ✓ Permitirá definir si los resultados son compartidos y acumulados en los paneles de control y reportes generales o son solo de consulta del propietario
- ✓ Permitirá utilizar scripts de Selenium para analizar páginas con lógicas de acceso complejas.
- ✓ Permitirá definir URLs explícitas para ser incluidas o excluidas en una tarea de escaneo.
- ✓ Permitirá definir extensiones de archivos para que sean excluidas de análisis.



PERÚ

Ministerio
de Transportes
y Comunicaciones

Autoridad Portuaria
Nacional

"Decenio de la Igualdad de Oportunidades para Mujeres y Hombres"
"Año de la unidad, la paz y el desarrollo"

- ✓ Deberá dar la opción de configurar la descomposición del Path para incluir directorios recursivos como nuevas URLs.
- ✓ Debe ser capaz de auditar:
 - Cookies
 - Encabezados (Headers)
 - Formularios
 - Links
 - Nombres de Parámetros
 - Valores de Parámetros
 - Elementos JSON
 - Elementos XML
 - Formularios UI (Entradas y grupos de botones asociados con código JavaScript)
 - Entradas UI (elementos de entrada huérfanos con los eventos del modelo de objeto de documento (DOM) asociado)
- ✓ Permitir definir una URL de un host remoto para testear una vulnerabilidad de RFI (Remote File Inclusion)
- ✓ Contar con la opción de definir la duración máxima de un escaneo.
- ✓ Contar con parámetros que limiten la cantidad de URLs que el sistema rastreará, la cantidad máxima de directorios, el tamaño máximo de una página que analizará y la cantidad máxima de redirecciones que el escaneo hará antes de detenerse.
- ✓ Permitir definir el user-agent con que el escaner explorará la aplicación.
- ✓ Permitirá definir opciones de pantalla que usará el escaner para la evaluación, tales como el ancho y el alto en pixeles.
- ✓ Contar con opciones para configurar la performance del escaneo tales como:
 - Máximo número de conexiones HTTP concurrentes
 - Máximo número de requerimientos HTTP por segundo
 - Detectar red congestionada y reducir la carga
 - Especificar el tiempo máximo de espera de las respuestas
 - Especificar el tiempo máximo de espera de un browser antes de abortar el escaneo
 - Especificar el número consecutivo de vencimientos de tiempo de espera (timeouts) antes de abortar el escaneo
- ✓ Tener la suficiente granularidad como para poder definir la habilitación/inhabilitación de tests de vulnerabilidades puntuales o por familias.
- ✓ El fabricante deberá poner a disposición acceso a una API que permita crear conectores, importar/exportar datos y automatizar procesos.
- ✓ Ser capaz de detectar vulnerabilidades que permitan la inyección de código.
- ✓ Deberá testear la aplicación e identificar vulnerabilidades de Cross-Site Scripting.
- ✓ Deberá contar con evaluaciones que identifiquen vulnerabilidades que permitan la exposición de datos.
- ✓ Deberá detectar vulnerabilidades y debilidades de configuración del Web Server.



Ministerio
de Transportes
y Comunicaciones

Autoridad Portuaria
Nacional

"Decenio de la Igualdad de Oportunidades para Mujeres y Hombres"
"Año de la unidad, la paz y el desarrollo"

- ✓ Deberá contar con múltiples evaluaciones relacionadas con SSL/TLS, identificando cifrados no soportados o débiles, certificados auto-firmados o expirados, versiones débiles u obsoletas de protocolo.
- ✓ debe ser segura de escanear en ambientes de producción.
- ✓ debe tener la capacidad de testear una aplicación web diseñada para el uso en dispositivos móviles.
- ✓ Deberá ser capaz de testear aplicaciones HTML5.
- ✓ Debe Ser capaz de lanzar escaneos bajo demanda y detenerlos durante su ejecución.
- ✓ Debe permitir ejecutar múltiples escaneos simultáneos.
- ✓ Debe entregar paneles de control que muestren indicadores estadísticos con número de vulnerabilidades por criticidad.
- ✓ Deberá entregar paneles de control que muestren indicadores de ejecución de los escaneos.
- ✓ Debe mostrar en los paneles de control, cuantas vulnerabilidades existen agrupadas por categoría de OWASP.
- ✓ Deberá mostrar resultados ordenados por vulnerabilidad o por aplicación y ordenando por severidad y cantidad.
- ✓ Dada una aplicación, el sistema deberá mostrar el histórico de escaneos realizados sobre la misma.
- ✓ Deberá contar con paneles de control que muestren estadísticas de vulnerabilidades por aplicación, por categoría de OWASP y por severidad.
- ✓ Deberá permitir crear paneles de control personalizados.
- ✓ A fin de validar las características técnicas mínimas ofertadas de la solución de la gestión del vulnerabilidades se el postor ganador deberá presentar para el perfeccionamiento del contrato el formato de cumplimiento del Anexo F debidamente sustentado, indicando las referencias técnicas (número de folio) evidenciadas en los documentos emitidos por el fabricante (folletos catálogos, brochures u otros documentos entendiéndose como otros documentos los siguientes: guías prácticas o hojas técnicas o website del fabricante o manuales o carta del fabricante). La carta del fabricante se podrá presentar solo para las características específicas que no se encuentren en la documentación publica o interna del fabricante y no para todas las características que se debe acreditar en el Anexo F. Asimismo, que en caso de presentar carta del fabricante esta deberá tener fecha actualizada a la fecha de la presentación de la documentación para el perfeccionamiento del contrato.

f) Servicio de Protección DDoS.

- ✓ El CONTRATISTA, deberá brindar el servicio de protección DDoS para la APN. El servicio deberá tener las siguientes características:
 - Se requiere de un servicio de mitigación de ataques de denegación de servicios en la nube, del CONTRATISTA.
 - La solución debe soportar IPV4 y IPV6.



PERÚ

Ministerio
de Transportes
y Comunicaciones

Autoridad Portuaria
Nacional

"Decenio de la Igualdad de Oportunidades para Mujeres y Hombres"
"Año de la unidad, la paz y el desarrollo"

- Capacidad de throughput inspección incluida debe ser de al menos del ancho de banda contratado.
- Capacidad de informar la cantidad de tráfico malicioso bloqueado, en bps, durante una mitigación activa en la nube.
- Capacidad de informar la cantidad de tiempo que una mitigación de nube lleva ejecutándose.
- El servicio incluirá la protección contra ataques de denegación de servicio hasta la capa 4 y/o hasta la capa 7.

g) Soporte de LAN gestionada.

✓ El CONTRATISTA, deberá brindar el servicio de soporte gestionado y la renovación de la garantía de fábrica de los equipos de comunicaciones propiedad de la APN. El servicio deberá tener las siguientes características:

- Si los equipos Switch instalados fallan (deja de funcionar), el CONTRATISTA, debe gestionar el cambio por otro similar o superior en un plazo del MRA de la marca
- Debe realizar atención de incidencias de los Switch de forma ilimitada, refiriéndose a la atención de requerimientos, incidencias y/o soporte técnico, ya sea de manera remota o presencial, cumpliendo los tiempos establecidos en los presentes términos de referencia.
- Actualizar el Firmware de los equipos de ser necesario.
- Renovar las garantías del fabricante de los equipos de comunicaciones de propiedad de la APN por 36 meses. Dichas garantías serán vigentes a partir de la firma del acta de activación del servicio, los certificados o cartas de garantía deben ser entregadas a la firma del acta de activación del servicio. Asimismo, se deben considerar los siguientes escenarios:
- Para los equipos de comunicaciones de propiedad de la APN descritos en el presente literal que cuenten aun con garantía antes de activar el servicio a contratar, el CONTRATISTA, se encargara de gestionar los cambios por garantía de fábrica y también de la gestión. En caso la garantía de fábrica de los equipos de propiedad de la APN descritos en el presente literal, venzan durante el desarrollo del contrato, el CONTRATISTA, deberá realizar la extensión de garantía de fabrica hasta donde el fabricante se lo permita (Dicha renovación de garantía deberá ser entregada por mesa de partes en el momento que realice la renovación. Esta renovación no generara costo para la entidad)o hasta la culminación del contrato, luego de ello la entidad asumirá los gastos por cambio de equipo ante alguna avería , pero el CONTRATISTA, continuara con el servicio de LAN gestionada realizando la administración, configuración y atención de incidencias y requerimientos, de dichos equipos.
- Para el caso de los equipos de propiedad de la APN, que se encuentren sin vigencia tecnológica (sin soporte de fabrica) al momento de la activación del servicio a contratar y que no se le pueda ampliar la garantía de fábrica, el CONTRATISTA, solo deberá brindar el servicio de soporte gestionado del equipo y en caso alguno de estos equipos fallara la entidad se hará cargo de su cambio y/o reparación²⁹.
- El equipamiento de comunicaciones para la Red gestionada de propiedad de la APN es el siguiente:

²⁹ Absolución Pliego N° 120 participante AMERICA MOVIL PERU S.A.C



Ministerio
de Transportes
y Comunicaciones

Autoridad Portuaria
Nacional

"Decenio de la Igualdad de Oportunidades para Mujeres y Hombres"
"Año de la unidad, la paz y el desarrollo"

Equipo	Marca	Modelo	Cantidad	Series
Switch-Core	JUNIPER	EX3300	02	<ul style="list-style-type: none"> GA0214510238 GA0214520292
Switch-Acceso	JUNIPER	EX2200	07	<ul style="list-style-type: none"> CT0213357276 CU0214330227 CT0214320149 CU0213394679 CT0214320260 CT0214490661 CT0210240983
Switch-Acceso	JUNIPER	EX2300	10	<ul style="list-style-type: none"> JW3620260611 JW3620261001 JW3620260622 JW3620261021 JW3620260935 JW3620260607 JW3620260542 JW3620260567 JW3620260603 JW3620261030
Switch-Acceso	CISCO	C9300-24T	02	<ul style="list-style-type: none"> FJC24431NXF FJC24431NXF
Switch-Acceso	ARUBA	2930F	04	<ul style="list-style-type: none"> CN83HL3248 CN83HL33BT CN83HL327C CN83HL3238
Access Point	ARUBA	IAP 315RW	06	<ul style="list-style-type: none"> CNF0J0T7B3 CNF0J0T7B4 CNF0J0T77P CNF0J0T77T CNF0J0T7DP CNF0J0T7GN
Access Point	ARUBA	IAP 205 RW	06	<ul style="list-style-type: none"> CN63HH85LH CN63HH85ML CN63HH85QX CN63HH85MW CN63HH85MV CN63HH85MN
Access Point	ARUBA	IAP 305 RW	07	<ul style="list-style-type: none"> CNJFJSS0K8 CNJFJSS0Q1 CNJ7JSSGGM CNJFJSS0H8 CNJ7JSS0K9 CNJFJSS005 CNJ7JSSFY0

- Para el caso del Access Point, el CONTRATISTA debe realizar un diagnóstico inicial de la red inalámbrica a fin de mejorar el rendimiento de esta. Si en caso fuera necesario reubicar

algunos de los equipos inalámbricos, el CONTRATISTA será responsable de realizar dicha actividad la cual incluirá el tendido de cableado de red, en la misma categoría con que se encuentre la red de la institución, siendo la APN la responsable de proporcionar la conexión eléctrica. Esta revisión deberá realizarse en la fase 02 de implementación del servicio y se detallará el resultado del diagnóstico y las mejoras realizadas si fuese el caso.

- Suprimido³⁰
- El CONTRATISTA, deberá tener en cuenta que uno de los swiches se encuentra en el CCCRE de la ciudad de Iquitos cuya marca es Aruba y modelo 2930F. Los demás equipos se encuentran distribuidos entre la sede central de la APN y el CCCRE del puerto del Callao.
- El servicio de soporte de LAN gestionada deberá detectar las fallas de lentitud en la red de datos de la sede central del CCCRE del puerto del Callao y del local anexo de la sede central de la APN (se precisa que existe una conexión de radio enlaces entre la sede central de la APN y el local anexo el cual se encuentra a 200 metros de distancia, la gestión del radio enlace está a cargo de APN), a fin de que puedan identificar problemas de altos consumos del ancho de banda de alguna estación de trabajo, debido a un ciberataque interno o externo³¹.

1.3 SERVICIO DE ENLACE DE DATOS CON EL CCCRE.

a) Enlace de Datos

- ✓ Los enlaces dedicados de transmisión tendrán las siguientes características:
 - Simétrico, deberá tener un overbooking 1:1 y un ancho de banda de 35 Mbps garantizado al 100% en ambos extremos, para la Sede Central ubicado en el Av. Santa Rosa 135 – La Perla – Callao y la Sede del CCCRE del Puerto del Callao, ubicado en Av. Manco Cápac S/N – Callao (Referencia: frente a la Av. Piérola).
 - El CONTRATISTA deberá de proveer dos equipos router, uno para la sede central y otro para el CCCRE del puerto del Callao, además de los equipos necesarios para la interconexión de la sede central de la APN y la sede del Centro de Control de Comunicaciones y Respuesta a Emergencias (CCCRE), del puerto del Callao.
 - A fin de validar las características técnicas mínimas ofertadas para estos dos router, debe presentar en su oferta el Formato de Cumplimiento del ANEXO A, debidamente sustentado, indicando las referencias técnicas (número de folio) evidenciadas en los documentos emitidos por el fabricante (folletos, catálogos, brochures u otros). El POSTOR ganador de la buena pro deberá presentar para el perfeccionamiento de contrato el formato de cumplimiento del Anexo A³².

³⁰ Absolución Pliego N° 121 participante AMERICA MOVIL PERU S.A.C

³¹ Absolución Pliego N° 122, 124 participante AMERICA MOVIL PERU S.A.C

³² Absolución Pliego N° 160 participante AMERICA MÓVIL PERU S.A.C, N° 190, 191 participante AMERICATEL PERU S.A

- Los enlaces dedicados deberán soportar QoS y diferenciar el tráfico de extremo a extremo para voz, datos y video según el requerimiento de la APN. La entidad indicará la configuración de los COS en la fase 02 de la implementación del servicio.
- El medio de transmisión requerido debe ser fibra óptica en la última milla.
- El servicio deberá contar con una Red IP/MPLS con el fin de cumplir con los requerimientos del APN.
- El backbone deberá ser propio y no rentados a terceros. El CONTRATISTA deberá garantizar que cumple con dicho requerimiento, para tener solo un punto de coordinación en los momentos que se genere una atención de soporte.

Asimismo, de manera opcional el acceso de ultima milla podra ser propio y no rentado de terceros³³.

- Para efectos de la propuesta, ninguno de los modelos ofertados podrá estar listados ni anunciado en el sitio web del fabricante como end-of-life o end-of-sale o end-of-support. Se deberá adjuntar para el perfeccionamiento del contrato el enlace público del fabricante o catálogos o brochures o guías prácticas o hojas técnicas, website o manuales o carta de fabricante que verifique que los modelos propuestos no están en ese listado - Ver Anexo A.
- El enrutador por instalar en las sedes usuarias deberá tener como mínimo las siguientes interfaces físicas para la conectividad de datos: 02 interfaces Ethernet 10/100/1000 Mbps.
- Soporte Técnico 24Hrs x 7 días a la semana, durante la vigencia del contrato y ante cualquier eventualidad en la transmisión.
- El retardo del enlace end to end (implica medición entre nodos del CONTRATISTA) tendrá un tiempo máximo de 30ms y la medición se realizará con paquetes de tamaño de 32 bytes. Dicha medición se realizará en la fase 03 de pruebas y se adjuntará dichos resultados en el informe final. Asimismo, se precisa que la medición será desde el puerto del Router de una sede a través de su IP de puerta de enlace, hasta el puerto del router de la otra sede y su puerta de enlace.
- La solución deberá permitir el cambio de la configuración de los COS durante el periodo del contrato sin costo alguno para la entidad.
- La disponibilidad del enlace de datos debe ser de al menos 99.50% mensual. Se entiende que la red en esta zona es propensa a una mayor frecuencia de cortes de fibra óptica.

1.4 SERVICIO DE TELEFONÍA FIJA DIGITAL

a) Telefonía Fija.

³³ Absolución Pliego N° 25 participante VIETTEL PERU S.A.C



Ministerio
de Transportes
y Comunicaciones

Autoridad Portuaria
Nacional

"Decenio de la Igualdad de Oportunidades para Mujeres y Hombres"
"Año de la unidad, la paz y el desarrollo"

- ✓ La cobertura para el servicio solicitado es de acuerdo con el cuadro siguiente:

Sede	Dirección	Cantidad de PRIs o SIP TRUNK o Troncal SIP	Canales de Voz	DIDs
Sede Central	Av. Santa Rosa 135 La Perla - Callao	02 PRI o SIP TRUNK o Troncal SIP	30	100

El servicio deberá de permitir el acceso sin restricciones a los siguientes destinos:

Minutos Fijos	Bolsa Incluida
Telefonía Fija Local	10,000 minutos mensuales
Telefonía Fija a Móvil Nacional	5,000 minutos mensuales
Larga Distancia Fijo Nacionales	1,800 minutos mensuales
Larga Distancia Fijo Internacionales	200 minutos mensuales
Larga Distancia Móvil Internacionales	100 minutos mensuales

- El servicio debe brindar la posibilidad de restringir las llamadas a teléfonos celulares en general (locales, nacionales e internacionales) a petición de la entidad.
- Las llamadas a celulares deben considerarse dentro de las bolsas contratadas y no deben generar costo adicional (salvo se haya consumido la totalidad de minutos de la bolsa).
- Las llamadas a destinos no contempladas en las bolsas descritas (rurales, satelitales) serán facturadas de manera adicional a precios de lista y deben ser facturados en el mismo documento de los consumos adicionales fuera de bolsa.

b) Detalles del servicio de Telefonía Fija Digital

- ✓ Uno de los dos E1 PRI o SIP TRUNK o Troncal SIP deberán ser configurado en modo activo/activo, el medio físico de transporte de ambos enlaces debe ser fibra óptica canalizada en todo su recorrido desde el punto de presencia del proveedor hasta el local central de la APN, garantizando de esta forma la calidad y continuidad del servicio. El enlace de respaldo deberá provenir de un nodo diferente al enlace principal, así como deberá utilizar una ruta distinta. Se precisa que son 100 DID distribuidos entre los 2 E1 PRI o SIP TRUNK o Troncal SIP. Se precisa que el segundo E1 PRI o SIP TRUNK o Troncal SIP, será para atender el desborde de llamadas del Primario y además que en caso el primario falle el secundario asumirá toda la carga, es decir atenderá llamadas entrantes y salientes.
- ✓ El Enlace Primario Principal (E1 PRI o SIP TRUNK o Troncal SIP) debe ser configurado con 30 canales digitales de comunicación; utilizando como medio de comunicación Fibra Óptica desde el punto de presencia del CONTRATISTA.



PERÚ

Ministerio
de Transportes
y Comunicaciones

Autoridad Portuaria
Nacional

"Decenio de la Igualdad de Oportunidades para Mujeres y Hombres"
"Año de la unidad, la paz y el desarrollo"

- ✓ El Enlace Primario Contingencia (E1 PR o SIP TRUNK o Troncal SIP) debe ser configurado con 30 canales digitales de comunicación; utilizando como medio de comunicación Fibra Óptica desde el punto de presencia del CONTRATISTA.
- ✓ Se debe asignar 100 números DIDs (para poder acceder a una extensión telefónica directamente sin pasar por una operadora). Se precisa que la cantidad de DOD deberá ser la misma que los DID.
- ✓ El tipo de interface de señalización ofrecido deberá ser E1 PRI o SIP TRUNK o Troncal SIP, utilizando el protocolo Euro ISDN. El PRI o SIP TRUNK o Troncal SIP deberá tener descubrimiento del número de la llamada entrante.
- ✓ Acceso gratuito a los servicios de emergencia.
- ✓ Presentación de identidad del usuario llamante.
- ✓ Garantía de privacidad en las telecomunicaciones. La garantía de privacidad de en las telecomunicaciones se encuentra acorde a lo establecido en el Art. 13 del TUO del Reglamento de la Ley de Telecomunicaciones.
- ✓ Capacidad de discado directo nacional (DDN), internacional (DDI) y restricciones de bloqueo.
- ✓ Servicio de facturación detallada de las conexiones o llamadas salientes, así como los minutos reales consumidos en forma mensual, los que deberán llegar mensualmente vía correo electrónico (se deberá enviar al siguiente correo: emisorelectronico1@apn.gob.pe) y en formato MS Excel, lo que permitirá a la entidad analizar sus consumos de manera detallada por cada DID, donde se detalle sus consumos llamada por llamada. Se precisa que, para la implementación del tarifador, el CONTRATISTA deberá proporcionar todos los softwares necesarios para su implementación. La entidad solo brindará un servidor virtual con las características que se solicite.
- ✓ Servicio sin restricciones de bloqueo para ningún tipo de destino definido en el cuadro de bolsas a contratar. Caso contrario deberá ser solicitado expresamente por la APN a través del área responsable del servicio.
- ✓ Bajo los principios de neutralidad no-discriminación igualdad de acceso y libre y leal competencia promovidos por OSIPTEL, el CONTRATISTA, debe de permitir el acceso a los servicios de larga distancia nacional y larga distancia internacional de otras operadoras de la competencia a consideración de la APN
- ✓ El CONTRATISTA deberá facilitar toda información solicitada por la APN referente a consumos desagregados (Llamadas Locales Fijo, fijo móvil, LDN y LDI), sin costo alguno y al finalizar cada periodo de facturación.
- ✓ El servicio de Telefonía debe brindar la facilidad de reportes por conjuntos de DIDs agrupados por centro de costo o unidad orgánica según defina la entidad.
- ✓ Conexión en HUNTING.

1.5 SERVICIO DE CENTRAL TELEFÓNICA - (TELEFONÍA INTERNA)

a) Equipo Central Telefónica



PERÚ

Ministerio
de Transportes
y Comunicaciones

Autoridad Portuaria
Nacional

"Decenio de la Igualdad de Oportunidades para Mujeres y Hombres"
"Año de la unidad, la paz y el desarrollo"

- El servicio deberá brindar una solución de Telefonía IP Privada Gestionada, para ello el CONTRATISTA brindará un equipo (appliance) de propósito dedicado en calidad de alquiler (Se precisa que una vez finalizado el plazo contractual, la entidad procederá a la devolución de los equipos entregados en alquiler), para garantizar un óptimo servicio el equipo debe ser de tecnología vigente. La central telefónica, deberán contar con las siguientes características mínimas:
 - El equipamiento deberá ser de solución tipo appliance de propósito específico con arquitectura todo en uno (all-in-one), de crecimiento modular a través de tarjetería (primarios y/o líneas analógicas), y basado en el protocolo SIP.
 - Para efectos de la propuesta, ninguno de los modelos ofertados podrá estar listados ni anunciado en el sitio web del fabricante como end-of-life o end-of-sale o end-of-support. Se deberá adjuntar para el perfeccionamiento del contrato el enlace público del fabricante o catálogos o brochures o guías prácticas o hojas técnicas, website o manuales o carta de fabricante que verifique que los modelos propuestos no están en ese listado – Ver Anexo G.
 - La central telefónica debe incluir los puertos para dos primarios. Se precisa que se podrá utilizar un equipo externo (Gateway) para recibir los primarios, siempre y cuando sea de la misma marca de la central telefónica propuesta o cuente con un certificado de interoperabilidad emitido por el fabricante.
 - La central telefónica debe tener la capacidad de integrar 60 teléfonos analógicos, de ser el caso se deberá incluir las licencias necesarias. Se precisa que la central telefónica deberá contar con puertos analógicos a través de módulos internos o tarjetas modulares o equipos externos (Gateways).
 - Debe contemplar 86 licencias para telefonía IP como mínimo.
 - El sistema de comunicaciones deberá permitir asignar hasta 300 códigos o más, para la realización de llamadas como mínimo, asociado a los permisos con los que cuenta cada usuario, por ejemplo, llamada a teléfonos fijos, teléfonos móviles, larga distancia nacional o larga distancia internacional.
 - La central debe permitir contestar las llamadas de un anexo a otro.
 - La central debe permitir crear grupos de anexos.
 - El sistema deberá estar habilitado para atender la capacidad de equipos telefónicos solicitados, teniendo capacidad para soporte de telefonía IP y analógica. Sin embargo, la solución deberá estar dimensionada para soportar un crecimiento de hasta un 100% como mínimo.
 - En caso de suministrarse licencias en software o hardware, éstas serán cedidas a perpetuidad y no deberán ser necesarios contratos de renovación periódicos. Para ello el CONTRATISTA, deberá entregar el certificado de las licencias de ser el caso, como anexo al informe final referente a la instalación y configuración del servicio.



PERÚ

Ministerio
de Transportes
y Comunicaciones

Autoridad Portuaria
Nacional

"Decenio de la Igualdad de Oportunidades para Mujeres y Hombres"
"Año de la unidad, la paz y el desarrollo"

- El sistema deberá proporcionar buzones de voz incorporados (built-in) para implementar la funcionalidad de correos de voz o voicemail y prevenir la pérdida de llamadas.
- El sistema deberá soportar servicios suplementarios tales como, llamada de emergencia, estación de secretaria, y barrido de llamada (opcional), entre otros, para cumplir con los diferentes requerimientos de servicio.
- El sistema deberá soportar IPv4 e IPv6.
- Se deberá considerar que, durante el periodo de contrato, la APN podrá solicitar el cambio de IPv4 a IPv6, así como la configuración en los equipos de comunicaciones (Switch) en calidad de alquiler y los equipos de comunicaciones de propiedad de la APN (los cuales cuentan con soporte para IPv6), para que se configure el protocolo IPv6 en la red telefónica fija, dicha configuración no tendrá costo para la institución. Se precisa que la configuración del protocolo IPv6 en los equipos alquilados y los equipos de propiedad de la APN estará a cargo del CONTRATISTA y sin costo para la APN.
- El sistema debe estar en capacidad de soportar los códecs de audio G.711a, G.711μ, G.729 o G.729AB.
- El sistema de comunicaciones deberá ser una plataforma de comunicaciones IP y soportar una gama de teléfonos IP que a su vez soporten estándares internacionales como Calidad de Servicio (QoS), G.711a, G.711μ, G.729 o G.729AB en conexión Ethernet, con switch incorporado, de 10/100 Mbps como mínimo.
- La central telefónica deberá estar en capacidad de integrarse sin problemas con un sistema de tarificación externo, en lo que se refiere a asignación de cuotas, que opcionalmente incluya cortes de llamadas, aviso de corte mediante mensajería entre otros.
- El sistema deberá permitir la personalización de la música de espera y poder permitirle la adición de mensajes Institucionales.
- Se deberá cambiar el actual saludo de la central telefónica de la APN, en la solución que este proponga. Para ello, El CONTRATISTA, deberá realizar la grabación del saludo en un estudio profesional de tal forma que dicho audio no presente ruido, ni voces robotizadas. La APN entregará al CONTRATISTA, el texto bajo el cual se realizará la grabación para que posteriormente este sea incluido en el sistema de la central telefónica, esta configuración deberá realizarse antes de la activación del servicio. Dicho audio deberá ser parte de los entregables del informe final referente a la instalación y configuración del servicio. El texto para la grabación del saludo se entregará en la fase 02 de implementación.
- El sistema de la central telefónica debe ser capaz de permitir que se pueda grabar un saludo de bienvenida con opciones de tal forma que el usuario externo, pueda seleccionar de forma rápida al área que desea llamar, asimismo en caso el usuario externo desee comunicarse con la operadora y esta esté ocupada, el sistema deberá enviar un mensaje de espera y



PERÚ

Ministerio
de Transportes
y Comunicaciones

Autoridad Portuaria
Nacional

"Decenio de la Igualdad de Oportunidades para Mujeres y Hombres"
"Año de la unidad, la paz y el desarrollo"

apenas la operadora libera la línea el mensaje de espera sea interrumpido para que ingrese la llamada.

- El sistema de la central Telefónica debe permitir que cuando la operadora se encuentre atendiendo una llamada e ingrese en ese mismo instante alguna llamada externa, el sistema deberá a través de un audio indicar que la operadora está ocupada, dando la opción de marcar el anexo o seguir esperando la atención de la operadora.
- Asimismo, las opciones que marque el usuario externo deberán estar relacionadas a uno o dos anexos, es decir si en caso un anexo se encuentra ocupado y ha timbrado más de 05 veces la llamada pasara al siguiente anexo que esté relacionado a la opción que se haya marcado y encaso este segundo anexo este ocupado, el sistema le indicara mediante un mensaje que el anexo está ocupado y dando la alternativa que marque otra opción o espere la atención de la operadora.
- Asimismo, durante el periodo de contrato se deberá garantizar que la APN pueda realizar hasta dos cambios del saludo sin costo alguno para la entidad. Es decir, el CONTRATISTA, deberá realizar hasta dos nuevas grabaciones del saludo, en caso la institución lo requiere.
- La administración deberá ser a través de una consola web, para la asignación de anexos, códigos, permisos de llamadas, entre otros.
- Las dimensiones de los equipos deberán ser para instalaciones en racks o gabinetes o bandejas empleando el estándar de 19".
- Para la funcionalidad de único número de contacto, el sistema tendrá la capacidad de configurar listas de acceso (incluyendo la posibilidad de restricciones hacia ciertos números) y programación de horarios para la distribución de las llamadas.
- Alimentación 220V AC 60Hz, incluyendo los cables de alimentación eléctrica para los tomacorrientes con líneas a tierra.
- El sistema de central telefónica deberá tener la capacidad de poder modificar las etiquetas de los teléfonos, es decir que la central telefónica tendrá la capacidad de modificar nombres y números de anexos de los teléfonos analógicos e IP
- Las funcionalidades de los teléfonos analógicos que son propiedad de la APN deberán de poder realizar lo siguiente:
 - ✓ Transferencia de llamadas.
 - ✓ Llamadas externas
 - ✓ Llamadas Internas
 - ✓ Captura de llamadas
 - ✓ Grupo de extensiones
 - ✓ Código personal
- Se deberá incluir módulos de tarjeta para la conexión de hasta 60 teléfonos analógicos.
- Los Teléfonos IP deben tener las siguientes facilidades:



PERÚ

Ministerio
de Transportes
y Comunicaciones

Autoridad Portuaria
Nacional

"Decenio de la Igualdad de Oportunidades para Mujeres y Hombres"
"Año de la unidad, la paz y el desarrollo"

- ✓ Restricción de llamadas (Restringir o bloquear ciertos números).
 - ✓ Grupos de extensiones
 - ✓ Captura de llamadas.
 - ✓ Código personal.
 - ✓ Conferencia tripartita.
 - ✓ Desvío de llamadas.
 - ✓ Rellamada.
 - ✓ Llamada en consulta.
 - ✓ Llamada externa.
 - ✓ Llamada interna.
 - ✓ Marcación por tonos DTMF o pulsos.
 - ✓ Interconexión de llamada sobre la extensión ocupada o en DND.
 - ✓ Identificación de llamadas.
 - ✓ Deshabilitación/Habilitación del teléfono IP por el usuario o administrador del sistema.
 - ✓ Teléfono con múltiples números, es decir que el teléfono pueda manejar varios números de extensión o DID's en simultaneo.
 - ✓ Supervisión visual permanente de otros anexos desde el teléfono IP. (opcional).
 - ✓ Marcación abreviada, es decir a que el usuario pueda invocar un directorio personal a través de la marcación de una tecla.
 - ✓ Movimiento de terminal mediante código.
 - ✓ Lista de llamadas ISDN no contestadas.
 - ✓ Se debe contar con una operadora automática que permita acceder directamente a un anexo interno desde una línea externa en una central telefónica además de dar una imagen corporativa a la empresa. Es decir, que la Central Telefónica pueda contar con un saludo de bienvenida en el cual cuenta con diversas opciones en las cuales el usuario externo pueda marcar y comunicarse con el anexo asociado a esa opción.
- A fin de validar las características técnicas mínimas ofertadas de la central telefónica el postor ganador deberá presentar para el perfeccionamiento del contrato el formato de cumplimiento del Anexo G debidamente sustentado, indicando las referencias técnicas (número de folio) evidenciadas en los documentos emitidos por el fabricante (folletos catálogos, brochures u otros documentos entendiéndose como otros documentos los siguientes: guías prácticas o hojas técnicas o website del fabricante o manuales o carta del fabricante). La carta del fabricante se podrá presentar solo para las características específicas que no se encuentren en la documentación pública o interna del fabricante y no para todas las características que se debe acreditar en el Anexo G. Asimismo, que en caso de presentar carta del fabricante esta deberá tener fecha actualizada a la fecha de la

presentación de la documentación para el perfeccionamiento del contrato.

b) software de tarificación de llamadas

- Reporte de llamadas entrantes / salientes por anexo, código y usuario
- Debe permitir asignar bolsa de minutos por usuarios y código de negocio, el software no deberá contar o cancelar la llamada después de haber utilizado el 100% de la bolsa de minutos asignada al código de negocio.
- Control de excesos de llamadas fijas y celulares vía alertas por email
- Debe permitir asignar una cantidad de minutos a un empleado para realizar llamadas³⁴
- El sistema debe permitir asignar código por llamadas por usuario como mínimo 300 códigos
- El software debe enviar los reportes programados por correo electrónico en formato Excel y Pdf
- Consultas por empleado, anexo, fecha, tipo de servicio, tipo de llamada y código de negocio
- El software de tarificación podrá ser instalado en servidor virtual que la APN proporcionará, con las características que el CONTRATISTA solicite, esto con la finalidad de ahorrar costos en la adquisición de un servidor, para la instalación del software de tarificación
- El CONTRATISTA, deberá coordinar con la APN, la asignación de la bolsa de minutos por código de negocio, dicha distribución de minutos deberá ser detallada en el informe final referente a la instalación y configuración del servicio.
- Alertas ante:
 - ✓ Exceso de duración de llamada
 - ✓ Uso de códigos no registrados o dados de baja
 - ✓ Detección de posible robo de clave
- El CONTRATISTA, deberá capacitar en el uso del software de tarificación hasta 02 especialistas de la APN, la capacitación tendrá una duración de dos horas (la capacitación podrá ser remota o presencial), se deberá entregar un manual de uso detallado (el manual podrá ser entregado con el informe final), esta actividad deberá realizarse antes de finalizado la fase 02 de la implementación del servicio a contratar³⁵.

c) Equipos Telefónicos

- ✓ El CONTRATISTA, deberá proporcionar 86 teléfonos IP en calidad de alquiler (Se precisa que, una vez finalizado el plazo contractual, la entidad procederá a la devolución de los equipos entregados), de dos (02) tipos: Las características mínimas de estos equipos son:

Telefonos IP de Tipo A (cantidad: 84 Teléfonos)

- Los teléfonos ofertados deben ser de la misma marca de la central telefónica
- Teléfono de dos (02) líneas basado en el protocolo SIP o protocolo telefonía basado en IP³⁶.

³⁴ Absolución Pliego N° 234 participante AMERICATEL PERU S.A

³⁵ Absolución Pliego N° 83 participante AMERICA MOVIL PERU S.A.C

³⁶ Absolución Pliego N° 239 participante AMERICATEL PERU S.A



PERÚ

Ministerio
de Transportes
y Comunicaciones

Autoridad Portuaria
Nacional

"Decenio de la Igualdad de Oportunidades para Mujeres y Hombres"
"Año de la unidad, la paz y el desarrollo"

- Pantalla LCD a color con resolución de al menos 320 x 240 píxeles o 240 x 320 píxeles.
- Dos puertos Ethernet 10/100/1000 Mbps.
- El color de los equipos deben ser Negro o Gris.
- Debe contar con al menos las siguientes teclas (En caso de que se oferte un teléfono con pantalla touch las teclas podrán ser virtuales) de funciones: transferencia de llamada, conferencia, manos libres/altavoz, modo audífonos, silencio, espera, ajuste de volumen.
- Debe contar con al menos 02 teclas de líneas, 5 teclas de navegación, 04 teclas de función suave (softkey) y 03 teclas programables como mínimo.
- Indicador visual de mensajes de voz (Message Waiting Indicator).
- Debe poder mostrar información histórica de llamadas perdidas, realizadas y recibidas.
- Soporte de los códecs G.711a, G.711µ, G.729 o G.729AB.
- Soporte de los protocolos 802.1p/q (VLAN).
- Soporte del protocolo 802.3af (Power Over Ethernet).
- Debe incluir al menos 10 tonos de timbrado predefinidos.
- A fin de validar las características técnicas mínimas ofertadas de los teléfonos IP de tipo A el postor ganador deberá presentar para el perfeccionamiento del contrato el formato de cumplimiento del Anexo H debidamente sustentado, indicando las referencias técnicas (número de folio) evidenciadas en los documentos emitidos por el fabricante (folletos catálogos, brochures u otros documentos entendiéndose como otros documentos los siguientes: guías prácticas o hojas técnicas o website del fabricante o manuales o carta del fabricante). La carta del fabricante se podrá presentar solo para las características específicas que no se encuentren en la documentación pública o interna del fabricante y no para todas las características que se debe acreditar en el Anexo H. Asimismo, que en caso de presentar carta del fabricante esta deberá tener fecha actualizada a la fecha de la presentación de la documentación para el perfeccionamiento del contrato.

Teléfonos IP de Tipo B (Cantidad: 02 teléfonos)

- Deben ser de la misma marca de la central telefónica.
- Teléfono de seis (06) líneas basado en el protocolo SIP o [protocolo telefonía basado en IP](#)³⁷.
- Pantalla LCD a color con resolución de al menos 800 x 480 píxeles o 480 x 800 píxeles
- Dos puertos Ethernet 10/100/100 Mbps
- El color de los equipos deben ser negro o gris
- Debe contar con al menos las siguientes teclas de funciones: transferencia de llamada, conferencia manos libres / altavoz, modo audífonos, silencio, espera, ajuste de volumen.

³⁷ Según Absolución Pliego N° 240 participante AMERICATEL PERU S.A



PERÚ

Ministerio
de Transportes
y Comunicaciones

Autoridad Portuaria
Nacional

"Decenio de la Igualdad de Oportunidades para Mujeres y Hombres"
"Año de la unidad, la paz y el desarrollo"

- Debe contar con al menos 06 teclas de líneas, 5 teclas de navegación, 04 teclas de función suave (softkey) y 5 teclas programables. En caso el CONTRATISTA, oferte teléfonos con pantalla táctil, las teclas podrán ser virtuales.
 - Indicador visual de mensajes de voz (Message Waiting Indicator).
 - Debe poder mostrar información histórica de llamadas perdidas, realizadas y recibidas.
 - Soporte de los códecs G.711a, G.711μ, G.729 o G.729AB.
 - Soporte de los protocolos 802.1p/q (VLAN).
 - Soporte del protocolo 802.3af (Power Over Ethernet).
 - Debe incluir al menos 10 tonos de timbrado predefinidos.
 - Capacidad para conectar módulos de expansión externos o módulos de expansión integrados con teclas físicas o virtuales (teclas DSS en la pantalla del teléfono). Debe incluir los módulos de expansión para cada uno de los equipos.
 - A fin de validar las características técnicas mínimas ofertadas de los teléfonos IP de tipo B el postor ganador deberá presentar para el perfeccionamiento del contrato el formato de cumplimiento del Anexo H debidamente sustentado, indicando las referencias técnicas (número de folio) evidenciadas en los documentos emitidos por el fabricante (folletos catálogos, brochures u otros documentos entendiéndose como otros documentos los siguientes: guías prácticas o hojas técnicas o website del fabricante o manuales o carta del fabricante). La carta del fabricante se podrá presentar solo para las características específicas que no se encuentren en la documentación pública o interna del fabricante y no para todas las características que se debe acreditar en el Anexo H. Asimismo, que en caso de presentar carta del fabricante esta deberá tener fecha actualizada a la fecha de la presentación de la documentación para el perfeccionamiento del contrato.
- ✓ La APN proveerá los puntos de red y el cableado para la interconexión de los teléfonos IP, todos los teléfonos IP, además de ser PoE, deberán venir con su adaptador de corriente en caso de no existir conexión a un switch de tipo PoE.
- ✓ De ser el caso la APN proporcionará los puntos de red y el cableado necesario hasta la Central Telefónica.
- ✓ Se debe considerar que de los 84 teléfonos IP de tipo A, 05 de ellos funcionarán en el CCCRE de Iquitos y los demás teléfonos del tipo A y los dos Teléfonos del Tipo B, serán distribuidos entre la sede central de la APN, el local anexo de la sede central y el CCCRE del puerto del Callao.

1.6 INFORME MENSUAL DE LOS COMPONENTES QUE FORMAN PARTE DE LOS SERVICIOS.



PERÚ

Ministerio
de Transportes
y Comunicaciones

Autoridad Portuaria
Nacional

"Decenio de la Igualdad de Oportunidades para Mujeres y Hombres"
"Año de la unidad, la paz y el desarrollo"

El CONTRATISTA, deberá hacer entrega de informes mensuales, se deberá presentar un informe por cada componente y por separado. A continuación, se detallan:

Informes del Servicios de Internet

a) Solución de Seguridad perimetral

- ✓ Informe que detalle la salud del clúster de Firewalls, dicho informe deberá incluir como mínimo: Procesamiento del CPU, consumo de la memoria Flash/RAM, estado del almacenamiento, eventos y alarmas del equipo, versión de sistema operativo y recomendaciones.
- ✓ Informe que detalle los ataques recibidos que incluya lo siguiente: Origen, destino, detalle del ataque y recomendaciones. Dicho detalle deberá presentarse no solo con imágenes sino en una matriz Excel y en una tabla en Word.
- ✓ Presentar de manera detallada la evaluación de buenas prácticas que se realiza con la herramienta que permite evaluar el nivel de adopción de buenas prácticas de configuración en el Next Generation Firewall.
- ✓ Detalle de todos los cambios realizados en la configuración del firewall, del mes correspondiente. Estos cambios serán los que haya solicitado la entidad o los que haya realizado el CONTRATISTA. Dicho detalle deberá presentarse en una matriz Excel como una bitácora de cambios.
- ✓ Reporte detallado de los malware de día cero, que se hayan detectado en el mes correspondiente. Dicho detalle deberá presentarse en una matriz Excel y en una tabla en Word.
- ✓ Reporte detallado con un dashboard gráfico que permita ver los usuarios conectados por VPN en el periodo correspondiente. Se debe poder visualizar la fecha de ingreso y salida, así como la red asignada y el usuario, esto deberá presentar en una matriz en Excel y en una tabla en Word.
- ✓ Conclusiones y recomendaciones.

b) Protección avanzada de puesto de trabajo y servidores

- ✓ Reporte detallado de las amenazas y ataques detectados en las 50 estaciones de trabajo o servidores. Se debe detallar las acciones realizadas por EDR en caso de detección de ataques.

c) Solución de administración de ancho de banda

- ✓ Informe que detalle la salud del equipo, deberá incluir como mínimo: Procesamiento del CPU, consumo de la memoria Flash/RAM,



PERÚ

Ministerio
de Transportes
y Comunicaciones

Autoridad Portuaria
Nacional

"Decenio de la Igualdad de Oportunidades para Mujeres y Hombres"
"Año de la unidad, la paz y el desarrollo"

estado del almacenamiento, eventos y alarmas del equipo, versión de sistema operativo y recomendaciones.

- ✓ Reporte que detalle el uso del ancho de banda por usuario o dirección IP, aplicaciones, y las recomendaciones para realizar las restricciones a fin de mejorar el uso del ancho de banda disponible en APN.
- ✓ Detalle gráfico del consumo del ancho de banda, del mes a fin de evaluar los picos de consumo.
- ✓ Detalle de todos los cambios realizados en la configuración del administrador de ancho de banda, del mes correspondiente. Estos cambios serán los que haya solicitado la entidad o los que haya realizado el CONTRATISTA.
- ✓ Conclusiones y recomendaciones

d) Servicio de Ciberdefensa

- ✓ Los informes mensuales deberán presentar las vulnerabilidades encontradas con el siguiente contexto:
 - Descripción
 - Ocurrencia
 - Evidencia
 - Remediación
 - Nuevas vulnerabilidades versus análisis anterior.
- ✓ Propuestas de mejoras para la seguridad perimetral.
- ✓ Conclusiones y recomendaciones.

e) Servicio de Gestion de Vulnerabilidades

- ✓ Reporte de vulnerabilidades que sean explotables, establecer el nivel de madurez del código de exploit (si aplica), documentar de qué forma se explota (malware, acceso remoto, con o sin credenciales), si el exploit está presente en frameworks reconocidos tales como Metasploit, Canvas, Core y otras.
- ✓ Reporte de las vulnerabilidades detectadas en los aplicativos webs y que acciones se deben realizar. Estas acciones deben ser explicadas de forma detallada.
- ✓ Reporte de los activos digitales de la APN y sus vulnerabilidades, se deberá precisar las evidencias y las posibles resoluciones.

f) Servicio de Protección DDoS

- ✓ Reporte de la cantidad de tráfico malicioso bloqueado, en bps, durante una mitigación activa en la nube.
- ✓ Reportar la cantidad de tiempo que una mitigación de nube lleva ejecutándose.
- ✓ Conclusiones y Recomendaciones



PERÚ

Ministerio
de Transportes
y Comunicaciones

Autoridad Portuaria
Nacional

"Decenio de la Igualdad de Oportunidades para Mujeres y Hombres"
"Año de la unidad, la paz y el desarrollo"

g) Servicio de LAN gestionado

- ✓ Se deberá hacer entrega de un reporte que detalle la salud de los equipos de comunicaciones detallados en el literal g) del numeral 1.1. de los términos de referencia (Procesamiento del CPU, consumo de la memoria Flash/RAM, estado del almacenamiento, eventos y alarmas del equipo) que forman parte del servicio.
- ✓ Detalle de todos los cambios realizados en la configuración de los equipos administrados en el presente componente, del mes correspondiente. Estos cambios serán los que haya solicitado la entidad o los que haya realizado el CONTRATISTA.
- ✓ Detalle de la actualización del Firmware de los equipos administrados, en caso se haya realizado o no en el mes correspondiente.

Informes del Servicio de Telefonía Fija

h) Servicio de Central Telefónica

- ✓ Reporte que detalle la salud (Procesamiento del CPU, consumo de la memoria Flash/RAM, estado del almacenamiento, eventos y alarmas del equipo) del Appliance central telefónica que forman parte del servicio.
- ✓ Reportes detallados de llamadas entrantes y salientes por anexo, código y usuario.
- ✓ Detalle de todos los cambios realizados en la configuración de la central telefónica en el presente componente, del mes correspondiente. Estos cambios serán los que haya solicitado la entidad o los que haya realizado el CONTRATISTA

Servicio de SLA

- ✓ Reporte detallado de la atención de incidencias y requerimientos que se hayan dado en el mes. Este reporte debe estar de acuerdo con los tiempos de respuesta que se detallan en el punto 7 de los presentes términos de referencia. El SLA deberá agregar los tiempos de atención descritos en el presente documento ante incidentes o eventos o requerimientos, referente al servicio y a los equipos descritos dentro del servicio en sí. En este detalle se debe incluir los números de tickets, la hora y fecha donde se crea el ticket para la incidencia o requerimiento, el tiempo de respuesta transcurrido, inicio del tiempo de atención, el tiempo de atención transcurrido hasta que se atendió el requerimiento, el tiempo de atención de incidencias transcurrido hasta que se atendió la incidencia y el detalle o descripción de la atención del requerimiento o incidencia.

Nota Importante: Todos los informes deberán presentar en formato digital en PDF, Word y Excel de corresponder. Dichos informes deberán presentarse hasta los 10 días calendarios contados a partir del día siguiente de culminado el periodo correspondiente. Los informes



"Decenio de la Igualdad de Oportunidades para Mujeres y Hombres"
"Año de la unidad, la paz y el desarrollo"

serán entregados a mesa de partes de la Autoridad Portuaria Nacional, ubicada en Av. Santa Rosa N°135, La Perla - Callao o a través de la ventanilla virtual de la entidad en la ruta: <https://ventanillavirtual.apn.gob.pe/login>; de lunes a viernes dentro del horario establecido por la Entidad.

1.7 INSTALACIÓN Y CONFIGURACIÓN DE LOS SERVICIOS

Posterior a la firma del contrato y posterior suscripción del acta de inicio de implementación del servicio, se seguirá las siguientes fases de implementación:

- ✓ Fase 01: Presentación y aprobación del plan de trabajo y revisión de la documentación adjunta.
- ✓ Fase 02: Ejecución.
- ✓ Fase 03: Pruebas.
- ✓ Fase 04: Cierre.

FASE 01: PRESENTACIÓN Y APROBACIÓN DE PLAN DE TRABAJO (hasta 09 días calendario)

- El CONTRATISTA firmará el acta de inicio de implementación del servicio al día siguiente de la recepción de la comunicación formal de la APN, en la cual se definirá al Jefe de Proyecto por parte de la APN, así como otros puntos necesarios para la puesta en marcha del servicio.
- A continuación, a los 07 días calendario, contados a partir del día siguiente de la firma del acta de inicio de implementación del servicio, se presentará el plan de trabajo detallado en el que se incluya el cronograma de los trabajos, listando las actividades a realizar en la APN, propuesta de la implementación, asimismo, se hará entrega de la relación de equipos y materiales que serán instalados. Dicho plan de trabajo será entregado por mesa de partes físico o virtual (por correo electrónico).
- El plan de trabajo del CONTRATISTA, junto con la documentación adjunta deberá ser revisada y aprobada por el jefe de proyecto de la APN, en un plazo no mayor de dos (02) días calendario, contados a partir del día siguiente de la recepción del plan de trabajo. La aprobación de dicho plan de trabajo se comunicará por correo electrónico al CONTRATISTA.
- Los correos electrónicos de ambas partes se definirán y se detallarán en el acta de inicio de implementación del servicio

FASE 02: EJECUCIÓN (hasta 120 días calendario)

- El CONTRATISTA, firmará el acta de inicio de la fase 02, al día siguiente de aprobado el plan de trabajo. Esta fase iniciará desde la firma de dicha acta.
- El CONTRATISTA será responsable por cualquier daño o avería causada sobre la infraestructura, equipamiento, mobiliario u otros, resultantes de la falta de procedimientos o medidas preventivas



PERÚ

Ministerio
de Transportes
y Comunicaciones

Autoridad Portuaria
Nacional

"Decenio de la Igualdad de Oportunidades para Mujeres y Hombres"
"Año de la unidad, la paz y el desarrollo"

tendientes a salvaguardar el patrimonio de la APN, debiendo subsanar de forma inmediata y resoluta todos los daños ocasionados asumiendo la total responsabilidad por los costos que demanden la inmediata reposición o normalización de los daños ocasionados.

- El CONTRATISTA, deberá garantizar en todo momento y circunstancia la seguridad del personal a su cargo durante la realización de los trabajos en las instalaciones de la APN, siendo de su entera y única responsabilidad cualquier hecho que comprometa o ponga en riesgo la vida o salud de estos.
- Los daños ocasionados por el CONTRATISTA durante la ejecución de los trabajos sobre la propiedad de terceros serán cubiertos por este, sin perjuicio de la APN.
- En el caso de daños involuntarios a los acabados, paredes o pisos de la APN, durante el proceso de instalación y puesta en marcha de la presente contratación, el CONTRATISTA debe realizar la reposición y/o acabado, con el mismo tipo de materiales o componentes.
- El CONTRATISTA deberá proporcionar todos los equipos y herramientas de trabajo en óptimas condiciones de uso y seguridad mínimos exigidos (cascos, uniformes, botas, guantes, anteojos, entre otros) para la totalidad del personal asignado a la presente contratación y dar cumplimiento a la Ley N° 29783 Ley de Seguridad y Salud en el Trabajo y su Reglamento.
- La APN, será responsable de proveer el espacio físico, la energía eléctrica estabilizada y el sistema de pozo a tierra.
- EL CONTRATISTA, se compromete a usar durante el desarrollo de sus actividades, materiales, accesorios, consumibles y otros elementos originales, los cuales cumplan con los estándares de probada calidad de fabricación y de marcas de reconocido prestigio, formalmente autorizadas para comercializarse en el país.
- El CONTRATISTA, deberá entregar los equipos en alquiler, con sus respectivas guías de remisión, a fin de que estos sean registrados por la institución.
- El CONTRATISTA será responsable de la configuración de las soluciones solicitadas.
- La instalación se efectuará sin afectar las labores de la Institución.
- La APN, garantizará al CONTRATISTA todos los accesos necesarios, para la realización de trabajos de implementación dentro de las instalaciones, siendo la entidad, la responsable de gestionar las autorizaciones de ingreso, desocupar los espacios, oficinas, pasillos donde vayan a ser ejecutados los trabajos de instalación.
- El CONTRATISTA, deberá capacitar como mínimo a 03 personas de la APN, en la Gestión y monitoreo de cada componente descrito en el numeral 01 de los presentes términos de referencia, cada transferencia de conocimiento deberá ser como mínimo de 03 horas por cada sistema o equipo propuesto. Esta capacitación deberá darse antes de concluir con la fase 02. La capacitación podrá realizarse de manera virtual o presencial.
- El CONTRATISTA, deberá capacitar en el uso del Teléfono de la operadora a al menos 02 especialistas de la APN, dicha capacitación deberá ser de al menos 02 horas, la cual deberá darse antes de la activación del servicio.



PERÚ

Ministerio
de Transportes
y Comunicaciones

Autoridad Portuaria
Nacional

"Decenio de la Igualdad de Oportunidades para Mujeres y Hombres"
"Año de la unidad, la paz y el desarrollo"

- El CONTRATISTA deberá instalar, configurar y poner en producción todo el equipamiento necesario para cada uno de los servicios que forman parte de los términos de referencia al 100%.
 - ✓ Servicio de acceso a internet dedicado.
 - ✓ Servicio de Seguridad Perimetral.
 - ✓ Servicio de enlace de datos con el CCCRE.
 - ✓ Servicio de telefonía fija digital.
 - ✓ Servicio de central telefónica - (telefonía interna).
- Una vez concluida esta fase se deberá firmar un acta de cierre de la Fase 02: Ejecución.

FASE 03: PRUEBAS (hasta 05 días calendario)

- La fase de prueba empezará a partir de la firma del acta de inicio de la Fase 03: Pruebas, la cual se firmará al día siguiente de la firma del acta de cierre de la fase 02: Ejecución.
- Las pruebas de conectividad y verificación de cada enlace y del servicio de telefonía fija se realizarán en presencia del Administrador de Red del Centro de Cómputo de la APN.
- La omisión de algún producto que al momento de las pruebas resulte necesario para la provisión de los servicios, o para el cumplimiento de las especificaciones funcionales o técnicas ofrecidas, obligará al CONTRATISTA a proveerlo sin cargo alguno.
- Cualquier defecto notificado por la APN al CONTRATISTA durante la realización de las pruebas de aceptación, será rectificado por este sin cargo alguno, teniendo como plazo máximo 02 (dos) días calendario a partir de su notificación.
- El CONTRATISTA debe contar con un protocolo de pruebas el cual deberá ser firmado por el especialista de la OTI de la APN y el técnico encargado de realizar dicho protocolo de pruebas.
- Se precisa que los defectos notificados por la APN al CONTRATISTA durante la realización de las pruebas de aceptación serán rectificados por el CONTRATISTA sin cargo alguno, siempre y cuando dichos defectos obedezcan a causa imputables al CONTRATISTA.
- Una vez concluida la fase de pruebas, se deberá firmar un acta de finalización de la Fase 03: Pruebas.

FASE 04: FIRMA DEL ACTA DE CIERRE Y ACTIVACIÓN DEL SERVICIO (02 día calendario)

- El acta de cierre se firmará al día siguiente de la firma del acta de finalización de la Fase 03: Pruebas.
- Al finalizar con los trabajos de instalación, configuración e implementación el CONTRATISTA entregará el informe final del proyecto, esto será en un plazo máximo de hasta 10 días calendarios contados a partir del día siguiente de haberse firmado el acta de cierre, detallando el desarrollo de las actividades desarrolladas en cada fase y detallando el desarrollo de los siguientes componentes³⁸:

³⁸ Según Absolución Pliego N° 163 participante AMERICA MOVIL PERU S.A.C



PERÚ

Ministerio
de Transportes
y Comunicaciones

Autoridad Portuaria
Nacional

"Decenio de la Igualdad de Oportunidades para Mujeres y Hombres"
"Año de la unidad, la paz y el desarrollo"

- ✓ Internet Dedicado
 - ✓ Enlace de datos
 - ✓ Seguridad Perimetral
 - ✓ Telefonía Digital.
 - ✓ Central Telefónica.
 - ✓ Red Gestionada.
 - ✓ Inventario de Equipamiento que forma parte de los servicios.
 - ✓ Mapa de red Físico/Lógico.
 - ✓ Accesos a la gestión de los equipos (usuario y clave de administrador)
 - ✓ Detalle de las configuraciones finales de cada componente de seguridad, switch core y switch de acceso.
 - ✓ Detalle gráfico de la configuración de las VLANs configurados en cada switch core y de acceso a fin de saber que redes están configuradas en cada puerto. Asimismo, se deberá entregar una matriz con el detalle en mención.
 - ✓ Se debe detallar las listas de las configuraciones en firewall de manera que sea entendible, además del código o comandos que se hayan podido ejecutar en los equipos.
 - ✓ Listado final de las configuraciones de las IP públicas, donde se detalle los puertos configurados.
 - ✓ Detalle de la última versión instalada del firmware de cada equipo instalado.
 - ✓ Se deberá adjuntar la copia de las guías de remisión de los equipos entregados y las actas y correos electrónicos que evidencien el cumplimiento de lo requerido en los términos de referencia.
- El informe Final debe ser entregado en digital a colores (en formato Microsoft Word 2019 o superior, el diseño de red lógico y físico en formato Microsoft Visio o AutoCAD). Dicho informe final será entregado en mesa de partes de manera encriptada, esto teniendo en cuenta que la información de dicho informe contiene información de contraseñas, direcciones IP e información de la configuración de la seguridad perimetral.
 - El Informe Final, debe contener un índice detallado, de tal forma que se pueda revisar con mayor facilidad el Checklist.
 - El CONTRATISTA, deberá entregar en el informe final manuales detallados de administración en formato digital de la central telefónica, los teléfonos IP, los Switch Core y firewall. Todos los manuales o guía rápidas deberán ser entregadas en su idioma original (inglés o español).
 - El acta de activación del servicio mensual se firmará el mismo día que se firme el acta de cierre del proyecto de implementación.

1.8 PERFIL DEL PERSONAL Y ACTIVIDADES A DESARROLLAR PARA LA EJECUCION DEL SERVICIO

El personal clave, que participará en el desarrollo de la implementación del servicio, realizará las siguientes actividades:

Un (01) jefe del Proyecto:

(suprimido³⁹)

³⁹ Absolución Pliego N° 32 participante VIETTEL PERU S.A.C, N°142 participante AMERICA MOVIL PERU S.A.C, N° 199,200 participante AMERICATEL PERU S.A

Actividades:

El jefe de proyecto estará a cargo de la presentación del plan de trabajo, así como la supervisión del cumplimiento de cada etapa de la instalación y configuración de los servicios contratados. Asimismo, estará a cargo de las coordinaciones y presentación de los avances del proyecto, así como gestionar cualquier inconveniente o incidencia originada por parte del CONTRATISTA, durante la implementación del servicio. Una vez culminada la fase de pruebas el jefe de proyecto del CONTRATISTA firmara el acta de activación del servicio, junto con el jefe del proyecto por parte de APN.

Dos (02) Técnicos de Networking:

Los especialistas deberán contar con el siguiente certificado:

- Certificado de Routing-Switching o sistema operativo emitido por el fabricante de los equipos de comunicaciones propuestos (Routers y Switch WAN).

Actividades:

Los técnicos para la solución de networking, estarán a cargo de la fase de ejecución de la instalación y configuración, cumpliendo con los tiempos establecidos en el plan de trabajo presentado por el jefe del proyecto por parte de la APN. Asimismo, se harán cargo de la atención de requerimientos e incidencias de la solución de los equipos de comunicaciones durante el periodo de contrato. Dichas atenciones podrán ser de manera remota u onsite, los tiempos de respuesta se detallan en el punto 7 de los presentes términos de referencia. Asimismo, el CONTRATISTA, podrá contar con un equipo de técnicos o especialistas en networking, quienes atenderán las incidencias y requerimientos en una primera instancia, y los dos especialistas de networking solicitados deberán atender en una segunda instancia la incidencia o requerimiento⁴⁰.

Dos (02) Especialistas de Seguridad:

Los especialistas deberán contar con los siguientes certificados:

El primer especialista deberá contar con los siguientes certificados:

- ✓ Certificado emitido por el fabricante de la solución de seguridad perimetral propuesto (Firewalls).
- ✓ Certificado emitido por el fabricante de la solución de administración de ancho de banda propuesta

⁴⁰ Absolución Pliego N° 84 participante AMERICA MOVIL PERU S.A.C

El Segundo Especialista de seguridad deberá contar con los siguientes certificados:

- ✓ Certificado emitido por el fabricante del servicio de ciberdefensa
- ✓ Certificado emitido por el fabricante del servicio de gestión de vulnerabilidades

Actividades:

Los técnicos para la solución de seguridad, estarán a cargo de la fase de ejecución de la instalación y configuración, cumpliendo con los tiempos establecidos en el plan de trabajo presentado por el jefe del proyecto por parte de la APN. Asimismo, se harán cargo de la atención de requerimientos e incidencias de la solución de los equipos de comunicaciones durante el periodo de contrato. Dichas atenciones podrán ser de manera remota u onsite, los tiempos de respuesta se detallan en el punto 7 de los presentes términos de referencia. Asimismo, el CONTRATISTA, podrá contar con un equipo de técnicos o especialistas de seguridad, quienes atenderán las incidencias y requerimientos en una primera instancia, y los dos especialistas de seguridad solicitados deberán atender en una segunda instancia la incidencia o requerimiento.⁴¹

Dos (02) Especialistas de Telefonía:

Los especialistas deberán contar con el siguiente certificado:

- Certificado emitido por el fabricante en la solución de telefonía fija propuesta.

Actividades:

Los especialistas para la solución de telefonía fija, estarán a cargo de la fase de ejecución de la instalación y configuración, cumpliendo con los tiempos establecidos en el plan de trabajo presentado por el jefe del proyecto por parte de la APN. Asimismo, se harán cargo de la atención de requerimientos e incidencias de la solución de los equipos de comunicaciones durante el periodo de contrato. Dichas atenciones podrán ser de manera remota u onsite, los tiempos de respuesta se detallan en el punto 7 de los presentes términos de referencia. Asimismo, el CONTRATISTA, podrá contar con un equipo de técnicos o especialistas de telefonía, quienes atenderán las incidencias y requerimientos en una primera instancia, y los dos especialistas de telefonía solicitados deberán atender en una segunda instancia la incidencia o requerimiento⁴².

⁴¹ Absolución Pliego N° 85 participante AMERICA MOVIL PERU S.A.C

⁴² Absolución Pliego N° 86 participante AMERICA MOVIL PERU S.A.C

Nota Importante: Para la acreditación de los certificados o constancias que se solicitan en este punto, se presentaran junto con el plan de trabajo que se presenta en la Fase 01 de la implementación del presente proyecto.

1.9 CONSIDERACIONES GENERALES

- a) El CONTRATISTA instalará y mantendrá actualizadas las versiones de software o firmware en los respectivos equipos de comunicaciones y seguridad asignados para el servicio, así como los equipos gestionados. Dicha actividad se realizará previa coordinación con la Oficina de Tecnologías de la Información de la APN.
- b) El CONTRATISTA permitirá el nuevo registro DNS a nivel de internet del servicio de correo electrónico de la institución, en caso lo solicite la entidad, sin costo adicional para la institución.
- c) En caso de ser necesario el realizar obras civiles dentro o fuera de la APN para la instalación del servicio requerido, estos deberán ser realizados por el CONTRATISTA quien asumirá los costos que puedan involucrar, estas obras deberán realizarse en la fase 02 de la implementación del proyecto.
- d) El CONTRATISTA deberá considerar el equipamiento necesario hasta el ingreso al puerto RJ45 del Switch de la Sede Central de APN y Local de CCCRE, transmitiendo a una velocidad mínima en la interface de comunicación de 10/100/1000 Base-T. La APN será responsable de garantizar espacio para el rack o gabinete, energía estabilizada, tomacorrientes.
- e) La APN brindara las facilidades de acceso a nuestros locales indicando la ruta de acceso para la fibra óptica, asimismo, se brindará punto de corriente estabilizada y conexión a UPS en los gabinetes del centro de cómputo para los equipos en calidad de alquiler que el CONTRATISTA haya ofertado.
- f) El CONTRATISTA, deberá considerar realizar administración compartida de toda la solución con la finalidad de minimizar los tiempos de respuesta con relación al soporte técnico. Esta administración se determinará en el acta de inicio de implementación. Se precisa que al solicitar la administración compartida no se aplicará penalidad al proveedor hasta que se demuestre se demuestre que la falla o mala configuración o demora es imputable al CONTRATISTA.
- g) El CONTRATISTA, deberá asegurar y garantizar que el ancho de banda y la operación de los equipos routers, sea la óptima y correcta a fin de que los servicios de videoconferencia con que cuenta la APN, puedan transmitirse de manera correcta, durante el tiempo de contrato.
- h) El CONTRATISTA es responsable de la operatividad de los enlaces de comunicación y del buen funcionamiento, licencias, actualización de hardware, firmware y software de sistema operativo de sus equipos de comunicación, siempre y cuando sea necesario para asegurar la calidad del servicio ofrecido y mantener el flujo de las aplicaciones de red del APN.



PERÚ

Ministerio
de Transportes
y Comunicaciones

Autoridad Portuaria
Nacional

"Decenio de la Igualdad de Oportunidades para Mujeres y Hombres"
"Año de la unidad, la paz y el desarrollo"

- i) El CONTRATISTA, deberá considerar el licenciamiento necesario para el correcto funcionamiento de todos los componentes que han detallado en punto 1 de los presentes términos de referencia y satisfacer los requerimientos mencionados del APN.
- j) El CONTRATISTA deberá garantizar la total privacidad de todos los canales de comunicaciones brindados al APN a través de un acuerdo de confidencialidad el cual se firmará al momento de la firma del contrato.
- k) EL CONTRATISTA deberá usar tubo corrugado, canaletas o bandejas metálicas para cubrir los excedentes de cable de fibra óptica de la toma de pared/techo a donde lo necesite, para conservar la decoración de las instalaciones de APN. El cableado de la red de datos, que se use para dicha interconexión deberá estar debidamente etiquetado. El CONTRATISTA, deberá usar patch cord categoría 6 para interconectar sus equipos.
- l) El CONTRATISTA de considerarlo necesario, podrá realizar una visita técnica a la sede central y CCCRE de la APN durante el desarrollo del procedimiento de selección, de tal manera de que elabore su plan de trabajo indicado en la Fase I del Numeral 1.6 de los presentes términos de referencia acorde a los requerimientos e infraestructura de los edificios. Las visitas serán guiadas en las fechas y horas coordinadas con el responsable de la OTI.
- m) El CONTRATISTA será responsable de la configuración de las soluciones solicitadas así mismo deberá asegurar que los equipos a proveer sean compatibles entre sí.
- n) De acuerdo con la ley N° 29956 (Ley que establece el derecho de portabilidad numérica en los servicios de telefonía fija), el CONTRATISTA, deberá considerar mantener la misma numeración de anexos con que cuenta actualmente la APN.
- o) Se precisa que, para el caso de la portabilidad numérica, la entidad entregará al CONTRATISTA, los siguientes documentos, en la fecha que se acuerde en el acta de inicio de implementación del servicio en mención:
 - ✓ Relación de líneas a portar con su respectivo minutos y servicios,
 - ✓ Constancia de no adeudo emitida por su operador actual,
 - ✓ Último recibo de su operador actual cancelado a la fecha,
 - ✓ Voucher de pago de este último recibo,
 - ✓ Formato de Portabilidad firmado.
- p) El CONTRATISTA, podrá realizar las actividades de atención de incidencia y requerimientos no solo a través del personal clave sino con apoyo de su staff de técnicos los cuales de manera opcional podrán cumplir con las capacitaciones descritas en el punto 1.7 de los presentes términos de referencia.
- q) En caso el CONTRATISTA, requiera realizar algún cambio de personal clave durante la ejecución del servicio contratado, este podrá hacerlo con 10 días calendario de anticipación y que cumpla con el perfil solicitado o sea superior. Para ello el CONTRATISTA deberá comunicar mediante carta a través de mesa de partes con el periodo antes mencionado.
- r) Será responsabilidad del CONTRATISTA la configuración de la Central Telefónica del APN y del acceso RDSI-PRI o SIP TRUNK o



Ministerio
de Transportes
y Comunicaciones

Autoridad Portuaria
Nacional

"Decenio de la Igualdad de Oportunidades para Mujeres y Hombres"
"Año de la unidad, la paz y el desarrollo"

Troncal SIP según sea el caso para las cuales los dos (02) enlaces trabajarán de tal forma que en cuanto uno se encuentre inoperativo el otro funcionará manteniendo el mismo número telefónico. Los enlaces de telefonía serán activo- activo considerando que a la trigésima llamada se conmutará al enlace de contingencia.

- s) De exceder los minutos contemplados en la bolsa, se deberá considerar la misma tarifa por minutos ofertada en la bolsa por cada tipo de destino, es decir deberá contemplar una tarifa única para cada tipo de llamadas:
1. Tarifa única para llamadas fijas locales.
 2. Tarifa única para llamadas LDN.
 3. Tarifa única para llamadas LDI.
 4. Tarifa única para llamadas Móviles.
- t) El CONTRATISTA deberá contar con un esquema de seguridad en las comunicaciones en su red que garantice el cumplimiento de las exigencias regulatorias en salvaguarda del secreto de las telecomunicaciones, en cualquiera de sus modalidades según los mecanismos propios de las tecnologías ofertadas.
- u) Las coordinaciones para la instalación de la línea dedicada serán realizadas por la OTI de la APN. Se dará por aceptada la entrega del servicio cuando resulte satisfactoria la puesta en producción de la línea de acceso a Internet, la Telefonía Fija, la entrega del equipamiento y la documentación respectiva.
- v) La APN devolverá los equipos que le hayan sido entregados y/o instalados bajo cualquier modalidad distinta a la venta (incluyendo equipos, routers, switches y/o cualquier otro equipo de propiedad del Contratista) en su totalidad al CONTRATISTA, una vez que finalice los 36 meses de contrato, esto se realizará en coordinación con la OTI de la APN, para el retiro de los equipos antes mencionados, el CONTRATISTA elaborará una guía de salida de dichos equipos y se firmará un acta de devolución. Estos equipos se entregarán sin más desgaste que su uso normal y diligente, aceptando que, en caso de pérdida, deterioro o robo la entidad asumirá el costo de estos.
- w) El CONTRATISTA, entregará en el último informe mensual un CD o USB, que contengan las configuraciones de todos los equipos de comunicaciones y de seguridad, tanto de los que son propiedad de la APN y de los de propiedad del CONTRATISTA.
- x) El CONTRATISTA, deberá conectar los puertos de telefonía analógica con la central telefónica propuesta, esto deberá realizarlo conectando patch cord los cuales serán proporcionados por el CONTRATISTA, estos patch cord serán de categoría 6 y el tamaño lo definirá el CONTRATISTA, considerando que será el responsable de incluir los ordenadores o patch panel necesarios para realizar dicha actividad. Asimismo, el CONTRATISTA, deberá etiquetar cada punto telefónico a fin de contar con una fácil identificación.
- y) En el caso que durante el tiempo de contrato alguno de los equipos en alquiler pasa a un estado de discontinuado, el CONTRATISTA procederá a realizar el cambio respectivo por la versión que reemplaza al equipo discontinuado, siempre y cuando cumpla con los requisitos técnicos mínimos solicitados en los presentes términos de referencia.



Ministerio
de Transportes
y Comunicaciones

Autoridad Portuaria
Nacional

"Decenio de la Igualdad de Oportunidades para Mujeres y Hombres"
"Año de la unidad, la paz y el desarrollo"

2) REQUISITOS DE CALIFICACIÓN DE LA EMPRESA QUE PRESTARÁ EL SERVICIO

A. CAPACIDAD TÉCNICA Y PROFESIONAL

A.1. EXPERIENCIA DEL PERSONAL CLAVE

Experiencia:

a) Un (01) jefe de Proyecto

Experiencia mínima de tres (03) años como Jefe de Proyectos o encargado de proyectos de telecomunicaciones o coordinador de proyectos; gestionando y/o supervisando y/o implementando proyectos de telecomunicaciones tales como Internet y/o transmisión de datos y/o Comunicaciones, conexión, redes y/o telefonía y/o Gestión y/o Supervisión de implementación de Proyectos de Servicios de Transmisión de Datos, Internet, Comunicaciones Unificadas, telefonía e infraestructura de Data Center.

b) Dos (02) Especialistas de Networking:

Estos técnicos deberán contar con experiencia mínima de 02 años en las implementaciones switching o gestión de redes de datos o Servicios de Internet o enlace de datos.

c) Dos (02) Especialistas de Seguridad:

Dicho personal deberá tener 02 años de experiencia mínima, en la implementación o configuración de soluciones de seguridad perimetral.

d) Dos (02) Especialista de Telefonía:

Dicho personal deberá tener 02 años⁴³ de experiencia mínima, en la implementación o configuración de Centrales Telefónica

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. Se precisa que la experiencia se contabilizará desde la fecha de emisión del título de profesional técnico o del título de bachiller profesional.

A.2 CALIFICACIONES DEL PERSONAL CLAVE

a) Un (01) Jefe de Proyecto

⁴³ Según Absolución Pliego N° 243 participante AMERICATEL PERU S.A

Formación Académica

Requisitos:

Profesional titulado en:

- Ingeniería de Telecomunicaciones o
- Ingeniería de Sistemas o
- Ingeniería Electrónica o
- Ingeniería Informática o
- Ingeniería de Computación e Informática o
- Ingeniería de Redes y Comunicación o
- Ingeniería de Software o
- Ingeniería de Redes de Computadoras y Comunicación de Datos o
- Ingeniería de Redes y Comunicación de Datos o
- Ingeniería de Redes y Comunicaciones o
- Ingeniería de Redes y Seguridad Informática o
- Ingeniería de Seguridad de la Información o
- Ingeniería de Sistemas e Informática⁴⁴

Acreditación:

El TÍTULO 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/>

b) Dos (02) Especialistas de Networking:

Formación Académica

Requisitos:

Ingeniero Profesional o Profesional Técnico Titulado o Bachiller en alguna de las siguientes carreras:

- Sistemas.
- Redes de datos
- Sistemas.
- Redes de datos
- Informática.
- Telecomunicaciones.
- Sistemas de Información.
- Computación y de Sistemas.
- Informática y de Sistemas.
- Electrónica.
- Redes y Comunicaciones de Datos
- Seguridad y Auditoría Informática
- Computación e Informática o
- Ingeniería de Redes y Comunicación o
- Ingeniería de Software o
- Electrónica y Telecomunicaciones o
- Redes de Computadoras y Comunicación de Datos o
- Redes y Comunicación de Datos o
- Redes y Comunicaciones o
- Redes y Seguridad Informática o
- Seguridad de la Información o
- Sistemas de Telecomunicaciones o
- Sistemas e Informática⁴⁵

Acreditación:

El GRADO O TÍTULO 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: <http://www.titulosinstitutos.pe/>, según corresponda.

c) Dos (02) especialistas de seguridad:

Formación Académica

⁴⁴ Absolución Pliego N° 62 participante VIETTEL PERU S.A.C

⁴⁵ Absolución Pliego N° 63, 65 participante VIETTEL PERU S.A.C N° 268, 270 participante WIN EMPRESAS S.A.C

Requisitos:

Ingeniero Profesional Técnico profesional Titulado o Bachiller en alguna de las siguientes carreras:

- Sistemas.
- Redes de datos
- Informática.
- Telecomunicaciones.
- Sistemas de Información.
- Computación y de Sistemas.
- Informática y de Sistemas.
- Electrónica
- Redes y Comunicaciones
- Seguridad y Auditoría Informática
- Computación e Informática o
- Ingeniería de Redes y Comunicación o
- Ingeniería de Software o
- Electrónica y Telecomunicaciones o
- Redes de Computadoras y Comunicación de Datos o
- Redes y Comunicación de Datos o
- Redes y Comunicaciones o
- Redes y Seguridad Informática o
- Seguridad de la Información o
- Sistemas de Telecomunicaciones o
- Sistemas e Informática⁴⁶

Acreditación:

El GRADO O TÍTULO 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: <http://www.titulosinstitutos.pe/>, según corresponda.

d) **Dos (02) Especialista de Telefonía:**

Formación Académica

Requisitos:

Profesional Técnico Titulado o Bachiller titulado en alguna de las siguientes carreras:

- Sistemas.
- Redes de datos
- Informática.
- Telecomunicaciones.
- Sistemas de Información.
- Computación y de Sistemas.
- Informática y de Sistemas.
- Electrónica
- Electrónica y Telecomunicaciones

Acreditación:

El GRADO O TÍTULO 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: <http://www.titulosinstitutos.pe/>, según corresponda.

⁴⁶ Absolución Pliego N° 62, 66 participante VIETTEL PERU S.A.C., pliego N° 144 participante AMERICA MOVIL PERU S.A.C N° 269, 271 participante WIN MPRESAS S.A.C

CAPACITACIÓN:

Jefe de Proyecto:

Requisito:

El jefe de proyecto deberá contar con la siguiente constancia o diplomado:

- Constancia de PMP o o Diploma de Dirección de Proyectos o Diploma en Gerencia de Proyectos o Diplomado en Gerencia de Proyectos y Calidad.

Acreditación:

Se precisa que en caso de las constancias o diplomados se deberá presentar indicando al menos 24 horas lectivas por cada constancia o diplomado presentada.⁴⁷.

A.3. HABILITACION

Requisito:

El postor debe contar con Autorización del Ministerio de Transportes y Comunicaciones para brindar el servicio de conmutación de transmisión de datos y/o el servicio de valor añadido de conmutación de datos por paquete.

Acreditación:

Copia del documento emitido por el Ministerio de Transportes y Comunicaciones que acredite su autorización para brindar el servicio de conmutación de transmisión de datos y/o el servicio de valor añadido de conmutación de datos por paquete y/o certificado de registro de empresas prestadoras de servicios de valor añadido.

	EXPERIENCIA DEL POSTOR EN LA ESPECIALIDAD
	<u>Requisitos:</u>
	<p>El POSTOR debe acreditar un monto facturado acumulado equivalente a ocho millones y 00/100 – S/ 8'000,000.00, por la contratación de servicios iguales o similares al objeto de la convocatoria, durante los 08 años anteriores a la fechade la presentación de las ofertas que se computarán desde la fecha de la conformidad o emisión del comprobante de pago, según corresponda. Seconsideran servicios similares a los siguientes:</p> <ul style="list-style-type: none">• Servicios de telecomunicaciones.• Servicios de transmisión de voz, datos y video.• Servicios de transmisión de voz.• Servicios de transmisión de datos.• Servicios de transmisión de video.• Servicios de acceso a internet.• Servicio de enlace de datos.• Servicios de arrendamiento de circuitos o tránsito de Internet• Servicios de Transmisión de datos en general• Servicio de Telefonía Fija• Servicio de Seguridad Gestionada• Servicio de Lineas Analogicas• Servicios de Plan de Telefonía y Datos• Servicios de Internet Móvil• Servicios de Internet• Servicios de Internet Dedicado• Servicios de Internet y Enlace de Datos• Servicio de conexion, interconexion y comunicacion mediante fibra optica.• Servicio de comunicacion mediante fibra optica.• Servicio de conexion, interconexion e internet en general.⁴⁸ <p><u>Acreditación:</u></p>

⁴⁷ Absolución Pliego N° 32 participante VIETTEL PERU S.A.C, N° 199,200 participante AMERICATEL PERU S.A

⁴⁸ Absolución Pliego N° 8 participante WIN EMPRESAS S.A.C ,N° 210, 215 participante AMERICATEL PERU S.A.



Ministerio
de Transportes
y Comunicaciones

Autoridad Portuaria
Nacional

"Decenio de la Igualdad de Oportunidades para Mujeres y Hombres"
"Año de la unidad, la paz y el desarrollo"

La experiencia del postor en la especialidad se acreditará con copia simple de (i) contratos u órdenes de servicios, y su respectiva conformidad o constancia de prestación; o (ii) comprobantes de pago cuya cancelación se acredite documental y fehacientemente, con voucher de depósito, nota de abono, reporte de estado de cuenta, cualquier otro documento emitido por Entidad del sistema financiero que acredite el abono o mediante cancelación en el mismo comprobante de pago¹, correspondientes a un máximo de veinte (20) contrataciones.

En caso los postores presenten varios comprobantes de pago para acreditar una sola contratación, se debe acreditar que corresponden a dicha contratación; de lo contrario, se asumirá que los comprobantes acreditan contrataciones independientes, en cuyo caso solo se considerará, para la evaluación, las veinte (20) primeras contrataciones indicadas en el **Anexo N° 8** referido a la Experiencia del Postor en la Especialidad.

En el caso de servicios de ejecución periódica o continuada, solo se considera como experiencia la parte del contrato que haya sido ejecutada durante los ocho (8) años anteriores a la fecha de presentación de ofertas, debiendo adjuntarse copia de las conformidades correspondientes a tal parte o los respectivos comprobantes de pago cancelados.

En los casos que se acredite experiencia adquirida en consorcio, debe presentarse la promesa de consorcio o el contrato de consorcio del cual se desprenda fehacientemente el porcentaje de las obligaciones que se asumió en el contrato presentado; de lo contrario, no se computará la experiencia proveniente de dicho contrato.

Asimismo, cuando se presenten contratos derivados de procesos de selección convocados antes del 20.09.2012, la calificación se ceñirá al método descrito en la Directiva "Participación de Proveedores en Consorcio en las Contrataciones del Estado", debiendo presumirse que el porcentaje de las obligaciones equivale al porcentaje de participación de la promesa de consorcio o del contrato de consorcio. En caso que en dichos documentos no se consigne el porcentaje de participación se presumirá que las obligaciones se ejecutaron en partes iguales.

Si el titular de la experiencia no es el postor, consignar si dicha experiencia corresponde a la matriz en caso que el postor sea sucursal, o fue transmitida por reorganización societaria, debiendo acompañar la documentación sustentatoria correspondiente.

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 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".



PERÚ

Ministerio
de Transportes
y Comunicaciones

Autoridad Portuaria
Nacional

"Decenio de la Igualdad de Oportunidades para Mujeres y Hombres"
"Año de la unidad, la paz y el desarrollo"

Si el postor acredita experiencia de una persona absorbida como consecuencia de una reorganización societaria, debe presentar adicionalmente el Anexo N° 9.

Cuando en los contratos, órdenes de servicios o comprobantes de pago el monto facturado se encuentre expresado en moneda extranjera, debe indicarse el tipo de cambio venta publicado por la Superintendencia de Banca, Seguros y AFP correspondiente a la fecha de suscripción del contrato, de emisión de la orden de servicios o de cancelación del comprobante de pago, según corresponda.

Sin perjuicio de lo anterior, los postores deben llenar y presentar el Anexo N° 8 referido a la Experiencia del Postor en la Especialidad.

Importante

- *Al calificar la experiencia del postor, se debe valorar de manera integral los documentos presentados por el postor para acreditar dicha experiencia. En tal sentido, aun cuando en los documentos presentados la denominación del objeto contractual no coincida literalmente con el previsto en las bases, se deberá validar la experiencia si las actividades que ejecutó el postor corresponden a la experiencia requerida.*
- *En el caso de consorcios, solo se considera la experiencia de aquellos integrantes que se hayan comprometido, según la promesa de consorcio, a ejecutar el objeto materia de la convocatoria, conforme a la Directiva "Participación de Proveedores en Consorcio en las Contrataciones del Estado".*

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.*

3) SISTEMA DE CONTRATACIÓN (Precios unitarios, suma alzada, esquema mixto, tarifa, porcentaje u honorario fijo con comisión de éxito)

Suma Alzada

4) LUGAR DE LA PRESTACIÓN DEL SERVICIO

Las labores serán realizadas en las instalaciones de la sede central de la APN
– Av. Santa Rosa N° 135 La Perla – Callao, el CCCRE del Puerto del Callao



Autoridad Portuaria
Nacional

"Decenio de la Igualdad de Oportunidades para Mujeres y Hombres"
"Año de la unidad, la paz y el desarrollo"

– Av. Manco Cápac S/N Callao, Local Anexo de la APN – Av. Santa Rosa N° 135 La Perla – Callao y CCCRE del Puerto de Iquitos en Av. La Marina S/N – Interior ENAPU.

5) PERIODO DE EJECUCIÓN

La implementación, instalación y puesta en producción de todos los servicios y sus componentes como parte del contrato no deberá exceder de los ciento treinta y seis (136) días calendario contados a partir del día siguiente de firmado el acta de inicio de implementación del servicio, dicha acta se firmará al día siguiente de la confirmación de recepción de la comunicación formal de la APN, para el inicio del servicio.

La ejecución de todos los servicios contratados será por un plazo de treinta y seis (36) meses contados a partir del día siguiente de la firma del acta de activación del servicio mensual.

6) FORMA Y CONDICIONES DE PAGO

- ✓ Los pagos se realizarán mensualmente al finalizar cada mes de servicio, ascendiendo el monto mensual a: 1/36 del monto del contrato, debiéndose contar con:
 - Conformidad emitida por OTI, después de haber recepcionado cada informe mensual presentado por el contratista. Dichos informes deberán presentarse hasta los 10 días calendarios contados a partir del día siguiente de culminado el periodo correspondiente. Los informes serán entregados a mesa de partes de la Autoridad Portuaria Nacional, ubicada en Av. Santa Rosa N°135, La Perla - Callao o a través de la ventanilla virtual de la entidad en la ruta: <https://ventanillavirtual.apn.gob.pe/login>; de lunes a viernes dentro del horario establecido por la Entidad.
 - Comprobante de pago (factura o recibo de servicios) mensual presentado por el contratista.
- ✓ Los comprobantes de pago podrán ser enviadas al correo emisorelectronico1@apn.gob.pe.
- ✓ El pago del servicio es a todo costo e incluye todos los impuestos de ley.
- ✓ El servicio de implementación no generara ningún pago.
- ✓ El pago se realizará de acuerdo con la estructura de costos presentada a la firma del contrato. Asimismo, el CONTRATISTA, deberá detallar en su facturación los componentes del servicio.

7) GARANTÍA Y SERVICIOS POST ACTIVACIÓN

- a) El servicio de soporte debe proveer una disponibilidad de 7x24x365 o 7x24x366 año bisiesto, para todos los componentes y servicios contenidos en el presente documento.
- b) El CONTRATISTA debe contar con un centro de atención del servicio que se encargue de brindar gestión, administración y seguridad de los servicios que contrata la APN. El servicio de soporte será permanente bajo



PERÚ

Ministerio
de Transportes
y Comunicaciones

Autoridad Portuaria
Nacional

"Decenio de la Igualdad de Oportunidades para Mujeres y Hombres"
"Año de la unidad, la paz y el desarrollo"

la modalidad 7x24x365 o 7x24x366 y contará con un sistema de gestión adecuado para reportar fallas y atenciones. El centro de atención deberá contar personal para atender cualquier consulta o problema a surgir con los servicios de Internet, enlace de datos y servicio de telefonía fija incluido cada componente de los servicios.

- c) El CONTRATISTA deberá, garantizar que la APN se contacte de forma directa con los especialistas de las soluciones requeridas en los presentes términos de referencia, de tal forma que los tiempos de atención sean óptimos.
- d) Debido a la importancia y la criticidad, el Nivel del Servicio (SLA) debe ser mínimo de 99.50% mensual para el servicio de enlace de datos y de 99.90% mensual para la conexión a Internet Dedicado y Telefonía Fija Digital.
- e) El "SLA" para el enlace será medido por el CONTRATISTA del Servicio, lo cual será validado por la OTI a través del registro de incidentes y requerimientos reportados de forma mensual el proveedor entregará a la APN un Informe mensual del SLA brindado.
- f) El CONTRATISTA, debe garantizar que su Centro de Atención supervise la disponibilidad del acceso en la red de datos durante todo el año.
- g) El CONTRATISTA deberá reparar o reemplazar sin costo para la APN los equipos rentados o componentes que sean necesarios para asegurar la prestación del servicio en caso de falla éstos. **Se precisa que la reparación o reemplazo será sin costo para la APN, cuando la falla o avería no sea responsabilidad de la Entidad.**
- h) El CONTRATISTA deberá entregar en su informe final referente a la instalación y configuración del servicio, el plan de mantenimiento preventivo de los equipos rentados y de los equipos gestionados, el mismo que se realizará dos veces al año durante el periodo de contrato de 36 meses y consistirá en la limpieza del hardware, componentes internos y actualización de las versiones de software y firmware de los equipos de propiedad de APN y de propiedad del CONTRATISTA. Una vez finalizado cada mantenimiento, el CONTRATISTA deberá emitir un informe detallado de dicho mantenimiento, documento que será presentado conjuntamente con los reportes mensuales del mes que se ejecute el mantenimiento.
- i) El CONTRATISTA deberá entregar a la APN, una nómina del personal técnico autorizado a realizar labores de mantenimiento en las sedes bajo contrato. Dicha nómina deberá ser entregada como mínimo 24 horas antes de realizarse los trabajos y actualizada cuando se produzcan cambios.
- j) En caso el CONTRATISTA, deba cambiar algún personal designado para realizar los trabajos de mantenimiento preventivo de los equipos de comunicación, este deberá comunicar a la APN con una anticipación de 05 días hábiles y deberá remitir la documentación que certifica al personal, para poder realizar las funciones planificadas en el mantenimiento



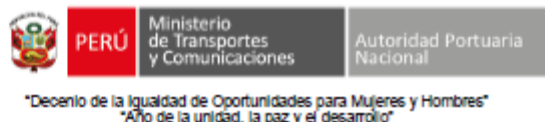
PERÚ

Ministerio
de Transportes
y Comunicaciones

Autoridad Portuaria
Nacional

"Decenio de la Igualdad de Oportunidades para Mujeres y Hombres"
"Año de la unidad, la paz y el desarrollo"

- k) Si los equipos appliance instalados, equipos telefónicos y los equipos gestionados fallan (deja de funcionar), el CONTRATISTA deberá repararlos o reemplazarlos sin costo para la entidad por otro similar o superior en el plazo del RMA de la marca. Adicionalmente, solo para los routers se debe reponer en un máximo de 04 horas, contados a partir de reportado el problema, por un equipo similar o superior de manera temporal mientras siga el proceso del RMA de la marca. **Se precisa que el CONTRATISTA, para los reemplazos podrá considerar tener un equipo en su almacén con las características similares o superiores al implementado en la sede de la Entidad.**
- l) Incluir las licencias necesarias de todo el equipamiento rentado y con soporte gestionado, para su correcto funcionamiento de acuerdo con los requerimientos antes mencionados, por el periodo de 36 meses correspondiente a la efectiva ejecución del servicio.
- m) Los equipos y componentes deben estar diseñados para operar bajo un escenario continuo de trabajo de 7x24x365, robusto, que asegure una disponibilidad del servicio del 99.90%.
- n) El CONTRATISTA se encargará de todos los cambios de configuraciones que la entidad necesite hacer de manera permanente 24 x 7, sin límite de cantidad de cambios, ni costos adicionales.
- o) La APN, podrá solicitar al CONTRATISTA, al menos 02 veces en el periodo de contrato, el traslado del equipamiento rentado y del equipamiento gestionado, de un gabinete hacia otro, dentro del centro de cómputo de la sede central de la APN, sin que esto origine algún costo para la institución. El traslado o reubicación también puede solicitarse para los circuitos digitales de los servicios de internet y telefonía fija, incluida la fibra óptica que llega al media converter.
- p) Toda la gestión de Soporte y Mantenimiento del Servicio de Seguridad Administrada es por parte del CONTRATISTA, lo cual incluye actualización de las listas, generación y envío de reportes.
- q) El CONTRATISTA y Sub-Contrata (de ser el caso), deberá contar con NOC (Network Operation Center) y a su vez que cuenten con una herramienta de mesa de ayuda, la cual opcionalmente podrá estar certificada en ITIL. El CONTRATISTA, deberá garantizar que cuenta con dicha herramienta.
- r) Asimismo, los tiempos de respuesta, de atención de requerimientos y solución para las incidencias o caídas del servicio serán las siguientes:
 - 1. **Tiempo de Respuesta:** Este tiempo inicia desde que la APN notifica la incidencia o requerimiento mediante correo electrónico al CONTRATISTA y luego este responde por el mismo medio con el número de ticket de atención. Este tiempo máximo de respuesta no debe ser mayor de una (01) hora.
 - 2. **Tiempo de Atención de Requerimientos:** Este tiempo inicia cuando se recibe mediante correo electrónico del CONTRATISTA, el ticket de



atención, hasta que el CONTRATISTA, informe mediante correo electrónico que se ha atendido el requerimiento. El tiempo máximo para atender el requerimiento será de hasta seis (06) horas.

3. **Tiempo de Solución de Caídas e Incidencias:** Este tiempo inicia cuando se recibe mediante correo electrónico del CONTRATISTA, el ticket de atención, hasta que el CONTRATISTA, informe mediante correo electrónico que se ha dado solución a la caída del servicio o la incidencia. El tiempo máximo de solución será de veinticuatro (24) horas. Se evaluará extender el plazo previa comunicación del prestador del servicio tomando en cuenta factores externos, ajenos al proveedor demostrables. El CONTRATISTA podrá contar con un router Backup en caso se presenten fallas de algunos de estos equipos. Asimismo, en caso de que algunos de los equipos de internet móvil (Modem), se reporte como dañado o averiado, este deberá ser cambiado en un periodo no mayor de 24 horas, contados a partir del envío de correo solicitando el cambio por avería.

Para el caso de los equipos en la ciudad de Iquitos, los tiempos de solución de caídas e incidencias serán de 24 horas cuando se trate de una caída en el circuito digital (router, fibra óptica o backbone de fibra de la zona) y para los reemplazos de los equipos de comunicaciones (switch y teléfonos IP), el tiempo de solución será de 96 horas⁴⁹.

8) PENALIDADES

La APN aplicará las penalidades correspondientes de acuerdo con lo establecido en la Ley de Contrataciones del Estado y su Reglamento.

9) OTRAS PENALIDADES

Las siguientes penalidades se aplicarán en caso de incumplimiento de los requerimientos mínimos expuesto en el presente documento. Se precisa que, en casos de afectación al servicio, por causas externas ajenas al operador (fortuito o fuerza mayor), puede ser reportada a las oficinas de atención del CONTRATISTA sin que ello signifique un supuesto de penalidad.

Otras penalidades			
N°	Supuestos de aplicación de penalidad	Forma de cálculo	Procedimiento
1	Cuando no se cumpla con los tiempos de respuesta o tiempos de atención de requerimientos o tiempos de solución de caídas e incidencias, detallados en el punto 7 del presente documento	1% ⁵⁰ de una UIT (Unidad impositiva tributaria) por cada hora o fracción de hora de retraso.	Se verificará el periodo de atención o solución del problema mediante el registro de correo electrónico de acuerdo con lo indicado en el punto 7 de los presentes términos de referencia.
2	Cuando no se cumpla con los tiempos de respuesta o de atención de las solicitudes de registro de DNS	Forma de Cálculo: 0.5% de una UIT por cada hora o fracción de hora de retraso.	Se verificará el periodo de respuesta y atención mediante correo electrónico.

10) CLAUSULA NORMAS ANTICORRUPCIÓN

⁴⁹ Absolución Pliego N° 37 participante VITTEL PERU S.A.C

⁵⁰ Absolución Pliego N° 92 participante VITTEL PERU S.A.C



PERÚ

Ministerio
de Transportes
y Comunicaciones

Autoridad Portuaria
Nacional

"Decenio de la Igualdad de Oportunidades para Mujeres y Hombres"
"Año de la unidad, la paz y el desarrollo"

El proveedor / contratista acepta expresamente que no llevara a cabo, acciones que están prohibidas por las leyes locales u otras leyes anti-corrupción. Sin limitar lo anterior, el proveedor / contratista se obliga a no efectuar algún pago, ni ofrecerá o transferirá algo de valor, a un funcionarios o empleado gubernamental o a cualquier tercero relacionado con el servicio aquí establecido de manera que pudiese violar las leyes locales u otras leyes anti-corrupción, sin restricción alguna.

En forma especial, el proveedor / contratista declara con carácter de declaración jurada que no se encuentra inmerso en algún proceso de carácter penal vinculado a presuntos ilícitos penales contra el Estado Peruano, constituyendo su declaración, la firma de este en la Orden de Servicio de la que estos términos de referencia forman parte integrante.

11) CLAUSULA NORMAS ANTISOBORNO

El proveedor, no debe ofrecer, negociar o efectuar, cualquier pago, objeto de valor o cualquier dádiva en general, o cualquier beneficio o incentivo ilegal en relación al contrato, que pueden constituir un incumplimiento a la ley, tales como robo, fraude, cohecho o tráfico de influencias, directa o indirectamente, o a través de socios, integrantes de los órganos de administración, apoderados, representantes legales, funcionarios, asesores o personas vinculadas, en concordancia o a lo establecido en el artículo 11 del TUO de la Ley de Contrataciones del Estado, Ley N° 30225, y artículo 7° de su Reglamento aprobado mediante Decreto Supremo N° 344-2018-EF.

Asimismo, el proveedor 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, participantes, integrantes de los órganos de administración apoderados, representantes legales, funcionarios, asesores y personas vinculadas en virtud a lo establecido en los artículos antes citados de la Ley de Contrataciones del Estado y su Reglamento.

Asimismo, el Proveedor se compromete a comunicar a las autoridades competentes, de manera directa y oportuna, cualquier acto o conducta ilícita o corrupta de la que tuviere conocimiento; así también en adoptar medidas técnicas, prácticas, a través de los canales dispuestos por la entidad.

De la misma manera, el proveedor es consciente que, de no cumplir con lo anteriormente expuesto, se someterá a la resolución del contrato y a las acciones civiles y/o penales que la entidad pueda accionar.

12) FECHA

04.08.2023

13) FIRMA Y SELLO ÁREA USUARIA

(firmado digitalmente por)

Ing. Mariela Gutarra Ramos
Jefa de la Oficina de TI

Nota importante: Para el perfeccionamiento del contrato, a fin de validar las características técnicas, el postor ganador deberá acreditar adjuntando los formatos de Cumplimiento de los anexos A, B, C, D, E, F, G y H debidamente sustentados a través de catálogos, brochures u otros documentos, entendiéndose como otros documentos los siguientes: guías prácticas o hojas técnicas o website del fabricante o manuales o carta de fabricante, indicando las referencias técnicas (número de folio) correspondiente. La documentación de sustento se podrá presentar en su idioma original (inglés o español). La carta del fabricante se podrá presentar solo para las características específicas que no se encuentren en la documentación pública o interna del fabricante y no para todas las características que se debe acreditar en los anexos. Asimismo, que en caso de presentar carta del fabricante esta deberá tener una antigüedad máxima de la fecha de la integración de bases.

Además de la carta del fabricante también pueden presentar carta de una filial del fabricante o carta de una empresa autorizada por el fabricante o carta del representante del fabricante o carta del distribuidor autorizado por el fabricante. Estos documentos deberán estar acompañados de la carta del fabricante que valide que son filiales o entes autorizados o representantes de la marca o distribuidor autorizado. Esta documentación solo se presentará para las características específicas que no se encuentren en la documentación pública o interna del fabricante y no para todas las características que se debe acreditar en los anexos⁵¹

FORMATOS DE CUMPLIMIENTOS

ANEXO A

Marca:
Modelo:

N°	Características técnicas mínimas de los Routers	Cumple (Si/No)	Folio
1	✓ Interfaces: seis (06) puertos 10/100/1000BaseT + 2SFP, 1 puerto USB.		
2	✓ Routing: BGP, OSPF, RIP v1/v2, Rutas estáticas, ECMP, RPF y enrutamiento basado en rutas y políticas.		
3	✓ Alta disponibilidad: Activo/Activo, Activo/Pasivo, VRRP.		
4	✓ Para efectos de la propuesta, ninguno de los modelos ofertados podrá estar listados ni anunciado en el sitio web del fabricante como end-of-life o end-of-sale o end-of-support. <u>Se deberá adjuntar para el perfeccionamiento del contrato el enlace público del fabricante o catálogos o brochures o guías prácticas o hojas técnicas, website o manuales o carta de fabricante que verifique que los modelos propuestos no están en ese listado</u>		

⁵¹ Absolución Pliego N° 168, 171 participante AMERICATEL PERU S.A



Ministerio
de Transportes
y Comunicaciones

Autoridad Portuaria
Nacional

"Decenio de la Igualdad de Oportunidades para Mujeres y Hombres"
"Año de la unidad, la paz y el desarrollo"

ANEXO B

Marca:

Modelo:

N°	Características técnicas mínimas de los Switch WAN	Cumple (Si/No)	Folio
1	Se requiere de un conmutador modular administrable de interfaces GigaEthernet que permita la operación en capa 2, capa 3 del modelo OSI.		
2	Para efectos de la propuesta, ninguno de los modelos ofertados podrá estar listados ni anunciado en el sitio web del fabricante como end-of-life o end-of-sale o end-of-support. <u>Se deberá adjuntar para el perfeccionamiento del contrato el enlace público del fabricante o catálogos o brochures o guías prácticas o hojas técnicas, website o manuales o carta de fabricante que verifique que los modelos propuestos no están en ese listado</u>		
3	Deberá disponer de al menos 08 puertos 10/100/1000BaseT. Las interfaces deberán permitir la auto negociación de la velocidad del puerto y del modo dúplex de la comunicación.		
4	Para la administración local se deberá considerar de al menos un (01) puerto de Consola RS232 o un (01) puerto RJ45 o un (01) puerto USB.		
5	La capacidad de tráfico mínimo que deberá procesar el equipo será no menor de 25Gbps de switch fabric y una tasa de envío de paquetes no menor a 20Mpps.		
6	Entre las funcionalidades básicas de administración, operación y mantenimiento se deberá considerar: SSHv2, HTTPS, Puerto Espejo (Port Mirroring), RMON, SNMP v2/v3, Netflow o Sflow, STMP, TACACS+, IEEE 802.1Q – VLAN trunking y tagging, IEEE 802.3ad – LACP, IEEE 802.3x – control de flujo de los puertos 10/100/1000BaseT, IEEE 802.1d – Spanning Tree Protocol, IEEE 802.1w – Rapid Spanning Tree Protocol, IEEE 802.1s – Múltiple Spanning Tree Protocol, IEEE 802.1ag – Ethernet OAM Connectivity Fault Management.		



Ministerio
de Transportes
y Comunicaciones

Autoridad Portuaria
Nacional

"Decenio de la Igualdad de Oportunidades para Mujeres y Hombres"
"Año de la unidad, la paz y el desarrollo"

ANEXO C

Marca:

Modelo:

N°	Características técnicas mínimas de los Firewall	Cumple (Si/No)	Folio
1	GENERALES		
2	La solución debe consistir en dos appliances de seguridad con funcionalidades de Next Generation Firewall (NGFW).		
3	Para efectos de la propuesta, ninguno de los modelos ofertados podrá estar listados ni anunciado en el sitio web del fabricante como end-of-life o end-of-sale o end-of-support. <u>Se deberá adjuntar el enlace público del fabricante o catálogos o brochures o guías prácticas hojas técnicas o website o manuales o carta de fabricante que verifique que los modelos propuestos no están en ese listado</u>		
4	La plataforma propuesta por el fabricante debe contar con certificación USGv6 para trabajar IPv6 tanto en Firewall como en IPS.		
	CAPACIDAD		
5	Throughput de Next Generation Firewall de 3 Gbps medido con tráfico productivo real (transacciones usando una mixtura de aplicaciones de capa 7, transacciones medidas en condiciones empresariales o transacciones HTTP 64KB de tamaño). No se aceptarán mediciones hechas con tráfico UDP o RFCs 3511, 2544, 2647 o 1242 o mixes de tráfico que no especifiquen tamaño de transacciones o paquetes.		
6	Throughput de Prevención de Amenazas de 1.5 Gbps medido con tráfico productivo real (transacciones usando una mixtura de aplicaciones de capa 7, transacciones medidas en condiciones empresariales o transacciones HTTP 64KB de tamaño), con las siguientes funcionalidades habilitadas simultáneamente: Control de aplicaciones, Sistema de Prevención de Intrusos (IPS), Antivirus/Antimalware de red, Antispyware/AntiBot, control de amenazas avanzadas de día cero (Sandboxing), Filtro de Archivos, y Logging activo. Si el fabricante tuviese diferentes niveles o modos de inspección de seguridad, el equipo ofertado deberá soportar el throughput requerido con el nivel o modo más alto de inspección. Se debe garantizar que el equipo no degrade su performance por debajo de lo requerido por la Entidad cuando se vayan habilitando los módulos de seguridad indicados en el modo más alto de inspección. No se aceptarán mediciones hechas con tráfico UDP o RFCs 3511, 2544, 2647 o 1242 o mixes de tráfico que no especifiquen tamaño de transacciones o paquetes.		
7	El equipo debe soportar como mínimo 290.000 sesiones simultáneas y 50.000 nuevas sesiones por segundo, medidos con paquetes HTTP de 1 byte.		
8	Disco de estado sólido interno de 120 GB o superior.		
9	Mínimo ocho (08) interfaces de red 10/100/1000 en cobre, formato RJ45 para tráfico de datos de la red		
10	Mínimo una (01) interfaz de consola RJ45,		
	CARACTERÍSTICAS GENERALES		
11	El dispositivo de seguridad debe soportar VLAN Tags 802.1q, agregación de links 802.3ad, policy based routing o policy based forwarding, ruteo multicast, jumbo frames, sub- interfaces ethernet lógicas, NAT de origen y destino.		



Ministerio
de Transportes
y Comunicaciones

Autoridad Portuaria
Nacional

"Decenio de la Igualdad de Oportunidades para Mujeres y Hombres"
"Año de la unidad, la paz y el desarrollo"

12	Debe soportar enrutamiento estático y dinámico (RIPv2, BGP y OSPFv2).		
	ALTA DISPONIBILIDAD		
13	Soporte a configuración de alta disponibilidad Activo/Pasivo y Activo/Activo, con despliegues de los equipos tanto en modo transparente como en modo capa 3 (L3).		
14	La configuración en alta disponibilidad debe sincronizar: Sesiones; Certificados de descifrado, Configuraciones, incluyendo, más no limitado a políticas de Firewall, NAT, QoS y objetos de red.		
15	Debe permitir cifrar la comunicación entre dos Firewall de HA durante la sincronización de las configuraciones.		
	FUNCIONALIDADES DE FIREWALL		
16	Control de políticas por zonas, puertos, direcciones IP, segmentos y/o rangos de red, región geográfica, usuarios y grupos de usuarios, aplicaciones grupos estáticos de aplicaciones, grupos dinámicos de aplicaciones (basados en sus atributos) y categorías de aplicaciones.		
17	Deberá ser posible la identificación de la aplicación y la inspección de malware, spyware y exploits dentro del tráfico cifrado por los protocolos en mención.		
18	Permitir el agendamiento de las políticas de seguridad.		
19	Debe ser posible especificar en las reglas de seguridad un grupo de objetos basados en IP y/o URL que se alimenten dinámicamente de una fuente externa.		
	DESCIFRADO DE TRÁFICO SSL/TLS		
20	Debe permitir descifrar el tráfico de navegación de usuarios a internet mediante la instalación de un certificado digital en los equipos.		
21	Debe permitir descifrar el tráfico entrante hacia servidores HTTPS publicados en internet importando el certificado del servidor en el Firewall.		
22	Debe ser capaz de inspección el tráfico cifrado, incluyendo el protocolo TLS 1.3.		
23	Debe tener la capacidad de bloquear la conexión hacia sitios web cifrados con protocolos obsoletos e inseguros.		
24	Debe identificar y notificar al cliente si está visitando una página web con certificado digital no válido o emisor no confiable, a pesar de no aplicar descifrado al tráfico SSL/TLS.		
25	Debe soportar certificados que utilice Subject Alternative Name (SAN) y Server Name Indication (SNI).		
	CONTROL DE APLICACIONES		
26	Reconocer por lo menos 3000 aplicaciones diferentes, incluyendo, más no limitando: el tráfico relacionado a peer-to-peer, redes sociales, acceso remoto, update de software, protocolos de red, voip, audio, video, proxy, mensajería instantánea, email.		
27	Debe procesar e inspeccionar aplicaciones que utilicen HTTP/2		
	PREVENCIÓN DE AMENAZAS CONOCIDAS		
28	Para seguridad del ambiente contra ataques, los dispositivos de seguridad deben poseer módulo de IPS (Intrusion Prevention System), Antivirus/Antimalware, Antispyware/Antibot.		
29	Capacidad de realizar DNS Sinkhole para la identificación de equipos comprometidos por spyware en entornos corporativos		
30	El equipo deberá soportar el throughput solicitado operando en el máximo nivel o modo de seguridad de inspección de IPS, Antivirus y Antispyware/Antibot.		
31	Las firmas deberán estar basadas en patrones del malware y no		



PERÚ

Ministerio
de Transportes
y Comunicaciones

Autoridad Portuaria
Nacional

"Decenio de la Igualdad de Oportunidades para Mujeres y Hombres"
"Año de la unidad, la paz y el desarrollo"

	únicamente en hashes, con el objetivo de detectar malware polimórfico que pertenezca a una misma familia.		
32	Debe sincronizar las firmas de seguridad cuando el Firewall se implementa en alta disponibilidad.		
	ANÁLISIS DE MALWARE DE DÍA CERO		
33	La solución propuesta debe incluir mecanismos de detección de amenazas de día cero, incluyendo una plataforma Sandboxing.		
34	La plataforma de Sandboxing deberá ser ofrecido en Nube (Cloud). Como mínimo se requiere que el Sandbox propuesto pueda detectar el malware de día cero en un tiempo no mayor a 5 minutos utilizando la emulación completa de malware en entornos Windows, Linux, Android y Mac (este tiempo de análisis se debe cumplir de manera paralela para todos los archivos enviados al Sandbox, considerando análisis dinámico completo, es decir, no incluye Firmas o Prefiltros)		
35	Deberá tener una disponibilidad del servicio de al menos 99.9% contabilizados mensualmente.		
36	Deberá ser un servicio propio del fabricante, no se aceptarán plataformas que tercericen el servicio de Sandboxing con entidades terceras.		
37	Deberá garantizar la privacidad y confidencialidad del contenido de los archivos analizados, para lo cual se requiere que el servicio cuente como mínimo con certificaciones SOC2 Tipo II de AICPA, FedRAMP.		
38	El malware de día cero deberá poder ser identificado dentro de la infraestructura de la Entidad, sin necesidad de enviar el archivo a ser analizado fuera de la red.		
39	Deberá soportar el análisis de archivos ejecutables (EXE), DLLs, ELF (Linux), archivos comprimidos (ZIP, 7ZIP, RAR) archivos office (.doc, .docx, .xls, .xlsx, .ppt, .pptx), archivos java (.jar e class), archivos de tipos script (.vbs, .ps1, .js), email link, flash, archivos de MacOS (mach-o, dmg, pkg) y Android APKs en el ambiente controlado.		
40	Permitir la subida de archivos al sandbox de forma manual y vía API.		
41	La solución debe realizar el análisis en un ambiente de hardware real, deshabilitando totalmente la habilidad de la amenaza de evadir sandboxing en máquinas virtuales.		
	FILTRO DE CONTENIDO WEB		
42	Permite especificar la política por tiempo, horario o determinado período (día, mes, año, día de la semana y hora)		
43	Deberá incluir la capacidad de creación de políticas basadas en la visibilidad e identificar el usuario que accede a una URL a través de la integración con servicios de directorio, autenticación vía Active Directory, LDAP en general y base de datos local.		
44	Debe soportar un cache local de URLs en el appliance, evitando el delay de comunicación/validación de las URLs		
45	Debe poseer al menos 70 categorías de URLs, incluyendo las de malware y phishing.		
46	Debe permitir la creación de categorías personalizadas.		
	PROTECCIÓN AVANZADA DE DNS		
47	La solución debe ser alimentada por un servicio de inteligencia global capaz de identificar decenas de millones de dominios maliciosos con análisis en tiempo real sin depender de firmas estáticas.		
48	El servicio de protección de DNS debe alimentarse de telemetría		



PERÚ

Ministerio
de Transportes
y Comunicaciones

Autoridad Portuaria
Nacional

"Decenio de la Igualdad de Oportunidades para Mujeres y Hombres"
"Año de la unidad, la paz y el desarrollo"

	provista por clientes a nivel mundial y más de 30 fuentes de inteligencia de amenazas de terceros.		
	IDENTIFICACION DE USUARIOS		
49	Debe incluir a capacidad de creación de políticas basadas en la visibilidad y control de usuarios y/o grupos de usuarios a través de la integración de servicios de autenticación vía LDAP, Active Directory, E- Novell Directory, Exchange y base de datos local.		
50	Debe poseer integración con Microsoft AD Domain Controller para la identificación de direcciones IP y usuarios. Esta integración se podrá realizar con o sin software agente.		
	VPN		
51	Soportar VPN Site-to-Site y Cliente-To-Site en protocolos IPSec o SSL.		
52	Debe soportar Split Tunnel para elegir los segmentos de red que serán enrutados por la VPN.		
53	Debe permitir los siguientes tipos de conexión del cliente al túnel VPN: ✓ Antes del usuario se autentique en la estación		
54	✓ Después de la autenticación del usuario en la estación usando Single Sign On (SSO); ✓ Bajo demanda del usuario		
55	El agente de VPN client-to-site debe ser compatible al menos con: Windows 7, Windows 8, Windows 10, MacOS X.		
56	Debe contar con un dashboard gráfico que permita monitorear a los usuarios conectados por VPN.		
57	Debe permitir al menos 300 usuarios concurrentes, el CONTRATISTA, debe considerar el licenciamiento necesario para cumplir con la cantidad de usuarios requeridos como mínimo.		
	CONSOLA DE ADMINISTRACION Y MONITOREO		
58	Con la finalidad de no degradar el performance de procesamiento de red y seguridad del Next Generation Firewall, la administración del equipo, gestión de reportes y gestión de logs deben contar con recursos dedicados de CPU, Memoria RAM y Disco Duro, ya sea integrado dentro del mismo appliance u otro appliance independiente del mismo fabricante		
59	Debe contar con un dashboard interactivo y gráfico que permita monitorear el uso de las aplicaciones en capa 7, sitios web visitados, actividad de los usuarios, actividad por IP (origen y destino), países origen y destino del tráfico, uso de las reglas de seguridad, actividad del tráfico malicioso, actividad de los usuarios VPN. Esta información podrá ser vista en base a Bytes y Sesiones, y ser filtrado en base a un rango de tiempo, IP, usuario, país y regla de seguridad.		
60	Ante escenarios donde existan dos o más administradores del Next Generation Firewall logueados y realizando cambios en simultáneo en la consola de gestión, la solución deberá de ser capaz de solo aplicar los cambios realizados por cada administrador individual, sin afectar o sobrescribir los cambios del otro administrador.		
61	Debe permitir la generación de logs de auditoría detallados, informando de la configuración realizada, el administrador que la realizó, su IP y el horario de la alteración;		
62	La plataforma de seguridad debe permitir realizar tareas de gestión a través del API basado en XML.		



Ministerio
de Transportes
y Comunicaciones

Autoridad Portuaria
Nacional

"Decenio de la Igualdad de Oportunidades para Mujeres y Hombres"
"Año de la unidad, la paz y el desarrollo"

ANEXO D

Marca:
Modelo:

N°	Características técnicas mínimas del software para el Servicio de Protección avanzada de puesto de trabajo y servidores	Cumple (Si/No)	Folio
1	Protección para 50 máquinas servidores y/o estaciones de trabajo compatible con los siguientes sistemas operativos: <ul style="list-style-type: none"> ✓ Windows 7 SP1 hasta Windows 10 ✓ Windows Server 2008 R2 SP1 hasta Server/Core2019 ✓ macOS Big Sur, Catalina, Mojave ✓ Ubuntu, Redhat (RHEL), CentOS, Oracle, Amazon AMI, SUSE Linux Enterprise Server, Fedora, Debian, Virtuozzo, Scientific Linux 		
2	Protección contra ransomware con tecnología Albasado en comportamiento.		
3	Prevención de ataques basada en archivos mediante inteligencia artificial estática y el servicio de inteligencia en nube del fabricante		
4	Detección de ataques fileless mediante IA de análisis de comportamiento		
5	Respuesta autónoma frente a amenazas/eliminación, cuarentena		
6	Respuesta de remediación/rollback autónoma, mediante una sola instrucción.		
7	Dispositivo en cuarentena de la red.		
8	Inventario de aplicaciones del dispositivo final.		
9	Detección de dispositivos no autorizados		
10	Vulnerabilidad de la aplicación del dispositivo final.		
11	Reglas de detección personalizadas con respuesta activa de acuerdo con el contexto.		
12	El portal de administración de la solución EDR debe contar con las siguientes características:		
13	Deberá ser una plataforma ampliada de detección y respuesta (XDR)		
14	Capacidad de administrar la autenticación y autorización mediante SSO, MFA, RBAC.		
15	Integración con la inteligencia de amenazas del propio fabricante y con los indicadores de amenaza de MITRE ATT&CK.		
16	Dashboard que permita el análisis de seguridad de los datos.		
17	Notificaciones configurables por email y Syslog		
18	La protección del dispositivo final deberá considerar: Inteligencia Artificial (AI) estática, IA basado en el análisis de comportamiento, protección frente a documentos, malware que se ejecuta en memoria, exploits, movimiento lateral de malware.		
19	No se requiere una conexión central para proteger el dispositivo final, ante la desconexión a Internet se mantendrá la protección de manera autónoma.		
20	Respuesta automática a Ransomware, con capacidad de reversión a una sola intrusión.		
21	Como respuesta del evento de ciberseguridad sobre el dispositivo final, la solución de EDR deberá realizar remediación y reversión a su estado original, cuarentena del dispositivo afectado, y protección con o sin acceso a Internet.		



Ministerio
de Transportes
y Comunicaciones

Autoridad Portuaria
Nacional

"Decenio de la Igualdad de Oportunidades para Mujeres y Hombres"
"Año de la unidad, la paz y el desarrollo"

22	Entre las características más importantes del EDR se deberá considerar: la detección de dispositivos sin el agente o no autorizados, inventario y vulnerabilidad de aplicaciones instaladas en el dispositivo final, control de dispositivo bluetooth, USB, control de Firewall OS con reconocimiento de ubicación.		
23	El servicio de EDR deberá considerar un argumento de ataque, brindar visibilidad a bajo nivel, profunda del incidente, y permitir la caza de amenazas.		
24	La solución de EDR deberá permitir determinar la causa raíz detrás de los actores de amenazas y responder de forma autónoma, sin depender de los recursos de la nube.		



Ministerio
de Transportes
y Comunicaciones

Autoridad Portuaria
Nacional

"Decenio de la Igualdad de Oportunidades para Mujeres y Hombres"
"Año de la unidad, la paz y el desarrollo"

ANEXO E

Marca:

Modelo:

N°	Características técnicas mínimas del administrador de ancho de banda	Cumple (Si/No)	Folio
1	Un equipo dedicado a la funcionalidad de gestionar ancho de banda, este componente o función no deberá estar embebida sobre enrutadores, firewalls, NGFW, UTM entre otras.		
2	Para efectos de la propuesta, ninguno de los modelos ofertados podrá estar listados ni anunciado en el sitio web del fabricante como end-of-life o end-of-sale o end-of-support. <u>Se deberá adjuntar el enlace público del fabricante o catálogos o brochures o guías prácticas o hojas técnicas o website o manuales o carta de fabricante que verifique que los modelos propuestos no están en ese listado.</u>		
3	Las reglas de clasificación se podrán configurar en múltiples niveles, mínimo 10, de forma que una regla pueda tener diferentes reglas hijo, y así sucesivamente.		
4	La construcción de políticas ha de realizarse de forma visual, representándose el árbol con los diferentes niveles de forma gráfica y no en modo tabla.		
5	Cada nodo del árbol de políticas ha de ser capaz de contraerse para facilitar la visibilidad de todas las reglas, o poder visualizar un único nodo y sus políticas hijas.		
6	Se debe disponer de un buscador que, al escribir una aplicación, puerto, IP, dibuje el camino que recorre en el árbol para saber rápidamente qué política se le está asignando.		
7	Aplicar reglas de QoS que contengan las siguientes opciones: <ul style="list-style-type: none"> ✓ Asignación de un mínimo de ancho de banda ✓ Limitación a un máximo ancho de banda ✓ Definición de diferentes prioridades ✓ Descartar aquellos paquetes no deseados (drop) ✓ Mantener el QoS original ✓ Eliminar el QoS para que sea más proclive a descartarse si hay saturación 		
8	Los catálogos de clasificación y control deben ser válidos para aplicar a cualquier nivel del árbol de clasificación (sin necesidad de definir a qué nivel corresponde la regla)		
9	Se debe disponer de capacidad de tener plantillas para poder clonar políticas.		
10	Se debe poder tener algoritmos de QoS para priorización y limitación de tráfico basado en % en vez de en valores estáticos o fijos.		
11	El elemento es transparente a nivel de transporte, sin cambios en las direcciones IP y puestos de origen destino.		
12	La solución de QoS ha de ser integrable dentro de una herramienta de analítica avanzada que permita todas las funcionalidades descritas en el módulo de reporting.		
13	El sistema de políticas debe tener autoprotección y detección de incongruencias en políticas impidiendo la creación de una política errónea y quedando marcado en el árbol de políticas en algún color aquella política que no		



PERÚ

Ministerio
de Transportes
y Comunicaciones

Autoridad Portuaria
Nacional

"Decenio de la Igualdad de Oportunidades para Mujeres y Hombres"
"Año de la unidad, la paz y el desarrollo"

	es válida impidiendo ser guardada.		
14	El equipo para ofertar debe disponer de un bypass externo y pasivo simultáneo de interfaces de cobre y/o de fibra óptica, dicho bypass deberá garantizar que en caso de falla eléctrica o de procesamiento de este equipo, el tráfico no se vea interrumpido y se garantice la continuidad de la conectividad de las interfaces en funcionamiento.		
15	El dispositivo de gestión de ancho de banda deberá poder soportar la optimización TCP de tráfico dentro de la misma caja, deberá poder hacer las siguientes funcionalidades de aceleración:		
16	La solución de optimización deberá ir en línea y cumplir con los siguientes requisitos: Optimización de tráfico encriptado por protocolo TLS (versiones 1.0, 1.1, 1.2 y 1.3) sin romper la encriptación extremo a extremo. Optimización de tráfico encriptado por protocolo SSL (versiones 2.0, 3.0) sin romper la encriptación extremo a extremo. Despliegue en un solo punto en el camino del tráfico. No deberá ser necesario desplegar parejas de elementos en cada extremo del tráfico a optimizar. Los parámetros de optimización se autoajustarán con algoritmos de aprendizaje. El elemento actuará como un enlace físico (bump-in-the-wire) que manda el tráfico entre dos puertos físicos sin necesidad de direcciones IP asignadas y sin cambiar las MACs de los paquetes que lo atraviesan. El elemento soporta agregación de enlaces. El elemento soporta VLANs. El elemento es compatible con los siguientes mecanismos de respaldo (failover): OSPF (opcional), BGP (opcional), 802.3ad. El elemento es transparente a nivel de transporte, sin cambios en las direcciones IP y puertos de origen destino.		
17	Capilaridad a nivel de Aplicaciones y reporting del gestor de ancho de banda		
18	Dicha parte de reportería deberá tener las siguientes capacidades de monitorización y analítica avanzada: o Creación de cuadros de mando personalizados a las necesidades del cliente. o Capacidad de hacer ZOOM o "Drill Down" desde una vista superior a otra vista más particular. o Capacidad de crear cuadros de mando con leyendas personalizadas, incrustar videos, o fotos explicativas en la página web del cuadro de mando. Capacidad de incrustar Logos o cualquier otra información. o Posibilidad de crear botones de búsqueda, cuadros de mando de búsquedas, posibilidad de hacer búsquedas múltiples por diversos criterios, etc. o Interfaz gráfica multilenguaje. o Interfaz gráfica debe soportar "modo claro" y "modo oscuro". o La interfaz gráfica debe auto-adaptarse a la resolución		



Ministerio
de Transportes
y Comunicaciones

Autoridad Portuaria
Nacional

"Decenio de la Igualdad de Oportunidades para Mujeres y Hombres"
"Año de la unidad, la paz y el desarrollo"

	<p>y/oal tipo de terminal: laptop, tableta, móvil, etc.</p> <ul style="list-style-type: none"> o Capacidad multitenant de acceso a las vistas de datos y a los datos. Dicha funcionalidad no puede ser de coste adicional. o Capacidad de multiplexar diferentes fuentes de datos en un único cuadro de mando. o Capacidad de creación de alarmas y eventos y planificación de eventos. o Notificación de alarmas en múltiples formatos tipo email, Slack, o similares. o Capacidad de visualizar umbrales de tres niveles, pudiendo seleccionar los colores, tanto para series temporales como agregadas y acelerómetros. o Capacidad de generación de informes e informes automatizados que se puedan programar y generar automáticamente en formato PDF y otros, tipo JPG o CSV. o Capacidad de creación mapas de "carreteras" que permitan visualizar por donde va un flujo, servicio o aplicación. Capacidad de autodescubrimiento de nodos de red. o Capacidad de generar múltiples vistas de datos en formatotabla, series temporales, diagramas, gráficos de barras, gráficos de agregación como por ejemplo tipo "pie" y otros muchos tipos. o Se podrán sacar informes y gráficas en función del tiempo, seleccionando mediante un calendario el periodo a visualizar. o Se podrá definir la resolución de los datos a visualizar, porejemplo: cada minuto, cada 5 minutos, etc. Incluso se podrá ir a resoluciones inferiores siempre y cuando se tengan datos con una resolución inferior. o Se podrán crear cuantos "dashboards" o cuadros de mando se desea y la forma de construirlos será mediante tarjetas (cards) que se pueden definir de cualquier tamaño, se podrán asignar colores, leyendas y en definitiva personalizar. o Dichas tarjetas estarán accesibles para los usuarios en función de sus privilegios y podrán ser particulares de un usuario o generales para ser utilizadas por muchos usuarios. o Las tarjetas deben permitir suscribirse a eventos creados en otras tarjetas. Es decir, haciendo click en un campo de una tarjeta, debe permitir que se aplique el filtro del valor seleccionado en otra u otras tarjetas. o Una tarjeta puede ser definida como filtro, de modo que permita crear una entrada de texto, una lista desplegable, botones de selección, etc. Dichos filtros han de aplicarse a las tarjetas predefinidas. o Las tarjetas pueden configurarse para aparecer invisibles en el cuadro de mando y aparecer sólo cuando se aplique un evento determinado 		
19	<p>Métricas, KPIs y tipos de aplicaciones necesarias de la herramienta:</p> <ul style="list-style-type: none"> o Calcular las siguientes métricas: o QoE • RTT 		



Ministerio
de Transportes
y Comunicaciones

Autoridad Portuaria
Nacional

"Decenio de la Igualdad de Oportunidades para Mujeres y Hombres"
"Año de la unidad, la paz y el desarrollo"

	<ul style="list-style-type: none"> • TCP duplicate ACK • TCP Packet lost • TCP Retransmission • TCP RTT Client site • TCP RTT Server site • Network • HTTP/HTTPS • Service Setup time • Mean data • Peak data • Service non accessibility • Session failure ratio • Session time • Set up time • Transactions • Data transfer cut off • Service access failure • Usuario • Duration Usage • Total activity • Start time • Stop time • VoIP • RTT • Caller ID • Session Time o Duration Time 		
20	La sonda de red debe ser capaz de realizar capturas de tráfico para poder generar PCAPs tanto para IPs concretas como para rangos de IPs. Dichas capturas se podrán truncar para de la carga útil del paquete. Se podrá seleccionar las IPs o VLANs desde donde se realiza la captura.		
21	Se podrá identificar el tráfico de un mismo flujo que pueda estar duplicado, tanto para la captura de paquetes como para la propia monitorización de la sonda DPI.		
22	Se podrá identificar un flujo o conexión independientemente de que pudiera haber en la red un Proxy, NAT o un cambio en la cabecera de los paquetes de dicha conexión.		
23	El sistema gestor de tráfico debe poder soportar, no licenciado de inicio, en el mismo equipo y sin HW adicional la capacidad de monitorizar todos los equipos externos al gestor que forman parte de la comunicación del enlace a Internet (FW, SW, Routers, Servidores u otros).		



PERÚ

Ministerio
de Transportes
y Comunicaciones

Autoridad Portuaria
Nacional

"Decenio de la Igualdad de Oportunidades para Mujeres y Hombres"
"Año de la unidad, la paz y el desarrollo"

ANEXO F

Marca:

Modelo:

N°	Características técnicas mínimas de la solución de la gestión de vulnerabilidades	Cumple (Si/No)	Folio
1	Deberá realizar escaneos de vulnerabilidades y evaluación de configuraciones (políticas) en forma programada y automática. Los resultados de estos deberán estar consolidados en un único sistema de gestión.		
2	Deberá coleccionar datos mediante escáneres activos, escáneres pasivos (análisis de tráfico de red) y agentes. No deberá haber límites en la cantidad de escáneres a desplegar en forma distribuida. Además, deberá contar con motores de escaneo públicos para escanear ambientes publicados a Internet.		
3	Deberá estar basado en un catálogo propio de vulnerabilidades que incluyan más de 160 mil evaluaciones diferentes y al menos 64 mil vulnerabilidades conocidas por un período no menor a 15 años.		
4	Deberá ser capaz de evaluar, no solo vulnerabilidades, sino auditar configuraciones y compararlas contra las mejores prácticas y frameworks de seguridad tales como CIS, CERT, CISA STIG, PCI y otros para la totalidad de activos licenciados, incluidos equipos de red, infraestructura de virtualización, Windows, Linux, Bases de Datos, Aplicaciones y otros sistemas. Estas auditorías podrán ser personalizables por la organización. Esta funcionalidad es también conocida como Policy Compliance. Se requiere esta capacidad sin límites de licenciamiento.		
5	La solución deberá contar con una API completa para integración mediante scripting automatizado y exportación de datos mediante llamados. Esta API deberá estar liberada y documentada y no deberá tener limitaciones de licencias en cantidad de llamados o sistemas que la consultan. Si no existe una licencia ilimitada, considerar la de mayor capacidad disponible.		
6	Deberá ser capaz de obtener vulnerabilidades de estaciones de trabajo en Internet (teletrabajo) y otros ambientes no conectados		
7	a la red del organismo, e inalcanzables por un escáner, mediante agente Windows, Linux y MacOS.		
8	Deberá contar con escaneos que solo auditen la existencia o inexistencia de parches de todo tipo de sistemas (Windows Desktop, Unix/Linux, equipos de red, aplicaciones y Otras plataformas).		
9	Deberá mantener registro de estado de vulnerabilidades por activo, de modo de identificar vulnerabilidades que, habiendo sido remediadas, volvieron a surgir en nuevos escaneos. Deberán registrarse las fechas de primera aparición, última aparición y reaparición. Además, se deberá contar con una vista de vulnerabilidades remediadas.		



Ministerio
de Transportes
y Comunicaciones

Autoridad Portuaria
Nacional

"Decenio de la Igualdad de Oportunidades para Mujeres y Hombres"
"Año de la unidad, la paz y el desarrollo"

10	Deberá reportar vulnerabilidades que sean explotables, establecer el nivel de madurez del código de exploit (si aplica), documentar de que forma se explota (malware, acceso remoto, con o sin credenciales), si el exploit está presente en frameworks reconocidos tales como Metasploit, Canvas, Core y otras.		
11	Deberá proporcionar control de acceso basado en roles y perfiles con suficiente granularidad para controlar a los usuarios el acceso a determinados conjuntos de datos y la funcionalidad que está disponible para los usuarios tales como ejecutar escaneos, cambiar configuraciones, acceder a los resultados, generar reportes, aceptar riesgos y otros casos de uso. Debe contar con roles predefinidos y permitir crear nuevos roles.		
12	Deberá presentar paneles de control predefinidos y personalizables que contengan datos estadísticos, gráficos de tendencias, información relevante mediante filtros, índices de riesgos y otros datos importantes.		
13	La solución deberá contar de forma nativa e incluida en su licenciamiento, la capacidad de conectarse a las API de Google Cloud Platform, AWS y Azure para el descubrimiento de nuevas instancias en entornos de nube. Además, deberá contar con escáneres pre-autorizados y disponibles en esos servicios de nube.		
14	La solución deberá utilizar motores de escaneo propios. No se aceptarán soluciones que utilicen motores de otros fabricantes o tecnologías open-source.		
15	Deberá contar con motores de escaneo públicos, listos para ser usados sin necesidad de despliegue para aplicaciones publicadas a Internet.		
16	Deberá contar con diferentes opciones de escáneres distribuidos globalmente y tener libertad de elegir cual utilizar.		
17	Deberá informar los rangos de IP utilizados por cada grupo de escáneres.		
18	La solución debe poder definir y administrar grupos de usuarios, incluida la limitación de las funciones de escaneo y el acceso a informes.		
19	Deberá contar con la opción de configurar métodos de autenticación de múltiples factores.		
20	Debe soportar todas las versiones de protocolos de transporte utilizados comúnmente en los sitios web actuales, incluyendo http://v.1.1, http v.1.0, SSL/TLS, http compression, http User Agent Configuration.		
21	La solución deberá estar basada en escaneos activos mediante tests remotos. No se tendrán en cuenta herramientas que analicen tráfico ni requieran la implementación de piezas desoftware o código en la aplicación o requiera la instalación de un gateway para su análisis.		



PERÚ

Ministerio
de Transportes
y Comunicaciones

Autoridad Portuaria
Nacional

"Decenio de la Igualdad de Oportunidades para Mujeres y Hombres"
"Año de la unidad, la paz y el desarrollo"

22	Debe contar con plantillas de scan que permitan escanear las vulnerabilidades de una aplicación y otros que permitan solo entender la estructura del sitio. Deberá también haber plantillas para auditar la versión de SSL/TLS implementada en la aplicación.		
23	Deberá contar con un repositorio de credenciales para ser utilizadas en los escaneos.		
24	Deberá permitir configurar una programación para ejecutar un escaneo en forma recurrente, programando la frecuencia o definiendo día y hora precisa de inicio.		
25	Deberá permitir configurar permisos de acceso y visibilidad a los resultados y de control y configuración de los parámetros de escaneo.		
26	Permitirá definir si los resultados son compartidos y acumulados en los paneles de control y reportes generales o son solo de consulta del propietario.		
27	Deberá tener la suficiente granularidad como para poder definir la habilitación/inhabilitación de tests de vulnerabilidades puntuales o por familias.		
28	El fabricante deberá poner a disposición acceso a una API que permita crear conectores, importar/exportar datos y automatizar procesos.		
29	Deberá ser capaz de detectar vulnerabilidades que permitan la inyección de código.		
30	Deberá contar con múltiples evaluaciones relacionadas con SSL/TLS, identificando cifrados no soportados o débiles, certificados auto-firmados o expirados, versiones débiles u obsoletas de protocolo.		
31	La solución deberá ser segura de escanear en ambientes de producción.		
32	La solución deberá tener la capacidad de testear una aplicación web diseñada para el uso en dispositivos móviles.		
33	La solución deberá ser capaz de testear aplicaciones HTML5.		
34	Deberá entregar paneles de control que muestren indicadores estadísticos con número de vulnerabilidades por criticidad.		
35	Deberá contar con paneles de control que muestren estadísticas de vulnerabilidades por aplicación, por categoría de OWASP y por severidad.		
36	Deberá permitir crear paneles de control personalizados.		



Ministerio
de Transportes
y Comunicaciones

Autoridad Portuaria
Nacional

"Decenio de la Igualdad de Oportunidades para Mujeres y Hombres"
"Año de la unidad, la paz y el desarrollo"

ANEXO G

Marca:

Modelo:

N°	Características técnicas mínimas de la Central Telefónica	Cumple (Si/No)	Folio
1	El equipamiento deberá ser de solución tipo appliance de propósito específico con arquitectura todo en uno (all-in-one), de crecimiento modular a través de tarjetería (para primarios y/o Líneas analógicas), y basado en el protocolo SIP.		
2	Para efectos de la propuesta, ninguno de los modelos ofertados podrá estar listados ni anunciado en el sitio web del fabricante como end-of-life o end-of-sale o end-of-support. <u>Se deberá adjuntar el enlace público del fabricante o catálogos o brochures o guías prácticas o hojas técnicas, website o manuales o carta de fabricante que verifique que los modelos propuestos no están en ese listado</u>		
3	La central debe permitir contestar las llamadas de un anexo a otro.		
4	La central debe permitir crear grupos de anexos.		
5	El sistema deberá proporcionar buzones de voz incorporados (built-in) para implementar la funcionalidad de correos de voz o voicemail y prevenir la pérdida de llamadas.		
6	El sistema deberá soportar servicios suplementarios tales como, llamada de emergencia, estación de secretaría, y barrido de llamada (opcional), entre otros, para cumplir con los diferentes requerimientos de servicio.		
7	El sistema deberá soportar IPv4 e IPv6.		
8	El sistema debe estar en capacidad de soportar los códecs de audio G.711a, G.711μ, G.729 o G.729AB.		
9	El sistema de comunicaciones deberá ser una plataforma de comunicaciones IP y soportar una gama de teléfonos IP que a su vez soporten estándares internacionales como Calidad de Servicio (QoS), G.711a, G.711μ, G.729 o G.729AB en conexión Ethernet, con switch incorporado, de 10/100 Mbps como mínimo.		
10	El sistema deberá permitir la personalización de la música de espera y poder permitirle la adición de mensajes Institucionales.		
11	La administración deberá ser a través de una consola web, para la asignación de anexos, códigos, permisos de llamadas, entre otros.		
12	Para la funcionalidad de único número de contacto, el sistema tendrá la capacidad de configurar listas de acceso (incluyendo la posibilidad de restricciones hacia ciertos números) y programación de horarios para la distribución de las llamadas.		
13	El sistema de central telefónica deberá tener la capacidad de poder modificar las etiquetas de los teléfonos.		



Ministerio
de Transportes
y Comunicaciones

Autoridad Portuaria
Nacional

"Decenio de la Igualdad de Oportunidades para Mujeres y Hombres"
"Año de la unidad, la paz y el desarrollo"

14	<p>Las funcionalidades de los teléfonos analógicos que son propiedad de la APN deberán de poder realizar lo siguiente:</p> <p>Transferencia de llamadas Llamadas externas Llamadas Internas Captura de llamadas Grupo de extensiones Código personal</p>		
15	<p>Los Teléfonos IP deben tener las siguientes facilidades:</p> <p>Restricción de llamadas. Grupos de extensiones Captura de llamadas. Código personal Desvío de llamadas Rellamada. Llamada en consulta Llamada externa. Llamada interna. Interconexión de llamada sobre la extensión ocupada o en DND. Identificación de llamadas. Deshabilitación/Habilitación del teléfono IP por el usuario o administrador del sistema. Teléfono con múltiples números. Marcación abreviada. Movimiento de terminal mediante código.</p> <p>Se debe contar con una operadora automática que permita acceder directamente a un anexo interno desde una línea externa en una central telefónica además de dar una imagen corporativa a la empresa.</p>		

ANEXO H



PERÚ

Ministerio
de Transportes
y Comunicaciones

Autoridad Portuaria
Nacional

"Decenio de la Igualdad de Oportunidades para Mujeres y Hombres"
"Año de la unidad, la paz y el desarrollo"

Marca:
Modelo:

N°	Características técnicas mínimas del Teléfono IP de Tipo A	Cumple (Si/No)	Folio
1	Los teléfonos ofertados deberán ser de la misma marca de la central telefónica.		
2	Teléfono de dos (02) líneas basado en el protocolo SIP.		
3	Pantalla LCD a color con resolución de al menos 320 x 240 píxeles o 240x320 píxeles.		
4	Dos puertos Ethernet 10/100/1000 Mbps.		
5	Debe contar con al menos las siguientes teclas de funciones: transferencia de llamada, conferencia, manos libres/altavoz, modo audífonos, silencio, espera, ajuste de volumen.		
6	Debe contar con al menos 02 teclas de líneas, 5 teclas de navegación, 04 teclas de función suave (softkey) y 03 teclas programables como mínimo.		
7	Indicador visual de mensajes de voz (Message Waiting Indicator).		
8	Debe poder mostrar información histórica de llamadas perdidas, realizadas y recibidas.		
9	Soporte de los códecs G.711a, G.711µ, G.729 o G.729AB.		
10	Soporte de los protocolos 802.1p/q (VLAN).		
11	Soporte del protocolo 802.3af (Power Over Ethernet).		
12	Debe incluir al menos 10 tonos de timbrado predefinidos		

N°	Características técnicas mínimas del Teléfono IP de Tipo B	Cumple (Si/No)	Folio
1	Los teléfonos ofertados deberán ser de la misma marca de la central telefónica.		
2	Teléfono de 6 líneas basado en el protocolo SIP.		
3	Pantalla LCD a color con resolución de al menos 800 x 480 píxeles o 480x800 píxeles.		
4	Dos puertos Ethernet 10/100/1000 Mbps.		
5	Debe contar con al menos las siguientes teclas de funciones (En caso de que se oferte un teléfono con pantalla touch las teclas podrán ser virtuales): transferencia de llamada, conferencia, manos libres/altavoz, modo audífonos, silencio, espera, ajuste de volumen.		
6	Debe contar con al menos 06 teclas de líneas, 5 teclas de navegación, 04 teclas de función suave (softkey) y 5 teclas programables. En caso el CONTRATISTA, oferte teléfonos con pantalla táctil, las teclas podrán ser virtuales.		
7	Indicador visual de mensajes de voz (Message Waiting Indicator).		
8	Debe poder mostrar información histórica de llamadas perdidas, realizadas y recibidas.		
9	Soporte de los códecs G.711a, G.711µ, G.729 o G.729AB.		
10	Soporte de los protocolos 802.1p/q (VLAN).		
11	Soporte del protocolo 802.3af (Power Over Ethernet).		
12	Debe incluir al menos 10 tonos de timbrado predefinidos.		

Importante

Para determinar que los postores cuentan con las capacidades necesarias para ejecutar el contrato, el comité de selección incorpora los requisitos de calificación previstos por el área usuaria en el requerimiento, no pudiendo incluirse requisitos adicionales, ni distintos a los siguientes:

3.2. REQUISITOS DE CALIFICACIÓN

A	CAPACIDAD LEGAL
	HABILITACIÓN
	<p><u>Requisitos:</u> El postor debe contar con autorización del Ministerio de Transportes y Comunicaciones para brindar el servicio de conmutación de transmisión de datos y/o el servicio de valor añadido de conmutación de datos por paquete</p>
	<p>Importante</p> <p><i>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.</i></p> <p><u>Acreditación:</u> Copia del documento emitido por el Ministerio de Transportes y Comunicaciones que acredite su autorización para brindar el servicio de conmutación de transmisión de datos y/o el servicio de valor añadido de conmutación de datos por paquete y/o certificado de registro de empresas prestadoras de servicio de valor añadido.</p> <p>Importante</p> <p><i>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.</i></p>
B	CAPACIDAD TÉCNICA Y PROFESIONAL
B.1	CALIFICACIONES DEL PERSONAL CLAVE
B.1.1	FORMACIÓN ACADÉMICA
	<p><u>Requisitos:</u> Un (01) Jefe de Proyecto Profesional titulado en Ingeniería de Telecomunicaciones o Ingeniería de Sistemas o Ingeniería Electrónica o Ingeniería Informática o Ingeniería de Computación e Informática o Ingeniería de Redes y Comunicación o Ingeniería de Software o Ingeniería de Redes de Computadoras y Comunicación de Datos o Ingeniería de Redes y Comunicación de Datos o Ingeniería de Redes y Comunicaciones o Ingeniería de Redes y Seguridad Informática o Ingeniería de Seguridad de la Información o Ingeniería de Sistemas e Informática⁵² del personal clave requerido como Jefe de Proyecto.</p> <p>Dos (02) Especialistas en Networking Ingeniero Profesional o Profesional técnico titulado o Bachiller en Sistemas, Redes de datos, Informática, Telecomunicaciones, Sistemas de Información, Computación y de Sistemas, Informática y de Sistemas, Electrónica, Redes y Comunicaciones de datos, Seguridad y Auditoría informática o Computación e Informática o Ingeniería de Redes y Comunicación o Ingeniería de Software o Electrónica y Telecomunicaciones o Redes de Computadoras y Comunicación de Datos o Redes y Comunicación de Datos o Redes y Comunicaciones o Redes y Seguridad Informática o Seguridad de la Información o Sistemas de Telecomunicaciones o Sistemas e Informática⁵³ del personal clave (cada uno) requerido como Especialista en Networking.</p> <p>Dos (02) Especialistas de Seguridad Ingeniero Profesional o profesional técnico titulado o Bachiller en Sistemas, Redes de datos, Informática, Telecomunicaciones, Sistemas de Información, Computación y de Sistemas, Informática y de Sistemas, Electrónica, Redes y Comunicaciones, Seguridad y Auditoría Informática o Computación e Informática o Ingeniería de Redes y Comunicación o Ingeniería de Software o Electrónica y Telecomunicaciones o Redes de Computadoras y Comunicación de Datos o Redes y Comunicación de Datos o Redes y Comunicaciones o Redes</p>

⁵² Absolución Pliego N° 62 participante VIETTEL PERU S.A.C

⁵³ Absolución Pliego N° 63,65 participante VIETTEL PERU S.A.C N° 268,270 participante WIN EMPRESAS S.A.C

	<p>y Seguridad Informática o Seguridad de la Información o Sistemas de Telecomunicaciones o Sistemas e Informática⁵⁴ del personal clave (cada uno) requerido como Especialista de Seguridad</p> <p>Dos (02) Especialistas de Telefonía Profesional técnico titulado o Bachiller en Sistemas, Redes de datos, Informática, Telecomunicaciones, Sistemas de Información, Computación y de Sistemas, Informática y de Sistemas, Electrónica, Electrónica y Telecomunicaciones del personal clave (cada uno) requerido como Especialista de Telefonía.</p> <p><u>Acreditación (todos):</u> El GRADO O TÍTULO PROFESIONAL 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: https://titulosinstitutos.minedu.gob.pe/, según corresponda.</p> <p>En caso EL GRADO O TÍTULO PROFESIONAL requerido no se encuentre inscrito en el referido registro, el postor debe presentar la copia del diploma respectivo a fin de acreditar la formación académica requerida.</p>
B.1.2	CAPACITACIÓN
	<p>Jefe de Proyecto <u>Requisitos:</u> Contar con un mínimo de 24 horas lectivas, en PMP o Dirección de Proyectos o Gerencia de Proyectos o Gerencia de Proyectos y Calidad. del personal clave requerido como JEFE DE PROYECTO.</p> <p><u>Acreditación:</u> Se acreditará con copia simple de constancias o diplomados⁵⁵.</p>
B.2	EXPERIENCIA DEL PERSONAL CLAVE
	<p><u>Requisitos:</u> 1.Experiencia mínima de tres (3) años como Jefe de Proyectos o encargado de proyectos de telecomunicaciones o Coordinador de proyectos; gestionando y/o supervisando y/o implementando Proyectos de Telecomunicaciones tales como Internet y/o Transmisión de Datos y/o Comunicaciones, conexión, redes y/o telefonía y/o Gestion y/o Supervisión de implementación de Proyectos de Servicios de Transmisión de Datos, Internet, Comunicaciones Unificadas, telefonía e infraestructura de Data Center del personal clave requerido como Jefe de Proyecto.</p> <p>2. Experiencia mínima de dos (2) años en las implementaciones switching o gestión de redes de datos o servicios de internet o enlace de datos del personal clave requerido (cada uno) como Especialista en Networking.</p> <p>3. Experiencia mínima de dos (2) años en la implementación o configuración de soluciones de seguridad perimetral (cada uno) como Especialista de Seguridad.</p> <p>4. Experiencia mínima de dos (2) años⁵⁶ en la implementación o configuración de Centrales Telefónica (cada uno) como Especialista de Telefonía.</p> <p><u>De presentarse experiencia ejecutada paralelamente (traslape), para el cómputo del tiempo de dicha experiencia sólo se considerará una vez el periodo traslapado.</u></p> <p><u>Acreditación:</u> 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.</p> <p>Importante</p>

⁵⁴ Absolución Pliego N° 64,66 participante VIETTEL PERU S.A.C N° 269,271 participante WIN EMPRESAS S.A.C

⁵⁵ Absolución Pliego N° 32 participante VIETTEL PERU S.A.C, N° 142 participante AMERICA MOVIL PERU S.A, N° 199,200 participante AMERICATEL PERU S.A

⁵⁶ Según Absolución Pliego N° 243 participante AMERICATEL PERU S.A

	<ul style="list-style-type: none"> 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
	<p><u>Requisitos:</u> El postor debe acreditar un monto facturado acumulado equivalente a S/ 8'000,000.00 (Ocho Millones y 00/100 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.</p> <p>Se consideran servicios similares a los siguientes: Servicios de telecomunicaciones, Servicios de transmisión de voz, datos y video, Servicio de transmisión de voz, Servicio de transmisión de datos, Servicios de transmisión de video, Servicios de accesos a internet, servicio de enlace de datos, Servicios de arrendamiento de circuitos o tránsito de Internet, Servicios de Transmisión de datos en general, Servicio de Telefonía Fija, Servicio de Seguridad Gestionada, Servicio de Líneas Analógicas, Servicios de Plan de Telefonía y Datos, Servicios de Internet Móvil, Servicios de Internet, Servicios de Internet Dedicado, Servicios de Internet y Enlace de Datos, Servicio de conexión, interconexión y comunicación mediante fibra óptica, Servicio de comunicación mediante fibra óptica, Servicio de conexión, interconexión e internet en general⁵⁷.</p> <p><u>Acreditación:</u> 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 pago⁵⁸, correspondientes a un máximo de veinte (20) contrataciones.</p> <p>En caso los postores presenten varios comprobantes de pago para acreditar una sola contratación, se debe acreditar que corresponden a dicha contratación; de lo contrario, se asumirá que los comprobantes acreditan contrataciones independientes, en cuyo caso solo se considerará, para la evaluación, las veinte (20) primeras contrataciones indicadas en el Anexo N° 8 referido a la Experiencia del Postor en la Especialidad.</p> <p>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.</p> <p>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.</p> <p>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</p>

⁵⁷ Según absolución Pliego N° 8 participante WIN EMPRESAS S.A.C N° 210,215 participante AMERICATEL PERU S.A

⁵⁸ 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".

Contrataciones del Estado”, debiendo presumirse que el porcentaje de las obligaciones equivale al porcentaje de participación de la promesa de consorcio o del contrato de consorcio. En caso que en dichos documentos no se consigne el porcentaje de participación se presumirá que las obligaciones se ejecutaron en partes iguales.

Si el titular de la experiencia no es el postor, consignar si dicha experiencia corresponde a la matriz en caso que el postor sea sucursal, o fue transmitida por reorganización societaria, debiendo acompañar la documentación sustentatoria correspondiente.

Si el postor acredita experiencia de otra persona jurídica como consecuencia de una reorganización societaria, debe presentar adicionalmente el **Anexo N° 9**.

Cuando en los contratos, órdenes de servicios o comprobantes de pago el monto facturado se encuentre expresado en moneda extranjera, debe indicarse el tipo de cambio venta publicado por la Superintendencia de Banca, Seguros y AFP correspondiente a la fecha de suscripción del contrato, de emisión de la orden de servicios o de cancelación del comprobante de pago, según corresponda.

Sin perjuicio de lo anterior, los postores deben llenar y presentar el **Anexo N° 8** referido a la Experiencia del Postor en la Especialidad.

Importante

- *Al calificar la experiencia del postor, se debe valorar de manera integral los documentos presentados por el postor para acreditar dicha experiencia. En tal sentido, aun cuando en los documentos presentados la denominación del objeto contractual no coincida literalmente con el previsto en las bases, se deberá validar la experiencia si las actividades que ejecutó el postor corresponden a la experiencia requerida.*
- *En el caso de consorcios, solo se considera la experiencia de aquellos integrantes que se hayan comprometido, según la promesa de consorcio, a ejecutar el objeto materia de la convocatoria, conforme a la Directiva “Participación de Proveedores en Consorcio en las Contrataciones del Estado”.*

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	
<p><u>Evaluación:</u></p> <p>Se evaluará considerando el precio ofertado por el postor.</p> <p><u>Acreditación:</u></p> <p>Se acreditará mediante el documento que contiene el precio de la oferta (Anexo N° 6).</p>		<p>La evaluación consistirá en otorgar el máximo puntaje a la oferta de precio más bajo y otorgar a las demás ofertas puntajes inversamente proporcionales a sus respectivos precios, según la siguiente fórmula:</p> $P_i = \frac{O_m \times PMP}{O_i}$ <p> <i>i</i> = Oferta P_i = Puntaje de la oferta a evaluar O_i = Precio <i>i</i> O_m = Precio de la oferta más baja PMP = Puntaje máximo del precio </p> <p style="text-align: right;">Hasta 100 puntos</p>

Importante

Los factores de evaluación elaborados por el comité de selección son objetivos y guardan vinculación, razonabilidad y proporcionalidad con el objeto de la contratación. Asimismo, estos no pueden calificar con puntaje el cumplimiento de los Términos de Referencia ni los requisitos de calificación.

CAPÍTULO V PROFORMA DEL CONTRATO

Importante

Dependiendo del objeto del contrato, de resultar indispensable, puede incluirse cláusulas adicionales o la adecuación de las propuestas en el presente documento, las que en ningún caso pueden contemplar disposiciones contrarias a la normativa vigente ni a lo señalado en este capítulo.

Conste por el presente documento, la contratación del servicio de internet, seguridad perimetral y telefonía fija para la sede central de la Autoridad Portuaria Nacional (APN) y servicio de enlace de datos entre el centro de control de comunicaciones y respuesta a emergencias (CCCRE) del Callao y la sede central, que celebra de una parte Autoridad Portuaria Nacional, en adelante LA ENTIDAD, con RUC N° 20509645150, con domicilio legal en Av. Santa Rosa N° 135 - La Perla, Callao, representada por [...], identificado con DNI N° [...], y de otra parte [...], con RUC N° [...], con domicilio legal en [...], inscrita en la Ficha N° [...] Asiento N° [...] del Registro de Personas Jurídicas de la ciudad de [...], debidamente representado por su Representante Legal, [...], con DNI N° [...], según poder inscrito en la Ficha N° [...], Asiento N° [...] del Registro de Personas Jurídicas de la ciudad de [...], a quien en adelante se le denominará EL CONTRATISTA en los términos y condiciones siguientes:

CLÁUSULA PRIMERA: ANTECEDENTES

Con fecha [...], el comité de selección adjudicó la buena pro del **CONCURSO PÚBLICO N° 001-2023-APN** para la contratación del servicio de internet, seguridad perimetral y telefonía fija para la sede central de la Autoridad Portuaria Nacional (APN) y servicio de enlace de datos entre el centro de control de comunicaciones y respuesta a emergencias (CCCRE) del Callao y la sede central, 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 la contratación del servicio de internet, seguridad perimetral y telefonía fija para la sede central de la Autoridad Portuaria Nacional (APN) y servicio de enlace de datos entre el centro de control de comunicaciones y respuesta a emergencias (CCCRE) del Callao y la sede central.

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 PAGO⁵⁹

LA ENTIDAD se obliga a pagar la contraprestación a EL CONTRATISTA en Soles, en pagos periódicos, luego de la recepción formal y completa de la documentación correspondiente, según lo establecido en el artículo 171 del Reglamento de la Ley de Contrataciones del Estado.

Para tal efecto, el responsable de otorgar la conformidad de la prestación deberá hacerlo en un plazo que no excederá de los siete (7) días de producida la recepción, salvo que se requiera efectuar pruebas que permitan verificar el cumplimiento de la obligación, en cuyo caso la conformidad se emite en un plazo máximo de quince (15) días, bajo responsabilidad de dicho funcionario.

⁵⁹ En cada caso concreto, dependiendo de la naturaleza del contrato, podrá adicionarse la información que resulte pertinente a efectos de generar el pago.

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 [.....] meses, el mismo que se computa a partir de día siguiente de la firma del acta de activación del servicio mensual.

El plazo para la implementación, instalación y puesta en producción de todos los servicios y sus componentes como parte del contrato no deberá exceder de los (.....) días calendario contados a partir del día siguiente de firmado el acta de inicio de implementación del servicio, dicha acta se firmará al día siguiente de la confirmación de recepción de la comunicación formal de la APN, para el inicio del servicio.

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.”

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 NOVENA: 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 la Oficina de Tecnologías de la Información 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

subsana no puede ser menor de cinco (5) ni mayor de quince (15) días. Si pese al plazo otorgado, EL CONTRATISTA no cumpliera a cabalidad con la subsanación, LA ENTIDAD puede otorgar al CONTRATISTA periodos adicionales para las correcciones pertinentes. En este supuesto corresponde aplicar la penalidad por mora desde el vencimiento del plazo para subsanar.

Este procedimiento no resulta aplicable cuando los servicios manifiestamente no cumplan con las características y condiciones ofrecidas, en cuyo caso LA ENTIDAD no otorga la conformidad, debiendo considerarse como no ejecutada la prestación, aplicándose la penalidad que corresponda por cada día de atraso.

CLÁUSULA DÉCIMA: 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 UNDÉCIMA: 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 UN (1) año contado a partir de la conformidad otorgada por LA ENTIDAD.

CLÁUSULA DUODÉCIMA: PENALIDADES

Si EL CONTRATISTA incurre en retraso injustificado en la ejecución de las prestaciones objeto del contrato, LA ENTIDAD le aplica automáticamente una penalidad por mora por cada día de atraso, de acuerdo a la siguiente fórmula:

$$\text{Penalidad Diaria} = \frac{0.10 \times \text{monto vigente}}{F \times \text{plazo vigente en días}}$$

Donde:

F = 0.25 para plazos mayores a sesenta (60) días o;

F = 0.40 para plazos menores o iguales a sesenta (60) días.

El retraso se justifica a través de la solicitud de ampliación de plazo debidamente aprobado. Adicionalmente, se considera justificado el retraso y en consecuencia no se aplica penalidad, cuando EL CONTRATISTA acredite, de modo objetivamente sustentado, que el mayor tiempo transcurrido no le resulta imputable. En este último caso la calificación del retraso como justificado por parte de LA ENTIDAD no da lugar al pago de gastos generales ni costos directos de ningún tipo, conforme el numeral 162.5 del artículo 162 del Reglamento de la Ley de Contrataciones del Estado.

Importante

De haberse previsto establecer penalidades distintas a la penalidad por mora, incluir dichas penalidades, los supuestos de aplicación de penalidad, la forma de cálculo de la penalidad para cada supuesto y el procedimiento mediante el cual se verifica el supuesto a penalizar, conforme el artículo 163 del Reglamento de la Ley de Contrataciones del Estado.

OTRAS PENALIDADES⁶⁰:

⁶⁰ De acuerdo a Absolución Pliego N° 92 participante AMERICA MOVIL PERU S.A.C

Otras penalidades			
N°	Supuestos de aplicación de penalidad	Forma de cálculo	Procedimiento
1	Cuando no se cumpla con los tiempos de respuesta o tiempos de atención de requerimientos o tiempos de solución de caídas e incidencias, detallados en el punto 7 del presente documento	1% ⁵⁰ de una UIT (Unidad impositiva tributaria) por cada hora o fracción de hora de retraso.	Se verificará el periodo de atención o solución del problema mediante el registro de correo electrónico de acuerdo con lo indicado en el punto 7 de los presentes términos de referencia.
2	Cuando no se cumpla con los tiempos de respuesta o de atención de las solicitudes de registro de DNS	Forma de Cálculo: 0.5% de una UIT por cada hora o fracción de hora de retraso.	Se verificará el periodo de respuesta y atención mediante correo electrónico.

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 TERCERA: 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 CUARTA: 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 QUINTA: 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 SEXTA: 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 SÉTIMA: SOLUCIÓN DE CONTROVERSIAS⁶¹

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 OCTAVA: 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 DÉCIMA NOVENA: 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.

De acuerdo con las bases integradas, la oferta y las disposiciones del presente contrato, las partes lo firman por duplicado en señal de conformidad en la ciudad de [.....] al [CONSIGNAR FECHA].

"LA ENTIDAD"

"EL CONTRATISTA"

Importante

Este documento puede firmarse digitalmente si ambas partes cuentan con firma digital, según la Ley N° 27269, Ley de Firmas y Certificados Digitales⁶².

⁶¹ 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).

⁶² Para mayor información sobre la normativa de firmas y certificados digitales ingresar a: <https://www.indecopi.gob.pe/web/firmas-digitales/firmar-y-certificados-digitales>

ANEXOS

ANEXO N° 1

DECLARACIÓN JURADA DE DATOS DEL POSTOR

Señores

COMITÉ DE SELECCIÓN

CONCURSO PÚBLICO N° 001-2023-APN

Presente.-

El que se suscribe, [.....], postor y/o Representante Legal de [CONSIGNAR EN CASO DE SER PERSONA JURÍDICA], identificado con [CONSIGNAR TIPO DE DOCUMENTO DE IDENTIDAD] N° [CONSIGNAR NÚMERO DE DOCUMENTO DE IDENTIDAD], con poder inscrito en la localidad de [CONSIGNAR EN CASO DE SER PERSONA JURÍDICA] en la Ficha N° [CONSIGNAR EN CASO DE SER PERSONA JURÍDICA] Asiento N° [CONSIGNAR EN CASO DE SER PERSONA JURÍDICA], **DECLARO BAJO JURAMENTO** que la siguiente información se sujeta a la verdad:

Nombre, Denominación o Razón Social :			
Domicilio Legal :			
RUC :	Teléfono(s) :		
MYPE ⁶³	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 servicios⁶⁴

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.

⁶³ 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.

⁶⁴ Consignar en el caso de procedimientos de selección por relación de ítems, cuando el monto del valor estimado del ítem no supere los doscientos mil Soles (S/ 200 000.00), cuando se haya optado por perfeccionar el contrato con una orden de servicios.

Importante

Cuando se trate de consorcios, la declaración jurada es la siguiente:

ANEXO N° 1

DECLARACIÓN JURADA DE DATOS DEL POSTOR

Señores

COMITÉ DE SELECCIÓN

CONCURSO PÚBLICO N° 001-2023-APN

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 ⁶⁵		Sí		No	
Correo electrónico :					

Datos del consorciado 2					
Nombre, Denominación o Razón Social :					
Domicilio Legal :					
RUC :		Teléfono(s) :			
MYPE ⁶⁶		Sí		No	
Correo electrónico :					

Datos del consorciado ...					
Nombre, Denominación o Razón Social :					
Domicilio Legal :					
RUC :		Teléfono(s) :			
MYPE ⁶⁷		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.

⁶⁵ 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.

⁶⁶ Ibídem.

⁶⁷ 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 servicios⁶⁸

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.

⁶⁸ Consignar en el caso de procedimientos de selección por relación de ítems, cuando el monto del valor estimado del ítem no supere los doscientos mil Soles (S/ 200 000.00), cuando se haya optado por perfeccionar el contrato con una orden de servicios.

ANEXO N° 2

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

Señores
COMITÉ DE SELECCIÓN
CONCURSO PÚBLICO N° 001-2023-APN
Presente.-

Mediante el presente el suscrito, postor y/o Representante Legal de [CONSIGNAR EN CASO DE SER PERSONA JURÍDICA], declaro bajo juramento:

- i. No haber incurrido y me obligo a no incurrir en actos de corrupción, así como a respetar el principio de integridad.
- ii. No tener impedimento para postular en el procedimiento de selección ni para contratar con el Estado, conforme al artículo 11 de la Ley de Contrataciones del Estado.
- iii. Conocer las sanciones contenidas en la Ley de Contrataciones del Estado y su Reglamento, así como las disposiciones aplicables de la Ley N° 27444, Ley del Procedimiento Administrativo General.
- iv. Participar en el presente proceso de contratación en forma independiente sin mediar consulta, comunicación, acuerdo, arreglo o convenio con ningún proveedor; y, conocer las disposiciones del Decreto Legislativo N° 1034, Decreto Legislativo que aprueba la Ley de Represión de Conductas Anticompetitivas.
- v. Conocer, aceptar y someterme a las bases, condiciones y reglas del procedimiento de selección.
- vi. Ser responsable de la veracidad de los documentos e información que presento en el presente procedimiento de selección.
- vii. Comprometerme a mantener la oferta presentada durante el procedimiento de selección y a perfeccionar el contrato, en caso de resultar favorecido con la buena pro.

[CONSIGNAR CIUDAD Y FECHA]

.....
**Firma, Nombres y Apellidos del postor o
Representante legal, según corresponda**

Importante

En el caso de consorcios, cada integrante debe presentar esta declaración jurada, salvo que sea presentada por el representante común del consorcio.

ANEXO N° 3

DECLARACIÓN JURADA DE CUMPLIMIENTO DE LOS TÉRMINOS DE REFERENCIA

Señores

COMITÉ DE SELECCIÓN

CONCURSO PÚBLICO N° 001-2023-APN

Presente.-

Es grato dirigirme a usted, para hacer de su conocimiento que luego de haber examinado las bases y demás documentos del procedimiento de la referencia y, conociendo todos los alcances y las condiciones detalladas en dichos documentos, el postor que suscribe ofrece el servicio de [CONSIGNAR OBJETO DE LA CONVOCATORIA], de conformidad con los Términos de Referencia que se indican en el numeral 3.1 del Capítulo III de la sección específica de las bases y los documentos del procedimiento.

[CONSIGNAR CIUDAD Y FECHA]

.....
**Firma, Nombres y Apellidos del postor o
Representante legal o común, según corresponda**

Importante

Adicionalmente, puede requerirse la presentación de documentación que acredite el cumplimiento de los términos de referencia, conforme a lo indicado en el acápite relacionado al contenido de las ofertas de la presente sección de las bases.

ANEXO N° 4

DECLARACIÓN JURADA DE PLAZO DE PRESTACIÓN DEL SERVICIO

Señores
COMITÉ DE SELECCIÓN
CONCURSO PÚBLICO N° 001-2023-APN
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 EN MESES] meses.

La implementación, instalación y puesta en producción de todos los servicios y sus componentes como parte del contrato no deberá exceder de los [CONSIGNAR EL PLAZO DE IMPLEMENTACION] días calendario.

[CONSIGNAR CIUDAD Y FECHA]

.....
Firma, Nombres y Apellidos del postor o
Representante legal o común, según corresponda

ANEXO N° 5

PROMESA DE CONSORCIO

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

Señores
COMITÉ DE SELECCIÓN
CONCURSO PÚBLICO N° 001-2023-APN
Presente.-

Los suscritos declaramos expresamente que hemos convenido en forma irrevocable, durante el lapso que dure el procedimiento de selección, para presentar una oferta conjunta al **CONCURSO PÚBLICO N° 001-2023-APN**.

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] [%]⁶⁹

[DESCRIBIR LAS OBLIGACIONES DEL CONSORCIADO 1]

2. OBLIGACIONES DE [NOMBRE, DENOMINACIÓN O RAZÓN SOCIAL DEL CONSORCIADO 2] [%]⁷⁰

[DESCRIBIR LAS OBLIGACIONES DEL CONSORCIADO 2]

TOTAL OBLIGACIONES 100%⁷¹

[CONSIGNAR CIUDAD Y FECHA]

⁶⁹ Consignar únicamente el porcentaje total de las obligaciones, el cual debe ser expresado en número entero, sin decimales.

⁷⁰ Consignar únicamente el porcentaje total de las obligaciones, el cual debe ser expresado en número entero, sin decimales.

⁷¹ Este porcentaje corresponde a la sumatoria de los porcentajes de las obligaciones de cada uno de los integrantes del consorcio.

.....
Consortiado 1
Nombres, apellidos y firma del Consortiado 1
o de su Representante Legal
Tipo y N° de Documento de Identidad

.....
Consortiado 2
Nombres, apellidos y firma del Consortiado 2
o de su Representante Legal
Tipo y N° de Documento de Identidad

Importante

De conformidad con el artículo 52 del Reglamento, las firmas de los integrantes del consorcio deben ser legalizadas.

ANEXO N° 6

PRECIO DE LA OFERTA

Señores
COMITÉ DE SELECCIÓN
CONCURSO PÚBLICO N° 001-2023-APN
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
Contratación del Servicio de Internet, Seguridad Perimetral, y Telefonía Fija para la Sede Central de la Autoridad Portuaria Nacional (APN) y Servicio de Enlace de Datos entre el Centro de Control de Comunicaciones y Respuesta a Emergencias (CCCRE) del Callao y la Sede Central	
TOTAL	

El precio de la oferta [CONSIGNAR LA MONEDA DE LA CONVOCATORIA] incluye todos los tributos, seguros, transporte, inspecciones, pruebas y, de ser el caso, los costos laborales conforme a la legislación vigente, así como cualquier otro concepto que pueda tener incidencia sobre el costo del servicio a contratar; excepto la de aquellos postores que gocen de alguna exoneración legal, no incluirán en el precio de su oferta los tributos respectivos.

[CONSIGNAR CIUDAD Y FECHA]

.....
Firma, Nombres y Apellidos del postor o
Representante legal o común, según corresponda

Importante

- *El postor debe consignar el precio total de la oferta, sin perjuicio que, de resultar favorecido con la buena pro, presente el detalle de precios unitarios para el perfeccionamiento del contrato.*
- *El postor que goce de alguna exoneración legal, debe indicar que su oferta no incluye el tributo materia de la exoneración, debiendo incluir el siguiente texto:*

Mi oferta no incluye [CONSIGNAR EL TRIBUTO MATERIA DE LA EXONERACIÓN]”.

ANEXO N° 8

EXPERIENCIA DEL POSTOR EN LA ESPECIALIDAD

Señores
COMITÉ DE SELECCIÓN
CONCURSO PÚBLICO N° 001-2023-APN
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 ⁷²	FECHA DE LA CONFORMIDAD DE SER EL CASO ⁷³	EXPERIENCIA PROVENIENTE ⁷⁴ DE:	MONEDA	IMPORTE ⁷⁵	TIPO DE CAMBIO VENTA ⁷⁶	MONTO FACTURADO ACUMULADO ⁷⁷
1										
2										
3										
4										

⁷² 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.

⁷³ 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.

⁷⁴ 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”*.

⁷⁵ Se refiere al monto del contrato ejecutado incluido adicionales y reducciones, de ser el caso.

⁷⁶ 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.

⁷⁷ 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 ⁷²	FECHA DE LA CONFORMIDAD DE SER EL CASO ⁷³	EXPERIENCIA PROVENIENTE ⁷⁴ DE:	MONEDA	IMPORTE ⁷⁵	TIPO DE CAMBIO VENTA ⁷⁶	MONTO FACTURADO ACUMULADO ⁷⁷
5										
6										
7										
8										
9										
10										
	...									
20										
TOTAL										

[CONSIGNAR CIUDAD Y FECHA]

.....
Firma, Nombres y Apellidos del postor o
Representante legal o común, según corresponda

ANEXO N° 9

DECLARACIÓN JURADA (NUMERAL 49.4 DEL ARTÍCULO 49 DEL REGLAMENTO)

Señores
COMITÉ DE SELECCIÓN
CONCURSO PÚBLICO N° 001-2023-APN
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/rmp/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° 10

**AUTORIZACIÓN DE NOTIFICACIÓN DE LA DECISIÓN DE LA ENTIDAD SOBRE LA
SOLICITUD DE AMPLIACIÓN DE PLAZO MEDIANTE MEDIOS ELECTRÓNICOS DE
COMUNICACIÓN**

(DOCUMENTO A PRESENTAR EN EL PERFECCIONAMIENTO DEL CONTRATO)

Señores
COMITÉ DE SELECCIÓN
CONCURSO PÚBLICO N° 001-2023-APN
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.