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

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

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

SIMBOLOGÍA UTILIZADA:

N°	Símbolo	Descripción
1	[ABC] / […….]	La información solicitada dentro de los corchetes sombreados debe ser completada por la Entidad durante la elaboración de las bases.
2	[ABC] / […….]	Es una indicación, o información que deberá ser completada por la Entidad con posterioridad al otorgamiento de la buena pro para el caso específico de la elaboración de la PROFORMA DEL CONTRATO; o por los proveedores, en el caso de los ANEXOS de la oferta.
3	**Importante** • *Abc*	Se refiere a consideraciones importantes a tener en cuenta por el comité de selección y por los proveedores.
4	***Advertencia*** • ***Abc***	Se refiere a advertencias a tener en cuenta por el comité de selección y por los proveedores.
5	**Importante para la Entidad** • *Xyz*	Se refiere a consideraciones importantes a tener en cuenta por el comité de selección y deben ser eliminadas una vez culminada la elaboración de las bases.

CARACTERÍSTICAS DEL DOCUMENTO:

Las bases estándar deben ser elaboradas en formato WORD, y deben tener las siguientes características:

N°	Características	Parámetros
1	Márgenes	Superior : 2.5 cm Inferior: 2.5 cm Izquierda: 2.5 cm Derecha: 2.5 cm
2	Fuente	Arial
3	Estilo de Fuente	Normal: Para el contenido en general Cursiva: Para el encabezado y pie de página Para las Consideraciones importantes (Ítem 3 del cuadro anterior)
4	Color de Fuente	Automático: Para el contenido en general Azul : Para las Consideraciones importantes (Ítem 3 del cuadro anterior)
5	Tamaño de Letra	16 : Para las dos primeras hojas de las Secciones General y Específica 11 : Para el nombre de los Capítulos. 10 : Para el cuerpo del documento en general 9 : Para el encabezado y pie de página Para el contenido de los cuadros, pudiendo variar, según la necesidad 8 : Para las Notas al pie
6	Alineación	Justificada: Para el contenido en general y notas al pie. Centrada : Para la primera página, los títulos de las Secciones y nombres de los Capítulos)
7	Interlineado	Sencillo
8	Espaciado	Anterior : 0 Posterior : 0
9	Subrayado	Para los nombres de las Secciones y para resaltar o hacer hincapié en algún concepto

INSTRUCCIONES DE USO:

1. *Una vez registrada la información solicitada dentro de los corchetes sombreados en gris, el texto deberá quedar en letra tamaño 10, con estilo normal, sin formato de negrita y sin sombrear.*

2. *La nota **IMPORTANTE** no puede ser modificada ni eliminada en la Sección General. En el caso de la Sección Específica debe seguirse la instrucción que se indica en dicha nota.*

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

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

BASES INTEGRADAS

CONCURSO PÚBLICO N.º 01-2025-SUNAFIL

PRIMERA CONVOCATORIA

CONTRATACIÓN DE SERVICIO DE ACCESO DEDICADO DE INTERNET DE BANDA ANCHA PARA LA SUNAFIL

DEBER DE COLABORACIÓN

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

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

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

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

SECCIÓN GENERAL

DISPOSICIONES COMUNES DEL PROCEDIMIENTO DE SELECCIÓN

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

CAPÍTULO I
ETAPAS DEL PROCEDIMIENTO DE SELECCIÓN

1.1. REFERENCIAS

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

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

1.2. CONVOCATORIA

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

1.3. REGISTRO DE PARTICIPANTES

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

Importante

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

1.4. FORMULACIÓN DE CONSULTAS Y OBSERVACIONES A LAS BASES

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

Importante

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

1.5. ABSOLUCIÓN DE CONSULTAS, OBSERVACIONES E INTEGRACIÓN DE BASES

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

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

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

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

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

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

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

1.7. FORMA DE PRESENTACIÓN DE OFERTAS

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

Las declaraciones juradas, formatos o formularios previstos en las bases que conforman la oferta deben estar debidamente firmados por el postor (firma manuscrita o digital, según la Ley Nº 27269, Ley de Firmas y Certificados Digitales[1]). Los demás documentos deben ser visados por el postor. En el caso de persona jurídica, por su representante legal, apoderado o mandatario designado para dicho fin y, en el caso de persona natural, por este o su apoderado. No se acepta el pegado de la imagen de una firma o visto. Las ofertas se presentan foliadas.

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

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

coincida con lo declarado a través del SEACE, prevalece la información declarada en los documentos escaneados.

- *No se tomarán en cuenta las ofertas que se presenten en físico a la Entidad.*

1.8. PRESENTACIÓN Y APERTURA DE OFERTAS

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

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

Importante

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

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

1.9. EVALUACIÓN DE LAS OFERTAS

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

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

1.10. CALIFICACIÓN DE OFERTAS

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

1.11. SUBSANACIÓN DE LAS OFERTAS

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

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

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

1.12. RECHAZO DE LAS OFERTAS

Previo al otorgamiento de la buena pro, el comité de selección revisa las ofertas económicas

que cumplen los requisitos de calificación, de conformidad con lo establecido para el rechazo de ofertas, previsto en el artículo 68 del Reglamento, de ser el caso.

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

1.13. OTORGAMIENTO DE LA BUENA PRO

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

1.14. CONSENTIMIENTO DE LA BUENA PRO

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

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

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

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

CAPÍTULO II
SOLUCIÓN DE CONTROVERSIAS DURANTE EL PROCEDIMIENTO DE SELECCIÓN

2.1. RECURSO DE APELACIÓN

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

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

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

Importante

- *Una vez otorgada la buena pro, el comité de selección, está en la obligación de permitir el acceso de los participantes y postores al expediente de contratación, salvo la información calificada como secreta, confidencial o reservada por la normativa de la materia, a más tardar dentro del día siguiente de haberse solicitado por escrito.*

  Luego de otorgada la buena pro no se da a conocer las ofertas cuyos requisitos de calificación no fueron analizados y revisados por el comité de selección.

- *A efectos de recoger la información de su interés, los postores pueden valerse de distintos medios, tales como: (i) la lectura y/o toma de apuntes, (ii) la captura y almacenamiento de imágenes, e incluso (iii) pueden solicitar copia de la documentación obrante en el expediente, siendo que, en este último caso, la Entidad deberá entregar dicha documentación en el menor tiempo posible, previo pago por tal concepto.*

- *El recurso de apelación se presenta ante la Mesa de Partes del Tribunal o ante las oficinas desconcentradas del OSCE.*

2.2. PLAZOS DE INTERPOSICIÓN DEL RECURSO DE APELACIÓN

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

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

CAPÍTULO III
DEL CONTRATO

3.1. PERFECCIONAMIENTO DEL CONTRATO

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

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

3.2. GARANTÍAS

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

3.2.1. GARANTÍA DE FIEL CUMPLIMIENTO

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

3.2.2. GARANTÍA DE FIEL CUMPLIMIENTO POR PRESTACIONES ACCESORIAS

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

Importante

- *En los contratos derivados de procedimientos de selección por relación de ítems, cuando el monto del ítem adjudicado o la sumatoria de los montos de los ítems adjudicados sea igual o menor a doscientos mil Soles (S/ 200,000.00), no corresponde presentar garantía de fiel cumplimiento de contrato ni garantía de fiel cumplimiento por prestaciones accesorias, conforme a lo dispuesto en el literal a) del artículo 152 del Reglamento.*

- *En los contratos periódicos de prestación de servicios en general que celebren las Entidades con las micro y pequeñas empresas, estas últimas pueden otorgar como garantía de fiel cumplimiento el diez por ciento (10%) del monto del contrato, porcentaje que es retenido por la Entidad durante la primera mitad del número total de pagos a realizarse, de forma prorrateada en cada pago, con cargo a ser devuelto a la finalización del mismo, conforme lo establecen los numerales 149.4 y 149.5 del artículo 149 del Reglamento y numeral 151.2 del artículo 151 del Reglamento.*

3.2.3. GARANTÍA POR ADELANTO

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

3.3. REQUISITOS DE LAS GARANTÍAS

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

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

Advertencia
Los funcionarios de las Entidades no deben aceptar garantías emitidas bajo condiciones distintas a las establecidas en el presente numeral, debiendo tener en cuenta lo siguiente: *1. La clasificadora de riesgo que asigna la clasificación a la empresa que emite la garantía debe encontrarse listada en el portal web de la SBS (http://www.sbs.gob.pe/sistema-financiero/clasificadoras-de-riesgo).* *2. Se debe identificar en la página web de la clasificadora de riesgo respectiva, cuál es la clasificación vigente de la empresa que emite la garantía, considerando la vigencia a la fecha de emisión de la garantía.* *3. Para fines de lo establecido en el artículo 148 del Reglamento, la clasificación de riesgo B, incluye las clasificaciones B+ y B.* *4. Si la empresa que otorga la garantía cuenta con más de una clasificación de riesgo emitida por distintas empresas listadas en el portal web de la SBS, bastará que en una de ellas cumpla con la clasificación mínima establecida en el Reglamento.* *En caso exista alguna duda sobre la clasificación de riesgo asignada a la empresa emisora de la garantía, se deberá consultar a la clasificadora de riesgos respectiva.* *De otro lado, además de cumplir con el requisito referido a la clasificación de riesgo, a efectos de verificar si la empresa emisora se encuentra autorizada por la SBS para emitir garantías, debe revisarse el portal web de dicha Entidad (http://www.sbs.gob.pe/sistema-financiero/relacion-de-empresas-que-se-encuentran-autorizadas-a-emitir-cartas-fianza).* *Los funcionarios competentes deben verificar la autenticidad de la garantía a través de los mecanismos establecidos (consulta web, teléfono u otros) por la empresa emisora.*

3.4. EJECUCIÓN DE GARANTÍAS

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

3.5. ADELANTOS

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

3.6. PENALIDADES

3.6.1. PENALIDAD POR MORA EN LA EJECUCIÓN DE LA PRESTACIÓN

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

3.6.2. OTRAS PENALIDADES

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

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

3.7. INCUMPLIMIENTO DEL CONTRATO

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

3.8. PAGOS

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

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

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

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

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

3.9. DISPOSICIONES FINALES

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

SECCIÓN ESPECÍFICA

CONDICIONES ESPECIALES DEL PROCEDIMIENTO DE SELECCIÓN

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

CAPÍTULO I
GENERALIDADES

1.1. ENTIDAD CONVOCANTE

Nombre	:	SUPERINTENDENCIA NACIONAL DE FISCALIZACION LABORAL
RUC N.º	:	20555195444
Domicilio legal	:	AV. SALAVERRY NRO. 655 (PISO 2 - MINISTERIO DE TRABAJO) JESUS MARIA – LIMA.
Teléfono:	:	013902800
Correo electrónico:	:	rbaez.uacp.sunafil@gmail.com; jpaez@sunafil.gob.pe, gestor_redes@sunafil.gob.pe

1.2. OBJETO DE LA CONVOCATORIA

El presente procedimiento de selección tiene por objeto la contratación del SERVICIO DE ACCESO DEDICADO DE INTERNET DE BANDA ANCHA PARA LA SUNAFIL.

1.3. EXPEDIENTE DE CONTRATACIÓN

El expediente de contratación fue aprobado mediante Formato Nro. 2 – solicitud y aprobación de expediente de contratación Nro. 08-2025-SUNAFIL/GG/OAD-AEC, el 27 de marzo de 2025.

1.4. FUENTE DE FINANCIAMIENTO

RECURSOS ORDINARIOS

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

1.5. SISTEMA DE CONTRATACIÓN

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

1.6. DISTRIBUCIÓN DE LA BUENA PRO

NO CORRESPONDE

1.7. ALCANCES DEL REQUERIMIENTO

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

1.8. PLAZO DE PRESTACIÓN DEL SERVICIO

Los servicios materia de la presente convocatoria se prestarán en el plazo de 1095 días calendarios (equivalente a 03 años), computados a partir del día siguiente de firmado el Acta de

Inicio.

Plazo de implementación:
El plazo para la ejecución de la implementación del proyecto, será de hasta noventa (90) días calendarios contados desde el día siguiente de la firma del contrato; según detalle:
• De hasta 85 días calendarios para Implementación del Servicio de Internet Dedicado, desde el día siguiente de la firma del contrato.
• De hasta 90 días calendarios para la entrega de documentación solicitada como entregable final de implementación, desde el día siguiente de la firma del contrato.

En concordancia con lo establecido en el expediente de contratación.

1.9. COSTO DE REPRODUCCIÓN Y ENTREGA DE BASES

Los participantes registrados tienen el derecho de recabar un ejemplar de las bases de forma gratuita, para cuyo efecto deben acercarse a la Unidad de Abastecimiento y control Patrimonial de la SUNAFIL.

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° 30225 - Ley de Contrataciones del Estado.
- Texto Único Ordenado de la Ley N° 30225 aprobado mediante Decreto Supremo N° 082- 2019-EF.
- Ley N° 32185 – Ley del Presupuesto del Sector Publico para el año fiscal 2025.
- Ley N° 32186 - Ley del Equilibrio Financiero del Presupuesto del Sector Público para el Año Fiscal 2025.
- Ley de Endeudamiento del Sector Publico para el año Fiscal 2025.
- Ley N° 27444 Ley del Procedimiento Administrativo General.
- Decreto Legislativo N° 1444, que modifica la Ley N° 30225 (vigente desde el 30 de enero de 2019).
- Decreto Supremo N° 344-2018-EF, que aprueba el Reglamento de la Ley N° 30225 Ley de Contrataciones del Estado y modificatorias vigentes (Decreto Supremo N° 234-2022- EF).
- Texto Único Ordenado de la Ley N° 27806, Ley de Transparencia y de Acceso a la Información Pública, aprobado por Decreto Supremo N° 043-2003-PCM.
- Ley N° 27806 – Ley de Transparencia y de Acceso a la Información Pública.
- Código Civil.
- Directivas y Opiniones del OSCE.
- Directiva N°001-2019-OSCE/CD – Bases y Solicitud de Expresión de Interés Estándar para los Procedimientos de Selección a Convocar en el Marco de la Ley N°30225 y sus modificatorias.
- Cualquier otra disposición legal vigente que permita desarrollar el objeto de la convocatoria, que no contravenga lo regulado por la Ley de Contrataciones del Estado.

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

CAPÍTULO II
DEL PROCEDIMIENTO DE SELECCIÓN

2.1. CALENDARIO DEL PROCEDIMIENTO DE SELECCIÓN

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

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

2.2. CONTENIDO DE LAS OFERTAS

La oferta contendrá, además de un índice de documentos[2], la siguiente documentación:

2.2.1. Documentación de presentación obligatoria

2.2.1.1. Documentos para la admisión de la oferta

a) Declaración jurada de datos del postor. (**Anexo Nº 1)**

b) Documento que acredite la representación de quien suscribe la oferta.

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

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

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

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

c) Declaración jurada de acuerdo con el literal b) del artículo 52 del Reglamento. **(Anexo Nº 2)**

d) Declaración jurada de cumplimiento de los Términos de Referencia contenidos en el numeral 3.1 del Capítulo III de la presente sección. (**Anexo Nº 3**)

---

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

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

e) Carta del fabricante que acredite que la solución de administración y control de ancho de banda debe ser de propósito especifico y no una funcionalidad dentro de alguna solución de seguridad o infraestructura IT (ej: firewall, UTM, NGFW, balanceadores, entre otros), como también debe ser una solución totalmente integrada y soportada directamente por el mismo fabricante a fin de garantizar un soporte integro, ***de acuerdo al literal A del numeral 5.2 de los TDR***

f) Carta del fabricante adjuntando la documentación publica de internet que la respalde, respecto a que los equipos no estén en etapa de obsolescencia o que hayan publicado y/o anunciado el "End-of-life" y/o "End-of-Support", o dejen de ser fabricadas, comercializadas y/o soportadas durante los 05 años siguientes a la instalación de los equipos a ser propuestos, ***de acuerdo al literal C (Solución de Seguridad Next Generation Firewall (NGFW), del numeral 5.2 (Funcionalidades requeridas) de los TDR.***

g) Documento (se aceptara declaración jurada donde se indique página web o link del fabricante)[4] que acredite que los sistemas operativos y/o firmware que operan en los equipos de seguridad firewall ofertados, no deberán tener más de diez (10) vulnerabilidades (CVE) anunciadas y/o publicadas, acumuladas en sus diferentes versiones durante los últimos 12 meses anteriores a la fecha de presentación de la oferta, ***de acuerdo al literal C (Solución de Seguridad Next Generation Firewall (NGFW), del numeral 5.2 (Funcionalidades requeridas) de los TDR.***

h) Documentación técnica (datasheet) y/o manuales y/o bochures emitidos públicamente por el propio fabricante de la solución de firewall, adjuntando el documento y enlace (URL) público de Internet del propio fabricante que lo sustente que acredite el cumplimiento referido a las capacidades de hardware y/o de rendimiento solicitadas, No se aceptarán cartas de fabricante y/o representantes locales, como un fundamento para el cumplimiento de estos requerimientos solicitados, de acuerdo al literal C (Solución de Seguridad Next Generation Firewall (NGFW), del numeral 5.2 (Funcionalidades requeridas) de los TDR.

i) Documentación que acredite al postor tener la autorización del Ministerio de Transportes y Comunicaciones para la prestación del servicio en la modalidad de Internet Servís o Proveedor (ISP), con cobertura a nivel nacional, acreditado con Copia de Autorización del MTC para la prestación del servicio. También se aceptará una copia del link que el MTC tiene publicado de REGISTRO PARA SERVICIO DE VALOR AÑADIDO en la Plataforma Digital Única del Estado Peruano y/o un Oficio emitido por el MTC, el cual precisan las Concesiones y/o Títulos Habilitantes para la prestación de Servicios Públicos de Telecomunicaciones, con las que cuenta el Postor y/o copia simple del Certificado de Registro de Empresas Prestadoras de Servicios de Valor Añadido emitido por el Ministerio de Trasporte y Comunicaciones.

j) Declaración jurada de plazo de prestación del servicio. **(Anexo Nº 4)**[5]

k) Promesa de consorcio con firmas legalizadas, de ser el caso, en la que se consigne los integrantes, el representante común, el domicilio común y las obligaciones a las que se compromete cada uno de los integrantes del consorcio así como el porcentaje equivalente a dichas obligaciones. (**Anexo Nº 5**)

l) El precio de la oferta en SOLES, Adjuntar obligatoriamente el **Anexo Nº 6.**

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

m) Declaración jurada del nivel de certificación y dirección del centro de datos, así como copia del certificado RATED II del centro de datos donde se encuentran los

[4] CONSULTA N° 54 DE ENTEL PERU S.A.

[5] 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.

componentes del servicio de Ciberdefensa.[6]

n) Declaración jurada indicando el nivel de certificación y los procesos, así como la copia del certificado del CyberSOC en ISO 27001.[7]

o) Se acreditará con un certificado emitido por una empresa consultora externa (certificadora en infraestructura) y/o un certificado emitido por una empresa especialista en servicios TI y/o infraestructura y/u otro documento que acredite la operación e infraestructura del NOC & SOC.[8]

p) Carta de fabricante de la plataforma AntiDDoS donde indique que el postor cuenta con la infraestructura para brindar el servicio, así como el cumplimiento técnico.

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

Advertencia

De acuerdo con el artículo 4 del Decreto Legislativo N° 1246, las Entidades están prohibidas de exigir a los administrados o usuarios la información que puedan obtener directamente mediante la interoperabilidad a que se refieren los artículos 2 y 3 de dicho Decreto Legislativo. En esa medida, si la Entidad es usuaria de la Plataforma de Interoperabilidad del Estado – PIDE[9] y siempre que el servicio web se encuentre activo en el Catálogo de Servicios de dicha plataforma, no corresponderá exigir los documentos previstos en los literales e) y f).

[6] CONSULTA N° 43 DE ENTEL PERU S.A.
[7] CONSULTA N° 45 y 56 DE ENTEL PERU S.A.
[8] CONSULTA N° 61 DE ENTEL PERU S.A.
[9] 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/

g) Domicilio para efectos de la notificación durante la ejecución del contrato.
h) Autorización de notificación de la decisión de la Entidad sobre la solicitud de ampliación de plazo mediante medios electrónicos de comunicación [10] (**Anexo N° 12**).
i) Detalle de los precios unitarios del precio ofertado[11].
j) Estructura de costos[12].
k) Documento donde acredite ser miembro activo del NAP PERÚ.
l) Documento en el que deberá demostrar tener acceso a (02) salidas Internacional (10 Gbps como mínimo) y con la finalidad de tener redundancia en las salidas internacionales.
m) Documento en el que deberá demostrar contar con dos (02) operadores TIER1 internacionales distintos con rutas físicas diferentes con los que deberá tener conexión directa a través de los enlaces de fibra óptica. Con ello se busca garantizar la continuidad del acceso a Internet requerido.
n) Documento donde deberá demostrar las ubicaciones físicas distintas de los Servidores de Nombres de Dominio (DNS) redundantes o las direcciones IP de los Servidores de Nombres de Dominio (DNS) redundantes ubicados en el centro de datos del proveedor bajo un esquema de alta disponibilidad.
o) Documentación donde deberá remitir las direcciones de sus nodos y/o PoP de los enlaces principal y de contingencia, debiendo demostrar que las conexiones de los enlaces para la sede central vienen de rutas diferentes.
p) Documentación donde deberá brindar una tabla de escalamiento para la atención de averías, el cual deberá indicar los números telefónicos de los responsables.
q) Documento con la relación de la marca y modelo de los equipos y soluciones que forman parte del servicio solicitado, sean si estas soluciones estén on-premise o en la nube, de acuerdo al siguiente formato:

Solución	Marca	Modelo	Tipo de Solución on-premise o nube	N° de Folio presentado por el Postor donde muestre la relación de las soluciones ofertadas
Equipamiento de Enrutamiento para el servicio de Internet				Folio N°….
Solución AntiDDoS				Folio N°….
Optimizador de Ancho de Banda				Folio N°….
Solución Firewalls				Folio N°….
Solución de Monitoreo				Folio N°….

r) Documentación donde se deberá demostrar de forma foliada las validaciones de las características esenciales para la solución optimizador de ancho de banda, mediante la presentación de hojas técnicas y/o folletos y/o catálogos y/o datasheet y/o link del fabricante y/o carta de fabricante (El postor ganador deberá asegurar que con dicha carta de fabricante se demuestre y/o valide cada característica esencial solicitada), donde se precise el cumplimiento técnico; para la solución indicada a nivel hardware y software en el idioma original

s) Para el servicio de Ethical Hacking, **deberá acreditar con documentación** del especialista ingeniero colegiado de sistemas, telecomunicaciones o electrónica con 5 años de experiencia

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

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

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

realizando servicios de Ethical Hacking y deberá contar con Certificación vigente ISO/IEC 27001 Senior Lead Implementer, ISO/IEC 27032 Senior Lead Cibersecurity Manager y Certified Ethical Hacker.

t) Acreditar el perfil del personal respecto las certificaciones:

Jefe de Proyecto (Supervisor de servicio)

- Certificado de PMP y/o programa especializado en dirección y gestión de las Telecomunicaciones y/o Diplomado de Gestión de Proyectos y/o Gerencia de Proyectos y Calidad y/o diploma de especialización en gestión de proyectos de telecomunicaciones con un mínimo de 90 horas.

Personal técnico-I

- Certificado en la solución de equipos routers propuestos por el postor para la instalación del servicio de internet. La certificación debe ser emitida por parte del fabricante de la solución ofertada. También se aceptarán cursos de equipamiento de comunicaciones y/o de enrutamiento de red de comunicaciones de al menos 12 horas en total, debiendo presentar los certificados correspondientes.

Personal técnico-II

- Certificado en la solución de administración de Ancho de Banda. El certificado debe ser emitida por parte del fabricante de la solución ofertada.
- Certificado en la solución de firewalls. El certificado debe ser emitida por parte del fabricante de la solución ofertada.

u) Copia del certificado del personal que deberá estar relacionado con la solución de monitoreo.[13]

v) Declaración jurada indicando el link de la Plataforma Online y la Descripción del Curso o Programa.[14]

Importante

- *En caso que el postor ganador de la buena pro sea un consorcio, las garantías que presente este para el perfeccionamiento del contrato, así como durante la ejecución contractual, de ser el caso, además de cumplir con las condiciones establecidas en el artículo 33 de la Ley y el artículo 148 del Reglamento, deben consignar expresamente el nombre completo o la denominación o razón social de los integrantes del consorcio, en calidad de garantizados, de lo contrario no podrán ser aceptadas por las Entidades. No se cumple el requisito antes indicado si se consigna únicamente la denominación del consorcio, conforme lo dispuesto en la Directiva "Participación de Proveedores en Consorcio en las Contrataciones del Estado".*

- *En los contratos periódicos de prestación de servicios en general que celebren las Entidades con las micro y pequeñas empresas, estas últimas pueden otorgar como garantía de fiel cumplimiento el diez por ciento (10%) del monto del contrato, porcentaje que es retenido por la Entidad durante la primera mitad del número total de pagos a realizarse, de forma prorrateada en cada pago, con cargo a ser devuelto a la finalización del mismo, conforme lo establece el numeral 149.4 del artículo 149 del Reglamento y numeral 151.2 del artículo 151 del Reglamento. Para dicho efecto los postores deben encontrarse registrados en el REMYPE, consignando en la Declaración Jurada de Datos del Postor (Anexo N° 1) o en la solicitud de retención de la garantía durante el perfeccionamiento del contrato, que tienen la condición de MYPE, lo cual será verificado por la Entidad en el link http://www2.trabajo.gob.pe/servicios-en-linea-2-2 opción consulta de empresas acreditadas en el REMYPE.*

- *En los contratos derivados de procedimientos de selección por relación de ítems, cuando el monto del ítem adjudicado o la sumatoria de los montos de los ítems adjudicados sea igual o menor a doscientos mil Soles (S/ 200,000.00), no corresponde presentar garantía de fiel cumplimiento de contrato ni garantía de fiel cumplimiento por prestaciones accesorias, conforme a lo dispuesto en el literal a) del artículo 152 del Reglamento.*

[13] CONSULTA N° 41 DE ENTEL PERU S.A.
[14] CONSULTA N° 49 y 50 ENTEL PERU S.A.

Importante

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

- *De conformidad con el Reglamento Consular del Perú aprobado mediante Decreto Supremo N° 076-2005-RE para que los documentos públicos y privados extendidos en el exterior tengan validez en el Perú, deben estar legalizados por los funcionarios consulares peruanos y refrendados por el Ministerio de Relaciones Exteriores del Perú, salvo que se trate de documentos públicos emitidos en países que formen parte del Convenio de la Apostilla, en cuyo caso bastará con que estos cuenten con la Apostilla de la Haya[15].*

- *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 Avenida Salaverry N°655 Jesús María – Piso 1 o en mesa de partes virtual al enlace https://aplicativosweb6.sunafil.gob.pe/si.mesaVirtual/, en horario de 8:30 horas a 16:30 horas.
De corresponder presentación de Carta Fianza, será de manera presencial en la dirección antes señalada.

2.5. FORMA DE PAGO

La Entidad realizará el pago de la contraprestación pactada a favor del contratista en de forma periódica en cuotas mensuales, cuyo porcentaje de pago serán en partes iguales en función al monto del contrato, previa conformidad de la Oficina de Tecnologías de la Información y Comunicaciones, para lo cual el contratista presentará mensualmente un informe del servicio integral dentro de los diez (10) primeros días calendario del siguiente periodo de la prestación de servicio en ejecución.

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

- Informe del funcionario responsable de la Oficina de Tecnologías de la Información y Comunicaciones emitiendo la conformidad de la prestación efectuada, previa entrega, por parte del contratista, de un informe mensual del servicio integral, el cual debe ser entregado dentro de los diez (10) primero días calendarios del siguiente periodo de la prestación de servicio en ejecución.
- Comprobante de pago.
- Entregables de acuerdo al detalle señalado en el numeral 6.1.2 de los términos de referencia.

Los documentos se entregarán en mesa de partes virtual de SUNAFIL sito en URL: https://aplicativosweb6.sunafil.gob.pe/si.mesaVirtual/ o Mesa de Partes Presencial ubicada en Av. Salaverry 655 – 4to piso, Jesús María, Lima, en el horario de 8:30 am a 16:30 horas. Asimismo, los entregables serán necesarios para la conformidad técnica.

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

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.

PERÚ | Superintendencia Nacional de Fiscalización Laboral | Gerencia General | Oficina de Tecnologías de la Información y Comunicaciones

"Decenio de la Igualdad de oportunidades para mujeres y hombres"
"Año de la recuperación y consolidación de la economía peruana"

TÉRMINOS DE REFERENCIA

SERVICIO DE ACCESO DEDICADO DE INTERNET DE BANDA ANCHA PARA SUNAFIL

I. AREA USUARIA

Oficina de Tecnologías de la Información y Comunicaciones (OTIC) de la Superintendencia Nacional de Fiscalización Laboral (SUNAFIL).

II. FINALIDAD PUBLICA

Garantizar a la Superintendencia Nacional de Fiscalización Laboral (SUNAFIL) un servicio de internet dedicado y simétrico, que centralice eficientemente la interconexión de sus sedes remotas a nivel nacional, incluidas las Intendencias Regionales (IRE) y las Plataformas de Inspección de Trabajo (PIT), mediante distribución de internet a través de fibra óptica. Esto permitirá optimizar las actividades de los usuarios institucionales y fortalecer la coordinación operativa, contribuyendo a una toma de decisiones más ágil y efectiva.

Asimismo, este servicio deberá contar con seguridad gestionada basada en tecnología Next Generation Firewall (NGFW), garantizando una conexión confiable, segura y de alta disponibilidad, con acceso continuo y eficiente a sistemas y aplicaciones web, así como su publicación en internet. De esta manera, se potenciará la productividad institucional y se facilitará el cumplimiento de los objetivos estratégicos y operativos de SUNAFIL, mejorando el servicio de fiscalización y promoción laboral en beneficio de la ciudadanía.

III. OBJETIVOS:

3.1. Objetivo General:

Contratar un servicio de internet dedicado y simétrico, con distribución mediante fibra óptica y seguridad gestionada basada en tecnología Next Generation Firewall (NGFW), centralizado en la sede principal de SUNAFIL, que permita la interconexión eficiente y segura de las Intendencias Regionales (IRE) y las Plataformas de Inspección de Trabajo (PIT) a nivel nacional. Este servicio debe garantizar alta disponibilidad, confiabilidad y seguridad en el intercambio de información, optimizando el acceso y uso de servicios digitales necesarios para el cumplimiento de las funciones institucionales.

3.2. Objetivo específico:

- ✓ Garantizar el acceso continuo, confiable y seguro a internet en la Sede Central y en las Intendencias Regionales (IRE) y Plataformas de Inspección de Trabajo (PIT), mediante un ancho de banda dedicado y simétrico, distribuido a través de fibra óptica y protegido con tecnología Next Generation Firewall (NGFW).
- ✓ Asegurar la interconexión eficiente y segura de las sedes remotas con los sistemas institucionales centralizados, optimizando el acceso a servicios

SUNAFIL Firmado digitalmente por: RUITON TORRES Erick Ciro FAU 20555195444 soft Motivo: Doy V° B° Fecha: 20/05/2025 14:53:53-0500
SUNAFIL Firmado digitalmente por PAEZ MARTINEZ Jose Antonio FAU 20555195444 soft Fecha: 2025.05.20 15:05:17 -05'00'
SUNAFIL Firmado digitalmente por TUBILLAS MONTOYA Martin Eloy FAU 20555195444 soft Fecha: 2025.05.20 16:06:06 -05'00'

digitales esenciales para el desempeño de funciones operativas y estratégicas.

- ✓ Garantizar la disponibilidad y estabilidad de la infraestructura digital para la publicación de servicios informáticos y aplicaciones web, asegurando un soporte adecuado a las actividades institucionales en beneficio de la ciudadanía.

IV. PLAN OPERATIVO INSTITUCIONAL (POI)

Tarea del POI: AOI00151000966-Gestión de los servicios TIC´s.

V. DESCRIPCIÓN DEL SERVICIO:

- Se requiere contratar un servicio de internet dedicado y simétrico, centralizado en la Sede Central de SUNAFIL, que permita la interconexión eficiente y segura con todas las Intendencias Regionales (IRE) y Plataformas de Inspección de Trabajo (PIT) a nivel nacional, utilizando distribución mediante fibra óptica y seguridad gestionada basada en tecnología Next Generation Firewall (NGFW).
- En la Sede Central (Cabecera), se deben implementar:
  - ✓ 2 enlaces de internet de 1340 Mbps configurados en modo Activo-Pasivo, garantizando alta disponibilidad, continuidad operativa y conmutación automática ante fallas.
  - ✓ La interconexión entre la Sede Central (Cabecera) y las Sedes Remotas (IRE y PIT) también deberá estar en alta disponibilidad, utilizando 2 enlaces redundantes (un enlace principal y un enlace de contingencia) configurados en modo Activo-Pasivo, asegurando conmutación automática y protección avanzada mediante NGFW.
- Respecto a la alta disponibilidad de los firewalls (NGFW) se precisa que se refiere al respaldo de los equipos firewalls, por lo que podría tener una de las siguientes configuraciones: (01) equipo Firewall y un (01) equipo Firewall spare; o (01) equipo Firewall Activo y un (01) equipo Firewall Pasivo; o (01) equipo Firewall Activo y un (01) equipo Firewall Activo, los cuales estarán instalados en el Datacenter de SUNAFIL, tal que garanticen la disponibilidad mínima del servicio requerido.[1]
- Para la interconexión de datos entre la Sede Central (Cabecera) y las Sedes Remotas (IRE y PIT), se utilizará un único enlace de fibra óptica por sede remota, conectado a la Cabecera en la Sede Central. Esto garantizará un flujo de información eficiente, seguro y confiable, con inspección de tráfico en tiempo real mediante NGFW.
- Las Sedes Remotas (IRE y PIT) contarán con un solo enlace de fibra óptica cada una, sin redundancia local, garantizando un acceso continuo y eficiente a internet y a los sistemas centralizados en la Sede Central (Cabecera).
- La distribución de internet en las sedes remotas se realizará a través de fibra óptica, garantizando baja latencia y alta disponibilidad en la interconexión de datos, utilizando tecnología de enrutamiento seguro y administración centralizada.
- La cantidad específica de ancho de banda requerida para cada Sede Regional

[1] Por absolución de consulta Nº 01 de la empresa NEXTNET S.A.C.

se detalla a continuación:

Tabla Nº 01				
ITEM	**SEDE CENTRAL/IRE/PIT**	**DIRECCION**	**ANCHO DE BANDA**	**SERVICIO**
1	**Sede Central INTERNET**	Av. Salaverry 655, Jesús María, Lima	1340 Mbps	INTERNET
	Sede Central (cabecera) donde se conectarán todas las sedes		1000 Mbps	DATOS
2	Intendencia Regional de Amazonas	Jr. Amazonas 570 – Ciudad de Chachapoyas	20 Mbps	DATOS
3	Intendencia Regional de Áncash	Av. Francisco Bolognesi N° 109, Ciudad de Chimbote, Provincia del Santa, Región Ancash.	40 Mbps	DATOS
4	Intendencia Regional de Apurímac	Jirón Puno 605, Distrito de Abancay, Provincia de Abancay, Región de Apurímac	20 Mbps	DATOS
5	Intendencia Regional de Arequipa	Calle Mariano Melgar 623, Urb. La Libertad, Distrito de Cerro Colorado, Arequipa	60 Mbps	DATOS
6	Intendencia Regional de Ayacucho	Urb. Aprovisa Mz. D Lt. 1, Distrito de	30 Mbps	DATOS
7	Intendencia Regional de Cajamarca	Jr. Silva Santisteban N° 183, Distrito y Provincia de Cajamarca. Departamento de Cajamarca	30 Mbps	DATOS
8	Intendencia Regional de Callao	Av. Sáenz Peña 214 - Callao	45 Mbps	DATOS
9	Intendencia Regional de Cusco	Av. Camino Real 100, Distrito de Cusco	45 Mbps	DATOS
10	Intendencia Regional de Huancavelica	Malecón Virgen de la Candelaria 175 - San Cristóbal, Ciudad de Huancavelica.	20 Mbps	DATOS
11	Intendencia Regional de Huánuco	Jr. Huallayco N° 1326 - 1328, Distrito y Provincia de Huánuco	30 Mbps	DATOS
12	Intendencia Regional de Ica	Av. José Matías Manzanilla N° 106 y Calle Lambayeque N° 117 y 119 – Ica	40 Mbps	DATOS

13	Intendencia Regional de Junín	Jr. Arequipa N° 1888 distrito de El Tambo, Huancayo - Junín	40 Mbps	DATOS
14	Intendencia Regional de La Libertad	Jr. Orbegoso 624 - 628 - Distrito y Provincia de Trujillo - La Libertad	60 Mbps	DATOS
15	Intendencia Regional de Lambayeque	Calle Abtao N° 130 Urbanización Santa Victoria, Provincia Chiclayo, departamento de Lambayeque	50 Mbps	DATOS
16	Intendencia Regional de Lima Provincias	Jr. San Román 420, Huacho	35 Mbps	DATOS
17	Intendencia Regional de Loreto	Jr. La Condamine N°173 Distrito de Iquitos, Provincia de Maynas. Departamento de Loreto	20 Mbps	DATOS
18	Intendencia Regional de Madre de Dios	Av. Lambayeque Mz. 3Y - Lote 5-A2, 656-Tambopata, Tambopata-Madre de Dios	15 Mbps	DATOS
19	Intendencia Regional de Moquegua	Av. Andrés Avelino Cáceres L-5. Distrito y Provincia Mariscal Nieto, Dpto. de Moquegua	30 Mbps	DATOS
20	Intendencia Regional de Pasco	Av. Los Incas 236 Urb. San Juan, Yanacancha, Cerro de Pasco	20 Mbps	DATOS
21	Intendencia Regional de Piura	Calle las Acacias Mz D Lt. 9, Urb 4 de enero - Ex Estadio. Piura	50 Mbps	DATOS
22	Intendencia Regional de Puno	Jr. 4 de noviembre, N° 514, Barrio San Martín – Puno	30 Mbps	DATOS
23	Intendencia Regional de San Martín	Calle Antonio Raymondi 519-521 Tarapoto, Provincia San Martin, Región San Martin	30 Mbps	DATOS
24	Intendencia Regional de Tacna	Av. 2 de mayo N° 81B, Dpto. Tacna, Prov. Tacna Región Tacna.	25 Mbps	DATOS
25	Intendencia Regional de Tumbes	Calle José Gálvez N° 225, ciudad de Tumbes.	25 Mbps	DATOS

26	Intendencia Regional de Ucayali	Jr. Víctor Montalvo 855 Mz 238-A Lote 19 Callería, ciudad de Pucallpa, provincia coronel Portillo, Ucayali	25 Mbps	DATOS
27	Intendencia de Lima Metropolitana – Sede Lima Norte	Av. Pacifico N° 563-567-569-Independencia - Lima	45 Mbps	DATOS
28	Intendencia de Lima Metropolitana – Sede Lima Sur	Jr. José María Vílchez 518 Mz 3 Lote 1, zona B San Juan de Miraflores	40 Mbps	DATOS
29	Intendencia de Lima Metropolitana – Sede Arenales	Av. Arenales N°815, Santa Beatriz, Lima	80 Mbps	DATOS

Este esquema de distribución de internet y seguridad gestionada con NGFW garantizará un acceso continuo, confiable y seguro a los sistemas y aplicaciones web centralizadas, optimizando el uso de servicios digitales para el cumplimiento de las funciones operativas y estratégicas de SUNAFIL

5.1. Característica de la contratación:

El servicio de Internet para la Sede Central deberá cumplir con las siguientes especificaciones:

5.1.1. Provisión del Servicio

- **Enlaces Dedicados y Simétricos**:
  Se requiere la provisión de dos (02) enlaces dedicados de Internet simétrico de 1340 Mbps cada uno, configurados en modo Activo-Pasivo, donde:
  - ✓ Uno será el enlace principal y el otro funcionará como contingencia para garantizar alta disponibilidad y continuidad operativa.
  - ✓ Se deberá asegurar la conmutación automática ante fallas en el enlace principal, minimizando la interrupción del servicio.
- **Overbooking 1:1:**
  El servicio deberá asegurar un Overbooking 1:1 para el tráfico nacional e internacional, aplicable a todo el enlace, incluyendo:
  - ✓ El tramo local y la salida internacional, garantizando la misma capacidad de ancho de banda en ambas direcciones (carga y descarga).
- **Escalabilidad:**
  Se debe permitir un crecimiento mínimo del 50% del ancho de banda contratado, garantizando la escalabilidad para futuros requerimientos de SUNAFIL.

5.1.2. Calidad y Disponibilidad

- **Disponibilidad del Servicio:**
  El servicio de Internet deberá garantizar una disponibilidad mínima

del 99.9%, medida mensualmente, asegurando alta continuidad operativa.

- ✓ En caso de falla del enlace principal, la activación del enlace de contingencia no se considerará como interrupción del servicio.

- **Calidad de la Comunicación:**
  Ambos enlaces de Internet deberán mantener una calidad óptima para la transmisión de voz, datos y video, garantizando:
  - ✓ Baja latencia, estabilidad en la comunicación y mínima fluctuación en el ancho de banda.
- **Confiabilidad y Continuidad del Servicio:**
  Se debe asegurar la confiabilidad y continuidad del servicio en todas las sedes conectadas, permitiendo el funcionamiento eficiente de las operaciones institucionales de SUNAFIL, incluyendo:
  - ✓ Acceso continuo a sistemas y aplicaciones web.
  - ✓ Interconexión eficiente y segura entre la Sede Central (Cabecera) y las Sedes Remotas (IRE y PIT).

5.1.3. Independencia de Rutas

1) Enlace de Internet Principal:

- Ingreso: Por la Av. Salaverry - Jr. Francisco de Zela, garantizando independencia de rutas físicas.
- Características Técnicas:
  - **Velocidad:** Enlace dedicado de 1340 Mbps simétrico.
  - **Medio:** Fibra óptica, asegurando estabilidad y alta capacidad de transmisión.
  - **Capacidad de Ampliación:** Se permite hasta un 50% de incremento temporal del ancho de banda para eventos especiales, previa solicitud y acuerdo con el proveedor.
- Estas ampliaciones podrán solicitarse **hasta dos (02) veces al año**, con una duración máxima de **24 horas por evento**, sin costo adicional. Las solicitudes serán gestionadas a través del **centro de atención del proveedor**, exclusivamente por **personal técnico de la OTIC** registrado previamente.

2) Enlace de Internet Contingencia:

- **Ingreso**: Por el Jr. Pablo Bermúdez, garantizando independencia de rutas respecto al enlace principal.
- **Características Técnicas:**
  - **Velocidad:** Enlace dedicado de 1340 Mbps simétrico, con velocidad constante.
  - **Medio:** Fibra óptica, asegurando alta estabilidad y confiabilidad en la transmisión de datos.

3) Consideraciones Generales

- Independencia de Rutas: Ambos enlaces deben cumplir con las mismas características técnicas y garantizar independencia de rutas, evitando puntos de fallo comunes.

a) Equipos y Configuración

- Modo de Operación: Los enlaces serán configurados en modo Activo/Standby, conectados a routers distintos (uno para cada enlace), ambos de la misma marca y modelo para asegurar compatibilidad y uniformidad.
- Alta Disponibilidad: Se incluirán dos (02) switches de acceso a Internet para garantizar alta disponibilidad y redundancia.
- Especificaciones de los Equipos:
  - Nuevos y sin uso previo, garantizando su integridad y durabilidad.
  - Tecnología vigente, adecuada para soportar las exigencias del servicio.
  - Capacidad suficiente para manejar el ancho de banda contratad.
- Administración de Equipos: La administración y mantenimiento de los routers y switches serán responsabilidad del contratista.

b) Equipamiento y Materiales

- **Provisión Integral**: El contratista deberá proporcionar todo el equipamiento necesario para la instalación, incluyendo:
  - Interfaces, conectores, cables y demás componentes requeridos para la interconexión con los equipos de la entidad.

c) Direccionamiento IP y Protocolos

- **Asignación de Direcciones IP:**
  - 64 direcciones IP públicas fijas IPv4, que incluyan dirección de red, broadcast y puerta de enlace.
  - 64 direcciones IP públicas fijas IPv6, como mínimo, para garantizar compatibilidad con tecnologías actuales y futura.

- **Protocolos de Comunicación:**
  - No se impondrán restricciones en el uso de protocolos, permitiendo el funcionamiento de:
    - Videoconferencia, video, telefonía IP, internet bajo demanda, almacenamiento en la nube, túneles VPN, entre otros.

d) Registros DNS

- **Gestión de DNS:**
  - El contratista deberá habilitar y gestionar los registros DNS de los dominios y subdominios solicitados por SUNAFIL en su servidor DNS, asegurando su accesibilidad y disponibilidad.

e) Responsabilidades de la Entidad

- **SUNAFIL** proporcionará los siguientes recursos para la implementación:
  - Toma corriente y energía eléctrica estabilizada para los equipos contratados.

- Espacio en el gabinete para la instalación del hardware.
- Puerto en el equipo firewall de la entidad para la interconexión segura.

f) Monitoreo y Gestión

- **Software de Monitoreo:**
  - El contratista deberá proporcionar un software de monitoreo para los routers que permita supervisar en tiempo real:
    - CPU, memoria, throughput, tráfico de red, disponibilidad, tiempos de respuesta y pérdida de paquetes.
  - Este software podrá residir en la plataforma de red del contratista y deberá ser accesible vía web, mediante credenciales seguras proporcionadas a SUNAFIL.

5.2. Equipamiento de Gestión y Seguridad de Internet:

A. Solución de Administración y Control de Ancho de Banda:

El contratista deberá proporcionar un servicio de Administración de Ancho de Banda para la Sede Central de SUNAFIL, sin costo adicional, mediante un equipo dedicado conectado directamente a los enlaces de Internet antes del Next Generation Firewall (NGFW). Este equipo clasificará y priorizará el tráfico por aplicaciones y categorías de contenido, optimizando el acceso a Internet y garantizando un uso eficiente de los recursos. Luego, el tráfico será redirigido al NGFW para aplicar políticas de seguridad avanzada, asegurando una gestión eficiente y una protección robusta de la infraestructura digital de SUNAFIL.

A.1 Características esenciales.[2]

- La solución de gestión y optimización de enlaces deberá permitir auditar, controlar y optimizar el ancho de banda contratado por SUNAFIL, identificando al menos 5000 firmas de tráfico de capa 7 mediante técnicas de clasificación como Deep Packet Inspection (DPI), garantizando así un control eficiente y detallado del uso de los recursos de red.
- Además, deberá cumplir con los siguientes requerimientos como mínimo, asegurando un control granular del tráfico de red y optimización del rendimiento para todas las aplicaciones y servicios críticos de la entidad:
  - La solución debe ser de propósito especifico y no una funcionalidad dentro de alguna solución de seguridad o infraestructura IT (ej: firewall, UTM, NGFW, balanceadores, entre otros), como también debe ser una solución totalmente integrada y soportada directamente por el mismo fabricante a fin de garantizar un soporte integro, lo cual debe ser confirmado por carta directamente del fabricante.
  - La solución ofertada debe estar licenciada para realizar su labor de

[2] Por absolución de consulta Nº 58 de la empresa ENTEL PERU S.A.

monitoreo y gestión de ancho de banda como mínimo de 1.5 Gbps Full Duplex como capacidad de ancho de banda total.

- La solución ofertada debe soportar una escalabilidad al menos del 50% de la capacidad mínima solicitada a fin de soportar crecimientos que se puedan requerir durante el tiempo del contrato.
- La solución ofertada debe estar en capacidad de soportar un mínimo de 3,000,000 de flujos concurrentes para las labores de monitoreo y administración del ancho de banda de todos los usuarios de la entidad.
- La solución debe usar técnicas de clasificación de tráfico en capa 7 por medio de DPI, además de la capacidad de permitir crear firmas personalizadas para identificar el tráfico propio de la entidad o que se considere necesario.
- El modo de integración a la red de la solución debe ser de forma transparente a nivel de transporte que no realice cambios de las direcciones IP ni de los puertos de la comunicación, como también se debe disponer de funcionalidades de bypass que permita garantizar que el tráfico sigue cursando la red en caso de fallo eléctrico o de procesos del propio equipo, esta funcionalidad de bypass puede ser tanto interna ~~como~~ o externa mientras se garantice que el equipo puede ser retirado o ingresado físicamente dentro de la red sin generar caídas o fallas de conexión de la red.
- La solución debe incluir como mínimo la capacidad para gestionar X segmentos físicos que permita su integración con la red de la entidad, se debe tener en cuenta que la conectividad ~~mínima requerida sea de tipo (cobre/fibra óptica (multimodo o monomodo) con velocidad de (1G o 10G)~~ debe ser como mínimo de 4 interfaces del tipo fibra óptica multimodo con velocidad de 10G para soportar dos bridges de conexión en bypass, para garantizar la máxima disponibilidad en caso de reemplazo de equipo por fallo del mismo y así evitar cortes de servicio.[3]
- La solución debe permitir la configuración del bypass de cada segmento físico de forma independiente permitiendo que la acción de bypass se pueda activar o desactivar en cada segmento sin afectar otro segmento dentro de la misma solución.
- Las firmas de tráfico se deben actualizar de forma periódica según estructura del fabricante ofertado a fin de garantizar la continua y correcta clasificación de tráfico, como también el proceso de actualización de las firmas puede ser automático o manual siempre y cuando el fabricante garantice su correcta implementación sin afectar el servicio.
- La consola de gestión de la solución debe ser totalmente grafica que permita una interacción fácil e intuitiva, esto aplica también para la sección de políticas donde se deben tener mecanismos que permita la identificación de la política que está siendo aplicada a un tráfico

[3] Por absolución de consulta Nº 36 de la empresa ENTEL PERU S.A.

especifico, estos mecanismos deben permitir filtrar o buscar basado al menos por dirección IP, numero de puerto y nombre aplicación para fines de resolución de problemas o análisis de la política que está siendo aplicada.

- La solución debe tener la capacidad de clasificar el tráfico de la entidad por medio de varios tipos de filtros o identificadores y que ellos puedan ser visualizado en reportes gráficos, los cuales deben ser como mínimo: Aplicación (capa 7), grupo de aplicaciones, protocolo, puerto, rango de puertos, conversaciones, direcciones IP, rango de direcciones IPs, subredes, VLAN y nombre de host.

A.2 Otras Características.[4]

- La solución debe tener la capacidad mínima de identificar automáticamente el tráfico por usuario de directorio activo que permita tener reportes de su consumo y como opcional la opción de generar políticas por usuario, esta capacidad deber ser por medio de la integración con el servicio de directorio activo de la entidad sin requerir la instalación de algún tipo de agente o algún tipo de software directamente sobre el servidor del servicio, se acepta la integración con agente en un servidor independiente y provisto exclusivamente para este servicio sin costos adicionales o indirectos para el contrato.
- La solución debe estar en capacidad de medir métricas de rendimiento que permita monitorear el tráfico de la red y de las aplicaciones, donde se garanticen mínimamente las siguientes métricas solicitadas:
  - Métricas de calidad de Experiencia - QoE
    - RTT
    - TCP duplicate ACK
    - TCP Packet lost
    - TCP Retransmission
    - TCP RTT Client side
    - TCP RTT Server side
  - Métricas de redes
    - Number of flows
    - Total, throughput
    - Total, volume
    - Downstream
    - Upstream
    - Packets transmit
    - Packets received
    - Activity duration
    - Max peak throughput
  - Métricas para tráfico Web (HTTP/HTTPS)

[4] Por absolución de consulta Nº 58 de la empresa ENTEL PERU S.A.

- 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

▪ Métricas para tráfico de VoIP

- RTT
- TCP duplicate ACK
- TCP Packet lost
- TCP Retransmission
- TCP RTT Client site
- TCP RTT Server site
- Caller ID
- Session Time
- Duration Time

➢ La solución debe permitir el editar métricas ya existentes o crear otras nuevas en función de los requerimientos de la entidad a fin de evaluar el rendimiento del tráfico del enlace gestionado, por lo cual, se debe poder realizar operaciones matemáticas para el cálculo de las nuevas métricas.

- La solución debe permitir la administración de ancho de banda por medio de múltiples niveles de configuración jerárquicos de tal forma que se pueda asignar una capacidad de ancho de banda o definir prioridad dentro de otra asignación de recursos.
- La solución debe permitir configurar los valores de ancho de banda en la política tanto por un número fijo como también por porcentaje (%), que permita ser calculado según la capacidad superior al tener una estructura de múltiples niveles jerárquicos.
- La consola de la solución debe ser de tipo web con estándar de tipo HTML5 y/o interfaz GUI[5] que permita el acceso desde cualquier navegador web aun de dispositivos móviles a fin de evitar dependencias en aplicaciones o servicios específicos y/u obsoletos que afecta el fácil acceso para los administradores.
- La solución debe ser altamente granular para permitir asignar políticas basado a los bridges, segmentos o interfaces en uso, como también por filtros de clasificación de tráfico como dirección IP, aplicaciones, entre otros.

[5] Por absolución de consulta Nº 77 de la empresa GTD PERU S.A.

- La solución debe permitir como mínimo las siguientes acciones de gestión de tráfico:
  - 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
- La solución deber proveer un sistema de autoprotección y detección de incongruencias en políticas configuradas impidiendo la creación de una definición errónea que afecte el correcto funcionamiento de la solución, evitando que se guarde la política y visualizando la política que presento el error detectado.
- La solución debe ofrecer capacidad de almacenamiento de datos de forma histórica que permita establecer la granularidad de visualización en función del tiempo de tal forma que se adapte a las necesidades de visualización histórica de datos de la entidad y como mínimo debe garantizar la retención de datos por todo el tiempo del contrato.
- La consola de la solución puede ser local al equipo o de forma externa siempre y cuando se entregue todo el HW y SW requerido para funcionamiento, dicha consola debe permitir capacidades de analítica y monitoreo, como también de gestión del ancho de banda cumpliendo con las siguientes capacidades mínimas:
  - Interfaz web grafica e intuitiva con opción multilenguaje como mínimo inglés y español que permita una mayor comprensión de las opciones disponibles
  - Debe incorporar dashboards predeterminados que permita realizar análisis generales, además de la capacidad de creación de cuadros de dashboards personalizados permitiendo seleccionar las variables que le componen y el tipo de gráfico y tabla para la correcta representación de los datos.
  - La creación de cuadros de mandos debe permitir usar las múltiples métricas que se han recolectado del tráfico aun las creadas de forma personalizada por los administradores de la solución
  - El acceso a la consola debe poder ser gestionada por múltiples usuarios donde se pueda crear roles y definir permisos personalizados permitiendo diferenciar usuarios administradores según el acceso a la información recolectada y configuración de la solución.
  - Capacidad de generación de reportes automatizados que se puedan programar con capacidad mínima de exportar en formato PDF, imagen (JPG y/o PNG[6]) y CSV~~, con capacidad de personalización como puede~~

[6] Por absolución de consulta Nº 80 de la empresa GTD PERU S.A.

~~ser el logo de la entidad~~.[7]

- Debe tener capacidad de creación de alarmas que permita seleccionar el tipo de métrica de tráfico o rendimiento a evaluar, definir múltiples umbrales de estado y capacidad de poder correlacionar con otras alarmas que permita definir con operadores lógicos y de comparación permitiendo tipificar de mejor forma una incidencia de acuerdo con su complejidad.
- La notificación de las alarmas debe como mínimo emitir en dos tipos de comunicación directa a los usuarios, siendo uno de ellos el correo electrónico (email) y el otro tipo de medio debe ser mensajería instantánea (ej:WhatsApp, Microsoft Teams o similares) que permita la rápida interacción con los funcionarios responsables de la entidad.
- Capacidades de auto-aprendizaje del comportamiento de consumo de ancho de banda que permita establecer análisis basado en desviaciones permitiendo adaptar dinámicamente las alarmas según a este aprendizaje, como también la capacidad de predecir consumos a futuro que permita hacer aprovisionamientos o ajustes de configuración que permita evitar situaciones de saturación.
- La solución debe permitir crear botones de búsqueda personalizados que permita seleccionar múltiples criterios de los filtros o identificadores de tráfico a fin de facilitar la búsqueda de información relevante requerida por la entidad.

B. Solución de Protección AntiDDoS:

El Contratista deberá brindar un Servicio de Protección Anti DDoS para el servicio de Internet desde su nube local que proteja del tráfico, dicho sistema debe contar con las siguientes características mínimas:

- La solución en la nube desplegada en la red del proveedor de servicios de internet deberá proteger el tráfico malicioso, siendo que este sea mitigado lo más cercano a la entrada de la red del contratista.
- Capacidad de throughput de protección incluida debe ser de al menos 25 Gbps de tráfico.
- El sistema de protección Anti DDoS debe proteger mínimamente contra ataques de inundación del tipo TCP SYN, TCP RST, UDP, ICMP.
- El sistema de protección Anti DDoS debe contar con firmas que permitan proteger contra ataques conocidos.
- EL sistema de protección Anti DDoS debe poder mitigar ataques de denegación de servicio de día cero, distribuidos y no distribuidos en base a la generación automática de firmas en tiempo real. La generación de firmas automáticas deberá ser en menos de 60 segundos y sin intervención humana[8].
- La solución deberá tener integrado un módulo de IPS (Sistema de Prevención de Intrusos).

[7] Por absolución de consulta Nº 37 de la empresa ENTEL PERU S.A.
[8] Por absolución de consulta Nº 60 de la empresa ENTEL PERU S.A.

- La solución deberá ser de tipo Stateless.
- La solución deberá soportar un incremento del tráfico originado por ataques de Denegación de Servicios del tipo volumétricos desde hasta un máximo del 100% del ancho de banda contratado.
- La solución deberá proteger frente a ataques de denegación de servicios en una arquitectura "always on", también denominada en línea o siempre activa. No se aceptarán soluciones de mitigación de ataques de denegación de servicios bajo una arquitectura de derivación de tráfico.
- El proveedor deberá brindar un reporte mensual de la actividad de seguridad relacionada a los ataques de denegación de servicios detectados y mitigados. La entidad recibirá el reporte mensual en un plazo no mayor de 10 días calendarios culminado el ciclo de facturación.
- El proveedor ~~deberá~~ podrá [9]brindar acceso a la plataforma (usuario de lectura) para la revisión de estadísticas por parte de la Entidad.

C. Solución de Seguridad Next Generation Firewall (NGFW):

El Contratista deberá proporcionar un Servicio de Seguridad Perimetral implementado en la Sede Central. Este servicio incluirá la instalación de dos (02) Equipos Next Generation Firewall configurados en Alta Disponibilidad (HAS), garantizando la continuidad operativa y la protección ininterrumpida de la red. Los equipos firewall deberán cumplir con las siguientes especificaciones:

1) Especificaciones técnicas mínimas:

- Rendimiento en Prevención de Amenazas: Rendimiento (throughput) de 10 Gbps (medido con Capacidades habilitadas de: Firewall, Control de Aplicaciones, IPS, URL Filtering, Antivirus y/o Antimalware, Anti-Bot o Antispyware o DNS Security[10] y Emulación Malware dia-cero.
- Rendimiento en NGFW - Next Generation Firewall: Rendimiento (throughput) de 30 Gbps (medido con Capacidades habilitadas de: Firewall, Control de Aplicaciones e IPS).
- Sesiones Concurrentes: 16'000,000 conexiones o sesiones concurrentes
- Conexiones por segundo: 350,000 conexiones o sesiones por segundo
- Interfaces de red:
  - 8 puertos de red 1GB (RJ45)
  - 04 interfaces 10 GB SFP+ (incluido transeivers) 01 puerto de consola RJ-45
  - 01 interfaz de gestión dedicada (out of band)
  - 01 puerto de consola

2) Funcionalidades requeridas:

[9] Por absolución de consulta Nº 89 de la empresa GTD PERÚ S.A.
[10] Por absolución de consulta Nº 53 de la empresa ENTEL PERÚ S.A.

- El sistema operativo deberá ser del fabricante de la solución de firewall ofertado, el mismo deberá venir de fábrica con el "harderning" necesario para no tener componentes y/o configuraciones que puedan causar vulnerabilidades.
- En ningún caso se podrá presentar soluciones con equipos que estén en etapa de obsolescencia o que hayan publicado y/o anunciado el "End-of-life" y/o "End-of-Support", o dejen de ser fabricadas, comercializadas y/o soportadas durante los 05 años siguientes a la instalación de los equipos a ser propuestos. Esto requerimiento deberá ser respaldado con una carta del fabricante adjuntando la documentación publica de Internet que la respalde.
- El fabricante de la solución de seguridad debe estar presente en los últimos 08 reportes de Gartner (Magic Quadrant), en el cuadrante de Líderes para Network Enterprise Firewalls.
- El fabricante de la solución de seguridad debe tener un porcentaje igual o superior al 98% de ratio de protección, en la última evaluación de Enterprise Firewall Report de CyberRatings para el año 2024.
- Los sistemas operativos y/o firmware que operan en los equipos de seguridad firewall ofertados, no deberán tener más de diez (10) vulnerabilidades (CVE) anunciadas y/o publicadas, acumuladas en sus diferentes versiones durante los últimos 12 meses anteriores a la fecha de presentación de propuestas.
- La solución de seguridad debe soportar la configuración de clúster en modo de operación en alta disponibilidad (HA).
- Debe soportar redundancia de enlaces WAN o de ISP (Internet Service Provider) redundantes, sin la necesidad de una licencia adicional o software/hardware de terceros.
- La redundancia de ISP emplea la detección de falla enlace para conmutación automática.
- Debe soportar sincronización de sesiones, para mantener vivas las conexiones activas y evitar la pérdida de datos cuando falla un miembro del clúster.
- Administración accesible a través de SSH y de interfaz Web segura (HTTPS).
- La herramienta debe ser capaz de realizar backup/restore de la configuración, permitiendo al administrador programar la realización de los backups en periodos diario, semanal y mensual. Asimismo, estos archivos pueden almacenarse tanto en los firewalls o en la consola de gestión.[11]
- Los backups pueden ser generados transferidos vía SFTP, SCP, FTP y localmente. El backup debe tener capacidad de ser cifrado.
- La comunicación entre la consola de gestión y los equipos de seguridad (firewall), debe ser cifrada y autenticada.

3) Funcionalidades de red:

[11] Por absolución de consulta N° 96 de la empresa GTD PERÚ S.A.

- La solución debe ser capaz de operar en modalidad Layer 3 (routing), modalidad in-line (bridge) y L2 (port mirroring y/o monitor mode).
- Deben soportar inspección del tráfico cifrado (SSL/HTTPS).
- Debe soportar enrutamiento con IPv4 e IPv6.
- Debe soportar DHCP en modos: Servidor DHCP y DHCP Relay (reenvío) en IPv4 e IPv6.
- Debe contar con un módulo de control QoS basado en prioridades y pesos para el control de: porcentaje del ancho de banda disponible, basado en prioridad de regla, ancho de banda mínimo garantizado y ancho de banda máximo, basado en límites.
- Debe contar con un módulo de control QoS garantizar el ancho de banda y controlar la latencia para aplicaciones de transmisión, como son Voz sobre IP (VoIP) y videoconferencia.
- Soporte de rutas estáticas, IPSec Routing, RIP, OSPFv2 y OSPFv3(IPv6), IGMP, PIM SM, PIM DM PIM SSM, BGP, EBGP Multihop (opcional)[12] y IPv6 BGP-4 (opcional)[13].
- Soporte de PBR (policy based routing) que permite ante la presencia de dos o más enlaces, se pueda decidir por que enlace ingresa y egresa un tráfico determinado.
- Debe soportar redundancia ~~de hasta 10~~ como mínimo 02 [14] enlaces ISP (Internet Service Provider) redundantes, sin la necesidad de una licencia adicional o software/hardware de terceros.
- La redundancia de ISP puede ser a nivel de "compartición de carga" (load sharing) y detección de falla enlace (primary/backup).
- Debe soportar sincronización de sesiones, para mantener vivas las conexiones activas y evitar la pérdida de datos cuando falla un miembro del clúster.
- La solución debe soportar registro de tablas ARP estáticas y dinámicas, definiendo cantidad de entradas ARP y el tiempo de duración.

4) Gestión de políticas:

- El equipo debe permitir la creación de políticas de acceso y de prevención de amenazas, con capacidad de seleccionar campos como: Redes y Grupos de Redes, Host, Zonas, Objetos Dinámicos, Dominios FQDN, Usuarios, Grupos de Usuarios, Clientes Remotos VPN, Servicios y Aplicaciones Web y Comunidad de VPN.
- Sobre la base de las políticas creadas debe tener capacidad de habilitar diversas acciones tales como: Accept, Drop, Reject, Limit (limitar ancho de banda) y habilitar autenticación de usuario final.
- Las reglas deben permitir manejo de ancho de banda de distintos protocolos y aplicaciones web, permitiendo la limitación del uso ancho de banda, tanto para carga (upload) y descarga (download)

[12] Por absolución de consulta N° 99 de la empresa GTD PERÚ S.A
[13] Por absolución de consulta N° 98 de la empresa GTD PERÚ S.A.
[14] Por absolución de consulta N° 100 de la empresa GTD PERÚ S.A.

por cada regla.

- Debe poder analizar la utilización de las reglas, con niveles de indicador: muy alto, alto, medio, bajo y cero, este último indicador permitirá identificar que dicha regla no ha tenido conexiones (sin uso). El uso también debe poder Identificarse numéricamente en miles, millones, gigas y teras de hits por regla. El contador de uso de la regla podrá configurase en ventanas de tiempo de: día, semana, mes y total.
- Las reglas de firewall deben poder establecer vigencia en base a objetos de tiempo, basado en periodos: diario, semanal, mensual y tener un horario de recurrencia en la cual la regla está vigente.
- Capacidad de crear reglas de firewall en base fuentes dinámicos externas, los cuales serán basados en fuentes de URL externas (HTTP/HTTPs) que contengan archivos planos (CSV) y/o JSON y/o (lista de direcciones IP, Dominios y/o URL)[15]. En el caso de archivos planos se debe poder el tipo de dato y los delimitadores. En caso de JSON debe emplear la sintaxis JQ.
- Las fuentes externas deben ser consultadas automáticamente por el firewall, con la finalidad de automatizar las reglas de acceso, no siendo necesario instalar reglas en el firewall.
- ~~Las reglas de firewall en base fuentes dinámicos externas deben soportar como mínimo Dirección IP, Rango de Red, IP y mascara de red y dominio FQDN.~~[16] Estas fuentes deberán ser efectivas en reglas de acceso tanto en origen como destino.
- En el caso de navegación en internet, debe tener capacidad de crear políticas con acciones de interacción al usuario final, tales como:
  - Preguntar al usuario si desea continuar o no, y deben indicar una razón para continuar.
  - Informar al usuario, ellos pueden continuar a la aplicación y/o página web[17] o cancelar el requerimiento.
  - Bloquear indicando al usuario final un mensaje de bloqueo a la aplicación y/o página web[18].
- Los mensajes de bloqueo e interacción con el usuario final deben ser editables en idioma y contenido.
- Soportar la creación de políticas basada en Geolocalización, configurando que el tráfico de determinado País y/o Países sean bloqueados o permitidos.
- Debe posibilitar la visualización de los países de origen y destino en los logs de acceso.
- Debe posibilitar la creación de bloqueo general de diversos países desde la interfaz gráfica y crear de excepciones utilizando políticas.
- Las actualizaciones de las direcciones o rangos de IP publica por

[15] Por absolución de consulta Nº 106 y 107 de la empresa GTD PERÚ S.A.
[16] Por absolución de consulta Nº 107 de la empresa GTD PERÚ S.A.
[17] Por absolución de consulta Nº 108 de la empresa GTD PERÚ S.A.
[18] Por absolución de consulta Nº 109 de la empresa GTD PERÚ S.A.

cada país, debe realizarse periódicamente y de manera automática.

- Debe tener capacidad de controlar el tipo de contenido para el tráfico entrante y saliente.
- El control se debe realizar por tipo de dato en tránsito, por lo menos de dos maneras: mediante el tipo de contenido, clasificado analizando el contenido del archivo, y mediante el tipo de archivo, analizando el ID o metadato del archivo.
- Los formatos de tipo de archivo a restringir deben ser como mínimo: PDF, Ejecutables (EXE, COM, DLL, DRV, SCR, VBX, SYS), Microsoft (Power Point, Excel, Word), archivos comprimidos (ZIP, 7Z, RAR, TAR, GZIP) y Bases de Datos (Microsoft Access, DB y DBF).

5) Prevención de intrusos – ips:

- La solución debe proveer un sistema de prevención de intrusos (IPS) integrado a la solución de seguridad.
- El IPS debe contar con mecanismo de detección de amenazas de múltiples métodos: detección por firmas, validación de protocolo, detección anómala, heurística y/o[19] análisis de comportamiento.
- El IPS debe contar con motor de identificación de patrones, que le permita diferenciar entre paquetes inofensivos y paquetes maliciosos, detectando expresiones regulares en los flujos de como un segundo nivel de análisis, para reducir la tasa de falsos positivos.
- El IPS debe poder detectar evasiones en la retransmisión de paquetes o el envío de paquetes maliciosos en la retransmisión, proveyendo capacidad de reensamblaje de flujo para conexiones TCP y reordenamiento de paquetes.
- La funcionalidad de IPS debe tener las siguientes capacidades:
- Detección y prevención de vulnerabilidades, incluidas herramientas de explotación conocidas y desconocidas, y protección contra CVE específicos.
  - Detección y prevención del uso indebido de un protocolo, para actividad maliciosa o amenaza potencial.
  - Detección y prevención de comunicaciones de malware salientes.
  - Detección y prevención de DNS tunneling, para intentos de fuga de datos o intentos de evasión.
  - Detección, prevención o restricción de ciertas aplicaciones que pueden causar amenazas a la seguridad de la red, como las aplicaciones P2P o de mensajería instantánea.
  - Detección y prevención de tipos de ataques genéricos que no cuenten aun con firmas predefinidas.
- Debe tener protección contra ataques de DoS (Denial of Service).
- Por cada protección o por todas las protecciones soportadas, debe permitir adicionar excepciones basadas en objetos de red o mediante las reglas de seguridad configuradas.

[19] Por absolución de consulta N° 113 de la empresa GTD PERÚ S.A.

- Debe detectar y bloquear ataques de red y de aplicación, protegiendo al menos los siguientes servicios: HTTP, SMTP, DNS, POP e IMAP,
- Las políticas de protección de IPS deben poder establecerse en base a parámetros tales como: número del CVE y nivel de severidad ~~y nivel de efectividad (confianza).~~[20]
- Debe permitir adicionar excepciones a las protecciones de IPS desde el log o de manera manual.
- Debe poder capturar paquetes de eventos de IPS, para proveer un análisis posterior.

6) Anti-bot y/o antispyware:

- La solución debe proveer una herramienta que haga descubrimiento de "bots" dentro de la red. Dicha herramienta debe bloquear la comunicación que intenten establecer los equipos infectados "bots" hacia las redes de los atacantes en Internet (botnet).
- La solución debe incluir al menos los siguientes métodos de identificación:
  - Identificación de direcciones web de Comando y Control utilizadas por los criminales para controlar los bots.
  - Identificación de patrones (fingerprints) de comunicación utilizada por cada familia de bots.
  - Identificación de comportamiento de bots.
- La solución debe contar con un repositorio en la nube del propio fabricante para la identificación de direcciones y patrones de comunicación de "botnet". El Anti-Bot se debe actualizar continuamente de manera automática.
- La solución debe contar con un repositorio en nube del fabricante que permita realizar consultas de direcciones IP, URL y recursos DNS no identificados y/o no clasificados.
- La solución debe tener una capa de protección DNS, para protección contra dominios maliciosos de malware basados en Algoritmos de Generación de Dominio (DGA) y DNS Tunneling, empleando protección basada en Machine Learning. Estas funcionalidades deben emplear las fuentes de inteligencia de amenazas en nube del propio fabricante.
- La solución debe contar con análisis la reputación de direcciones URL, direcciones IP y los dominios externos (DNS) a los que acceden los equipos en la red, para identificar y prevenir actividad conocida o sospechosa, como Command and Control (C&C).

7) Control de aplicaciones y url filtering:

- La solución debe ser capaz de identificar, permitir o bloquear aplicaciones y páginas Web.
- Se requiere que capacidad de detección de ~~10,000~~ 5000[21]

[20] Por absolución de consulta Nº 117 de la empresa GTD PERÚ S.A
[21] Por absolución de consulta Nº 118 de la empresa GTD PERÚ S.A

aplicaciones en la base de datos de control de aplicaciones para la aplicación de políticas.

- La base de datos de control de aplicaciones debe actualizarse por un servicio basado en la nube, la actualización debe ser periódica y automática.
- Debe permitir la creación de firmas personalizadas para el Control de Aplicaciones y URL Filtering, mediante herramientas del propio del fabricante.
- Debe alertar al usuario cuando una aplicación o página web fuera bloqueada.
- Solución debe soportar como mínimo 70 categorías de URL Filtering, que incluya categorías para protección de riesgo informático, tales como: Phishing, SPAM, Botnets, Anonymizer, Artificial Intelligence (AI) Hacking, Inactive Sites y Spyware/ Malicious Sites.
- Debe ser posible definir nuevas aplicaciones y sitios web, así como categorías y grupos que no estén definidos dentro de la base de datos.
- Debe ser posible permitir o bloquear aplicaciones o sitios al menos por los siguientes parámetros: Aplicación Individual, URL o aplicación, categorías, niveles de riesgo, reglas individuales (usuarios) y grupos de usuarios.
- La solución debe categorizar las aplicaciones y URLs por factor de riesgo.
- Debe ser posible definir la política de seguridad de aplicaciones y URLs basada en identidades de usuario.
- Solución debe inspeccionar el tráfico web cifrado (SSL/TLS) de los usuarios, y permitir excepciones granulares de inspección para proteger la privacidad de los usuarios y/o cumplir con regulaciones.
- Debe permitir la categorización de los sitios HTTPS basado en el contenido del campo SNI (Server Name Indication), sin la necesidad de descifrar el tráfico web.
- Debe poder realizar la implementación de TLS 1.3 para inspección de canal cifrado y HTTP/2.
- Debe soportar la inspección de tráfico HTTPS sobre puertos no estándar (distinto a los puertos HTTP/HTTPS).

8) Prevención de amenazas:

- Debe utilizar el repositorio de inteligencia de amenazas en nube del propio fabricante, para recibir actualizaciones de firmas y consultar en el repositorio la clasificación y/o reputación de direcciones IP, Dominios, URL, redes de Comando y Control y ataques DoS.
- Debe tener capacidad de clasificación y análisis de archivos y posterior validación en el repositorio de inteligencia de amenazas en nube del propio fabricante, sin generar un impacto en el rendimiento de la red.
- Los equipos deben tener integrada la detección y prevención de virus y amenazas (antimalware).

- La inspección de archivos y prevención de amenazas debe ser en el tráfico entrante y saliente.
- Debe tener capacidad de protección de pre-infección del malware que fue identificado en los archivos.
- Deberá realizar análisis de malware y bloquearlos en al menos los siguientes protocolos: Web (HTTP, HTTPS), Mail (SMTP o POP3), SMB y FTP.
- Debe tener una base de datos local de firmas de malware y cache de reputación de URL, para una respuesta rápida. Si una URL no está ubicada en la cache, debe ser consultada automáticamente en el repositorio de Inteligencia de amenazas en nube para su clasificación y prevención.
- Debe soportar Inspección de tráfico cifrado/encriptado sobre protocolo HTTPS, tanto tráfico entrante (Inbound), como tráfico saliente (Outbound).
- Debe impedir la descarga de malware desde Internet, impidiendo el acceso a sitios que se sabe que relacionados con Malware.
- Debe tener capacidades de inspección y prevención de amenaza en el canal cifrado SSH, con las siguientes capacidades:
  - Bloquear ataques en canal SSH.
  - Bloquea la transmisión de virus a través de los protocolos SCP y SFTP.
  - Prevenir el descifrado de contraseñas en fuerza bruta de servidores SSH/SFTP.
  - Prevenir el uso de criptografía vulnerable en el canal SSH.
  - Prevenir el uso de clientes y servidores SSH vulnerables.
- Debe soportar para la alimentación de IoC (Indicadores de Compromiso) desde fuentes externas, en formato CSV ~~y~~ y/o STIX XML (Structured Threat Information Expression) y/o listas dinámicas externas (EDL)[22] para la prevención de amenazas
- Los IoC deben ser actualizados automáticamente de acuerdo con un intervalo definido en la consola.
- Los IoC definidos en las fuentes externas deberán poder ser como mínimo: URL, Dominio, IP, Rango de IP, Hash (MD5, SHA1, SHA256) y campos de correo (Mail From, To, CC, Subject).

9) Prevención de amenazas desconocidas o de día cero:

- La solución debe ser capaz de identificar y prevenir ataques y malware no conocido, presentes en documentos y/o archivos ejecutables.
- La solución debe ser capaz de emular los archivos identificados en el firewall de forma automática, a través del envío y posterior análisis en la nube del propio fabricante de la solución de firewall para la Emulación de Malware (SandBox).
- La solución debe proteger a los usuarios internos, de manera que

[22] Por absolución de consulta N° 123 de la empresa GTD PERÚ S.A.

prevenga el acceso o descarga a los archivos en tanto estos son analizados en el equipo de emulación, si el archivo en benigno se entrega el archivo original al usuario y si el archivo el maligno se deniega su acceso o descarga.

- La solución debe proporcionar la capacidad de protección contra ataques de malware desconocido y de día cero antes de que se hayan creado protecciones de firmas estáticas.
- La solución debe proveer prevención en tiempo real de malware desconocido en las descargas web y canal de correo electrónico.
- La solución deberá poder emular archivos para la identificación de malware que viajan en los protocolos: HTTP, HTTPS, SMTP, IMAP, CIFS, SMBv3, SMBv3 multi-channel y FTP.
- La solución deberá poder emular al menos los siguientes tipos de archivos: Adobe PDF, Microsoft Office (documentos y plantillas), DLL, Java, Flash, Scripts, archivos comprimidos (ZIP, 7Z, RAR, GZ, TGZ, TAR, TAR.GZ y JAR), ejecutables (EXE, COM, LNK, DLL, DRV, SYS, SCR, VBX) y archivos de MacOS (APP, DMG, PKG).
- Cada archivo emulado en el SandBox debe generar un reporte detallado que incluya información forense sobre la actividad maliciosa originada por el archivo. Este reporte debe mostrar una matriz grafica con las técnicas y tácticas empleadas por el malware sobre la base del framework de ciberseguridad MITRE ATT&CK.
- El motor de emulación debe detectar llamadas API, cambios en el sistema de archivos, cambios en el registro, conexiones de red, procesos de sistema.
- El motor de emulación debe analizar y emular los URL contenidos en documentos Microsoft Office y PDF, para detectar y prevenir descargas maliciosas de malware.
- El motor de emulación debe emplear mecanismos de Machine Learning para detectar y prevenir ataques ocultos sobre archivos LNK (accesos directos) tales como: Icon Spoofing, File Attribute Manipulation, Shortened URLs.
- El motor de emulación debe contar con tecnologías de ML basadas en Redes Neuronales (Neural Networks) para la detección de amenazas en los archivos Microsoft Office y PDF.
- Las soluciones deben admitir motores de detección automatizados basados en machine learning.
- La solución debe ser capaz de soportar escaneo de enlaces (links) dentro de correos para detección de malware.
- La solución debe ser resistente a los casos en los que el código de shell o el malware no se ejecutarían si detectaran la existencia de un entorno virtual.
- La solución deberá tener capacidad de extracción de amenazas o CDR (Content Disarm Reconstruction), en las descargas de archivos desde Internet incluyendo el canal cifrado HTTPS para prevenir el riesgo al interior de la red corporativa. Debe tener la capacidad de limpiar archivo durante su análisis, extrayendo el componente activo

de riesgo o malicioso que encuentran dentro de los archivos, y, además, poder transformar el archivo en un formato PDF. Esta funcionalidad debe soportar como mínimo los siguientes tipos de archivo para el canal web y correo:

- Microsoft Excel (XLS, XLSX, XLSB, XLSM, XLTX, SLTM)
- Microsoft Word (DOC, DOCX, DOCM, DOTX, DOTM, DOT)
- Microsoft Power Point (PPT, PPS, PPTX, PPTM, POTX, POTM, PPSX)
- Adobe PDF (PDF, FDF)

- Así mismo, la capacidad de extracción y/o transformación de los archivos para prevención de amenazas, debe ser efectuada en los archivos adjuntos en canal de correo (en modalidad Mail Transfer Agent) para los formatos:
  - Imágenes (JPEG, JPG, BMP, PSD, GIF, TIF, PNG)
  - XML, TXT, HTML, JS.
- La extracción de malware deberá retirar los componentes de riesgo de los documentos tales como: Macros, Objetos Embebidos, Enlaces (Linked Objects), PDF JavaScripts y PDF Launch.

10) VPN IPSec:

- Debe soportar IPSec VPN Client-to-Site con capacidad de 200 usuarios concurrentes
- Debe soportar túneles VPN punto a punto Site-to-Site de manera ilimitada o hasta la máxima capacidad soportada por el equipamiento.
- Debe permitir almacenar una base de usuarios local que permita realizar autenticación, sin depender de un dispositivo externo.
- Deben soportar encriptación AES-128 y AES-256 para las fases I y II de IKE.
- Deben soportar integridad en MD5, SHA1, SHA-256, SHA-512, AES-XCBX para las fases I y II de IKE.
- Debe soportar al menos los siguientes grupos Diffie-Hellman: Grupo 2 (1024 bit), Grupo 5 (1536 bit), Grupo 14 (2048 bit), Grupo 19 (256-bit ECP) y Grupo 20 (384-bit ECP) para las fases I y II de IKE.
- Debe poder integrarse con Directorio Activo Microsoft para crear reglas de control de acceso a través de VPN, empleando: usuarios, grupos de usuarios, maquinas, dirección IP y redes.
- Debe poder integrarse con Azure AD (Microsoft) mediante SAML para autenticación en el acceso remoto de clientes VPN.
- El cliente VPN, debe instalarse sobre sistemas operativos Windows, Linux y MacOS

11) Identificación de usuarios:

- La solución debe proveer diferentes métodos para obtener las identidades de los usuarios, tales como:
  - Sin agente, haciendo búsquedas al Directorio Activo Microsoft.

- Con agente implementado en los servidores de Directorio Activo Microsoft.
- Empleando un Portal Cautivo.
- Empleando un Proveedor de Identidad (IdP) basado en SAML

- La solución debe soportar el uso del protocolo WMI (Windows management instrumentation).
- La solución debe soportar el uso del protocolo Kerberos (Transparent Kerberos Authentication).
- Debe proveer un "Portal Cautivo", para autentificar a los usuarios que no están dentro del Directorio Activo, los usuarios que no tienen plataforma Windows y/o los usuarios invitados.
- Cuando se detecte que los usuarios no se han autenticado, la solución tiene que redireccionarlos a un Portal Cautivo, a través del protocolo HTTP.
- Debe soportar al menos los siguientes métodos de autenticación: nombre de usuario y contraseña, que podrá ser configurado en la base de dates Interna del equipo, servidor de LDAP.
- La solución debe integrarse con el servicio de Azure AD (Microsoft) para la autenticación y autorización de usuarios en las reglas de acceso del firewall.

12) Logs, reportes y monitorización

- Debe tener capacidad de generar logs de seguridad y los del sistema.
- Debe tener capacidad de logs de auditoría que muestre cada operación realizada por el administrador.
- Capacidad de monitorizas los siguientes valores de los firewalls:
  - Versión del SO y productos instalados y serial number.
  - Tiempo de actividad del sistema (system uptime).
  - Consumo grafico de CPU
  - Consumo grafico de memoria RAM
  - Grafica del tráfico total a nivel de paquetes (packet rate).
  - Grafica del tráfico total a nivel de throughput.
  - Aplicaciones de alto riesgo y el TOP de usuarios que usan aplicaciones de alto riesgo.
- Los logs de emulación de malware del firewall deben estar tener información detallada de los ataques, exponiendo las técnicas y tácticas de MITRE ATT&CK que fueron empleadas. Debe tener la capacidad de realizar búsqueda en base a técnicas o tácticas específicas.
- Debe tener una vista de los ataques detectados, con la siguiente información:
  - Numero de host en la red infectados con malware.
  - Número de ataques prevenidos.
  - Numero de archivos maliciosos bloqueados.
- Debe tener una vista en formato "línea de tiempo" de los ataques detectados, con la siguiente información:
  - Línea de tiempo con los hosts en la red infectados con

malware.
- Línea de tiempo de los Ciber Ataques detectados por los módulos de IPS, Anti-Virus, Anti-Bot, Emulación.
- Debe tener la capacidad de poder crear y editar los gráficos de información (widgets) en diferentes tipos tales como: tablas, cuadros (columnas, barras, pie), línea de tiempo, mapa e infografía.

- El correlacionado de eventos, debe tener capacidad de respuesta automática, en base a eventos de seguridad según políticas definidas. Las acciones de respuesta automáticas deben ser: enviar un correo electrónico, generar un SNMP Trap, bloquear una IP origen de donde proviene el evento, bloquear un ataque distribuido que provienen de múltiples orígenes.
- Debe tener capacidad de vistas de los tuneles VPN donde se muestre el estado de los peers y la Fase 1 y Fase 2. Debe proveer una vista de los usuarios remotos por VPN, donde muestre las estadísticas de los usuarios remotos en tiempo real.

13) Portal de administración:

- Consola de gestión del tipo SaaS, del propio fabricante de la solución de firewall ofertado. El nivel de SLA del servicio SaaS deberá ser del 99.9%.
- Debe tener las capacidades de gestión de políticas, almacenamiento, análisis y retención de logs, correlación de eventos de seguridad y reportes de todos los firewalls ofertados.
- Debe tener retención de logs de 03 meses.
- La consola centralizada deberá tener la capacidad licenciada para gestionar todos los firewalls ofertados.
- La consola centralizada debe permitir el despliegue de actualizaciones y parches de seguridad en los firewalls gestionados.
- Debe permitir el acceso concurrente de administradores y la instalación de políticas en modo simultaneo.
- Debe tener capacidad de revisión histórica de políticas, identificando la fecha y hora en la que fueron instaladas, así mismo identificando las revisiones y cambios que fueron instalados y quien realizo los cambios. Debe tener capacidad de revertir a una versión especifica de política.
- La consola debe contar un flujo de aprobación de cambios. Esta función debe permitir la opción de revisar y aprobar los cambios de configuración realizados por otros administradores antes de publicarlos. Se puede definir qué administradores deben enviar sus cambios para su aprobación y qué administradores están autorizados para aprobar los cambios de otros.
- En el proceso de instalación, debe realizar una validación de las reglas en la política, para verificar que son consistentes y no presentan reglas redundantes. Si se verifican errores, la política no deberá ser instalada.

- Debe contar con un motor de tareas específicas, que permita automatizar las notificaciones por correo electrónico en base los estados de los cambios en las políticas de seguridad, antes y después de:
  - Publicación de política de seguridad
  - Aprobación de política de seguridad
  - Rechazo de una política de seguridad
  - Luego de la instalación de una política de seguridad
- La herramienta debe integrar en una única consola gráfica segmentando el estado general de todos los dispositivos administrados, la configuración de la política de seguridad, los logs registrados y el monitoreo de toda la plataforma.
- Debe incluir una herramienta que administre centralizadamente la licencia de todos los equipos, controlados desde la estación de administración.
- La herramienta debe permitir gestionar de forma centralizada los túneles VPN y las VPN de acceso remoto de los usuarios.
- La herramienta debe permitir sesiones concurrentes de diferentes usuarios o dispositivos para los cambios de políticas.
- La herramienta debe permitir la creación de perfiles de administradores, basados en roles, que accedan a secciones parciales de administración o a la totalidad, indicando también si los perfiles son de solo lectura o lectura/escritura.
- Capacidad de gestión y operaciones mediante API (Rest API), para lectura de información y enviar comandos.
- Debe contar con capacidad de envío (forward) de eventos hacia un SIEM o syslog server externos, empleando protocolos TLS sobre TCP, TCP y UDP.
- La seguridad con los SIEM o syslog, se podrá realizar mediante el uso de certificados cuando se emplea TLS sobre TCP.
  - NOTA: Todo el cumplimiento referido a las capacidades de hardware y/o de rendimiento solicitadas, se deberá verificar a través de la documentación técnica (datasheet) y/o manuales y/o bochures emitidos públicamente por el propio fabricante de la solución de firewall, adjuntando el documento y enlace (URL) público de Internet del propio fabricante que lo sustente. No se aceptarán cartas de fabricante y/o representantes locales, como un fundamento para el cumplimiento de estos requerimientos solicitados.

D. Solución de Monitoreo y Gestión de Red:

El postor debe suministrar herramientas para la supervisión del funcionamiento de sus enlaces en alquiler, crear diagramas topológicos detallados de la Red en tiempo real. Analizador de Tráfico LAN y Sistema para gestión permanente y proactivo de Servicios, tales como:

Monitoreo de Enlaces

- Suministro del hardware y software requerido para uso exclusivo de la herramienta de monitoreo, incluir todas las licencias requeridas para su óptimo funcionamiento, el cual debe ser instalado en la Sede del cliente e incluyendo la base de datos.
- Suministro e instalación de solución de monitoreo que permita el análisis y captura del flujo de tráfico generado para al menos 50 dispositivos o interfaces WAN o backbone. También se aceptará, el monitoreo en 50 dispositivos y 50 interfaces, los cuales serán sin costo adicional para la entidad.[23]
- Esta solución debe permitir visualizar y analizar la variación de los flujos de tráfico al menos cada 60 segundos e incluir espacio de almacenamiento (storage) suficiente como para almacenar dicha información durante al menos (01) año manteniendo la granularidad de 60 segundos. Esta solución es un entregable del proyecto que será administrada por el Cliente y debe estar preparada para permitir un incremento del 25% de equipos y sin costo para la entidad, debe contar con los siguientes módulos activos:
- Analizador de tráfico Netflow (NetFlow Traffic Analyzer).
- Gestor de direcciones IP (IP Address Manager), mínimo 250 direcciones IP.
- Supervisión del Rendimiento de Red (Network Performance Monitoring).
- URL Monitoring: 10 URLs
- La solución de monitoreo debe medir como mínimo:
  - Tráfico de ancho de banda entrante y saliente en periodos: diario, semanal, mensual y anual.
  - Monitorear la disponibilidad de los enlaces y mediciones críticas de la red, incluida la pérdida de paquetes, errores y descartes.
  - Monitoreo del Hardware de los diferentes dispositivos de red.
  - Historial de alarmas con umbrales personalizables.
  - Consumo por aplicaciones, mínimo requerido: HTTP, HTTPS, SMTP, ICMP Y Netbios.
  - Consumo según el puerto, protocolo y dirección IP o red.
  - Soporte de VLAN`s, dentro de las cuales se incluirán las de Gestión, Servidores, Voz, Video y Datos.
- La solución de monitoreo deberá permitir realizar diagramas topológicos detallados de la red en tiempo real en capa 2 o capa 3.
- La solución de monitoreo deberá permitir realizar diseño de Data center y Rack en 3D
- Reportes estadísticos del comportamiento de los enlaces contratados.
- La solución de monitoreo debe incluir un módulo de Capacity Planning que permita lo siguiente:
  - El Software de Monitoreo debe permitir Reportes en Tiempo Real con

[23] Por absolución de consulta N° 39 de la empresa ENTEL PERÚ S.A.

granularidad de 1 minuto para muestreos de intervalos de 24 horas a fin de detectar tráfico anómalo, aplicaciones, conversaciones, Top Senders y Top Receivers.

- El Software de Monitoreo debe permite tener granularidad de al menos 1 minuto para la data almacenada en la base de datos que debe ser incluida y para el periodo de al menos de 1 año con el objetivo de tener reportes granulares y realizar comparativos mensuales para el sustento y planificación de la capacidad.

- La implementación de la solución de monitoreo deberá ser instalada en la sede de la entidad, para ello se aceptará sea en una versión appliance o virtual, en caso sea virtual, la entidad, proveerá la máquina virtual para su implementación y el proveedor deberá incluir el sistema operativo (Windows o Linux), las bases de datos y el licenciamiento necesario de la herramienta.
- La solución de monitoreo debe permitir hasta diez (10) usuarios concurrentes.
- Generación de Alertas mediante Email, SMS, IT Workflow, SNMP Trap Processing y web alarm.
- Debe permitir crear vistas en 3D del datacenter y los pisos con racks (frontal y rear) y permita el monitoreo de los equipos en tiempo real para identificación de fallas utilizando código de colores, permitiendo la personalización del tamaño del piso. Tamaño del rack (42U, 38U, etc.) y tamaño d ellos dispositivos (2U, 1U, etc.) y rotación de la vista del mismo
- Deberá incluir un módulo de analítica que permita lo siguiente:
  - Información detallada para mejorar la disponibilidad y el rendimiento de la red permitiendo el análisis de los datos y presentar el comportamiento y las tendencias de la red utilizando al menos 100 KPIs.
  - Realizar el seguimiento del inventario y de la utilización de los recursos para optimizar la utilización actual y prever la planificación de la capacidad.
  - Correlacionar las tendencias de las alarmas con la frecuencia de los cortes.
  - Visión holística de los servicios permitiendo definir clusters de procesos empresariales claves que pueden ser monitoreados utilizando vistas de negocio.

Herramienta Automate Mapping y Troubleshooting

- El Contratista debe implementar una solución completa que permita crear diagramas topológicos detallados de la Red en tiempo real, así como guardar el historial de los registros. Debe permitir descubrir como mínimo, los siguientes tipos de equipos (Router, Switches L2, Switches L3, Firewall, Load Balancers, WAN Optimizer, WAPs). La solución debe recopilar la información de los equipos descubiertos por SNMP capturando como mínimo: Dirección IP, Marca, Modelo, MAC y debe tener la opción de poder

exportar esta información del inventario de los equipos descubiertos en un archivo MS Excel/CSV. Asimismo, debe disponer la opción de documentar la información recopilada y deberá exportarla en un archivo PDF y/o Word.

- La solución debe permitir exportar los mapas/diagramas de red en formato MS Visio, asimismo debe ser capaz de descubrir e identificar como mínimo seis mil (6,000) tipos de dispositivos y al menos 300 diferentes marcas/modelo de equipos en la red. Debe visualizar el Troubleshooting en tiempo real, diagnosticando el diseño y resaltar los errores o problemas en la configuración (BGP, OSPF, RIP Routing).
- Capacidad de visualización de la red usando la integración de Google map con el objetivo de tener una visibilidad de la distribución de los dispositivos en todas las sedes.
- La solución debe permitir el acceso de múltiples usuarios bajo un esquema cliente servidor, con una simultaneidad de mínimo diez (10) usuarios, con una capacidad de descubrir un mínimo de 200 dispositivos de red (switches, routers, firewall, etc.) ~~y~~ o soportar como mínimo para 2000 puertos/interfaces (sumatoria de puertos/interfaces de switches, routers, firewall, etc.)[24].
- La herramienta deberá ser implementada por personal certificado por la marca y deberá incluir un curso de capacitación de al menos 4 horas. El certificado del personal debe ser presentado para la suscripción del contrato. Asimismo, el certificado debe estar relacionado con la solución de monitoreo.[25]

E. Servicios Integrales de Ciberseguridad:

El postor deberá proporcionar herramientas para la supervisión continua del funcionamiento de los enlaces en alquiler, así como establecer medidas de seguridad que garanticen la integridad, disponibilidad y confidencialidad de la información transmitida.

Servicio de Ethical Hacking

- El postor deberá incluir un Servicio de Ethical Hacking que incluya el siguiente alcance como mínimo y a realizarse dentro de los 30 días de firmado el contrato:
- Objetos de evaluación: Routers, firewalls, servicios expuestos hacia Internet (web, correo, bases de datos, DNS, entre otros.) y cualquier componente que constituya un elemento crítico en la seguridad perimetral de la entidad.
- Cantidad de objetos de evaluación: 08 direcciones IP públicas.
- Tipo: Black Box.
- Recopilación de la mayor cantidad de información susceptible de ser utilizada para romper cualquiera de las protecciones de las que pudiera disponer la entidad.

[24] Por absolución de consulta Nº 40 de la empresa ENTEL PERÚ S.A.
[25] Por absolución de consulta Nº 41 de la empresa ENTEL PERÚ S.A.

- Escaneo de la red: Análisis de la red con el objetivo de obtener un mapa de la misma.
- Escaneo de puertos, identificación de servicios y sistemas operativos.
- Determinar, utilizando herramientas comerciales disponibles además de herramientas exclusivas y técnicas manuales, las deficiencias de seguridad que existen en los sistemas incluidos dentro del servicio.
- Intentos de obtener cuentas de usuarios (login y password) del sistema a través de herramientas automáticas y técnicas manuales utilizadas por los hackers. Revisión de passwords por defecto del sistema y diccionarios de passwords.
- Analizar vulnerabilidades en las aplicaciones WEB y componentes que pudieran poner al descubierto la seguridad del servicio, desde Internet.[26]
- Realizar pruebas de Denegación de Servicios previa coordinación con el área informática.

  El servicio debe ser realizado por ingeniero titulado y colegiado de sistemas y/o telecomunicaciones y/o electrónica y/o informático y/o informático y de sistemas[27] con 5 años de experiencia realizando servicios de Ethical Hacking y deberá contar con Certificación vigente ISO/IEC 27001 Senior Lead Implementer, ISO/IEC 27032 Senior Lead Cibersecurity Manager y Certified Ethical Hacker. Dicha documentación deberá ser presentada con la firma del contrato.

Servicio de Ciberdefensa

- El contratista, deberá entregar un Servicio de Ciberdefensa propio o de un tercero, los componentes de este servicio deberán ser alojados en una nube (en caso de ser en nube debe ser alojado en un centro de datos certificado RATED II como mínimo y ubicado en territorio nacional). Se acreditará mediante una declaración jurada del nivel de certificación y dirección del centro de datos, así como copia del certificado RATED II del centro de datos donde se encuentran los componentes del servicio de Ciberdefensa, como parte de la presentación de la oferta;[28] siendo el contratista el encargado de brindar los recursos de hardware y software necesarios para su servicio, dicho servicio debe ser operado por un CyberSOC certificado en ISO27001 en gestión de incidentes, gestión de cambios y ciberseguridad (el postor debe presentar una declaración jurada indicando el nivel de certificación y los procesos, así como la copia del certificado de CyberSOC en ISO 27001, para la presentación de la oferta)[29]. Este servicio deberá permitir mediante el análisis de logs de la solución de seguridad NGFW y Administrador de Ancho de Banda, permita realizar investigaciones y escalar incidentes con las siguientes características:

[26] Por absolución de consulta N° 42 de la empresa ENTEL PERÚ S.A.
[27] Por absolución de consulta N° 64 y 65 de la empresa GTD PERÚ S.A.
[28] Por absolución de consulta N° 43 y 56 de la empresa ENTEL PERÚ S.A.
[29] Por absolución de consulta N° 45 y 56 de la empresa ENTEL PERÚ S.A.

- Capas adicionales como analítica de comportamiento de usuarios (UEBA), 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.
- El portal debe actuar como una interfaz gráfica de usuario (GUI) que muestre investigaciones que fueron realizadas por los componentes (SIEM UEBA, SOAR, I.A.), es decir que la herramienta cuenta con la auditoria de usuarios que realizaron cambios en la misma.
- Capas adicionales al SIEM como analítica de comportamiento de usuarios (UEBA), 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 y/o 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.
- 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.
- La Inteligencia de amenazas debe comprobar todas las comunicaciones salientes; alertar sobre la comunicación con la IP, dominios y URL maliciosos; y finalizar la conexión inmediatamente, todo esto sucede en tiempo real.
- La investigación forense de procesos en curso de presuntas actividades maliciosas y amenazas cibernéticas, incluyendo el análisis post mortem de incidentes verificados, se llevará a cabo utilizando la herramienta parte del servicio de Ciberdefensa. A través de esta herramienta, se identificará el origen del ataque, se determinará la causa raíz y se proporcionará información sobre quién inició el ataque. El análisis forense se realizará de manera integral y exhaustiva utilizando todas las capacidades y

funcionalidades que ofrece la herramienta de Ciberdefensa. Mínimo de 4 horas mensuales de ser requerido.

- Soporte para integración a cualquier solución de seguridad, fuente de registro y Endpoint a través de Syslog.
- 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).
- Deberá de enviar boletines de seguridad con noticias y/o vulnerabilidades que pudiera afectar a la entidad.
- Como parte del servicio se debe incluir un (1) análisis de brechas y amenazas avanzadas persistentes para la red de servidores críticos por cada año de contrato a realizarse dentro de los primeros 30 días de la firma de contrato, para lo cual por cada análisis debe instalar durante al menos 4 semanas un appliance físico de propósito específico (instalado en la Sede Central) y cumplir con lo siguiente:
- La plataforma deberá cumplir mínimamente las siguientes especificaciones:
  - Throughput de Detección: 2 Gbps
  - Sesiones concurrentes (HTTP): 1'500,000
  - Nuevas sesiones / segundo (HTTP): 25,000
  - Storage: 1 TB (HDD)
  - Interfaces: 4 x 1GE
  - Factor de Forma: 1U
- La solución debe desplegarse en modo de operación de tapping.
- Admitir análisis por correlación de amenazas, correlación entre amenazas desconocidas, comportamiento anormal y comportamiento de aplicaciones para descubrir amenazas o ataques potenciales.
- Detección avanzada de amenazas basadas en comportamiento.
- Detección, de al menos 2,000 familias de programas maliciosos, conocidos y desconocidos, incluyendo virus, desbordamiento, gusanos, troyanos, etc.
- Debe ser compatible con descubrir de forma efectiva los bots de la intranet y evitar nuevos ataques de amenazas avanzadas mediante la comparación de la información obtenida con la base de datos de direcciones de C&C.
- Admitir la actualización automática de la biblioteca de firmas de defensa de Botnet/C&C.
- Admitir dos tipos de base de datos de direcciones C&C: la base de datos de direcciones IP y la base de datos de dominio.
- Soportar al menos 8,000 firmas. Debe admitir firmas personalizadas, manual, actualizaciones automáticas de inserción o extracción de firmas y una enciclopedia de amenazas integrada.
- Soporte para desbordamiento de búfer, inyección SQL y detección de ataques por scripting de Cross-site.
- Soportar al menos 13 millones de firmas de antivirus, con actualizaciones de firma manual o automática.

- Detección de ataques de protocolos anormales, detección de ataques ARP, DoS / DDoS, SYN Flood, DNS query flood,
- Verificación de actividad sospechosa y maliciosa en la red de la entidad
- Verificación de vulnerabilidades en la red.
- Se incluirá un informe personalizado con las recomendaciones para tomar las medidas correctivas del caso.
- El postor debe indicar el modelo y marca del sistema o equipos a utilizar antes de iniciar cada análisis.
- Como parte del servicio se debe incluir protección DLP para un total de 100 endpoints con sistema operativo Windows, cuyas versiones podrán ser Windows 10, Windows Server 2016 y en adelante, dicha protección debe contar con las siguientes características mínimas:
  - Capacidad de hacer un descubrimiento y clasificación de los datos en cada endpoint, para la clasificación debe contar con plantillas predefinidas y mecanismos personalizados como OCR, palabras clave, RegEx y huellas digitales.
  - Capacidad de hacer la identificación y registro de las acciones de usuarios sobre los archivos protegidos para detener un intento de robo de datos de acuerdo con las políticas configuradas.
  - Capacidad de monitoreo de los navegadores y uso de servicios en nube de terceros para permitir la transferencia solo de archivos autorizados.
  - Capacidad de aplicar controles sobre periféricos como USB e impresoras.
  - Capacidad para emitir informes y alertas.
  - La disponibilidad de información histórica de los eventos debe ser de por los últimos ~~30~~ 15[30] días

Capacitación

Se deberá incluir un curso o programa de Certificación en Ciberseguridad Aplicada a través de una plataforma online educativa, de al menos 20 horas y brindado por un centro de entrenamiento dedicado y para al menos 4 personas y que incluya laboratorios interactivos, casos reales y simulaciones en tiempo real para cada uno de los siguientes temas:

- Security Operations Center & Management.
- Ciber amenazas, IoCs y Metodologías de Ataques.
- Incidentes, Eventos y Logs.
- Security Information and Event Management (SIEM).
- Detección avanzada de incidentes con Inteligencia de Amenazas.
- Respuesta a Incidentes.

Los accesos a la plataforma de capacitación, podrán estar disponibles al menos 30 días para que los participantes completen el curso o programa y se deberá entregar una constancia al finalizar el curso o programa.[31]

[30] Por absolución de consulta Nº 44 de la empresa ENTEL PERÚ S.A.
[31] Por absolución de consulta Nº 48 de la empresa ENTEL PERÚ S.A.

La capacitación se realizará durante el plazo de implementación del servicio.[32]

El postor ganador debe presentar una declaración jurada indicando el link de la Plataforma Online y la Descripción del Curso o Programa, para la suscripción del contrato[33].

5.3. Consideraciones adicionales:

- ✓ Como parte de la habilitación del presente servicio, el contratista deberá proveer todos los equipos necesarios para cumplir con lo solicitado en el presente documento, dicho equipamiento deberá tener la capacidad de soportar todo el tráfico y ancho de banda según lo solicitado.
- ✓ El contratista deberá realizar los trabajos necesarios dentro o fuera de la entidad para la instalación de los servicios propuestos, sin costo adicional a la entidad.
- ✓ El servicio incluirá todo el equipamiento, conectores, cables, componentes y materiales necesarios para la interconexión de los equipos proporcionados por el contratista con los equipos de comunicación de la entidad.
- ✓ Los equipos de conexión Internet deberán ser administrados por el contratista. Sin embargo, se deberán entregar a la entidad, usuarios de acceso para realizar el monitoreo de estos.
- ✓ La entidad debe tener asignado usuarios, para el acceso a través de un portal web o interface de comando (CLI) mediante credenciales de acceso modo lectura de los routers implementados, solución next generation firewall, solución AntiDDoS y acceso de escritura a la solución de administración de ancho de banda y solución de monitoreo.
- ✓ El contratista deberá realizar la implantación del servicio en forma paralela al servicio actual para mantener la continuidad el servicio, hasta el momento que se finalice la implementación del servicio de internet y también finalice la implementación del nuevo servicio de interconexión mediante enlace de fibra óptica entre Sede Central y las Sedes Regionales de la SUNAFIL.
- ✓ El plazo de contratación de los servicios será de 1095 días calendarios (equivalente a 03 años), duración que se cuenta a partir del día siguiente de firmado el Acta de Inicio del Servicio de Internet Dedicado, entre un representante de la SUNAFIL y del contratista.
- ✓ Los materiales, conectores, componentes, equipos y otros, deberán ser entregados en perfectas condiciones para su uso y deben ser nuevos, en donde los rótulos permitan identificar las características y la marca respectiva y si fuera el caso deberá estar impreso en el mismo bien, en caso se utilice cableado UTP este deberá ser de categoría 6A. Se precisa que los equipos requeridos deberán ser nuevos, de primer uso y contar con tecnología vigente; entiéndase como tecnología vigente que no deben estar en EOL declarados por el fabricante (no encontrarse en End of Sale ni en End of Life).

[32] Por absolución de consulta N° 10 de la empresa NEXTNET S.A.C.
[33] Por absolución de consulta N° 49 y 50 de la empresa ENTEL PERÚ S.A.

- ✓ Todo el material utilizado en la instalación (cables, conectores, adaptadores y otros que se necesiten) deberá ser suministrado por el contratista, estando alineados con las características de los equipos.
- ✓ La implementación final de todo el requerimiento para la puesta en ejecución, deberá garantizar que todos los componentes del servicio solicitado se encuentren totalmente operativos.
- ✓ Quedará a disposición de cada postor, la posibilidad de visitar las instalaciones de la Sede Central de la SUNAFIL, con el fin de informarse debidamente sobre el lugar donde se implementará el servicio, como de todo cuanto pudiera influir para el justiprecio que se haga del mismo.
- ✓ El contratista deberá brindar la transferencia de conocimiento teórico/práctico de forma virtual en la administración, configuración y monitoreo por cada uno de los equipos o solución que forman parte del servicio propuesto con un mínimo de 20 horas académicas para cuatro (04) personas de la Oficina de Tecnologías de la Información y Comunicaciones de la entidad. La transferencia de conocimiento deberá ser brindada en horarios que no afecte las labores cotidianas, dentro del plazo de noventa (90) días para la implementación del servicio. Los costos asociados serán responsabilidad del contratista. La transferencia de conocimiento deberá ser brindada por personal calificado en las soluciones implementadas por el contratista, materia del presente servicio.
- ✓ El contratista debe poseer un Centro Operaciones de Seguridad (SOC) propio para la gestión del servicio, atención y solución de averías de seguridad (24.x7x365) durante el tiempo de duración del contrato. Asimismo, debe contar con un centro de operaciones de Red (NOC) para la gestión del servicio, atención y solución de averías relacionados a los equipos del proveedor y enlaces del servicio de internet. Se acreditará con un certificado emitido por una empresa consultora externa (certificadora en infraestructura) y/o un certificado emitido por una empresa especialista en servicios TI y/o infraestructura y/u otro documento que acredite la operación e infraestructura del NOC & SOC, siendo presentado para la etapa de presentación de la oferta.[34]
- ✓ El proveedor deberá contar con un call center 0800 local y propio para atender las incidencias.
- ✓ El proveedor deberá contar con un Servidor de Nombres de Dominio (DNS) redundantes y distribuidos en locales distintos o Servidor de Nombres de Dominio (DNS) redundantes ubicados en el mismo centro de datos bajo un esquema de alta disponibilidad.
- ✓ El contratista debe ser responsable de la actualización oportuna de parches y de hacer las copias de respaldo de la configuración y políticas de la solución propuesta de tipo on-premise físico y/o virtual que forman parte del servicio.

5.4. Atención de averías y/o requerimientos del servicio:

- ✓ El contratista deberá contar con un centro de operaciones o centro de servicios para registrar las averías y/o requerimientos presentados durante el

[34] Por absolución de consulta Nº 61 de la empresa ENTEL PERÚ S.A.

servicio. La atención debe ser permanente de manera 7x24x365 por los 36 meses que dura el servicio.

- ✓ Se entenderá por avería a una interrupción parcial o total de los servicios, así como a una pérdida de la calidad de los mismos.
- ✓ La entidad podrá efectuar llamadas de servicio de lunes a domingo incluyendo feriados desde las 00:00 hasta las 24:00 horas, ante cualquier incidencia, problema, avería o requerimiento suscitado en el presente servicio (incluye todas las soluciones implementadas según términos de referencia).
- ✓ El contratista establecerá canales de comunicación para la atención de las averías las 24 horas del día, por el tiempo de dure el servicio.
- ✓ El contratista deberá hacer llegar a la SUNAFIL el nivel de escalamiento con los números de contacto, este documento deberá ser entregado como parte de los entregables finales de la implementación del servicio. También se aceptará que a través de las llamadas telefónicas por parte de la Entidad hacia el Contratista sea para el reporte de avería y generación de ticket.
- ✓ Las llamadas de servicio se sujetarán a lo siguiente: Se podrán efectuar telefónicamente o por correo electrónico (considerándose todas estas formas igualmente válidas).
- ✓ En caso de la interrupción o pérdida del servicio de Internet, el centro de operaciones del contratista, deberá remitir un ticket que corresponde a la incidencia o avería presentada. El tiempo de la pérdida de la disponibilidad del servicio será a partir de la interrupción o pérdida del servicio de Internet.
- ✓ La entidad también podrá notificar a través de canales de comunicación la interrupción o pérdida de calidad, incluyendo la siguiente información: fecha, hora, descripción del problema y contacto en la SUNAFIL, la misma que será registrado en el centro de operaciones o centro de servicios del contratista.
- ✓ Los tipos de criticidad respecto averías, problemas o incidencia, se detallan a continuación:
  I. Muy Critico: Falla total del servicio de Internet e impedimento severo de operación. Modo de atención: On site y/o remoto.
  II. Critico: Lentitud, intermitencia o degradación del servicio o perdida de un enlace de Internet. Operación impactada, pero funcional. Modo de atención: On site y/o remoto.
  III. Normal: Solicitud de modificaciones de configuración y absolución de consultas. Modo de atención: On site y/o remoto.
- ✓ Los tiempos para generación de ticket, atención de requerimiento y solución de averías, son los siguientes:
  - El tiempo de respuesta máximo para la generación de un ticket de atención de una incidencia (avería) o requerimiento, será de 30 minutos, contada desde que la entidad reporta la incidencia (avería) y el técnico del Centro de Operaciones del contratista le asigna un ticket de atención.
  - El tiempo máximo de subsanación de una avería muy crítica, por perdida del servicio, a satisfacción de la entidad será contado desde que el centro de operaciones del contratista asigna un ticket de atención hasta la solución de la incidencia (avería), será de cuatro (04) horas como máximo.
  - El tiempo de subsanación de una avería crítica, para los casos de lentitud

o intermitencia o degradación de servicio o perdida de un enlace de Internet, a satisfacción de la entidad será contado desde que el centro de operaciones del contratista asigna un ticket de atención hasta la solución de la incidencia (avería), será de ocho (08) horas como máximo.

- La solicitud de modificaciones de configuración y absolución de consultas, sobre los equipos y/o soluciones que administre el contratista, no deberán exceder de las doce (12) horas, adicionalmente durante el tiempo de contrato el contratista deberá atender modificaciones de configuración de manera ilimitada.
- Se precisa también que, para el reemplazo de los equipos de firewall y administración de ancho de banda en caso de avería o incidencia, se podrá aceptar los tiempos de RMA del fabricante.
- Toda actividad o provisión de bienes que tenga que ejecutar el contratista para subsanar la avería y continuar con la prestación del servicio afectado se realizará sin costo para la entidad.
- El contratista debe asegurar que se cumpla el porcentaje de disponibilidad del servicio solicitado.
- No serán considerados como parte del tiempo de atención de acuerdo a los SLAs requeridos, los tiempos ocasionados por los siguientes casos excluidos:
  - ✓ En situaciones de catástrofe, vandalismo, robos y eventos naturales (terremotos, desplazamientos, lluvias, huaycos) u otros excepcionales como los causados por accidentes en el local como aniego, incendio, derrumbe.
  - ✓ Actividades de mantenimiento planificado por parte de la Entidad o del proveedor actual de la Entidad, a raíz de las cuales la red o parte de esta queda fuera de servicio por un período.
  - ✓ Interrupción o degradación del servicio causado por negligencia, error u omisión de cliente. (Ej. Manipulación de cables, cambios en configuración de equipos, etc.)
  - ✓ Interrupción o degradación del servicio causado por falla en los equipos de propiedad y responsabilidad del cliente (Ej. Switches LAN, UPS, etc.)
  - ✓ Falla o suspensión eléctrica en la localidad.
  - ✓ En caso el contacto de la entidad registrado en el ticket de avería no esté disponible, demore en responder y/o se presenten demoras de permisos de accesos para la atención de la avería por parte de la entidad.
  - ✓ En caso no exista facilidades para el transporte (huelgas en carretera, deslizamientos, disponibilidad de medios de transporte, restricciones gubernamentales, emergencias sanitarias, aislamiento focalizado, inmovilización social, rondas campesinas y/o pobladores que no permitan el ingreso a sus localidades u otro ocasionado por terceros), lo cual debe ser comprobado por el contratista.
  - ✓ Eventos de avería masiva causada por terceros, lo cual debe ser comprobado por el contratista.

5.5. Prestaciones accesorias a la prestación principal:

No aplica.

5.6. Plan de Trabajo:

- ✓ El contratista deber presentar un plan de trabajo para la implementación del servicio, el mismo que deberá ser presentado a los diez (10) días como máximo contados a partir del día siguiente de suscrito el contrato, estos días serán parte del plazo de implementación del servicio.
- ✓ La implementación deberá estar a cargo de un jefe de Proyecto, quien se encargará de coordinar con la Oficina de Tecnologías de la Información y Comunicaciones de la SUNAFIL la implementación y puesta en producción del servicio en mención.

5.7. Requisitos del Proveedor y personal:

El postor deberá cumplir con los siguientes requisitos:

- ✓ El postor ganador de la buena pro como parte de la documentación para la suscripción del contrato, deberá demostrar tener acceso a (02) salidas Internacional (10 Gbps como mínimo) y con la finalidad de tener redundancia en las salidas internacionales.
- ✓ El postor ganador de la buena pro como parte de la documentación para la suscripción del contrato, deberá demostrar contar con dos (02) operadores TIER1 internacionales distintos con rutas físicas diferentes con los que deberá tener conexión directa a través de los enlaces de fibra óptica. Con ello se busca garantizar la continuidad del acceso a Internet requerido.
- ✓ El postor debe validar tener la autorización del Ministerio de Transportes y Comunicaciones para la prestación del servicio en la modalidad de Internet Servís o Proveedor (ISP), con cobertura a nivel nacional, acreditado con Copia de Autorización del MTC para la prestación del servicio, esto debe ser anexada como documentación obligatoria, para la evaluación técnica en la presentación de la oferta. También se aceptará una copia del link que el MTC tiene publicado de REGISTRO PARA SERVICIO DE VALOR AÑADIDO en la Plataforma Digital Única del Estado Peruano y/o un Oficio emitido por el MTC, el cual precisan las Concesiones y/o Títulos Habilitantes para la prestación de Servicios Públicos de Telecomunicaciones, con las que cuenta el Postor y/o copia simple del Certificado de Registro de Empresas Prestadoras de Servicios de Valor Añadido emitido por el Ministerio de Trasporte y Comunicaciones.
- ✓ El postor ganador deberá ser miembro activo del NAP PERÚ, el cual se debe acreditar mediante un documento para la suscripción del contrato.
- ✓ El postor ganador de la buena pro como parte de la documentación para la suscripción del contrato, deberá demostrar las ubicaciones físicas distintas de los Servidores de Nombres de Dominio (DNS) redundantes o las direcciones IP de los Servidores de Nombres de Dominio (DNS) redundantes ubicados en el centro de datos del proveedor bajo un esquema de alta disponibilidad.
- ✓ El postor ganador de la buena pro como parte de la documentación para la suscripción del contrato, deberá remitir las direcciones de sus nodos y/o PoP de los enlaces principal y de contingencia, debiendo demostrar que las

conexiones de los enlaces para la sede central vienen de rutas diferentes.

- ✓ El postor ganador deberá brindar una tabla de escalamiento para la atención de averías, el cual deberá indicar los números telefónicos de los responsables, lo cual se deberá presentar como documento adicional para la suscripción del contrato.
- ✓ El postor ganador de la buena pro como parte de la documentación para la suscripción del contrato, de acuerdo al formato inferior deberá presentar la relación de la marca y modelo de los equipos y soluciones que forman parte del servicio solicitado, sean si estas soluciones estén on-premise o en la nube.

Solución	Marca	Modelo	Tipo de Solución on-premise o nube	N° de Folio presentado por el Postor donde muestre la relación de las soluciones ofertadas
Equipamiento de Enrutamiento para el servicio de Internet				Folio N°....
Solución AntiDDoS				Folio N°....
Optimizador de Ancho de Banda				Folio N°....
Solución Firewalls				Folio N°....
Solución de Monitoreo				Folio N°....

- ✓ El postor ganador de la buena pro como parte de la documentación para la suscripción del contrato, de acuerdo al formato inferior deberá demostrar de forma foliada las validaciones de las características esenciales para la solución el optimizador de ancho de banda, mediante la presentación de hojas técnicas y/o folletos y/o catálogos y/o datasheet y/o link del fabricante y/o carta de fabricante. (El postor ganador deberá asegurar que con dicha carta de fabricante se demuestre y/o valide cada característica esencial solicitada), donde se precise el cumplimiento técnico; para la solución indicada a nivel hardware y software en el idioma original.
- ✓ El Contratista deberá tener el personal para la ejecución del servicio solicitado, deberá estar liderado por un Jefe de Proyecto e integrado por personal técnico de acuerdo a los siguientes perfiles:

Perfil del personal:

- Jefe de Proyecto (01 persona): Gestionar el proyecto de manera integral en base a las buenas prácticas del PMI, debe contar con Certificado PMP, será el encargado de coordinar con la entidad la implementación del servicio en mención, a través de reuniones técnicas debiendo elaborar para cada reunión un acta, a su vez deberá presentar los entregables

solicitados en el presente documento.

- Personal técnico (02 personas como mínimo): Realizar la instalación completa del equipamiento ofertado, realizar las configuraciones solicitadas por la SUNAFIL para la implementación del servicio integral.

Formación Académica y experiencia:

Jefe de Proyecto (Supervisor de servicio) – (01 persona):

- Profesional de las siguientes carreras: Bachiller o Ingeniero Titulado en Sistemas o Electrónica o Computación o Informática o Redes o Telecomunicaciones o Redes y Comunicaciones de Datos.
- Deberá contar con Certificado de PMP y/o programa especializado en dirección y gestión de las Telecomunicaciones y/o Diplomado de Gestión de Proyectos y/o Gerencia de Proyectos y Calidad y/o Diploma de especialización en gestión de proyectos de telecomunicaciones con un mínimo de 90 horas.
- Contar con dos (02) años como mínimo de experiencia en gestión de proyectos de Interconexión o Internet, o gestión y/o supervisión de proyectos de implementación en servicios de internet e internet dedicado o [35], en gestionar y/o supervisar y/o liderar la implementación de proyectos de telecomunicaciones (acceso a internet y/o transmisión de datos y/o red privada virtual) y/o servicios de TI, como jefe de Proyectos. También se aceptará la denominación de cargos como: gerente de proyectos y/o director de proyectos y/o gestor de proyectos y/o jefe de servicios y/o supervisor de proyecto y/o gestor de TI y/o coordinador de proyecto y/o analista de proyecto u otro cargo relacionado a proyectos[36].

Personal técnico-I (01 persona como mínimo):

- Técnico titulado o Bachiller o Ingeniero Titulado en Sistemas y/o Electrónica y/o Computación y/o Informática y/o Redes y/o Telecomunicaciones y/o (Redes y Comunicaciones de Datos).[37]
- Certificado en la solución de equipos routers propuestos por el postor para la instalación del servicio de internet. La certificación debe ser emitida por parte del fabricante de la solución ofertada. También se aceptarán cursos de equipamiento de comunicaciones y/o de enrutamiento de red de comunicaciones de al menos 12 horas en total, debiendo presentar los certificados correspondientes.
- Experiencia de 02 años como mínimo en implementación y/o soporte de equipos de comunicaciones para interconexión de datos o internet dedicado y/o en la implementación y/o instalación y/o configuración de los servicios de telecomunicaciones (acceso a internet y/o transmisión de datos y/o red privada virtual) y/o soporte de servicios de telecomunicaciones, como coordinador y/o especialista y/o implementador y/o administrador y/o analista de equipos de comunicaciones para interconexión de datos/transmisión de datos/red privada virtual o internet

[35] Por absolución de consulta N° 32 de la empresa ENTEL PERU S.A.
[36] Por absolución de consulta N° 31 de la empresa ENTEL PERÚ S.A
[37] Por absolución de consulta N° 51 de la empresa ENTEL PERÚ S.A

dedicado u otro cargo relacionado a la función del personal técnico I[38].

Personal técnico-II (01 persona como mínimo):

- Técnico titulado o Bachiller o Ingeniero Titulado en Sistema y/o Electrónica y/o Computación y/o Informática y/o Redes y/o Telecomunicaciones y/o (Redes y Comunicación de Datos)[39].
- Certificado en la solución de administración de Ancho de Banda. El certificado debe ser emitida por parte del fabricante de la solución ofertada.
- Certificado en la solución de firewalls. El certificado debe ser emitida por parte del fabricante de la solución ofertada.
- Experiencia de 02 años como mínimo en implementación y/o soporte de equipos de administración de ancho de banda o de seguridad.

El postor ganador deberá presentar el certificado PMP y/o programa especializado en dirección y gestión de las Telecomunicaciones y/o Diplomado de Gestión de Proyectos y/o Gerencia de Proyectos y Calidad y/o diploma de especialización en gestión de proyectos de telecomunicaciones con un mínimo de 90 horas, para el jefe de proyecto y demás certificados solicitados del personal técnico I y personal técnico II, como documentación adicional para la suscripción del contrato.

5.8. Normas obligatorias y/o voluntarias:

No aplica.

VI. PLAZO DE PRESTACIÓN

Plazo de ejecución:

El servicio tendrá una duración de 1095 días calendarios (equivalente a 03 años), computados a partir del día siguiente de firmado el Acta de Inicio.

Plazo de implementación:

El plazo para la ejecución de la implementación del proyecto, será de hasta noventa (90) días calendarios contados desde el día siguiente de la firma del contrato; según detalle:

- De hasta 85 días calendarios para Implementación del Servicio de Internet Dedicado, desde el día siguiente de la firma del contrato.
- De hasta 90 días calendarios para la entrega de documentación solicitada como entregable final de implementación, desde el día siguiente de la firma del contrato.

6.1. Entregables:

6.1.1 Entregable Final de Implementación

El contratista deberá presentar los siguientes documentos, según plazos señalados a continuación:

- Informe técnico final, en el cual se detalle:
  - ✓ El diagrama topológico (Diseño considerando el tipo de enlace de conectividad ofertado; así como el ancho de banda propuesto para

[38] Por absolución de consulta N° 31 de la empresa ENTEL PERÚ S.A
[39] Por absolución de consulta N° 52 de la empresa ENTEL PERÚ S.A

la Sede Central).

- ✓ Numero de Circuito o del Enlace de Internet para temas de Soporte.
- ✓ Direcciones IP Públicas.
- ✓ Inventario, descripción y cantidad del equipamiento de red instalada como parte del requerimiento para el presente servicio.
- ✓ Detalle de la implementación (instalación, Configuración y Puesta en Producción o checklist), en el cual se detalle los procedimientos y/o configuración realizada, equipos utilizados.
- ✓ Credenciales de acceso modo lectura de los routers implementados, monitoreo de routers, solución AntiDDoS y acceso de escritura a la solución de administración de ancho de banda.

6.1.2 Entregables mensuales de Servicio

El Contratista deberá presentar un informe mensual conjuntamente con la facturación correspondiente a la prestación del servicio; según se detalla:

- Reporte mensual de las incidencias ocurridas.
- Reporte mensual de la disponibilidad del servicio.
- Reporte mensual de la utilización del ancho de banda de los enlaces de internet dedicado en la Sede Central de SUNAFIL.
- Reporte mensual de control de tráfico del equipo administrador de ancho de banda.
- Reporte de control y recomendaciones del servicio de la solución de protección AntiDDoS o Reportes mensuales técnicos generados por la herramienta, con información sobre el detalle de ataques por origen, destino, por aplicación, fecha y hora.

Dicho informe deberá ser entregado por el contratista dentro de los diez (10) primeros días calendario del siguiente periodo de la prestación de servicio en ejecución.

Los documentos entregables se entregarán en mesa de partes virtual de SUNAFIL sito en URL: https://aplicativosweb6.sunafil.gob.pe/si.mesaVirtual/ o Mesa de Partes Presencial ubicada en Av. Salaverry 655 – 4to piso, Jesús María, Lima, en el horario de 8:30 am a 16:30 horas. Asimismo, los entregables serán necesarios para la conformidad técnica.

VII. LUGAR DE LA PRESTACIÓN

En la Sede Central de la SUNAFIL, ubicada en Av. Salaverry 655 - 4to. Piso, Jesús María, Lima, adecuándose a los horarios requeridos y ambientes establecidos por la entidad.

VIII. CONFORMIDAD DEL SERVICIO

Conformidad del Servicio de Implementación:

La conformidad será emitida por la Oficina de Tecnologías de la Información y Comunicaciones, dentro de un plazo máximo de siete (07) días calendarios de producida la recepción de los entregables finales de la Implementación del Servicio. (Ver 6.1.1).

Conformidad de la Prestación del Servicio:

La conformidad será emitida por la Oficina de Tecnologías de la Información y

Comunicaciones, dentro de un plazo máximo de siete (07) días calendarios de producida la recepción de los informes mensuales emitidos por el Contratista. (Ver 6.1.2).

IX. FORMA DE PAGO

La Entidad realizará el pago de la contraprestación pactada a favor del contratista en de forma periódica en cuotas mensuales, cuyo porcentaje de pago serán en partes iguales en función al monto del contrato, previa conformidad de la Oficina de Tecnologías de la Información y Comunicaciones, para lo cual el contratista presentará mensualmente un informe del servicio integral dentro de los diez (10) primeros días calendario del siguiente periodo de la prestación de servicio en ejecución.

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

- ✓ Informe del funcionario responsable de la Oficina de Tecnologías de la Información y Comunicaciones emitiendo la conformidad de la prestación efectuada, previa entrega, por parte del contratista, de un informe mensual del servicio integral, el cual debe ser entregado dentro de los diez (10) primero días calendarios del siguiente periodo de la prestación de servicio en ejecución.
- ✓ Comprobante de pago.
- ✓ Entregables de acuerdo al detalle señalado en el numeral 6.1.2 de los términos de referencia.

Los documentos se entregarán en mesa de partes virtual de SUNAFIL sito en URL: https://aplicativosweb6.sunafil.gob.pe/si.mesaVirtual/ o Mesa de Partes Presencial ubicada en Av. Salaverry 655 – 4to piso, Jesús María, Lima, en el horario de 8:30 am a 16:30 horas. Asimismo, los entregables serán necesarios para la conformidad técnica.

X. PENALIDADES APLICABLES

10.1. Penalidades por mora:

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 atraso, de acuerdo a la siguiente fórmula:

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

Donde F tiene los siguientes valores:

a) Para plazos menores o iguales a sesenta (60) días: F = 0.40.
b) Para plazos mayores a sesenta (60) días: F=0.25

10.2. Otras penalidades:

La entidad aplicará penalidades por incumplimiento en la disponibilidad del servicio y por retraso en la presentación de entregables dentro de la ejecución del servicio, de acuerdo a la siguiente tabla:

Interrupciones del Servicio de Internet Dedicado de la Sede Central (imputables al contratista)	
Porcentaje de disponibilidad (Tolerancia) del servicio	**% Deducible de la facturación mensual**
Mayor o igual a 99.90%	0%
Menor a 99.90% y Mayor o igual a 99.50%	1%
Menor a 99.50% y Mayor o igual a 99.00%	3%
Menor a 99.00% y Mayor o igual a 98.00%	5%
Menor a 98.00% y Mayor o igual a 97.00%	7%
Menor a 97.00% y Mayor o igual a 96.00%	9%
Menor a 96.00%	10%
100% = 24 horas x n (n = días del mes. Por ejemplo: en marzo, n=31; en abril, n=30)	
Para efectos del cálculo de la penalidad, se acumularán las horas en las que el servicio se haya interrumpido en el mes. Para efectos de la penalidad, no se contabilizarán para la disponibilidad del servicio, las interrupciones del servicio a causa de terceros o desastres naturales.	

La entidad aplicará penalidades por incumplimiento en la presentación tardía de los entregables del servicio y demora en solución de averías, de acuerdo al siguiente detalle:

N°	Supuestos de aplicación de penalidad	Penalidad	Procedimiento
1	Por demora en la presentación de los entregables mensuales, de acuerdo a los plazos establecidos en los términos de referencia.	1% UIT por cada día de retraso	Informe técnico de la OTIC.
2	Tiempo de resolución de una avería muy crítica	0.3% UIT por cada hora de retraso	Informe técnico de la OTIC.
3	Tiempo de resolución de una avería critica	0.2% UIT por cada hora de retraso	Informe técnico de la OTIC.
4	Tiempo de resolución de una incidencia o requerimiento normal	0.1% UIT por cada hora de retraso	Informe técnico de la OTIC.

XI. CONFIDENCIALIDAD

El contratista queda expresamente obligado a mantener absoluta confidencialidad y reserva sobre la información fruto de la compra, servicio, implementación, o cualquier otro aspecto relacionado con la entidad, no pudiendo difundir, aplicar ni comunicar a terceros información a la que haya tenido acceso durante ejecución del servicio, no pudiendo copiar o utilizar esta información con fin distinto a su objeto ni tampoco ceder a otros ni siquiera a efectos de conservación. Esta obligación se mantendrá incluso después de la firma de conformidad del servicio.

Se precisa que se encuentran excluidos de la cláusula de confidencialidad los siguientes supuestos:

1. Resulte accesible al público por causa distinta del incumplimiento de la obligación de confidencialidad por la parte receptora.
2. Haya sido publicada con anterioridad a la fecha de la firma de contrato.
3. Se encuentre en poder de la parte receptora y no esté sujeta a cualquier otro

impedimento o restricción puesto de manifiesto a la otra Parte en el momento de la revelación o luego de ella.

4. Sea recibida a través de terceros sin restricciones y sin que implique incumplimiento del Contrato.
5. Sea independientemente desarrollada por la parte receptora, siempre que no se hubiese utilizado para ello la información confidencial proporcionada por la otra Parte.
6. Deba ser revelada para dar cumplimiento de una orden de naturaleza judicial o administrativa, en cuyo caso la Parte receptora deberá informar a la otra Parte en forma inmediata a la sola recepción de la citada orden.

XII. RESPONSABILIDAD POR VICIOS OCULTOS

El contratista es responsable por la calidad ofrecida y por los vicios ocultos por tres (03) años contado a partir de la conformidad otorgada por la Entidad. La recepción conforme de la entidad no enerva su derecho a reclamar posteriormente por defectos o vicios ocultos.

XIII. DECLARACIÓN DEL POSTOR

El postor declara que ni él ni ninguno de los accionistas, socios o empresas vinculadas, ni cualquiera de sus respectivos directores, funcionarios, empleados, asesores, representantes legales o agentes, ha pagado, recibido, ofrecido ni intentado pagar, recibir u ofrecer ningún pago o comisión ilegal en relación con la presente contratación.

XIV. REQUISITOS DE CALIFICACIÓN

A	**CAPACIDAD LEGAL**
	HABILITACIÓN
	Requisitos:
	Autorización del Ministerio de Transportes y Comunicaciones para la prestación del servicio en la modalidad de Internet Servís o Proveedor (ISP), con cobertura a nivel nacional.
	Importante
	De conformidad con la Opinión N° 186-2016/DTN, la habilitación de un postor, está relacionada con cierta atribución con la cual debe contar el proveedor para poder llevar a cabo la actividad materia de contratación, este es el caso de las actividades reguladas por normas en las cuales se establecen determinados requisitos que las empresas deben cumplir a efectos de estar habilitadas para la ejecución de determinado servicio o estar autorizadas para la comercialización de ciertos bienes en el mercado.
	Acreditación: Se acreditará con la copia simple de la documentación que autoriza la prestación del servicio de Telecomunicaciones en el Perú, en la modalidad Internet Servicie Provider – ISP. También se aceptará una copia del link que el MTC tiene publicado de REGISTRO PARA SERVICIO DE VALOR AÑADIDO en la Plataforma Digital Única del Estado Peruano y/o un Oficio emitido por el MTC, el cual precisan las Concesiones y/o Títulos Habilitantes para la prestación de Servicios Públicos de

	Telecomunicaciones, con las que cuenta el Postor y/o copia simple del Certificado de Registro de Empresas Prestadoras de Servicios de Valor Añadido emitido por el Ministerio de Transporte y Comunicaciones. *Importante* *En el caso de consorcios, cada integrante del consorcio que se hubiera comprometido a ejecutar las obligaciones vinculadas directamente al objeto de la convocatoria debe acreditar este requisito.*
B	**CAPACIDAD TÉCNICA Y PROFESIONAL**
B.3	**CALIFICACIONES DEL PERSONAL CLAVE**
B.3.1	**FORMACIÓN ACADÉMICA**
	Requisitos: Bachiller o Ingeniero Titulado en Sistemas o Electrónica o Computación o Informática o Redes o Telecomunicaciones o Redes y Comunicaciones de Datos, del personal clave como Jefe de Proyecto. Técnico titulado o Bachiller o Ingeniero Titulado en Sistemas y/o Electrónica y/o Computación y/o Informática y/o Redes y/o Telecomunicaciones y/o (Redes y Comunicaciones de Datos)[40], del personal clave requerido como Personal Técnico – I. Técnico titulado o Bachiller o Ingeniero Titulado en Sistemas y/o Electrónica y/o Computación y/o Informática y/o Redes y/o Telecomunicaciones y/o (Redes y Comunicaciones de Datos)[41], del personal clave requerido como Personal Técnico – II. Acreditación: El grado de bachiller, título profesional y/o título técnico será verificado por el comité de selección en el Registro Nacional de Grados Académicos y Títulos Profesionales en el portal web de la Superintendencia Nacional de Educación Superior Universitaria - SUNEDU a través del siguiente link: https://enlinea.sunedu.gob.pe/ // o en el Registro Nacional de Certificados, Grados y Títulos a cargo del Ministerio de Educación a través del siguiente link: http://www.titulosinstitutos.pe/, según corresponda. En caso del grado de bachiller, título profesional y/o título técnico 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.

[40] Por absolución de consulta N° 51 de la empresa ENTEL PERÚ S.A
[41] Por absolución de consulta N° 52 de la empresa ENTEL PERÚ S.A

B.4	EXPERIENCIA DEL PERSONAL CLAVE
	Requisitos: **Jefe de Proyecto – (01 persona):** Contar con dos (02) años como mínimo de experiencia en gestión de proyectos de Interconexión o Internet, o gestión y/o supervisión de proyectos de implementación en servicios de internet e internet dedicado o [42], en gestionar y/o supervisar y/o liderar la implementación de proyectos de telecomunicaciones (acceso a internet y/o transmisión de datos y/o red privada virtual) y/o servicios de TI, como Jefe de Proyectos. También se aceptará la denominación de cargos como: gerente de proyectos y/o director de proyectos y/o gestor de proyectos y/o jefe de servicios y/o supervisor de proyecto y/o gestor de TI y/o coordinador de proyecto y/o analista de proyecto u otro cargo relacionado a proyectos, del personal clave requerido como Jefe de Proyecto. **Personal técnico-I (01 persona como mínimo):** Experiencia de 02 años como mínimo en implementación y/o soporte de equipos de comunicaciones para interconexión de datos o internet dedicado y/o en la implementación y/o instalación y/o configuración de los servicios de telecomunicaciones (acceso a internet y/o transmisión de datos y/o red privada virtual) y/o soporte de servicios de telecomunicaciones, como coordinador y/o especialista y/o implementador y/o administrador y/o analista de equipos de comunicaciones para interconexión de datos/transmisión de datos/red privada virtual o internet dedicado u otro cargo relacionado a la función del personal técnico I, del personal clave requerido como Personal Técnico – I. **Personal técnico-II (01 persona como mínimo):** Experiencia de 02 años como mínimo en implementación y/o soporte de equipos de administración de ancho de banda o de seguridad, como especialista o profesional o implementador o administrador o analista u otro cargo relacionado a la función del personal técnico II[43], del personal clave requerido como Personal Técnico – II. De presentarse experiencia ejecutada paralelamente (traslape), para el cómputo del tiempo de dicha experiencia sólo se considerará una vez el periodo traslapado. Acreditación: La experiencia del personal clave se acreditará con cualquiera de los siguientes documentos: (i) copia simple de contratos y su respectiva conformidad o (ii) constancias o (iii) certificados o (iv) cualquier otra documentación que, de manera fehaciente demuestre la experiencia del personal propuesto. **Importante** • *Los documentos que acreditan la experiencia deben incluir los nombres y apellidos del personal clave, el cargo desempeñado, el plazo de la*

[42] Por absolución de consulta N° 32 de la empresa ENTEL PERU S.A.
[43] Por absolución de consulta N° 31 de la empresa ENTEL PERÚ S.A

	prestación indicando el día, mes y año de inicio y culminación, el nombre de la Entidad u organización que emite el documento, la fecha de emisión y nombres y apellidos de quien suscribe el documento. • *En caso los documentos para acreditar la experiencia establezcan el plazo de la experiencia adquirida por el personal clave en meses sin especificar los días se debe considerar el mes completo.* • *Se considerará aquella experiencia que no tenga una antigüedad mayor a veinticinco (25) años anteriores a la fecha de la presentación de ofertas.* • *Al calificar la experiencia del personal, se debe valorar de manera integral los documentos presentados por el postor para acreditar dicha experiencia. En tal sentido, aun cuando en los documentos presentados la denominación del cargo o puesto no coincida literalmente con aquella prevista en las bases, se deberá validar la experiencia si las actividades que realizó el personal corresponden con la función propia del cargo o puesto requerido en las bases.*	
C	**EXPERIENCIA DEL POSTOR EN LA ESPECIALIDAD**	
	Requisitos: El postor debe acreditar un monto facturado acumulado equivalente a dos millones de soles (S/. 2´000,000), por la contratación de servicios iguales o similares al objeto de la convocatoria, durante los ocho (8) años anteriores a la fecha de la presentación de ofertas que se computarán desde la fecha de la conformidad o emisión del comprobante de pago, según corresponda. Se considerarán servicios similares los siguientes: Servicio de Interconexión de Datos y/o Servicio de Internet Dedicado o Simétrico y/o Servicio de Ancho de Banda y/o Servicio de Internet en general y/o Servicio Integral de Telecomunicaciones y/o Servicio de Transmisión de datos y/o Servicio de Internet dedicado y enlace de datos y/o servicio de arrendamiento de circuitos o tránsito de internet y/o Servicio de transmisión de voz y datos. Acreditación: La experiencia del postor en la especialidad se acreditará con copia simple de (i) contratos u órdenes de servicios, y su respectiva conformidad o constancia de prestación; o (ii) comprobantes de pago cuya cancelación se acredite documental y fehacientemente, con voucher de depósito, nota de abono, reporte de estado de cuenta, cualquier otro documento emitido por Entidad del sistema financiero que acredite el abono o mediante cancelación en el mismo comprobante de pago [1], correspondientes a un máximo de veinte (20) contrataciones. En caso los postores presenten varios comprobantes de pago para acreditar una sola	

[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".*

	contratación, se debe acreditar que corresponden a dicha contratación; de lo contrario, se asumirá que los comprobantes acreditan contrataciones independientes, en cuyo caso solo se considerará, para la evaluación, las veinte (20) primeras contrataciones indicadas en el **Anexo N° 8** referido a la Experiencia del Postor en la Especialidad. En el caso de servicios de ejecución periódica o continuada, solo se considera como experiencia la parte del contrato que haya sido ejecutada durante los ocho (8) años anteriores a la fecha de presentación de ofertas, debiendo adjuntarse copia de las conformidades correspondientes a tal parte o los respectivos comprobantes de pago cancelados. En los casos que se acredite experiencia adquirida en consorcio, debe presentarse la promesa de consorcio o el contrato de consorcio del cual se desprenda fehacientemente el porcentaje de las obligaciones que se asumió en el contrato presentado; de lo contrario, no se computará la experiencia proveniente de dicho contrato. Asimismo, cuando se presenten contratos derivados de procesos de selección convocados antes del 20.09.2012, la calificación se ceñirá al método descrito en la Directiva "Participación de Proveedores en Consorcio en las Contrataciones del Estado", debiendo presumirse que el porcentaje de las obligaciones equivale al porcentaje de participación de la promesa de consorcio o del contrato de consorcio. En caso que en dichos documentos no se consigne el porcentaje de participación se presumirá que las obligaciones se ejecutaron en partes iguales. Si el titular de la experiencia no es el postor, consignar si dicha experiencia corresponde a la matriz en caso que el postor sea sucursal, o fue transmitida por reorganización societaria, debiendo acompañar la documentación sustentatoria correspondiente. Si el postor acredita experiencia de 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.*

CAPÍTULO IV
FACTORES DE EVALUACIÓN

La evaluación se realiza sobre la base de cien (100) puntos.

Para determinar la oferta con el mejor puntaje y el orden de prelación de las ofertas, se considera lo siguiente:

FACTOR DE EVALUACIÓN		PUNTAJE / METODOLOGÍA PARA SU ASIGNACIÓN
A.	**PRECIO**	
	Evaluación: Se evaluará considerando el precio ofertado por el postor. Acreditación: Se acreditará mediante el documento que contiene el precio de la oferta **(Anexo N° 6)**.	La evaluación consistirá en otorgar el máximo puntaje a la oferta de precio más bajo y otorgar a las demás ofertas puntajes inversamente proporcionales a sus respectivos precios, según la siguiente fórmula: $Pi = \frac{Om \times PMP}{Oi}$ **i** = Oferta **Pi** = Puntaje de la oferta a evaluar **Oi** = Precio i **Om** = Precio de la oferta más baja **PMP** = Puntaje máximo del precio **[100] puntos**

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 ACCESO DEDICADO DE INTERNET DE BANDA ANCHA PARA LA SUNAFIL**, que celebra de una SUPERINTENDENCIA NACIONAL DE FISCALIZACION LABORAL, en adelante LA ENTIDAD, con RUC Nº 20555195444, con domicilio legal en Av. Salaverry Nro. 655 2do piso, Jesús María representada por [……..…], identificado con DNI Nº [……], y de otra parte […….....], con RUC Nº [.....], con domicilio legal en […….....], inscrita en la Ficha N° […….....] Asiento N° […….....] del Registro de Personas Jurídicas de la ciudad de [……], debidamente representado por su Representante Legal, […….....], con DNI N° [……..], según poder inscrito en la Ficha N° [……..], Asiento N° [……] del Registro de Personas Jurídicas de la ciudad de [……], a quien en adelante se le denominará EL CONTRATISTA en los términos y condiciones siguientes:

CLÁUSULA PRIMERA: ANTECEDENTES

Con fecha [……..], el comité de selección adjudicó la buena pro del **CONCURSO PÚBLICO Nº 01-2025-SUNAFIL,** para la contratación de **SERVICIO DE ACCESO DEDICADO DE INTERNET DE BANDA ANCHA PARA LA SUNAFIL,** a [INDICAR NOMBRE DEL GANADOR DE LA BUENA PRO], cuyos detalles e importe constan en los documentos integrantes del presente contrato.

CLÁUSULA SEGUNDA: OBJETO

El presente contrato tiene por objeto **SERVICIO DE ACCESO DEDICADO DE INTERNET DE BANDA ANCHA PARA LA SUNAFIL.**

CLÁUSULA TERCERA: MONTO CONTRACTUAL

El monto total del presente contrato asciende a [CONSIGNAR MONEDA Y MONTO], que incluye todos los impuestos de Ley.

Este monto comprende el costo del servicio, todos los tributos, seguros, transporte, inspecciones, pruebas y, de ser el caso, los costos laborales conforme a la legislación vigente, así como cualquier otro concepto que pueda tener incidencia sobre la ejecución del servicio materia del presente contrato.

CLÁUSULA CUARTA: DEL PAGO[16]

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

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

LA ENTIDAD debe efectuar el pago de las contraprestaciones pactadas a favor del CONTRATISTA dentro de los diez (10) días calendario siguientes de otorgada la conformidad de los servicios,

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

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 mil noventa y cinco (1095) días calendarios (equivalente a 03 años), computados a partir del día siguiente de firmado el Acta de Inicio.

Plazo de implementación:
El plazo para la ejecución de la implementación del proyecto, será de hasta noventa (90) días calendarios contados desde el día siguiente de la firma del contrato; según detalle:
• De hasta 85 días calendarios para Implementación del Servicio de Internet Dedicado, desde el día siguiente de la firma del contrato.
• De hasta 90 días calendarios para la entrega de documentación solicitada como entregable final de implementación, desde el día siguiente de la firma del contrato.

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 DÉCIMA: CONFORMIDAD DE LA PRESTACIÓN DEL SERVICIO

La conformidad de la prestación del servicio se regula por lo dispuesto en el artículo 168 del Reglamento de la Ley de Contrataciones del Estado. La conformidad será otorgada por la Oficina de Tecnologías e la Información y Comunicaciones en el plazo máximo de [siete (7) días de producida la recepción.

De existir observaciones, LA ENTIDAD las comunica al CONTRATISTA, indicando claramente el

sentido de estas, otorgándole un plazo para subsanar no menor de dos (2) ni mayor de ocho (8) días. Dependiendo de la complejidad o sofisticación de las subsanaciones a realizar el plazo para subsanar no puede ser menor de cinco (5) ni mayor de quince (15) días. Si pese al plazo otorgado, EL CONTRATISTA no cumpliese a cabalidad con la subsanación, LA ENTIDAD puede otorgar al CONTRATISTA periodos adicionales para las correcciones pertinentes. En este supuesto corresponde aplicar la penalidad por mora desde el vencimiento del plazo para subsanar.

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

CLÁUSULA UNDÉCIMA: DECLARACIÓN JURADA DEL CONTRATISTA

EL CONTRATISTA declara bajo juramento que se compromete a cumplir las obligaciones derivadas del presente contrato, bajo sanción de quedar inhabilitado para contratar con el Estado en caso de incumplimiento.

CLÁUSULA DUODÉCIMA: RESPONSABILIDAD POR VICIOS OCULTOS

La conformidad del servicio por parte de LA ENTIDAD no enerva su derecho a reclamar posteriormente por defectos o vicios ocultos, conforme a lo dispuesto por los artículos 40 de la Ley de Contrataciones del Estado y 173 de su Reglamento.

El plazo máximo de responsabilidad del contratista es de [CONSIGNAR TIEMPO EN AÑOS, NO MENOR DE UN (1) AÑO] año(s) contado a partir de la conformidad otorgada por LA ENTIDAD.

CLÁUSULA DÉCIMA TERCERA: PENALIDADES

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

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

Donde:

F = 0.25 para plazos mayores a sesenta (60) días o;
F = 0.40 para plazos menores o iguales a sesenta (60) días.

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

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

Otras penalidades:
La entidad aplicará penalidades por incumplimiento en la disponibilidad del servicio y por retraso en la atención de averías dentro de la ejecución del servicio, de acuerdo a la siguiente tabla:

Interrupciones del Servicio de Internet Dedicado de la Sede Central (imputables al contratista)	
Porcentaje de disponibilidad (Tolerancia) del servicio	**% Deducible de la facturación mensual**
Mayor o igual a 99.90%	0%
Menor a 99.90% y Mayor o igual a 99.50%	1%
Menor a 99.50% y Mayor o igual a 99.00%	3%
Menor a 99.00% y Mayor o igual a 98.00%	5%
Menor a 98.00% y Mayor o igual a 97.00%	7%
Menor a 97.00% y Mayor o igual a 96.00%	9%
Menor a 96.00%	10%
100% = 24 horas x n (n = días del mes. Por ejemplo: en marzo, n=31; en abril, n=30)	
Para efectos del cálculo de la penalidad, se acumularán las horas en las que el servicio se haya interrumpido en el mes. Para efectos de la penalidad, no se contabilizarán para la disponibilidad del servicio, las interrupciones del servicio a causa de terceros o desastres naturales.	

La entidad aplicará penalidades por incumplimiento en la presentación tardía de los entregables del servicio y demora en solución de averías, de acuerdo al siguiente detalle:

N°	Supuestos de aplicación de penalidad	Penalidad	Procedimiento
1	Por demora en la presentación de los entregables mensuales, de acuerdo a los plazos establecidos en los términos de referencia.	1% UIT por cada día de retraso	Informe técnico de la OTIC.
2	Tiempo de resolución de una avería muy crítica	0.3% UIT por cada hora de retraso	Informe técnico de la OTIC.
3	Tiempo de resolución de una avería critica	0.2% UIT por cada hora de retraso	Informe técnico de la OTIC.
4	Tiempo de resolución de una incidencia o requerimiento normal	0.1% UIT por cada hora de retraso	Informe técnico de la OTIC.

Estas penalidades se deducen de los pagos a cuenta o del pago final, según corresponda; o si fuera necesario, se cobra del monto resultante de la ejecución de la garantía de fiel cumplimiento.

Estos dos (2) tipos de penalidades pueden alcanzar cada una un monto máximo equivalente al diez por ciento (10%) del monto del contrato vigente, o de ser el caso, del ítem que debió ejecutarse.

Cuando se llegue a cubrir el monto máximo de la penalidad por mora o el monto máximo para otras penalidades, de ser el caso, LA ENTIDAD puede resolver el contrato por incumplimiento.

CLÁUSULA DÉCIMA CUARTA: RESOLUCIÓN DEL CONTRATO

Cualquiera de las partes puede resolver el contrato, de conformidad con el numeral 32.3 del artículo 32 y artículo 36 de la Ley de Contrataciones del Estado, y el artículo 164 de su Reglamento. De darse el caso, LA ENTIDAD procederá de acuerdo a lo establecido en el artículo 165 del Reglamento de la Ley de Contrataciones del Estado.

CLÁUSULA DÉCIMA QUINTA: RESPONSABILIDAD DE LAS PARTES

Cuando se resuelva el contrato por causas imputables a algunas de las partes, se debe resarcir los daños y perjuicios ocasionados, a través de la indemnización correspondiente. Ello no obsta la

aplicación de las sanciones administrativas, penales y pecuniarias a que dicho incumplimiento diere lugar, en el caso que éstas correspondan.

Lo señalado precedentemente no exime a ninguna de las partes del cumplimiento de las demás obligaciones previstas en el presente contrato.

CLÁUSULA DÉCIMA SEXTA: ANTICORRUPCIÓN

EL CONTRATISTA declara y garantiza no haber, directa o indirectamente, o tratándose de una persona jurídica a través de sus socios, integrantes de los órganos de administración, apoderados, representantes legales, funcionarios, asesores o personas vinculadas a las que se refiere el artículo 7 del Reglamento de la Ley de Contrataciones del Estado, ofrecido, negociado o efectuado, cualquier pago o, en general, cualquier beneficio o incentivo ilegal en relación al contrato.

Asimismo, el CONTRATISTA se obliga a conducirse en todo momento, durante la ejecución del contrato, con honestidad, probidad, veracidad e integridad y de no cometer actos ilegales o de corrupción, directa o indirectamente o a través de sus socios, accionistas, participacionistas, integrantes de los órganos de administración, apoderados, representantes legales, funcionarios, asesores y personas vinculadas a las que se refiere el artículo 7 del Reglamento de la Ley de Contrataciones del Estado.

Además, EL CONTRATISTA se compromete a i) comunicar a las autoridades competentes, de manera directa y oportuna, cualquier acto o conducta ilícita o corrupta de la que tuviera conocimiento; y ii) adoptar medidas técnicas, organizativas y/o de personal apropiadas para evitar los referidos actos o prácticas.

Finalmente, EL CONTRATISTA se compromete a no colocar a los funcionarios públicos con los que deba interactuar, en situaciones reñidas con la ética. En tal sentido, reconoce y acepta la prohibición de ofrecerles a éstos cualquier tipo de obsequio, donación, beneficio y/o gratificación, ya sea de bienes o servicios, cualquiera sea la finalidad con la que se lo haga.

CLÁUSULA DÉCIMA SÉTIMA: MARCO LEGAL DEL CONTRATO

Sólo en lo no previsto en este contrato, en la Ley de Contrataciones del Estado y su Reglamento, en las directivas que emita el OSCE y demás normativa especial que resulte aplicable, serán de aplicación supletoria las disposiciones pertinentes del Código Civil vigente, cuando corresponda, y demás normas de derecho privado.

CLÁUSULA DÉCIMA OCTAVA: SOLUCIÓN DE CONTROVERSIAS[17]

Las controversias que surjan entre las partes durante la ejecución del contrato se resuelven mediante conciliación o arbitraje, según el acuerdo de las partes.

Cualquiera de las partes tiene derecho a iniciar el arbitraje a fin de resolver dichas controversias dentro del plazo de caducidad previsto en la Ley de Contrataciones del Estado y su Reglamento.

Facultativamente, cualquiera de las partes tiene el derecho a solicitar una conciliación dentro del plazo de caducidad correspondiente, según lo señalado en el artículo 224 del Reglamento de la Ley de Contrataciones del Estado, sin perjuicio de recurrir al arbitraje, en caso no se llegue a un acuerdo entre ambas partes o se llegue a un acuerdo parcial. Las controversias sobre nulidad del contrato solo pueden ser sometidas a arbitraje.

El Laudo arbitral emitido es inapelable, definitivo y obligatorio para las partes desde el momento de su notificación, según lo previsto en el numeral 45.21 del artículo 45 de la Ley de Contrataciones del Estado.

CLÁUSULA DÉCIMA NOVENA: FACULTAD DE ELEVAR A ESCRITURA PÚBLICA

Cualquiera de las partes puede elevar el presente contrato a Escritura Pública corriendo con todos los gastos que demande esta formalidad.

CLÁUSULA VIGÉSIMA: DOMICILIO PARA EFECTOS DE LA EJECUCIÓN CONTRACTUAL

[17] 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).

Las partes declaran el siguiente domicilio para efecto de las notificaciones que se realicen durante la ejecución del presente contrato:

DOMICILIO DE LA ENTIDAD: Av. Salaverry Nro. 655 2do piso, Jesús María – Lima.

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 Nº 27269, Ley de Firmas y Certificados Digitales[18].

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

ANEXOS

ANEXO Nº 1

DECLARACIÓN JURADA DE DATOS DEL POSTOR

Señores
COMITÉ DE SELECCIÓN
CONCURSO PÚBLICO Nº 01-2025-SUNAFIL-1
Presente.-

El que se suscribe, [……..], postor y/o Representante Legal de [CONSIGNAR EN CASO DE SER PERSONA JURÍDICA], identificado con [CONSIGNAR TIPO DE DOCUMENTO DE IDENTIDAD] N° [CONSIGNAR NÚMERO DE DOCUMENTO DE IDENTIDAD], con poder inscrito en la localidad de [CONSIGNAR EN CASO DE SER PERSONA JURÍDICA] en la Ficha Nº [CONSIGNAR EN CASO DE SER PERSONA JURÍDICA] Asiento Nº [CONSIGNAR EN CASO DE SER PERSONA JURÍDICA], **DECLARO BAJO JURAMENTO** que la siguiente información se sujeta a la verdad:

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

Autorización de notificación por correo electrónico:

Autorizo que se notifiquen al correo electrónico indicado las siguientes actuaciones:

1. Solicitud de la descripción a detalle de todos los elementos constitutivos de la oferta.
2. Solicitud de reducción de la oferta económica.
3. Solicitud de subsanación de los requisitos para perfeccionar el contrato.
4. Solicitud para presentar los documentos para perfeccionar el contrato, según orden de prelación, de conformidad con lo previsto en el artículo 141 del Reglamento.
5. Respuesta a la solicitud de acceso al expediente de contratación.
6. Notificación de la orden de servicios[20]

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.

[19] 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.

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

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

ANEXO Nº 1

DECLARACIÓN JURADA DE DATOS DEL POSTOR

Señores
COMITÉ DE SELECCIÓN
CONCURSO PÚBLICO Nº 01-2025-SUNAFIL-1
Presente.-

El que se suscribe, [……..], representante común del consorcio [CONSIGNAR EL NOMBRE DEL CONSORCIO], identificado con [CONSIGNAR TIPO DE DOCUMENTO DE IDENTIDAD] N° [CONSIGNAR NÚMERO DE DOCUMENTO DE IDENTIDAD], **DECLARO BAJO JURAMENTO** que la siguiente información se sujeta a la verdad:

Datos del consorciado 1					
Nombre, Denominación o Razón Social :					
Domicilio Legal :					
RUC :	Teléfono(s) :				
MYPE[21]		Sí		No	
Correo electrónico :					

Datos del consorciado 2					
Nombre, Denominación o Razón Social :					
Domicilio Legal :					
RUC :	Teléfono(s) :				
MYPE[22]		Sí		No	
Correo electrónico :					

Datos del consorciado …					
Nombre, Denominación o Razón Social :					
Domicilio Legal :					
RUC :	Teléfono(s) :				
MYPE[23]		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.

[21] 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.

[22] Ibídem.

[23] Ibídem.

4. Solicitud para presentar los documentos para perfeccionar el contrato, según orden de prelación, de conformidad con lo previsto en el artículo 141 del Reglamento.
5. Respuesta a la solicitud de acceso al expediente de contratación.
6. Notificación de la orden de servicios[24]

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.

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

ANEXO Nº 2

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

Señores
COMITÉ DE SELECCIÓN
CONCURSO PÚBLICO Nº 01-2025-SUNAFIL-1
Presente.-

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

i. No haber incurrido y me obligo a no incurrir en actos de corrupción, así como a respetar el principio de integridad.

ii. No tener impedimento para postular en el procedimiento de selección ni para contratar con el Estado, conforme al artículo 11 de la Ley de Contrataciones del Estado.

iii. Conocer las sanciones contenidas en la Ley de Contrataciones del Estado y su Reglamento, así como las disposiciones aplicables de la Ley N° 27444, Ley del Procedimiento Administrativo General.

iv. Participar en el presente proceso de contratación en forma independiente sin mediar consulta, comunicación, acuerdo, arreglo o convenio con ningún proveedor; y, conocer las disposiciones del Decreto Legislativo Nº 1034, Decreto Legislativo que aprueba la Ley de Represión de Conductas Anticompetitivas.

v. Conocer, aceptar y someterme a las bases, condiciones y reglas del procedimiento de selección.

vi. Ser responsable de la veracidad de los documentos e información que presento en el presente procedimiento de selección.

vii. Comprometerme a mantener la oferta presentada durante el procedimiento de selección y a perfeccionar el contrato, en caso de resultar favorecido con la buena pro.

[CONSIGNAR CIUDAD Y FECHA]

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

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

ANEXO Nº 3

DECLARACIÓN JURADA DE CUMPLIMIENTO DE LOS TÉRMINOS DE REFERENCIA

Señores
COMITÉ DE SELECCIÓN
CONCURSO PÚBLICO Nº 01-2025-SUNAFIL-1
Presente.-

Es grato dirigirme a usted, para hacer de su conocimiento que luego de haber examinado las bases y demás documentos del procedimiento de la referencia y, conociendo todos los alcances y las condiciones detalladas en dichos documentos, el postor que suscribe ofrece el servicio de SERVICIO DE ACCESO DEDICADO DE INTERNET DE BANDA ANCHA PARA LA SUNAFIL[25], 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.

[25] CONSULTA N° 15 DE NEXTNET S.A.C.

ANEXO Nº 4

DECLARACIÓN JURADA DE PLAZO DE PRESTACIÓN DEL SERVICIO

Señores
COMITÉ DE SELECCIÓN
CONCURSO PÚBLICO Nº 01-2025-SUNAFIL-1
Presente.-

Mediante el presente, con pleno conocimiento de las condiciones que se exigen en las bases del procedimiento de la referencia, me comprometo a prestar el servicio objeto del presente procedimiento de selección en el plazo de [CONSIGNAR EL PLAZO OFERTADO].

[CONSIGNAR CIUDAD Y FECHA]

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

ANEXO Nº 5

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

Señores
COMITÉ DE SELECCIÓN
CONCURSO PÚBLICO Nº 01-2025-SUNAFIL-1
Presente.-

Los suscritos declaramos expresamente que hemos convenido en forma irrevocable, durante el lapso que dure el procedimiento de selección, para presentar una oferta conjunta al **CONCURSO PÚBLICO Nº 01-2025-SUNAFIL-1**

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]	[%] [26]
	[DESCRIBIR LAS OBLIGACIONES DEL CONSORCIADO 1]	
2.	OBLIGACIONES DE [NOMBRE, DENOMINACIÓN O RAZÓN SOCIAL DEL CONSORCIADO 2]	[%] [27]
	[DESCRIBIR LAS OBLIGACIONES DEL CONSORCIADO 2]	
	TOTAL OBLIGACIONES	100%[28]

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

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

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

[CONSIGNAR CIUDAD Y FECHA]

.....	.....
Consorciado 1	**Consorciado 2**
Nombres, apellidos y firma del Consorciado 1	**Nombres, apellidos y firma del Consorciado 2**
o de su Representante Legal	**o de su Representante Legal**
Tipo y N° de Documento de Identidad	**Tipo y N° de Documento de Identidad**

Importante

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

ANEXO Nº 6

PRECIO DE LA OFERTA

Señores
COMITÉ DE SELECCIÓN
CONCURSO PÚBLICO Nº 01-2025-SUNAFIL-1
Presente.-

Es grato dirigirme a usted, para hacer de su conocimiento que, de acuerdo con las bases, mi oferta es la siguiente:

CONCEPTO	PRECIO TOTAL
TOTAL	

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

[CONSIGNAR CIUDAD Y FECHA]

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

Importante

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

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

ANEXO Nº 8

EXPERIENCIA DEL POSTOR EN LA ESPECIALIDAD

Señores
COMITÉ DE SELECCIÓN
CONCURSO PÚBLICO Nº 01-2025-SUNAFIL-1

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 [29]	FECHA DE LA CONFORMIDAD DE SER EL CASO[30]	EXPERIENCIA PROVENIENTE[31] DE:	MONEDA	IMPORTE[32]	TIPO DE CAMBIO VENTA[33]	MONTO FACTURADO ACUMULADO [34]
1										
2										
3										
4										

[29] 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.

[30] 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.

[31] 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"*.

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

[33] 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.

[34] 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 [29]	FECHA DE LA CONFORMIDAD DE SER EL CASO[30]	EXPERIENCIA PROVENIENTE[31] DE:	MONEDA	IMPORTE[32]	TIPO DE CAMBIO VENTA[33]	MONTO FACTURADO ACUMULADO [34]
5										
6										
7										
8										
9										
10										
	…									
20										
TOTAL										

[CONSIGNAR CIUDAD Y FECHA]

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

ANEXO Nº 9

DECLARACIÓN JURADA
(NUMERAL 49.4 DEL ARTÍCULO 49 DEL REGLAMENTO)

Señores
COMITÉ DE SELECCIÓN
CONCURSO PÚBLICO Nº 01-2025-SUNAFIL-1
Presente.-

Mediante el presente el suscrito, postor y/o Representante Legal de [CONSIGNAR EN CASO DE SER PERSONA JURÍDICA], declaro que la experiencia que acredito de la empresa [CONSIGNAR LA DENOMINACIÓN DE LA PERSONA JURÍDICA] como consecuencia de una reorganización societaria, no se encuentra en el supuesto establecido en el numeral 49.4 del artículo 49 del Reglamento.

[CONSIGNAR CIUDAD Y FECHA]

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

Importante
A efectos de cautelar la veracidad de esta declaración, el postor puede verificar la información de la Relación de Proveedores Sancionados por el Tribunal de Contrataciones del Estado con Sanción Vigente en http://portal.osce.gob.pe/rnp/content/relación-de-proveedores-sancionados. *También le asiste dicha facultad al órgano encargado de las contrataciones o al órgano de la Entidad al que se le haya asignado la función de verificación de la oferta presentada por el postor ganador de la buena pro.*

Nro. Orden	RUC/Código	Nombre o Razón Social	Tipo Formulación	Sección	Numeral	Literal	Página	Consulta u Observación	Artículo y norma que se vulnera(en el caso de observaciones)	Fecha y Hora de Envío.	Fecha y Hora de 1er registro.	Estado del Registro.	Análisis y respuesta respecto de la consulta u observación presentada	Precisión de aquello que se incorporará en las Bases a integrarse, de corresponder
1	20546904106	NEXTNET S.A.C.	Consulta	Específico	V	viñeta 2	2	En las bases dice: La interconexión entre la Sede Central (Cabecera) y las Sedes Remotas (IRE y PIT) también deberá estar en alta disponibilidad, utilizando 2 enlaces redundantes configurados en modo Activo-Pasivo, asegurando conmutación automática y protección avanzada mediante NGFW. Consulta Se solicita a la entidad aclarar que para el servicio de datos , la sede central solo tendrá un enlace principal y un enlace de contingencia, y no 2 enlaces redundantes y para las sedes remotas solo será un enlace.		2025-04-16 18:43:25.0	2025-04-16 18:29:38.0	Enviado	Se aclara al participante que. Según el TDR: En la Sede Central (Cabecera), se deben implementar: (...) ✓La interconexión entre la Sede Central (Cabecera) y las Sedes Remotas (IRE y PIT) también deberá estar en alta disponibilidad, utilizando 2 enlaces redundantes configurados en modo Activo-Pasivo, asegurando conmutación automática y protección avanzada mediante NGFW. Asimismo, en los TDR, dice: • Las Sedes Remotas (IRE y PIT) contarán con un solo enlace de fibra óptica cada una, sin redundancia local, garantizando un acceso continuo y eficiente a internet y a los sistemas centralizados en la Sede Central (Cabecera). Por lo mencionado en los TDR, se precisa que el enlace cabecera en la Sede Central debe contar con redundancia, es decir un enlace principal y un enlace de contingencia, en modo Activo-Pasivo. Asimismo, en las sedes remotas sera un solo enlace. Asimismo, respecto a la alta disponibilidad de los firewalls (NGFW) se precisa que se refiere al respaldo de los equipos firewalls, por lo que podría tener una de las siguientes configuraciones: (01) equipo Firewall y un (01) equipo Firewall spare; o (01) equipo Firewall Activo y un (01) equipo Firewall Pasivo; o (01) equipo Firewall Activo y un (01) equipo Firewall Activo, los cuales estarán instalados en el Datacenter de SUNAFIL, tal que garanticen la disponibilidad mínima del servicio requerido.	V. Descripción del servicio. se agregará: (...) (un enlace principal y un enlace de contingencia) (...) Respecto a la alta disponibilidad de los firewalls (NGFW) se precisa que se refiere al respaldo de los equipos firewalls, por lo que podría tener una de las siguientes configuraciones: (01) equipo Firewall y un (01) equipo Firewall spare; o (01) equipo Firewall Activo y un (01) equipo Firewall Pasivo; o (01) equipo Firewall Activo y un (01) equipo Firewall Activo, los cuales estarán instalados en el Datacenter de SUNAFIL, tal que garanticen la disponibilidad mínima del servicio requerido.
2	20546904106	NEXTNET S.A.C.	Consulta	Específico	5.2	B,2da viñe	35	En las bases dice: Capacidad de throughput de protección incluida debe ser de al menos 25Gbps de trafico Consulta Se solicita a la entidad con el fin de la libre e igualitaria participacion, confirmar si la capacidad de troughtput de proteccion incluida de antiddos podrá ser de al menos 20Gbps.		2025-04-16 18:43:25.0	2025-04-16 18:30:59.0	Enviado	No se confirma. Teniendo en consideración que el servicio AntiDdos debe estar en la nube local del proveedor donde el trafico de Internet del proveedor es mayor y por ello la plataforma de mitigación debe tener capacidad de Throughput de 25Gbps. Se precisa que, de acuerdo con la indagacion a traves del estudio de mercado, existe pluralidad de postores y fabricantes que cumplen con dicho requerimiento.	
3	20546904106	NEXTNET S.A.C.	Consulta	Específico	Capítulo I	1.8	13	Solicitamos nos precisen si, en relación a lo indicado en el numeral 1.8 en el cual se indica que los servicios se prestarán en el plazo de 1095 días calendarios (equivalente a 03 años); y, además se menciona que el plazo de implementación será de 90 días calendarios, para el llenado del Anexo N° 04 ¿ ¿Declaración jurada de plazo de prestación del servicio¿ se deberá consignar en el plazo ofertado únicamente el plazo de duración de los servicios, es decir, el plazo de 1095 días calendarios (equivalente a 03 años).		2025-04-16 18:43:25.0	2025-04-16 18:35:12.0	Enviado	Se aclara al participante que, el plazo de ejecución de la prestación del servicio que se establecerá en el Anexo N° 4 es de 1095 días calendarios, computados a partir del día siguiente de firmada el acta de inicio.	
4	20546904106	NEXTNET S.A.C.	Consulta	Específico	Capítulo 2	2.2.1.1. b	15	De la revisión efectuada al presente numeral, se observa que la Entidad solicita que se presente una serie de documentos obligatorios para la presentación y admisión de la oferta, y el perfeccionamiento del contrato, entre ellos, la copia de vigencia del poder del representante legal de la empresa que acredite que cuenta con facultades para perfeccionar el contrato y la copia del DNI del representante legal en caso de persona jurídica. Sobre el particular, es importante precisar que de acuerdo a lo dispuesto en las Bases Estándar de Adjudicación Simplificada para la Contratación de Servicios en general, aprobado con Directiva N° 001-2019-OSCE/CD y en concordancia a lo establecido en el artículo 04° del Decreto Legislativo N° 1246, no corresponde que la Entidad contratante exija los referidos documentos cuando la misma sea usuaria de la Plataforma de Interoperabilidad del Estado (PIDE) ello debido a que la citada documentación puede ser obtenida directamente mediante la interoperabilidad, teniendo en cuenta además, que no es posible tramitar vigencias de poder ante la Superintendencia Nacional de Registros Públicos - SUNARP. En ese sentido y, solicitamos eliminar la documentación obligatoria requerida en los literales b) para la presentación y admisión de la oferta, y el perfeccionamiento del contrato	Directiva N° 001-2019-OSCE/CD Artículo 04° del Decreto Legislativo N° 1246 Numeral 47.	2025-04-16 18:43:25.0	2025-04-16 18:35:53.0	Enviado	Se aclara al participante que, actualmente la Superintendencia Nacional de Fiscalización Laboral SUNAFIL, no tiene implementado el acceso a la Plataforma Nacional de Interoperabilidad (PIDE), para la obtención de la vigencia de poderes del representante legal de la empresa; por lo cual, es responsabilidad del participante o postor evaluar íntegramente las bases del procedimiento de selección, considerando que allí está establecido las reglas definitivas y entre ellas que documentos deberán presentar para la admisión de la oferta; en estricto cumplimiento de las normas sobre contrataciones públicas.	
5	20546904106	NEXTNET S.A.C.	Consulta	Específico	Capítulo 2	2.3	17	El artículo 35° del Reglamento de la Ley de Contrataciones del Estado señala que el sistema de precios unitarios resulta aplicable en las contrataciones de bienes, servicios en general, consultorías y obras, cuando no puede conocerse con exactitud o precisión las cantidades o magnitudes requeridas. En tal sentido, en la medida que el sistema de contratación utilizado en el presente procedimiento de selección es a suma alzada, se solicita eliminar este documento de los requisitos para el perfeccionamiento del contrato.	Artículo 35° del Reglamento la Ley de Contrataciones del Estado	2025-04-16 18:43:25.0	2025-04-16 18:36:58.0	Enviado	Se aclara al participante que, al tenerse conocimiento sobre el plazo a contratarse que es de 1095 días calendarios (equivalente a 03 años) respecto a la prestación del servicio a recibir, en la presente contratación se ha previsto aplicar el sistema contratación a Suma Alzada, así mismo, al tenerse un plazo de contratación de 1095 días calendario que equivalen a 03 años o 36 meses y siendo el pago en forma periódica en cuotas mensuales, cuyo porcentaje de pago serán en partes iguales en función al monto del contrato; por lo que, conforme las bases estándar aprobadas por el OSCE, es un requisito la presentación del detalle de los precios unitarios siempre y cuando la contratación se realice bajo el sistema a suma alzada. Ahora bien, señalar que, el DETALLE DE LOS PRECIOS UNITARIOS DEL PRECIO OFERTADO, se refiere a señalar el precio unitario del costo mensual de la prestación del servicio	
6	20546904106	NEXTNET S.A.C.	Consulta	Específico	Capítulo 2	2.5	20	En tanto el servicio que se prestará a favor de la Entidad califica como un servicio público, solicitamos confirmar que ante la falta de pago oportuno injustificado, el Operador/Contratista podrá suspender el servicio de acuerdo con el procedimiento establecido en el Artículo 66° y el Numeral 1.1 del Anexo 8 de la Norma de las Condiciones de Uso de los Servicios Públicos de Telecomunicaciones aprobado por Resolución de Consejo Directivo Nº 172-2022-CD/OSIPTEL; sin que ello sea considerado como un incumplimiento o causal de penalidad para el Contratista.		2025-04-16 18:43:25.0	2025-04-16 18:37:37.0	Enviado	Se aclara que, ante una eventual falta de pago oportuno injustificado, el contratista deberá cumplir sus obligaciones contractuales, a fin de garantizar la continuidad del servicio contratado; sin perjuicio de ello, en caso exista alguna controversia con respecto al plazo del pago por parte de la Entidad, se deberá sujetar a los mecanismos de solución de controversias que la Ley de Contrataciones del Estado contempla. Además, el contratista podrá gestionar lo respectivo a lo señalado en el numeral 171.2. del Reglamento de la Ley de Contrataciones del Estado, Ley 30225, la cual señala: "En caso de retraso en el pago, el contratista tiene derecho al pago de intereses legales, los que se computan desde la oportunidad en que el pago debió efectuarse".	

7	20546904106	NEXTNET S.A.C.	Consulta	Específico	Capítulo 3	5.1.1	25	Solicitamos se confirme que, para la imputación de responsabilidades por la existencia de daños irreparables en los equipos brindados para el servicio, se evaluará previamente si esta deberá recaer sobre el contratista o sobre la Entidad, siendo que, de comprobarse que el referido daño fue originado por el uso negligente imputable al usuario, será la Entidad quien asuma los costos adicionales por la mencionada contingencia.		2025-04-16 18:43:25.0	2025-04-16 18:39:00.0	Enviado	Se aclara al participante que, en caso de daños irreparables en los equipos brindados para la prestación del servicio, previamente se evaluará la imputación de responsabilidades, a fin de determinar si corresponde al contratista o a la Entidad. De comprobarse que el daño fue originado por un uso negligente imputable al usuario, será la Entidad quien asuma los costos adicionales que se deriven de dicha contingencia.	
8	20546904106	NEXTNET S.A.C.	Consulta	Específico	Capítulo 3	5.1.2	25	En relación al porcentaje de disponibilidad , solicitamos a la Entidad confirmar que, como operadores del servicio de telecomunicaciones, el cumplimiento de la obligación de calidad requerida en la página indicada, se restringe al cumplimiento de las normas regulatorias vigentes emitidas por el Ministerio de Transportes y Telecomunicaciones y el OSIPTEL (Decreto Supremo N° 013-93-TTC - Texto Único Ordenado de la Ley de Telecomunicaciones y demás normas vigentes), reconociéndose que el servicio podría verse afectado por causas externas ajenas al operador; supuesto en el cual la afectación del servicio deberá ser reportada a las centrales de atención que se indiquen en la oferta, a fin de darle la atención correspondiente, sin que ello genere la aplicación de ninguna penalidad.		2025-04-16 18:43:25.0	2025-04-16 18:39:42.0	Enviado	Se aclara al participante que, debe cumplir y asegurar los niveles de disponibilidad indicados en los Terminos de Referencia. Asimismo, se reconoce que el servicio puede verse afectado por causas externas ajenas al operador, sin que ello genere la aplicación de ninguna penalidad y no se contabilizarán para la disponibilidad del servicio, de acuerdo a lo establecido en el TDR y las normas regulatorias vigentes emitidas por el Ministerio de Transportes y Comunicaciones y el OSIPTEL, tales como el Decreto Supremo N.° 013-93-TCC – Texto Único Ordenado de la Ley de Telecomunicaciones y demás disposiciones aplicables. Asimismo, según TDR, en caso de la interrupción o pérdida del servicio de Internet, el centro de operaciones del contratista, deberá remitir un ticket que corresponde a la incidencia o avería presentada. El tiempo de la pérdida de la disponibilidad del servicio será a partir de la interrupción o pérdida del servicio de Internet, en caso el servicio puede verse afectado por causas externas ajenas al operador (a causa de terceros o desastres naturales u otros) no se contabilizarán para la disponibilidad del servicio.	
9	20546904106	NEXTNET S.A.C.	Consulta	Específico	Capítulo 3	5.1.2	25	En relación al porcentaje de disponibilidad , solicitamos a la Entidad confirmar que, como operadores del servicio de telecomunicaciones, el cumplimiento de la obligación de calidad requerida en la página indicada, se restringe al cumplimiento de las normas regulatorias vigentes emitidas por el Ministerio de Transportes y Telecomunicaciones y el OSIPTEL (Decreto Supremo N° 013-93-TTC - Texto Único Ordenado de la Ley de Telecomunicaciones y demás normas vigentes), reconociéndose que el servicio podría verse afectado por causas externas ajenas al operador; supuesto en el cual la afectación del servicio deberá ser reportada a las centrales de atención que se indiquen en la oferta, a fin de darle la atención correspondiente, sin que ello genere la aplicación de ninguna penalidad.		2025-04-16 18:43:25.0	2025-04-16 18:40:46.0	Enviado	Se aclara al participante que, debe cumplir y asegurar los niveles de disponibilidad indicados en los Terminos de Referencia. Asimismo, se reconoce que el servicio puede verse afectado por causas externas ajenas al operador, sin que ello genere la aplicación de ninguna penalidad y no se contabilizarán para la disponibilidad del servicio, de acuerdo a lo establecido en el TDR y las normas regulatorias vigentes emitidas por el Ministerio de Transportes y Comunicaciones y el OSIPTEL, tales como el Decreto Supremo N.° 013-93-TCC – Texto Único Ordenado de la Ley de Telecomunicaciones y demás disposiciones aplicables. Asimismo, según TDR, en caso de la interrupción o pérdida del servicio de Internet, el centro de operaciones del contratista, deberá remitir un ticket que corresponde a la incidencia o avería presentada. El tiempo de la pérdida de la disponibilidad del servicio será a partir de la interrupción o pérdida del servicio de Internet, en caso el servicio puede verse afectado por causas externas ajenas al operador (a causa de terceros o desastres naturales u otros) no se contabilizarán para la disponibilidad del servicio.	
10	20546904106	NEXTNET S.A.C.	Consulta	Específico	Capítulo 3	5.2	51	Las bases requieren que se incluya un curso o programa de Certificación en Ciberseguridad Aplicada a través de una plataforma online educativa, sobre esto, les solicitamos precisar el momento de la ejecución contractual (implementación, prestación del servicio u otro) en el cual deberá ser llevada a cabo dicho curso.		2025-04-16 18:43:25.0	2025-04-16 18:41:18.0	Enviado	Se aclara al participante que el curso o programa de Certificación en Ciberseguridad Aplicada deberá ser brindada durante la etapa de implementación.	5.2. Equipamiento de Gestión y Seguridad de Internet: E. Servicios Integrales de Ciberseguridad: Capacitación. Se agregará: La capacitacion se realizara durante el plazo de implementación del servicio.
11	20546904106	NEXTNET S.A.C.	Consulta	Específico	Capítulo 3	5.4	53	Solicitamos se confirme que para la imputación de responsabilidades por la existencia de averías en el servicio (corte, caída o degradación del servicio), se evaluará previamente si estas deberán recaer sobre el contratista o sobre la Entidad, siendo que, de comprobarse que la referida contingencia fue originada por la Entidad o por un hecho ajeno a las partes (caso fortuito o fuerza mayor), no se generará ningún tipo de penalidad en contra del contratista ni se le imputará ningún incumplimiento.		2025-04-16 18:43:25.0	2025-04-16 18:41:54.0	Enviado	Se aclara al participante que, para la imputación de responsabilidades por la existencia de averías en el servicio (corte, caída o degradación del servicio), se evaluará previamente si estas deberán recaer sobre el contratista o sobre la Entidad, siendo que, de comprobarse que la referida contingencia fue originada por la Entidad o por un hecho ajeno a las partes (caso fortuito o fuerza mayor), no se generará ningún tipo de penalidad en contra del contratista ni se le imputará ningún incumplimiento.	
12	20546904106	NEXTNET S.A.C.	Consulta	Específico	Capítulo V	CLAUS- 11	71	Solicitamos suprimir la presente cláusula; toda vez que, en la Ley de Contrataciones ni en su Reglamento existe un supuesto de inhabilitación por incumplimiento de obligaciones.		2025-04-16 18:43:25.0	2025-04-16 18:42:40.0	Enviado	Se aclara al participante que, dicha cláusula se encuentra establecida en las Bases Estándar de Concurso Público para la contratación de servicios en general, aprobado mediante Directiva N° 001-2019-OSCE/CD vigente, suprimir la cláusula en cuestión acarrearía una nulidad ya que se estaría contraviniendo con lo establecido en la antes citada directiva. Es preciso indicar que el presente cuestionamiento no es una observación, sino una solicitud, más aún cuando no se ha formulado correctamente su consulta; toda vez que en la CLAUSULA DECIMA no se señala por ningún extremo el termino "existe un supuesto de inhabilitación por incumplimiento de obligaciones"	
13	20546904106	NEXTNET S.A.C.	Consulta	Específico	Capítulo V	CLAUS. 18	73	En relación con el convenio arbitral incluido en el acápite indicado de las Bases, solicitamos a la Entidad precisar que el tipo de arbitraje será institucional, toda vez que, de conformidad con el numeral 1 del artículo 223° del Reglamento de la Ley de Contrataciones del Estado, las controversias que surjan entre las partes se resuelven mediante arbitraje institucional. Asimismo, de acuerdo con el artículo 230° del referido Reglamento, con la finalidad de garantizar que el laudo arbitral sea lo más imparcial posible, indicar de manera expresa que el Tribunal Arbitral que tenga a su cargo la solución de las eventuales controversias que surjan con relación al contrato, estará conformado por tres (3) árbitros.		2025-04-16 18:43:25.0	2025-04-16 18:43:22.0	Enviado	Se aclara y precisa al participante que, al ser el arbitraje será institucional de conformidad con el numeral 1 del artículo 223° del Reglamento de la Ley de Contrataciones del Estado, las controversias que surjan entre las partes se resuelven mediante arbitraje institucional. Asimismo, de acuerdo con el artículo 230° del referido Reglamento, con la finalidad de garantizar que el laudo arbitral sea lo más imparcial posible, indicar de manera expresa que el Tribunal Arbitral que tenga a su cargo la solución de las eventuales controversias que surjan con relación al contrato, estará conformado por tres (3) árbitros.	
14	20546904106	NEXTNET S.A.C.	Consulta	Específico	Capítulo I	1.8	13	Teniendo en consideración que el plazo del servicio es único para todos los postores, solicitamos a la Entidad se sirva completar el texto del Anexo N° 4, correspondiente al plazo del servicio, ello para evitar distintas interpretaciones entre los postores. En caso no admita lo requerido, favor de confirmar que se deberá ingresar únicamente el plazo de prestación del servicio especificado en el numeral 1.8 de las bases.		2025-04-16 19:19:50.0	2025-04-16 18:55:47.0	Enviado	Se aclara al participante que, el plazo de ejecución de la prestación del servicio que se establecerá en el Anexo N° 4 es de 1095 días calendarios, computados a partir del día siguiente de firmada el acta de inicio.	
15	20546904106	NEXTNET S.A.C.	Consulta	Específico	Capítulo I	Anexo N° 3	80	Teniendo en consideración que el objeto de la convocatoria es único para todos los postores, solicitamos a la entidad se sirva completar el texto del Anexo N° 3, correspondiente al objeto de la convocatoria, ello para evitar distintas interpretaciones entre los postores		2025-04-16 19:19:50.0	2025-04-16 18:57:20.0	Enviado	Se aclara al participante que, el objeto de la convocatoria es: "SERVICIO DE ACCESO DEDICADO DE INTERNET DE BANDA ANCHA PARA LA SUNAFIL"	AGREGAR ANEXO 3 (…) SERVICIO DE ACCESO DEDICADO DE INTERNET DE BANDA ANCHA PARA LA SUNAFIL(…)
16	20546904106	NEXTNET S.A.C.	Consulta	Anexo	ANEXO 6	-	84	Solicitamos a la Entidad se sirva completar el texto del Anexo N° 6 correspondiente al CONCEPTO, ello para evitar distintas interpretaciones entre los postores.		2025-04-16 19:19:50.0	2025-04-16 19:00:42.0	Enviado	Se aclara al participante que, la denominación de la presente contratación, corresponde al: SERVICIO DE ACCESO DEDICADO DE INTERNET DE BANDA ANCHA PARA LA SUNAFIL, el mismo que será consignado según corresponda, en la oferta del postor.	
17	20546904106	NEXTNET S.A.C.	Consulta	Específico	2.2.1.1	e	16	De acuerdo con el literal e) Se solicita que se considere como válida la presentación de carta de distribuidor autorizado para la acreditación de la solución de administración y control de ancho de banda.		2025-04-16 19:19:50.0	2025-04-16 19:03:56.0	Enviado	No se confirma lo indicado por el postor, debido a que una carta del fabricante proporciona la máxima garantía de autenticidad del producto o componente, ya que proviene directamente de la fuente de producción, eliminando cualquier duda sobre su origen y legitimidad; por lo cual, no se acepta la consulta.	

18	20546904106	NEXTNET S.A.C.	Consulta	Específico	2.2.1.1	f	16	De acuerdo con el literal f) Se solicita que se considere como válida la presentación de carta de distribuidor para acreditar lo indicado en dicho literal		2025-04-16 19:19:50.0	2025-04-16 19:06:04.0	Enviado	No se confirma lo indicado por el postor, debido a que una carta del fabricante proporciona la máxima garantía de autenticidad del producto o componente, ya que proviene directamente de la fuente de producción, eliminando cualquier duda sobre su origen y legitimidad; por lo cual, no se acepta la consulta.	
19	20546904106	NEXTNET S.A.C.	Consulta	Específico	c	n° 2,viñ2	34	De acuerdo con lo señalado en las bases, en donde se exige la presentación de una carta de fabricante para acreditar la obsolescencia de los equipos ofertados, se solicita admitir como válida la presentación de una carta de distribuidor y una declaración jurada. Asimismo, incluirlo dentro de los documentos de presentación obligatoria 2.2.1.		2025-04-16 19:19:50.0	2025-04-16 19:16:35.0	Enviado	No se confirma lo indicado por el postor, se precisa que se debe presentar una carta del fabricante, en la cual se precise y referencia que los equipos propuestos no presentan obsolencia.	
20	20546904106	NEXTNET S.A.C.	Consulta	Específico	2.3	m	18	De acuerdo con el literal m) Se solicita a la entidad aclarar que la demostración de las rutas físicas de los 02 operadores TIER1 se podrá acreditar y/o sustentar a través de la presentación de un diagrama o topología de salidas internacionales.		2025-04-16 19:19:50.0	2025-04-16 19:19:40.0	Enviado	Se confirma lo indicado por el postor. Se aceptará como documento para la acreditación de las rutas físicas de los 02 operadores TIER1, la presentación de un diagrama o topología de salidas internacionales.	
21	20106897914	ENTEL PERU S.A.	Consulta	Específico	2.2.1.1	-	16	"En las bases dice: 2.2.1.1. Documentos para la admisión de la oferta Teniendo en cuenta que el numeral 2.2.1 de las Bases Estándar para la contratación de servicios en general, aprobada mediante Directiva N° 001-2019-OSCE/CD, dispone que: ""El órgano encargado de las contrataciones o comité de selección, según corresponda, no podrá exigir al postor la presentación de documentos que no hayan sido indicados en los acápites ¿Documentos para la admisión de la oferta¿. Solicitamos a la Entidad confirmar que los documentos señalados en el numeral 2.2.1.1, serán los únicos necesarios para la admisión de las ofertas presentadas por los postores."		2025-04-16 19:41:14.0	2025-04-16 19:32:26.0	Enviado	Se aclara al participante que, es responsabilidad del participante o postor evaluar Integramente las bases del procedimiento de selección, considerando que allí está establecido las reglas definitivas y entre ellas que documentos deberán presentar para la admisión de la oferta; en estricto cumplimiento de las normas sobre contrataciones públicas.	
22	20106897914	ENTEL PERU S.A.	Consulta	Específico	2.2.1.1	h	16	"En las bases dice: i) Documentación que acredite el postor tener la autorización del Ministerio de Transporte y Comunicaciones para la prestacion (¿) Solicitamos suprimir el presente requerimiento, toda vez que la acreditación de la capacidad legal del postor ya se encuentra contemplada en el numeral XIV ""Requisitos de Calificación"". Esto con el propósito de evitar la duplicidad de información en la propuesta."		2025-04-16 19:41:14.0	2025-04-16 19:32:52.0	Enviado	Se aclara al participante que, es suficiente presentar un (01) documento de la autorización del Ministerio de Transporte y Comunicaciones solicitado, la cual, dicha presentación de documento en su oferta corresponderá para la acreditación de lo solicitado en el literal i) de los documentos para la admisión de la oferta y el litera A) de los Requisitos de calificación, esto con el propósito de evitar la duplicidad de información en la propuesta.	
23	20106897914	ENTEL PERU S.A.	Consulta	Específico	2.5	-	20	"En las bases dice: FORMA DE PAGO Para la prestación principal y prestación accesoria, solicitamos confirmar que, luego de transcurridos 03 meses sin que la entidad haya cancelado la contraprestación mensual correspondiente al servicio prestado por el contratista, en aplicación de lo dispuesto en el artículo 71° del TUO de las Condiciones de Uso de los Servicios Públicos de Telecomunicaciones, modificado con Resolución de Consejo Directivo N° 96-2018-CD/OSIPTEL, el operador de telecomunicaciones podrá suspender el servicio por falta de pago, sin que ello implique la aplicación de penalidades y/o se forme parte, en caso de corresponder, del porcentaje de cumplimiento del nivel de servicio requerido."		2025-04-16 19:41:14.0	2025-04-16 19:33:13.0	Enviado	Se aclara que, ante una eventual falta de pago oportuno injustificado, el contratista deberá cumplir sus obligaciones contractuales, a fin de garantizar la continuidad del servicio contratado; sin perjuicio de ello, en caso exista alguna controversia con respecto al plazo del pago por parte de la Entidad, se deberá sujetar a los mecanismos de solución de controversias que la Ley de Contrataciones del Estado contempla. Además, el contratista podrá gestionar lo respectivo a lo señalado en el numeral 171.2. del Reglamento de la Ley de Contrataciones del Estado, Ley 30225, la cual señala: "En caso de retraso en el pago, el contratista tiene derecho al pago de intereses legales, los que se computan desde la oportunidad en que el pago debió efectuarse".	
24	20106897914	ENTEL PERU S.A.	Consulta	Específico	2.5	-	20	"En las bases dice: FORMA DE PAGO Agradeceremos precisar la glosa con la cual se deberá facturar el presente servicio, a fin de considerar la información correcta en las facturas o recibos a emitir."		2025-04-16 19:41:14.0	2025-04-16 19:33:35.0	Enviado	Se aclara al participante que, la glosa exacta para la facturación del servicio será definida en coordinación con el postor ganador, con la finalidad de asegurar que las facturas o recibos sean emitidos con la información requerida por la Entidad para su adecuada tramitación.	
25	20106897914	ENTEL PERU S.A.	Consulta	Específico	2-5	-	20	"En las bases dice: FORMA DE PAGO Solicitamos confirmar que, sin afectar el valor del monto adjudicado, en caso de que el inicio de la prestación del servicio no coincida con el ciclo de facturación del operador adjudicatario de la buena pro, la primera facturación incluiría un cargo por el prorrateo del servicio brindado durante los días previos al inicio del correspondiente ciclo de facturación, situación que se presentará también con el último recibo que se emita en el marco del Contrato."		2025-04-16 19:41:14.0	2025-04-16 19:33:55.0	Enviado	Se aclara al participante que, con relación al ciclo de facturación es un aspecto de la fase de ejecución contractual; consideramos que en su momento las áreas competentes lo definirán con el contratista.	
26	20106897914	ENTEL PERU S.A.	Consulta	Específico	2.5	-	20	"En las bases dice: FORMA DE PAGO Solicitamos confirmar que aceptará el ciclo de facturación que se le asigne el postor ganador de la Buena Pro, el cuál será el más cercano a la fecha de activación del servicio."		2025-04-16 19:41:14.0	2025-04-16 19:34:13.0	Enviado	Se aclara al participante que, con relación al ciclo de facturación es un aspecto de la fase de ejecución contractual; consideramos que en su momento las áreas competentes lo definirán con el contratista.	
27	20106897914	ENTEL PERU S.A.	Consulta	Específico	2.5	-	20	"En las bases dice: FORMA DE PAGO Agradeceremos confirmar si la forma de pago indicada será a mes vencido, es decir una vez que se cierre el ciclo mensual de facturación que indique el proveedor"		2025-04-16 19:41:14.0	2025-04-16 19:34:53.0	Enviado	Se aclara al participante que, la Entidad realizará el pago de la contraprestación pactada a favor del contratista en de forma periódica en cuotas mensuales, cuyo porcentaje de pago serán en partes iguales en función al monto del contrato, previa conformidad de la Oficina de Tecnologías de la Información y Comunicaciones, para lo cual el contratista presentará mensualmente un informe del servicio integral dentro de los diez (10) primeros días calendario del siguiente periodo de la prestación de servicio en ejecución. Por lo mencionado, el pago mensual sera despues del mes de servicio, presentación del informe mensual (entregable) y conformidad del area usuaria.	

28	20106897914	ENTEL PERU S.A.	Consulta	Específico	5.7	-	56	"En las bases dice: El postor debe validar tener la autorización del Ministerio de Transporte y Comunicaciones para la prestacion (¿) Solicitamos suprimir el presente requerimiento, toda vez que la acreditación de la capacidad legal del postor ya se encuentra contemplada en el numeral XIV ""Requisitos de Calificación"". Esto con el propósito de evitar la duplicidad de información en la propuesta."		2025-04-16 19:41:14.0	2025-04-16 19:35:34.0	Enviado	Se aclara al participante que, es suficiente presentar un (01) documento de la autorización del Ministerio de Transporte y Comunicaciones solicitado, la cual, dicha presentación de documento en su oferta corresponderá para la acreditación de lo solicitado en el literal i) de los documentos para la admisión de la oferta y el litera A) de los Requisitos de calificación, esto con el propósito de evitar la duplicidad de información en la propuesta.	
29	20106897914	ENTEL PERU S.A.	Consulta	Específico	5.7	-	57	"En la base dice: El postor ganador de la buena pro como parte de la documentación para la suscripción del contrato, de acuerdo al formato inferior deberá demostrar de forma foliadas las validaciones de las características esenciales para la solución el optimizador de ancho de banda, mediante la presentación de hojas técnicas y/o folletos y/o catálogos y/o datasheet y/o link de fabricante y/o carta de fabricante (¿). Agradeceremos se pueda incluir en las bases el formato al que se hace referencia en dicho párrafo. De no contar con uno definido le agradeceremos, se precisa si la acreditación podrá presentarse en un formato libre."		2025-04-16 19:41:14.0	2025-04-16 19:36:09.0	Enviado	Se aclara al participante que la presentación de sustentación de las características esenciales para el optimizador de ancho de banda será en formato libre.	
30	20106897914	ENTEL PERU S.A.	Consulta	Específico	5.7	-	59	"En la base dice: PLAZO DE PRESTACIÓN Para la ejecución de los trabajos de implementación que requieran ejecutarse en vía pública, resulta necesario contar con la obtención de las autorizaciones, permisos y/o títulos habilitantes emitidos por las autoridades competentes (entre ellas, municipalidades y/o Ministerio de Cultura). Respecto de este tipo de autorizaciones y/o títulos habilitantes su emisión se encuentra sujeto al cumplimiento por parte de la autoridad competente de los plazos de ley establecidos para dicho procedimiento. En atención a ello, solicitamos a la Entidad confirmar que las demoras por parte de las autoridades competentes en la emisión de los trámites de permisos y/o títulos habilitantes determinarán la suspensión del plazo de implementación previsto en las Bases hasta que haya quedado subsanado el inconveniente, sin que ello genere la aplicación de ninguna penalidad en contra del contratista, por no representar un retraso atribuible a él. Ello, sin perjuicio de la facultad del contratista de solicitar la ampliación de plazo que resulte necesaria."		2025-04-16 19:41:14.0	2025-04-16 19:36:35.0	Enviado	Se aclara al participante que, en caso de retraso en la obtención de los permisos municipales o del Ministerio de Cultura, dicho retraso será considerado un hecho generador de demora. En este contexto, el contratista podrá solicitar una ampliación de plazo, ya que dicha demora no será imputable al contratista, y no se aplicarán penalidades.	
31	20106897914	ENTEL PERU S.A.	Consulta	Específico	XIV	B.4	64	"En las bases dice: EXPERIENCIA DEL PERSONAL CLAVE Para el personal clave solicitado para los perfiles Jefe de Proyecto, Gestor de Proyecto,Personal Técnico I yII, agradeceremos confirmar que independientemente que las denominaciones de los cargos que ocupe o haya desempeñado en la empresa el profesional propuesto por el postor no coincida literalmente con la denominación de los cargos fijados en las Bases (pues cada empresa puede tener otra denominación para la misma función), se validará la experiencia del profesional en las funciones o actividades realizadas, en la medida que la constancia de trabajo se señale que el personal propuesto ha desarrollado las funciones o actividades solicitadas."		2025-04-16 19:41:14.0	2025-04-16 19:38:44.0	Enviado	Se precisa que si bien está planteada como consulta es una observación y se absuelve como observación, por lo cual se acoge parcialmente y se confirma que tambien se aceptarán otros cargos relacionado a proyectos u otros cargos relacionados a la función del personal tecnico I y II.	5.7. Requisitos del Proveedor y personal: Formación Académica y experiencia: Jefe de Proyecto (Supervisor de servicio) – (01 persona): Se agregará (…) u otro cargo relacionado a proyectos. Personal técnico-I (01 persona como mínimo): Se agregará (…) u otro cargo relacionado a la función del personal técnico I. B.4 EXPERIENCIA DEL PERSONAL CLAVE Jefe de Proyecto – (01 persona): Se agregará (…) u otro cargo relacionado a proyectos. Personal técnico-I (01 persona como mínimo): Se agregará (…) u otro cargo relacionado a la función del personal técnico I. Personal técnico-II (01 persona como mínimo): u otro cargo relacionado a la función del personal técnico II.
32	20106897914	ENTEL PERU S.A.	Consulta	Específico	XIV	B.4	64	"En la base dice: Contar con dos (02) años como mínimo de experiencia en gestión de proyectos de interconexión o Internet (¿). Para el perfil Jefe de Proyecto, agradeceremos confirmar que también se aceptará experiencia mínima de dos (02) años en la gestión y/o supervisión de proyectos de implementación en servicios de internet e internet dedicado. "		2025-04-16 19:41:14.0	2025-04-16 19:39:18.0	Enviado	Se precisa que si bien está planteada como consulta es una observación y se absuelve como observación, por lo cual se acoge parcialmente y se confirma que tambien se aceptara, como experiencia del jefe de proyecto la gestión y/o supervisión de proyectos de implementación en servicios de internet e internet dedicado.	5.7. Requisitos del Proveedor y personal: Formación Académica y experiencia: Jefe de Proyecto (Supervisor de servicio) – (01 persona): Se agregará: (…) o gestión y/o supervisión de proyectos de implementación en servicios de internet e internet dedicado o B.4 EXPERIENCIA DEL PERSONAL CLAVE Requisitos: Jefe de Proyecto – (01 persona): Se agregará: (…) o gestión y/o supervisión de proyectos de implementación en servicios de internet e internet dedicado.
33	20106897914	ENTEL PERU S.A.	Consulta	Anexo	Anexo 3	-	80	"En las bases dice: ANEXO N° 3 DECLARACIÓN JURADA DE CUMPLIMIENTO DE LOS TÉRMINOS DE REFERENCIA ¿¿ el postor que suscribe ofrece el servicio de [CONSIGNAR EL OBJETO DE LA CONVOCATORIA] ¿ ¿ Agradeceremos confirmar que en el Anexo N° 3, para el OBJETO DE LA CONVOCATORIA, se debe considerar el siguiente objeto: ""SERVICIO DE ACCESO DEDICADO DE INTERNET DE BANDA ANCHA PARA LA SUNAFIL"", esto con el fin de consignar la información correcta en este anexo."		2025-04-16 19:41:14.0	2025-04-16 19:40:07.0	Enviado	Se aclara al participante que, el objeto de la convocatoria es: "SERVICIO DE ACCESO DEDICADO DE INTERNET DE BANDA ANCHA PARA LA SUNAFIL"	

34	20106897914	ENTEL PERU S.A.	Consulta	Anexo	Anexo 4	-	81	"En las bases dice: ANEXO Nº 4 DECLARACIÓN JURADA DE PLAZO DE PRESTACIÓN DEL SERVICIO ""... el plazo de [CONSIGNAR EL PLAZO OFERTADO]"" Agradeceremos confirmar que en el Anexo N° 4, para CONSIGNAR EL PLAZO OFERTADO, se debe considerar el siguiente plazo: ""1095 días calendario (equivalente a 03 años)¿, o de lo contrario indicar que en este Anexo N° 4 se deberá completar la información detallada en el numeral 1.8. PLAZO DE PRESTACIÓN DEL SERVICIO; esto con el fin de consignar la información correcta en este anexo."		2025-04-16 19:41:14.0	2025-04-16 19:40:30.0	Enviado	Se aclara al participante que, el plazo de ejecución de la prestación del servicio que se establecerá en el Anexo N° 4 es de 1095 días calendarios, computados a partir del día siguiente de firmada el acta de inicio.	
35	20106897914	ENTEL PERU S.A.	Consulta	Específico	Anexo 6	-	84	"En las bases dice: ANEXO Nº 6 PRECIO DE LA OFERTA Con el fin de presentar correctamente el Anexo N° 6, agradeceremos completar la información referente a CONCEPTO o de lo contrario indicar que en este Anexo N° 6 se deberá completar la columna ¿Concepto¿ con el objeto de la convocatoria detallado en el numeral 1.2 de la Sección Específica de las Bases ""SERVICIO DE ACCESO DEDICADO DE INTERNET DE BANDA ANCHA PARA LA SUNAFIL"", esto con el fin de consignar la información correcta en este anexo."		2025-04-16 19:41:14.0	2025-04-16 19:40:55.0	Enviado	Se aclara al participante que, la denominación de la presente contratación, corresponde al: SERVICIO DE ACCESO DEDICADO DE INTERNET DE BANDA ANCHA PARA LA SUNAFIL, el mismo que será consignado según corresponda, en la oferta del postor.	
36	20106897914	ENTEL PERU S.A.	Consulta	Específico	5.2	A	28	"Se indica: ""A. Solución de Administración y Control de ancho de Banda"" Consulta: Considerando que el ancho de banda de Internet es de 1340Mbps, sírvase confirmar que el equipo de Administración y Control de ancho de banda debe incluir al menos 4 interfaces 10Gbpa Fibra Óptica multimodo para soportar dos bridges de conexión cons soporte bypass externo para garantizar la máxima disponibilidad en caso de reemplazo de equipo por fallo del mismo y así evitar cortes de servicio."		2025-04-16 22:52:15.0	2025-04-16 22:34:00.0	Enviado	Se precisa que si bien está planteada como consulta es una observación y se absuelve como observación, por lo cual se acoge parcialmente, con el objetivo de aclarar el requerimiento de la entidad y de que los postores dimensionen correctamente las soluciones a proponer, por lo cual la solución debe incluir como mínimo la capacidad para gestionar X segmentos físicos que permita su integración con la red de la entidad, se debe tener en cuenta que la conectividad mínima requerida debe ser como mínimo de 4 interfaces del tipo fibra óptica multimodo con velocidad de 10G para soportar dos bridges de conexión en bypass para garantizar la máxima disponibilidad en caso de reemplazo de equipo por fallo del mismo y así evitar cortes de servicio.	5.2. Equipamiento de Gestión y Seguridad de Internet: A. Solución de Administración y Control de ancho de Banda Se suprimira (...) como Se agregará: (...) **o** Se suprimira: (...) minima requerida sea de tipo (cobre/fibra óptica (multimodo o monomodo) con velocidad de (1G o 10G) Se agregará: (...) debe ser como mínimo de 4 interfaces del tipo fibra óptica multimodo con velocidad de 10G para soportar dos bridges de conexión en bypass para garantizar la máxima disponibilidad en caso de reemplazo de equipo por fallo del mismo y así evitar cortes de servicio.
37	20106897914	ENTEL PERU S.A.	Consulta	Específico	5.2	A	34	"Dice: Capacidad de generación de reportes automatizados que se puedan programar con capacidad mínima de exportar en formato PDF, imagen (JPG) y CSV, con capacidad de personalización como puede ser el logo de la entidad. Agradeceremos considerar este punto como opcional, a fin de permitir la pluralidad de marcas y postores."		2025-04-16 22:52:15.0	2025-04-16 22:34:44.0	Enviado	No se considerara como opcional,porque el formato PDF es ideal para la generación de informes finales y presentarlos a la dirección y a otros areas/oficinas debido a que mantiene el formato original, las gráficas y el diseño, asegurando una visualización uniforme en cualquier dispositivo o sisterna operativo, por lo cual no se acepta que sea opcional. Sin embargo, no se solicitara la capacidad de personalización como puede ser el logo de la entidad.	5.2. Equipamiento de Gestión y Seguridad de Internet: A. Solución de Administración y Control de Ancho de Banda: Se suprimira: (…) con capacidad de personalización como puede ser el logo de la entidad
38	20106897914	ENTEL PERU S.A.	Consulta	Específico	5.2	D	47	"Se indica: ""D. Solución de Monitoreo y Gestión de Red:"" Consulta: Sírvase confirmar que la entidad proveerá los espacios y facilidades técnicas para el equipo que alojará la solución requerida."		2025-04-16 22:52:15.0	2025-04-16 22:35:16.0	Enviado	Se aclara al participante, la entidad proveera los espacios necesarios y facilidades tecnicas para el equipo que alojará cada una de las soluciones; por lo cual, se acepta lo indicado por el postor.	
39	20106897914	ENTEL PERU S.A.	Consulta	Específico	5.2	D	48	"Se indica: ""D. Solución de Monitoreo y Gestión de Red: (...) Monitoreo de Enlaces: (...) * Suministro e instalación de solución de monitoreo que permita el análisis y captura del flujo de tráfico generado para el menos 50 dispositivos o interfaces WAN o backbone"" Consulta: Con el objetivo de dimensionar correctamente la solución a ofrecer hacia la entidad, sírvase confirmar que se requiere considerar al menos 50 dispositivos y 50 interfaces más el 25% de crecimiento solicitado en el apartado de Monitoreo de Enlaces los cuales serán sin costo adicional para la entidad."		2025-04-16 22:52:15.0	2025-04-16 22:35:44.0	Enviado	Se aclara al participante que, también se aceptara, el monitoreo en 50 dispositivos y 50 interfaces, los cuales serán sin costo adicional para la entidad.	5.2. Equipamiento de Gestión y Seguridad de Internet: D. Solución de Monitoreo y Gestión de Red: Monitoreo de Enlaces Se agregará: (...) También se aceptará, el monitoreo en 50 dispositivos y 50 interfaces, los cuales serán sin costo adicional para la entidad.
40	20106897914	ENTEL PERU S.A.	Consulta	Específico	5.2	D	48	"Se indica: ""D. Solución de Monitoreo y Gestión de Red: (...) Herramienta Automate Mapping y Troubleshooting: (...) * La solución debe permitir el acceso de múltiples usuarios bajo un esquema cliente servidor, (...), con capacidad de descubrir un mínimo de 200 dispositivos y soportar para 2000 puertos de switches"" Consulta: Sírvase confirmar que ""con capacidad de descubrir un mínimo de 200 dispositivos y soportar para 2000 puertos de switches"" se refiere que la herramienta debe descubrir la cantidad de dispositivos switches cuya sumatoria de puertos sea como mínimo 2000 puertos de switches."		2025-04-16 22:52:15.0	2025-04-16 22:36:11.0	Enviado	Se aclara el requerimiento de la entidad para que los postores dimensionen correctamente las soluciones a proponer, se acepta parcialmente la consulta; por lo cual la solución debe permitir el acceso de múltiples usuarios bajo un esquema cliente servidor, con una simultáneidad de mínimo diez (10) usuarios, con una capacidad de descubrir un mínimo 200 dispositivos de red (switches, routers, firewall, etc.) o soportar para 2000 puertos/interfaces (sumatoria de puertos/interfaces de switches, routers, firewall, etc.).	5.2. Equipamiento de Gestión y Seguridad de Internet: D. Solución de Monitoreo y Gestión de Red: Herramienta Automate Mapping y Troubleshooting Se agregará: (...) de red (switches, routers, firewall, etc.) (…) o soportar como mínimo para 2000 puertos/interfaces (sumatoria de puertos/interfaces de switches, routers, firewall, etc.).

41	20106897914	ENTEL PERU S.A.	Consulta	Específico	5.2	E	48	"Se indica: ""D. Solución de Monitoreo y Gestión de Red: (...) * La herramienta deberá ser implementada por personal certificado por la marca..:"" Consulta: Sírvase confirmar que se deberá incluir como parte de la oferta la certificación ténica del personal solicitado."		2025-04-16 22:52:15.0	2025-04-16 22:36:45.0	Enviado	No se confirma, sin embargo el certificado del personal debe ser presentado para la suscripción del contrato. El certificado del personal debe ser relacionado con la solución de monitoreo.	5.2. Equipamiento de Gestión y Seguridad de Internet: D. Solución de Monitoreo y Gestión de Red: Herramienta Automate Mapping y Troubleshooting Se agregará: (…) El certificado del personal debe ser presentado para la suscripción del contrato. Asimismo, el certificado debe estar relacionado con la solución de monitoreo. 2.3.Requisitos para perfeccionar el contrato: Se agrega: u) Copia del certificado del personal que deberá estar relacionado con la solución de monitoreo.
42	20106897914	ENTEL PERU S.A.	Consulta	Específico	5.2	E	48	"Se indica: ""E. Servicios Integrales de Ciberseguridad: (...) Servicio de Ethical Hacking: (...) * Analizar vulnerabilidades en las aplicaciones WEB y componentes que pudieran poner al descubierto la seguridad del servicio."" Consulta: Con el objetivo de dimensionar correctamente la solución a ofrecer hacia la entidad, sírvase confirmar que el análisis de vulnerabilidaes de aplicaciones WEB será realizado desde internet."		2025-04-16 22:52:15.0	2025-04-16 22:37:11.0	Enviado	Se aclara al participante que, el análisis de vulnerabilidaes de aplicaciones WEB será realizado desde internet.	5.2. Equipamiento de Gestión y Seguridad de Internet: E. Servicios Integrales de Ciberseguridad: Servicio de Ethical Hacking Se agregará: (…) desde Internet.
43	20106897914	ENTEL PERU S.A.	Consulta	Específico	5.2	E	51	"Se indica: ""E. Servicios Integrales de Ciberseguridad: (...) Servicio de Ciberdefensa: (...) * ...alojado en un centro de datos certificado RATED II como mínimo y ubicado en territorio nacional"" Consulta: Sírvase confirmar que la certificación RATED II podrá ser a nivel de contrucción, el cual deberá ser indicado mediante una Declaración Jurada como parte de la oferta indicando el nivel de certificación y dirección del centro de datos."		2025-04-16 22:52:15.0	2025-04-16 22:40:56.0	Enviado	Se precisa que si bien está planteada como consulta es una observación y se absuelve como observación, por lo cual se acoge parcialmente y se confirma que, tambien se aceptará, que el postor debe presentar una declaración jurada del nivel de certificación y dirección del centro de datos , así como copia del certificado RATED II del centro de datos donde se encuentran los componentes del servicio de Ciberdefensa, como parte de la presentación de la oferta.	5.2. Equipamiento de Gestión y Seguridad de Internet: E. Servicios Integrales de Ciberseguridad: Servicio de Ciberdefensa Se agregará: (...) Se acreditará mediante una declaración jurada del nivel de certificación y dirección del centro de datos, así como copia del certificado RATED II del centro de datos donde se encuentran los componentes del servicio de Ciberdefensa, como parte de la presentación de la oferta. 2.2.1.1. Documentos para la admisión de la oferta Se agrega m) Declaración jurada del nivel de certificación y dirección del centro de datos, así como copia del certificado RATED II del centro de datos donde se encuentran los componentes del servicio de Ciberdefensa.
44	20106897914	ENTEL PERU S.A.	Consulta	Específico	5.2	E	51	Dice: "La disponibilidad de información histórica de los eventos debe ser de por lo menos los últimos 30 días. Agradeceremos considerar que la información histórica debe ser de por lo menos 15 días.		2025-04-16 22:52:15.0	2025-04-16 22:42:49.0	Enviado	Se precisa que si bien está planteada como consulta es una observación y se absuelve como observación, por lo cual se acoge parcialmente y se confirma, con el objetivo de permitir la pluralidad de postores y marcas, se acepta parcialmente la consulta; por lo cual como parte del servicio de ciberdefensa se aceptará que la protección DLP sea como mínimo de 15 días.	E. Servicios Integrales de Ciberseguridad: (…) Servicio de Ciberdefensa: Se suprime: (…) 30 se agrega: (…) 15.
45	20106897914	ENTEL PERU S.A.	Consulta	Específico	5.2	E	51	"Se indica: ""E. Servicios Integrales de Ciberseguridad: (...) Servicio de Ciberdefensa: (...) * ...CyberSOC certificado en ISO27001 en gestión de incidentes, gestión de cambios y ciberseguridad."" Consulta: Sírvase confirmar que la certificación ISO27001 deberá ser versión 2022 como mínimo y deberá ser indicado mediante una Declaración Jurada como parte de la oferta indicando el nivel de certificación y los procesos."		2025-04-16 22:52:15.0	2025-04-16 22:43:27.0	Enviado	Se precisa que si bien está planteada como consulta es una observación y se absuelve como observación, por lo cual se acoge, con el objetivo de validar la certificación del Cybersoc, el postor debe presentar una declaración jurada indicando el nivel de certificación y los procesos, asi como la copia del certificado de CyberSOC ISO 27001, para la presentación de la oferta.	5.2. Equipamiento de Gestión y Seguridad de Internet: E. Servicios Integrales de Ciberseguridad: Servicio de Ciberdefensa Se agregará: (...) (el postor debe presentar una declaración jurada indicando el nivel de certificación y los procesos, así como la copia del certificado del CyberSOC en ISO 27001, para la presentación de la oferta) 2.2.1.1. Documentos para la admisión de la oferta Se agrega n) Declaración jurada indicando el nivel de certificación y los procesos, así como la copia del certificado del CyberSOC en ISO 27001.
46	20106897914	ENTEL PERU S.A.	Consulta	Específico	5.2	E	51	"Se indica: ""E. Servicios Integrales de Ciberseguridad: (...) Servicio de Ciberdefensa: (...) * Verificación de vulnerabilidades en la red"" Consulta: Con el objetivo de dimensionar correctamente la solución a ofrecer hacia la entidad, sírvase confirmar si los activos a realizar la verificación de vulnerabilidades en la red son IP públicas o privadas."		2025-04-16 22:52:15.0	2025-04-16 22:43:56.0	Enviado	Se aclara al participante que, para que los postores puedan dimensionar correctamente la solución a proponer, por lo cual el análisis de vulnerabilidades de red se realizarán a las mismas 8 IPs públicas del Servicio de Ethical Hacking.	
47	20106897914	ENTEL PERU S.A.	Consulta	Específico	5.2	E	51	"Se indica: ""E. Servicios Integrales de Ciberseguridad: (...) Servicio de Ciberdefensa: (...) * Verificación de vulnerabilidades en la red"" Consulta: Con el objetivo de dimensionar correctamente la solución a ofrecer hacia la entidad, sírvase confirmar que se refiere a las 8 IPs Públicas solicitadas."		2025-04-16 22:52:15.0	2025-04-16 22:44:24.0	Enviado	Se aclara al participante que, para que los postores puedan dimensionar correctamente la solución a proponer, por lo cual el análisis de vulnerabilidades de red se realizarán a las mismas 8 IPs públicas del Servicio de Ethical Hacking.	

48	20106897914	ENTEL PERU S.A.	Consulta	Específico	5.2	E	51	"Se indica: ""E. Servicios Integrales de Ciberseguridad: (...) Capacitación: Se deberá incluir un curso o programa de Certificación en Ciberseguridad Aplicada a través de una plataforma online educativa, de al menos 20 horas y brindado por un centro de entrenamiento dedicado y para al menos 4 personas y que incluya laboratorios interactivos, (...)"" Consulta: Considerando que es una plataforma online educativa y brindada por un centro de entrenamiento dedicado, sírvase confirmar que los accesos a dicha plataforma deberán estar disponibles al menos 30 días para que los participantes completen el curso o programa y se deberá entregar una constancia al finalizar el curso o programa."		2025-04-16 22:52:15.0	2025-04-16 22:44:49.0	Enviado	Se aclara al participante; por lo cual el curso o programa de Certificación en Ciberseguridad Aplicada debe estar disponible por 30 días para que los participantes completen el curso o programa y se deberá entregar una constancia al finalizar el curso o programa..	5.2. Equipamiento de Gestión y Seguridad de Internet: E. Servicios Integrales de Ciberseguridad: Capacitación. Se agregará: (…) Los accesos a la plataforma de capacitación, podrán estar disponibles al menos 30 días para que los participantes completen el curso o programa y se deberá entregar una constancia al finalizar el curso o programa.
49	20106897914	ENTEL PERU S.A.	Consulta	Específico	5.2	E	51	"Se indica: ""E. Servicios Integrales de Ciberseguridad: (...) Capacitación: Se deberá incluir un curso o programa de Certificación en Ciberseguridad Aplicada a través de una plataforma online educativa, de al menos 20 horas y brindado por un centro de entrenamiento dedicado y para al menos 4 personas y que incluya laboratorios interactivos, (...)"" Consulta: Con la finalidad de validar el cumplimiento, sírvase confirmar que deberá adjuntarse una Declaración Jurada indicando el link de la Plataforma Online Dedicada y la Descripción del Curso o Programa a ofrecer."		2025-04-16 22:52:15.0	2025-04-16 22:45:15.0	Enviado	Se precisa que si bien está planteada como consulta es una observación y se absuelve como observación, por lo cual se acoge parcialmente y se confirma que; el postor ganador debe presentar una declaración jurada indicando el link de la Plataforma Online y la Descripción del Curso o Programa, para la suscripción del contrato.	5.2. Equipamiento de Gestión y Seguridad de Internet: E. Servicios Integrales de Ciberseguridad: Capacitación. Se agregará: (…) El postor ganador debe presentar una declaración jurada indicando el link de la Plataforma Online y la Descripción del Curso o Programa, para la suscripción del contrato. 2.3. Requisitos para perfeccionar el contrato. v) Declaración jurada indicando el link de la Plataforma Online y la Descripción del Curso o Programa.
50	20106897914	ENTEL PERU S.A.	Consulta	Específico	5.4	-	54	"Se indica: ""E. Servicios Integrales de Ciberseguridad: (...) Capacitación: Se deberá incluir un curso o programa de Certificación en Ciberseguridad Aplicada a través de una plataforma online educativa, de al menos 20 horas y brindado por un centro de entrenamiento dedicado y para al menos 4 personas y que incluya laboratorios interactivos, (...)"" Consulta: Con la finalidad de validar el cumplimiento, sírvase confirmar que deberá adjuntarse una Declaración Jurada indicando el link de la Plataforma Online Dedicada y la Descripción del Curso o Programa a ofrecer."		2025-04-16 22:52:15.0	2025-04-16 22:45:44.0	Enviado	Se precisa que si bien está planteada como consulta es una observación y se absuelve como observación, por lo cual se acoge parcialmente y se confirma que; el postor ganado ganador debe presentar una declaración jurada indicando el link de la Plataforma Online y la Descripción del Curso o Programa, para la suscripción del contrato.	5.2. Equipamiento de Gestión y Seguridad de Internet: E. Servicios Integrales de Ciberseguridad: Capacitación. Se agregará: (…) El postor ganador debe presentar una declaración jurada indicando el link de la Plataforma Online y la Descripción del Curso o Programa, para la suscripción del contrato. 2.3. Requisitos para perfeccionar el contrato. v) Declaración jurada indicando el link de la Plataforma Online y la Descripción del Curso o Programa.
51	20106897914	ENTEL PERU S.A.	Consulta	Específico	5.7	-	58	"Se indica: ""Personal técnico-I (01 persona como mínimo): Requisitos: - Técnico titulado o Bachiller o Ingeniero titulado en Sistema o Electrónica o Computación o Informática o Redes o Telecomunicaciones o Redes y Comunicaciones de Datos"" Consulta: Considerando que algunas universidades emiten los títulos con doble programa, sírvase confirmar que se aceptará: Técnico titulado o Bachiller o Ingeniero titulado en Sistema y/o Electrónica y/o Computación y/o Informática y/o Redes y/o Telecomunicaciones y/o Redes y Comunicación de Datos"		2025-04-16 22:52:15.0	2025-04-16 22:46:13.0	Enviado	Se aclara al participante; por lo cual el personal técnico-I debera ser Técnico titulado o Bachiller o Ingeniero titulado en Sistema y/o Electrónica y/o Computación y/o Informática y/o Redes y/o Telecomunicaciones y/o (Redes y Comunicación de Datos)-	5.7. Requisitos del proveedor y personal: Se modificara: Personal técnico-I (01 persona como mínimo): (…) Sistema y/o Electrónica y/o Computación y/o Informática y/o Redes y/o Telecomunicaciones y/o (Redes y Comunicación de Datos). B.3. CALIFICACIONES DEL PERSONAL CLAVE B.3.1. FORMACION ACADEMICA Requisitos: Se modificará para el personal tecnico I: (,,,) Sistemas y/o Electrónica y/o Computación y/o Informática y/o Redes y/o Telecomunicaciones y/o (Redes y Comunicaciones de Datos)
52	20106897914	ENTEL PERU S.A.	Consulta	Específico	5.7	-	58	"Se indica: ""Personal técnico-II (01 persona como mínimo): Requisitos: - Técnico titulado o Bachiller o Ingeniero titulado en Sistema o Electrónica o Computación o Informática o Redes o Telecomunicaciones o Redes y Comunicaciones de Datos"" Consulta: Considerando que algunas universidades emiten los títulos con doble programa, sírvase confirmar que se aceptará: Técnico titulado o Bachiller o Ingeniero titulado en Sistema y/o Electrónica y/o Computación y/o Informática y/o Redes y/o Telecomunicaciones y/o Redes y Comunicación de Datos"		2025-04-16 22:52:15.0	2025-04-16 22:46:39.0	Enviado	Se aclara al participante; por lo cual el personal técnico-II debera ser Técnico titulado o Bachiller o Ingeniero titulado en Sistema y/o Electrónica y/o Computación y/o Informática y/o Redes y/o Telecomunicaciones y/o (Redes y Comunicación de Datos).	5.7. Requisitos del proveedor y personal: (…) Se modificará: Personal técnico-II (01 persona como mínimo): (…) Sistema y/o Electrónica y/o Computación y/o Informática y/o Redes y/o Telecomunicaciones y/o (Redes y Comunicación de Datos). B.3. CALIFICACIONES DEL PERSONAL CLAVE B.3.1. FORMACION ACADEMICA Requisitos: Se modificará para el personal tecnico II: (,,,) Sistemas y/o Electrónica y/o Computación y/o Informática y/o Redes y/o Telecomunicaciones y/o (Redes y Comunicaciones de Datos).
53	20106897914	ENTEL PERU S.A.	Consulta	Específico	5.2	C	33	"En el Literal C, numeral 5.2, dice: Rendimiento en prevención de amenazas: Rendimiento (throughput) de 10 Gbps (medido con capacidades habilitadas de: Firewall, Control de Aplicaciones, IPS, URL Filtering, Antivirus, Anti-Bot o AntiSpyware y Emulación de malware día-cero). Consulta: En vista que los términos que emplean los distintos fabricantes para las capacidades de seguridad pueden variar en su nomenclatura, se solicita por favor considerar los términos de la siguiente manera, siempre manteniendo el mismo alcance para el requerimiento y rendimiento solicitado: Rendimiento en prevención de amenazas: Rendimiento (throughput) de 10 Gbps (medido con capacidades habilitadas de: Firewall, Control de Aplicaciones, IPS, URL Filtering, Antivirus y/o Antimalware, Anti-Bot o AntiSpyware o DNS Security y Emulación de malware día-cero)."		2025-04-16 22:52:15.0	2025-04-16 22:47:04.0	Enviado	Se precisa que si bien está planteada como consulta es una observación y se absuelve como observación, por lo cual se acoge y se confirma que Rendimiento en prevención de amenazas: Rendimiento (throughput) de 10 Gbps (medido con capacidades habilitadas de: Firewall, Control de Aplicaciones, IPS, URL Filtering, Antivirus y/o Antimalware, Anti-Bot o AntiSpyware o DNS Security y Emulación de malware día-cero)."	5.2. Equipamiento de Gestión y Seguridad de Internet: C. Solución de Seguridad Next Generation Firewall (NGFW): 1) Especificaciones técnicas mínimas: Se agregara: (…) y/o Antimalware (…) o DNS Security

54	20106897914	ENTEL PERU S.A.	Consulta	Específico	2.2.1	g	16	"Dice: g) Documento que acredite que los sistemas operativos y/o firmware que operan en los equipos de seguridad firewall ofertados, no deberán tener más de diez (10) vulnerabilidades (CVE) anunciadas y/o publicadas, acumuladas en sus diferentes versiones durante los últimos 12 meses anteriores a la fecha de presentación de la oferta, de acuerdo al literal C (Solución de Seguridad Next Generation Firewall (NGFW), del numeral 5.2 (Funcionalidades requeridas) de los TDR. Consulta: Se solicita a la Entidad confirmar que para acreditar este punto, podrá ser realizado a través de una declaración jurada del postor donde se indique la página web o link del fabricante donde se muetre que los sistemas operativos y/o firmware que operan en los equipos de seguridad firewall ofertados, no deberán tener más de diez (10) vulnerabilidades (CVE) anunciadas y/o publicadas, acumuladas en sus diferentes versiones durante los últimos 12 meses anteriores a la fecha de presentación de la oferta."		2025-04-16 22:52:15.0	2025-04-16 22:47:48.0	Enviado	Se precisa que, para una mayor participacion y mejor entendimiento del requerimiento, se aceptara en la presentación de la oferta, la declaración jurada del postor donde se indique la página web o link del fabricante.	2.2.1.1. Documentos para admisión de oferta Se agrega g) (….) (se aceptara declaración jurada donde se indique página web o link del fabricante)
55	20106897914	ENTEL PERU S.A.	Consulta	Específico	5.2	B	33	"Dice: b) Solución de Protección AntiDDoS Consulta: Se solicita a la Entidad aclarar como se acreditarán las características técnicas del AntiDDoS."		2025-04-16 22:52:15.0	2025-04-16 22:48:31.0	Enviado	Se precisa que el postor deberá presentar una carta de fabricante de la plataforma AntiDDoS donde indique que el postor cuenta con la infraestructura para brindar el servicio, así como el cumplimiento técnico, para la presentación de la oferta técnica.	2.2.1.1. Documentos para admisión de oferta Se agrega: p) Carta de fabricante de la plataforma AntiDDoS donde indique que el postor cuenta con la infraestructura para brindar el servicio, así como el cumplimiento técnico
56	20106897914	ENTEL PERU S.A.	Consulta	Específico	5.2	E	49	"Dice: Servicio de Ciberdefensa ¿ El contratista, deberá entregar un Servicio de Ciberdefensa propio o de un tercero, los componentes de este servicio deberán ser alojados en una nube (en caso de ser en nube debe ser alojado en un centro de datos certificado RATED II como mínimo y ubicado en territorio nacional) siendo el contratista el encargado de brindar los recursos de hardware y software necesarios para su servicio, dicho servicio debe ser operado por un CyberSOC certificado en ISO27001 en gestión de incidentes, gestión de cambios y ciberseguridad. Este servicio deberá permitir mediante el análisis de logs de la solución de seguridad NGFW y Administrador de Ancho de Banda, permita realizar investigaciones y escalar incidentes con las siguientes características: Consulta: Se solicita a la Entidad aclarar con que documentación se sustentará este requerimiento y en que etapa del proceso."		2025-04-16 22:52:15.0	2025-04-16 22:49:01.0	Enviado	Se aclara al participante que, respecto al servicio de Ciberdefensa; por lo cual el postor debe presentar una declaración jurada del nivel de certificación y dirección del centro de datos, así como copia del certificado RATED II del centro de datos donde se encuentran los componentes del servicio de Ciberdefensa, como parte de la presentación de la oferta. Asimismo, el postor debe presentar una copia del certificado de CyberSOC para la presentación de la oferta como parte de su oferta.	5.2. Equipamiento de Gestión y Seguridad de Internet: E. Servicios Integrales de Ciberseguridad: Servicio de Ciberdefensa Se agregará: (...) Se acreditará mediante una declaración jurada del nivel de certificación y dirección del centro de datos, así como copia del certificado RATED II del centro de datos donde se encuentran los componentes del servicio de Ciberdefensa, como parte de la presentación de la oferta. (...) (el postor debe presentar una declaración jurada indicando el nivel de certificación y los procesos, así como la copia del certificado del CyberSOC en ISO 27001, para la presentación de la oferta) 2.2.1.1. Documentos para la admisión de la oferta Se agrega m) Declaración jurada del nivel de certificación y dirección del centro de datos, así como copia del certificado RATED II del centro de datos donde se encuentran los componentes del servicio de Ciberdefensa. n) Declaración jurada indicando el nivel de certificación y los procesos, así como la copia del certificado del CyberSOC en ISO 27001.
57	20106897914	ENTEL PERU S.A.	Consulta	Específico	5.2	E	49	"Dice: Servicio de Ciberdefensa ¿ El contratista, deberá entregar un Servicio de Ciberdefensa propio o de un tercero, los componentes de este servicio deberán ser alojados en una nube (en caso de ser en nube debe ser alojado en un centro de datos certificado RATED II como mínimo y ubicado en territorio nacional) siendo el contratista el encargado de brindar los recursos de hardware y software necesarios para su servicio, dicho servicio debe ser operado por un CyberSOC certificado en ISO27001 en gestión de incidentes, gestión de cambios y ciberseguridad. Este servicio deberá permitir mediante el análisis de logs de la solución de seguridad NGFW y Administrador de Ancho de Banda, permita realizar investigaciones y escalar incidentes con las siguientes características: Consulta: Se solicita a la Entidad aclarar que el servicio de ciberdefensa podrá ser realizado por un CyberSOC propio o terciarizado."		2025-04-16 22:52:15.0	2025-04-16 22:49:30.0	Enviado	Se aclara al participante; en el servicio de ciberdefensa podrá ser realizado por un Cybersoc propio o de un tercero con certificación ISO 27001.	
58	20106897914	ENTEL PERU S.A.	Consulta	Específico	5.2	A	49	"Dice: A) Solución de Administración y Control de Ancho de Banda Consulta: Se solicita a la Entidad confirmar que se podrá sustentar las características técnicas de la Solución de Administración y Control de Ancho de Banda con carta del fabricante."		2025-04-16 22:52:15.0	2025-04-16 22:49:53.0	Enviado	Sa aclara que esta documentación será presentada como Documentación para el perfeccionamiento de contrato. Asimismo, debera sustentar las caracteristicas esenciales indicados en el numeral 5.2. Equipamiento de Gestión y Seguridad de Internet: A. Solución de Administración y Control de Ancho de Banda, señaladas en el literal A.1 Caracteristicas esenciales. Según TDR, tambien se puede validar las caracteristicas esenciales de la Solución de Administración y Control de Ancho de Banda con carta del fabricante.	5.2. Equipamiento de Gestión y Seguridad de Internet: A. Solución de Administración y Control de Ancho de Banda: Se agregará: (…) A.1 Características esenciales. (…) A.2 Otras Características.
59	20106897914	ENTEL PERU S.A.	Consulta	Específico	2.2.1	h	16	"Dice: h) Documentación técnica (datasheet) y/o manuales y/o bochures emitidos públicamente por el propio fabricante de la solución de firewall, adjuntando el documento y enlace (URL) público de Internet del propio fabricante que lo sustente que acredite el cumplimiento referido a las capacidades de hardware y/o de rendimiento solicitadas, No se aceptarán cartas de fabricante y/o representantes locales, como un fundamento para el cumplimiento de estos requerimientos solicitados, de acuerdo al literal C (Solución de Seguridad Next Generation Firewall (NGFW), del numeral 5.2 (Funcionalidades requeridas) de los TDR. Consulta: Se solicita a la Entidad confirmar que al indicar la acreditación del cumplimiento referido a las capacidades de hardware y/o de rendimiento solicitada, hace referencia al numeral 1) Especificaciones técnicas mínimas del literal C (Solución de Seguridad Next Generation Firewall (NGFW). "		2025-04-16 22:52:15.0	2025-04-16 22:50:34.0	Enviado	Se aclara al participante, que el requerimiento indicando en el literal h) del numeral 2.2.1.1 Documentos para la admision de la oferta, se refieren a numeral 1 del literal C. Solución de Seguridad Next Generation Firewall (NGFW).	

60	20106897914	ENTEL PERU S.A.	Consulta	Específico	5.2	B	33	"Dice: b) Solución de Protección AntiDDoS EL sistema de protección Anti DDoS debe poder mitigar ataques de denegación de servicio de día cero, distribuidos y no distribuidos en base a la generación automática de firmas en tiempo real. Consulta: Se solicita a la Entidad confirmar que la generación de firmas automáticas será en menos de 20 segundo y sin intervención humana."		2025-04-16 22:52:15.0	2025-04-16 22:51:03.0	Enviado	Se precisa que si bien está planteada como consulta es una observación y se absuelve como observación, por lo cual se no acoge parcialmente; Sin embargo, tambien se aceptara que la generación de firmas automáticas será en menos de 60 segundos y sin intervención humana.	5.2. Equipamiento de Gestión y Seguridad de Internet: B. Solución de Protección AntiDDoS: Se agregará: (…) La generación de firmas automáticas deberá ser en menos de 60 segundos y sin intervención humana.
61	20106897914	ENTEL PERU S.A.	Consulta	Específico	5.3	B	33	"Dice: El contratista debe poseer un Centro Operaciones de Seguridad (SOC) propio para la gestión del servicio, atención y solución de averías de seguridad (24 x7x365) durante el tiempo de duración del contrato. Asimismo, debe contar con un centro de operaciones de Red (NOC) para la gestión del servicio, atención y solución de averías relacionados a los equipos del proveedor y enlaces del servicio de internet. Consulta: Se solicita a la Entidad indicar como se acreditará este requerimiento y en que fase del proceso de selección."		2025-04-16 22:52:15.0	2025-04-16 22:51:40.0	Enviado	Se precisa que si bien está planteada como consulta es una observación y se absuelve como observación, por lo cual se acoge y se confirma que se acreditará con un certificado emitido por una empresa consultora externa (certificadora en infraestructura) y/o un certificado emitido por una empresa especialista en servicios TI y/o infraestructura y/u otro documento que acredite la operación e infraestructura del NOC & SOC, siendo presentado para la etapa de presentación de la oferta.	5.3. Consideraciones adicionales: Se agregará: (…) Se acreditará con un certificado emitido por una empresa consultora externa (certificadora en infraestructura) y/o un certificado emitido por una empresa especialista en servicios TI y/o infraestructura y/u otro documento que acredite la operación e infraestructura del NOC & SOC, siendo presentado para la etapa de presentación de la oferta. 2.2.1.1. Documentos para admisión de oferta Se agrega o) Se acreditará con un certificado emitido por una empresa consultora externa (certificadora en infraestructura) y/o un certificado emitido por una empresa especialista en servicios TI y/o infraestructura y/u otro documento que acredite la operación e infraestructura del NOC & SOC
62	20494313503	WIREHUAD S.A.C.	Observación	Específico	5	5.7	56	El postor ganador deberá ser miembro activo del NAP PERU. El cual debe acreditar mediante un documento para la suscripción del contrato. EN ESTE PUNTO DEBO SEÑALAR QUE EXISTE UNA CLARA TRANSGRESION AL ART. 2 DE LA LCE, SOBRE EL PRINCIPIO DE: LIBERTAD DE CONCURRENCIA, IGUALDAD DE TRATO Y COMPETENCIA EN LAS CONTRATACIONES DEL ESTADO, POR LO QUE SE PUEDE PRESUMIR UN DIRECCIONAMIENTO A UN POSTOR O GRUPO DE POSTORES QUE SOLO CUMPLEN DICHA EXIGENCIA, PRECISANDO QUE LOS PROCEDIMIENTOS DE SELECCIÓN DEBEN SER UN libre acceso y participación de proveedores en los procesos de contratación, evitando exigencias y formalidades costosas e innecesarias, y prohibiendo prácticas que limiten o afecten la libre concurrencia de proveedores, asimismo prohibiendo la existencia de privilegios o ventajas y el trato discriminatorio como también la provisión de información clara y coherente, garantizando la libertad de concurrencia y que la contratación se desarrolle bajo condiciones de igualdad de trato, objetividad e imparcialidad. POR LO QUE SOLICITAMOS SUPRIMIR DICHA EXIGENCIA, A FIN DE PODER CONTAR CON MAYOR PARTICIPACION DE POSTORES Y TENER UNA GAMA DE PROPUESTAS QUE PUEDAN SER EVALUADOS.		2025-04-16 23:03:00.0	2025-04-16 22:51:49.0	Enviado	No se acoge la observación. Se mantiene la exigencia de que el postor ganador sea miembro activo del NAP Perú, debiendo acreditarlo mediante documento correspondiente al momento de la suscripción del contrato. Cabe precisar que esta condición no constituye una limitación a la libre concurrencia, ya que durante la etapa de estudio de mercado se identificaron diversos proveedores que cumplieron con este requisito y presentaron cotizaciones válidas, lo cual evidencia que no restringe la participación ni favorece a un único postor. Asimismo, la participación activa en el NAP Perú es una condición técnica necesaria para garantizar la calidad, estabilidad y eficiencia del servicio requerido, en línea con los objetivos institucionales y con la necesidad de asegurar el cumplimiento oportuno y adecuado de las prestaciones contratadas. En ese sentido, la exigencia responde a criterios técnicos objetivos, no siendo una formalidad innecesaria ni una barrera de acceso, sino una medida alineada con los principios de eficiencia, calidad del servicio, libre concurrencia y trato igualitario, conforme lo establece el marco normativo vigente.	
63	20494313503	WIREHUAD S.A.C.	Consulta	Específico	5	5.7	58	Considerar Certificado de solución de solución de firewalls. El certificado debe ser emitida por parte del fabricante donde indique que es partner de marca ofertada de la plataforma de nube para almacenamiento de backup.		2025-04-16 23:03:00.0	2025-04-16 23:02:36.0	Enviado	No se confirma, para el Personal Tecnico II, se requiere contar con certificado de la solucion de firewalls, el cual debe ser emitido por el fabricante de la solucion ofertada, en referencia a: C. Solución de Seguridad Next Generation Firewall (NGFW). Lo indicado por el postor: plataforma de nube para almacenamiento de backup, no guarda relación con la solución de firewall.	
64	20421780472	GTD PERÚ S.A	Consulta	Específico	2.3	s	18	DICE: REQUISITOS PARA PERFECCIONAR EL CONTRATO: S) Para el servicio de Ethical Hacking, deberá acreditar con documentación del especialista ingeniero colegiado de sistemas , telecomunicaciones o electrónica con 5 años de experiencia realizando servicios de Ethical Hacking y deberá contar con Certificación vigente ISO/IEC 27001 Senior Lead Implementer, ISO/IEC 27032 Senior Lead Cibersecurity Manager y Certified Ethical Hacker. CONSULTA: Sirvase confirmar a la Entidad, que se aceptará el grado de Ingeniero Informático y de Sistemas, para el especialista a fin de permitir mayor pluralidad de postores.		2025-04-16 23:48:07.0	2025-04-16 23:26:17.0	Enviado	Se confirma parcialmente. Las carreras solicitadas son las mínimas necesaria para el personal que brindará el servicio de Ethical Hacking, Sin embargo, se modificará en: sistemas y/o telecomunicaciones y/o electrónica y/o Informática y/o Informático y de sistemas.	E. Servicios Integrales de Ciberseguridad: Servicio de Ethical Hacking Se modificará: (…) sistemas y/o telecomunicaciones y/o electrónica y/o Informático y/o Informático y de sistemas.
65	20421780472	GTD PERÚ S.A	Consulta	Específico	2.3	s	18	DICE: REQUISITOS PARA PERFECCIONAR EL CONTRATO: S) Para el servicio de Ethical Hacking, deberá acreditar con documentación del especialista ingeniero colegiado de sistemas , telecomunicaciones o electrónica con 5 años de experiencia realizando servicios de Ethical Hacking y deberá contar con Certificación vigente ISO/IEC 27001 Senior Lead Implementer, ISO/IEC 27032 Senior Lead Cibersecurity Manager y Certified Ethical Hacker. CONSULTA: A fin de permitir mayor apertura de postores, sírvase confirmar a la entidad que el especialista asignado, podrá ser un profesional titulado de las carreras de sistemas o telecomunicaciones o electrónica o Informática y de Sistemas , pudiendo quedar de forma opcional el estar colegiado y/o habilitado, dado que es más un tema administrativo que no genera valor a la experiencia solicitada y limitaría la pluralidad de los postores.		2025-04-16 23:48:07.0	2025-04-16 23:26:59.0	Enviado	Se confirma parcialmente. Las carreras solicitadas son las mínimas necesaria para el personal que brindará el servicio de Ethical Hacking, Sin embargo, se modificará en: sistemas y/o telecomunicaciones y/o electrónica y/o Informática y/o Informático y de sistemas. Asimismo, este personal deberá estar colegiado.	E. Servicios Integrales de Ciberseguridad: Servicio de Ethical Hacking Se modificará: (…) sistemas y/o telecomunicaciones y/o electrónica y/o Informático y/o Informático y de sistemas.

66	20421780472	GTD PERÚ S.A	Consulta	Específico	2.3	s	18	DICE: REQUISITOS PARA PERFECCIONAR EL CONTRATO: S) Para el servicio de Ethical Hacking, deberá acreditar con documentación del especialista ingeniero colegiado de sistemas , telecomunicaciones o electrónica con 5 años de experiencia realizando servicios de Ethical Hacking y deberá contar con Certificación vigente ISO/IEC 27001 Senior Lead Implementer, ISO/IEC 27032 Senior Lead Cibersecurity Manager y Certified Ethical Hacker. CONSULTA: A fin de permitir mayor pluralidad de postores, sírvase confirmar a la Entidad que se aceptarán las siguientes certificaciones para el especialista de ethical hacking: - CJPTE: Certified Penetration Testing Engineer (R) - CJSWAE: Certified Secure Web Application Engineer (R) - GIAC Certified Forensic Exmaniner - GCFE - Certified Ethical Hacker v7 - Certified Information Systems Security Professional - CISSP		2025-04-16 23:48:07.0	2025-04-16 23:27:34.0	Enviado	Se precisa que si bien está planteada como consulta es una observación y se absuelve como observación, por lo cual no se acoge. Al ser un servicio especializado, se solicitado que el especialista deberá contar con Certificación vigente ISO/IEC 27001 Senior Lead Implementer, ISO/IEC 27032 Senior Lead Cibersecurity Manager y Certified Ethical Hacker	
67	20421780472	GTD PERÚ S.A	Consulta	Específico	2.3	s	18	DICE: REQUISITOS PARA PERFECCIONAR EL CONTRATO: S) deberá contar con Certificación vigente ISO/IEC 27001 Senior Lead Implementer, ISO/IEC 27032 Senior Lead Cibersecurity Manager y Certified Ethical Hacker. CONSULTA: Sírvase confirmar, si la Entidad requiere que el especialista cuente con las tres certificaciones mencionadas o podría contar con al menos una (01) certificación vigente, pudiendo quedar el texto de la siguiente forma: deberá de contar con al menos una (01) Certificación vigente en ISO/IEC 27001 Senior Lead Implementer o ISO/IEC 27032 Senior Lead Cibersecurity Manager o Certified Ethical Hacker.		2025-04-16 23:48:07.0	2025-04-16 23:28:11.0	Enviado	Se precisa que si bien está planteada como consulta es una observación y se absuelve como observación, por lo cual no se acoge. Al ser un servicio especializado, se solicitado que el especialita deberá tener deberá contar con Certificación vigente ISO/IEC 27001 Senior Lead Implementer, ISO/IEC 27032 Senior Lead Cibersecurity Manager y Certified Ethical Hacker	
68	20421780472	GTD PERÚ S.A	Consulta	Específico	5.2	a	28	Dice: 5.2 Equipamiento de Gestión y Seguridad de Internet Consulta: Sugerimos amablemente a la entidad incluir que de la solución ofertada el fabricante cuente con un centro de soporte (TAC) en Latinoamérica, con personal propio del fabricante y diferente al del oferente en este proceso, que permita el acceso a soporte de cualquier nivel en español latinoamericano en horario local.		2025-04-16 23:48:07.0	2025-04-16 23:28:38.0	Enviado	No se confirma lo indicado por el participante; debido a que lo solicitado supone incluir un cambio sustancial en lo Términos de referencia y con el modelo actual de Términos de referencia se logró la pluralidad en la etapa de Indagación de mercado.	
69	20421780472	GTD PERÚ S.A	Consulta	Específico	5.2	a	28	Dice: La solución ofertada debe estar en capacidad de soportar un mínimo de 3.000.000 de flujos concurrentes para las labores de monitoreo y administración del ancho de banda de todos los usuarios de la entidad. Consulta: Sugerimos a la entidad considerar un mayor número de flujos concurrentes sobre la solución ofertada dado que para la administración y monitoreo del ancho de banda solicitado se requiere de una solución robusta y escalable que no genere problemas de disponibilidad sobre la plataforma, por lo que sugerimos que el mínimo de flujos concurrentes sea de 20.000.000		2025-04-16 23:48:07.0	2025-04-16 23:29:19.0	Enviado	No se confirma lo indicado por el postor, con el objetivo de permitir la pluralidad de postores y no encarecer la solución innecesariamente, no se acepta la consulta; debido a que lo solicitado supone un cambios sustancial en lo Términos de referencia y con el modelo actual de Términos de referencia se logró la pluralidad en la etapa de indagació de mercado.	
70	20421780472	GTD PERÚ S.A	Consulta	Específico	5.2	a	29	Dice: La solución debe incluir como mínimo la capacidad para gestionar X segmentos físicos que permita su integración con la red de la entidad, se debe tener en cuenta que la conectividad mínima requerida sea de tipo (cobre/fibra óptica (multimodo o monomodo) con velocidad de (1G o 10G).		2025-04-16 23:48:07.0	2025-04-16 23:29:59.0	Enviado	El participante no plantea una consulta.	
71	20421780472	GTD PERÚ S.A	Consulta	Específico	5.2	a	29	DICE: La consola de gestión de la solución debe ser totalmente gráfica que permita una interacción facil e intuitiva,esto aplica también para la sección de políticas donde se deben tener mecanismos que permita la indentificación de la política que está siendo aplicada a un tráfico específico.... CONSULTA: Sírvase aclarar a que se refiere solución totalmente gráfica?		2025-04-16 23:48:07.0	2025-04-16 23:30:27.0	Enviado	Se aclara lo indicado por el postor, por lo cual la consola de gestión de la solución debe ser principalmente gestionado en modo gráfico (interfaz gráfica de usuario - GUI).	
72	20421780472	GTD PERÚ S.A	Consulta	Específico	5.2	a	29	DICE: La solución debe tener la capacidad miníma de identificar automaticamente el tráfico por usuario de directorio activo que permita tener reportes de su consumo y como opcional la opción de generar políticas por usuario, esta capacidad debe ser por medio de la integración con el servicio de directorio activo CONSULTA: Sírvase confirmar si permite crear políticas de seguridad basadas en grupos de usuarios definidos en el servicio de Directorio Activo. Asimismo, mencionar la cantidad de grupos que tiene el AD.		2025-04-16 23:48:07.0	2025-04-16 23:31:34.0	Enviado	No se confirma lo indicado por el postor; debido a que lo solicitado supone un cambio sustancial en los Términos de referencia y con el modelo actual de Términos de referencia se logró la pluralidad en la etapa de Estudio de mercado. Asimismo, la información solicitada en relación a la cantidad de grupos AD es información confidencial que solamente será proporcionado al postor ganador, en caso lo requiera.	
73	20421780472	GTD PERÚ S.A	Consulta	Específico	5.2	a	30	Dice: La solución debe estar en capacidad de medir métricas de rendimiento que permita monitorear el tráfico de la red, donde se garanticen mínimamente las siguientes métricas solicitadas: Observaciones: Solicitamos amablemente a la entidad que este ítem sea opcional, ya que esto imposibilita la pluralidad de oferentes.		2025-04-16 23:48:07.0	2025-04-16 23:32:04.0	Enviado	No se confirma lo indicado por el postor; debido a que con el modelo actual de Términos de referencia se logró la pluralidad de postores en la etapa de Estudio de mercado. Asimismo, las métricas requeridas: Métricas de calidad de experiencia - QoE, Métricas de redes, Métricas de tráfico WEb (HTTP/HTTPS) y Métricas para tráfico de VoIP son parámetros necesarios para poder realizar diversos descartes cuando suceden incidentes en la red tales como latencia, saturación, etc.	
74	20421780472	GTD PERÚ S.A	Consulta	Específico	5.2	a	30	DICE: La solución debe tener la capacidad de medir métricas de rendimiento que permita monitorear el tráfico de red y de las aplicaciones, donde se garantice mínimamente las siguientes métricas solicitadas CONSULTA: Sírvase confirmar si las métricas asociadas al tráfico de VoIP como identificador de llamada (Caller ID), tiempo de sesión y duración, puede ser excluidas sin afectar el cumplimiento del resto de los indicadores de rendimiento requeridos por la solución.		2025-04-16 23:48:07.0	2025-04-16 23:32:27.0	Enviado	No se confirma lo indicado por el postor; precisando que las metricas de rendimiento para trafico de VoIP, son metricas necesarios para poder realizar diversos descartes cuando suceden incidentes en VoIP, y luego tomar las medidas para asegurar que las llamadas de voz tengan suficiente ancho de banda y se realicen con alta calidad, sin interrupciones ni retrasos, por lo cual no se acepta la consulta; debido a que con el modelo actual de Términos de referencia se logró la pluralidad de postores en la etapa de indagación de mercado.	

75	20421780472	GTD PERÚ S.A	Consulta	Específico	5.2	a	30	DICE: La solución debe permitir el editar métricas ya existentes o crear otras nuevas en función de los requerimientos de la entidad a fin de evaluar el rendimiento del tráfico del elance gestionado CONSULTA: Se solicita confirmar si habrá una migración de configuración desde un firewall existente. En tal caso, se deberá indicar la marca y modelo del equipo origen, las funcionalidades activas, así como el número estimado de políticas de seguridad, perfiles configurados y cualquier otro elemento relevante que deba ser considerado en el proceso de transición.		2025-04-16 23:48:07.0	2025-04-16 23:32:53.0	Enviado	No se confirma lo indicado por el postor; debido a que la información solicitada en relación a la marca y modelo de los equipos actuales de seguridad es información confidencial y sensible que solamente será proporcionado al postor ganador, en caso lo requiera. Asimismo, se precisa, para la solución de administración y control de ancho de banda no se realizará una migración de configuración desde un firewall existente.	
76	20421780472	GTD PERÚ S.A	Consulta	Específico	5.2	a	31	Dice: La solución debe permitir configurar los valores de ancho de banda en la política tanto por un número fijo como también por porcentaje (%) que permita ser calculado según la capacidad superior al tener una estructura de múltiples niveles jerárquicos. Consulta: Solicitamos amablemente a la entidad que la configuración de los valores de ancho de banda en la política por porcentaje (%) sea opcional ya que la configuración por valores fijos permite un control más preciso sobre la red, además que, la configuración de los valores de ancho de banda en la política por porcentaje (%) es una característica que cumple un solo oferente, por lo que esto imposibilita la pluralidad de oferentes.		2025-04-16 23:48:07.0	2025-04-16 23:33:23.0	Enviado	No se confirma lo indicado por el postor, precisando que, en el caso el proveedor de servicios de internet (ISP) aumente el ancho de banda total disponible, las políticas configuradas en porcentaje se ajustarán automáticamente sin necesidad de una intervención manual extensa, por lo cual no se acepta la consulta.	
77	20421780472	GTD PERÚ S.A	Consulta	Específico	5.2	a	31	Dice: La consola de la solución debe ser de tipo web con estándar HTML5 como mínimo que permita el acceso desde cualquier navegador web aun de dispositivos móviles a fin de evitar dependencias en aplicaciones o servicios específicos y/u obsoletos que afecta el fácil acceso para los administradores. Consulta: Solicitamos amablemente a la entidad considerar añadir como característica adicional que la consola de la solución sea de tipo GUI, esto para garantizar la pluralidad de oferentes.		2025-04-16 23:48:07.0	2025-04-16 23:34:01.0	Enviado	Se aclara al participante; por lo cual la consola de gestión de la solución tambien se aceptará ser gráfica (interfaz gráfica de usuario - GUI).	5.2. Equipamiento de Gestión y Seguridad de Internet: A. Solución de Administración y Control de Ancho de Banda: A.2 Otras Caracteristicas. Se agregará: (…) y/o interfaz GUI
78	20421780472	GTD PERÚ S.A	Consulta	Específico	5.2	a	31	Dice: La solución deber proveer un sistema de autoprotección y detección de incongruencias en políticas configuradas impidiendo la creación de una definición errónea que afecte el correcto funcionamiento de la solución, evitando que se guarde la política y visualizando la política que presento el error detectado. Consulta: Solicitamos amablemente a la entidad que este ítem sea opcional, ya que esto imposibilita la pluralidad de oferentes.		2025-04-16 23:48:07.0	2025-04-16 23:34:31.0	Enviado	No se confirma lo indicado por el postor, la solución de administración de ancho de banda debe detectar errores o conflictos en las políticas de configuración, esto ayuda a prevenir comportamientos inesperados o fallos en la red. De esta manera, se minimiza el tiempo de inactividad y garantiza una experiencia de red consistente para los usuarios; por lo cual no se acepta la consulta.	
79	20421780472	GTD PERÚ S.A	Consulta	Específico	5.2	a	31	Dice: La solución debe ofrecer capacidad de almacenamiento de datos de forma histórica que permita establecer la granularidad de visualización en función del tiempo de tal forma que se adapte a las necesidades de visualización histórica de datos de la entidad y como mínimo debe garantizar la retención de datos por todo el tiempo del contrato. Consulta: Solicitamos amablemente a la entidad considerar mínimo dos (2) años de tiempo de retención de datos con el fin de optimizar los recursos de almacenamiento y alinearse con las necesidades específicas de administración de ancho de banda.		2025-04-16 23:48:07.0	2025-04-16 23:34:56.0	Enviado	No se confirma lo indicado por el postor, cuando ocurre un incidente de seguridad, los logs son cruciales para entender qué pasó, cómo sucedió, qué sistemas se vieron afectados y qué acciones tomó el atacante. Esto permite una respuesta más efectiva, la contención del daño y la implementación de medidas para prevenir futuros incidentes; por lo tanto, es de suma importancia contar con la información necesaria por todo el tiempo del contrato; por lo cual no se acepta la consulta.	
80	20421780472	GTD PERÚ S.A	Consulta	Específico	5.2	a	32	Dice: Capacidad de generación de informes automatizados que se puedan programar con capacidad mínima de exportar en formato PDF, imagen (JPG) y CSV, con capacidad de personalización como puede ser el logo de la entidad. Consulta: Solicitamos amablemente a la entidad que el formato de imagen requerido para la generación de informes sea imagen (JPG y/o PNG), esto para garantizar la pluralidad de oferentes.		2025-04-16 23:48:07.0	2025-04-16 23:35:21.0	Enviado	Se aclara al participante, teniendo en cuenta que el formato solicitado es de imagen y existen conversores comerciales entre el formato solicitado por la entidad y el formato propuesto y con el objetivo de permitir la pluralidad de postores; se acepta la consulta.	5.2. Equipamiento de Gestión y Seguridad de Internet: A. Solución de Administración y Control de Ancho de Banda: A.2 Otras Caracteristicas. Se agregará: y/o PNG
81	20421780472	GTD PERÚ S.A	Consulta	Específico	5.2	a	32	Dice: La notificación de las alarmas debe como mínimo emitir en dos tipos de comunicación directa a los usuarios, siendo uno de ellos el correo electrónico (email) y el otro tipo de medio debe ser mensajería instantánea (ej: WhatsApp. Microsoft Teams o similares) que permita la rápida interacción con los funcionarios responsables de la entidad. Consulta: Solicitamos amablemente a la entidad que el medio de comunicación de mensajería instantánea sea opcional o retirado ya que esto solo lo cumple un oferente y esto imposibilita la pluralidad de oferentes.		2025-04-16 23:48:07.0	2025-04-16 23:35:50.0	Enviado	No se confirma lo indicado por el postor, las aplicaciones de mensajería instantánea se utiliza y revisa con frecuencia en los dispositivos móviles reduciendo alertas directamente asegurando que el administrador de red sea notificado de problemas críticos de ancho de banda de manera inmediata, sin depender de la revisión constante de correos electrónicos o paneles de control; por lo cual no se acepta la consulta.	
82	20421780472	GTD PERÚ S.A	Consulta	Específico	5.2	a	32	Dice: Capacidades de auto-aprendizaje del comportamiento de consumo de ancho de banda que permita establecer análisis basado en desviaciones permitiendo adaptar dinámicamente las alarmas según a este aprendizaje, como también la capacidad de predecir consumos a futuro que permita hacer aprovisionamientos o ajustes de configuración que permita evitar situaciones de saturación. Consulta: Solicitamos amablemente a la entidad que las capacidades de aunto-aprendizaje del comportamiento de consumo de ancho de banda sea opcional o retirado ya que esto solo lo cumple un oferente y esto imposibilita la pluralidad de oferentes.		2025-04-16 23:48:07.0	2025-04-16 23:36:16.0	Enviado	No se confirma lo indicado por el postor, precisando que, un administrador de ancho de banda con auto-aprendizaje puede establecer una línea base del comportamiento "normal" del ancho de banda a lo largo del tiempo, considerando patrones diarios, semanales y mensuales. Una vez establecida esta línea base, el sistema puede identificar automáticamente cualquier desviación significativa, lo que podría detectarse problemas como ataques DDoS, malware consumiendo ancho de banda, fallas en equipos o un uso inusual por parte de algún usuario o aplicación. Esto permite al administrador de red tomar medidas preventivas antes de que el rendimiento de la red se vea seriamente afectado.; por lo cual no se acepta la consulta. Asimismo, se requiere esta característica de la solución debido a que puede predecir consumos de ancho de banda a futuro que permitan luego hacer aprovisionamientos o ajustes de configuración y evitar de esta manera situaciones de saturación.	
83	20421780472	GTD PERÚ S.A	Consulta	Específico	5.2	a	33	Dice: Capacidad de throughput de protección incluida debe ser de al menos 25Gbps de tráfico. Consulta: Con la finalidad de permitir pluralidad de postores y considerando que el Servicio de Internet es de 1,340Mbps, se solicita a la entidad confirmar que se aceptarán soluciones AntiDDoS cuya capacidad de protección se encuentre licenciado para cubrir el incremento de 100%, es decir, 2.6Gbps ~ 3Gbps.		2025-04-16 23:48:07.0	2025-04-16 23:36:50.0	Enviado	No se confirma. Teniendo en consideración que el servicio AntiDdos debe estar en la nube local del proveedor donde el trafico de Internet del proveedor es mayor y por ello la plataforma de mitigación debe tener capacidad de Throughput de 25Gbps. Se precisa que, de acuerdo con la indagacion a traves del estudio de mercado, existe pluralidad de postores y fabricantes que cumplen con dicho requerimiento.	

84	20421780472	GTD PERÚ S.A	Consulta	Específico	5.2	a	33	Dice: El sistema de protección AntiDDoS debe contar con firmas que permitan proteger contra ataques conocidos. Consulta: Entendemos que el propósito de la entidad es asegurar la utilización de la mejor tecnología de mitigación disponible para su protección. En aras de fomentar la pluralidad de proponentes y considerando que cada fabricante implementa estrategias tecnológicas distintas, solicitamos la revisión de este requerimiento para que no dependa exclusivamente de la creación de firmas en tiempo real, sino que permitan también otras estrategias de defensa como la implementación de algoritmos adaptativos en múltiples capas (de L3 a L7) que trabajen en conjunto e incluyan la inteligencia del fabricante. Esta metodología permite una mitigación dinámica y eficaz contra ataques emergentes y multivectoriales, respondiendo de forma efectiva a amenazas complejas sin recurrir a la generación de firmas, que en el caso de ataques multivector suele incrementar la tasa de falsos positivos.		2025-04-16 23:48:07.0	2025-04-16 23:37:37.0	Enviado	No se confirma, según TDR la solución de protección Anti DDoS permitira proteger mínimamente contra ataques de inundación del tipo TCP SYN, TCP RST, UDP, ICMP y otros tipos de ataques de denegación de servicio. Asimismo, tiene un modulo de IPS (Sistema de Prevención de Intrusos) que actua en multiples capas.	
85	20421780472	GTD PERÚ S.A	Consulta	Específico	5.2	a	33	Dice: El sistema de protección AntiDDoS debe poder mitigar ataques de denegación de servicio de día cero, distribuidos y no distribuidos en base a la generación automática de firmas en tiempo real. Consulta: Entendemos que el propósito de la entidad es asegurar la utilización de la mejor tecnología de mitigación disponible para su protección. En aras de fomentar la pluralidad de proponentes y considerando que cada fabricante implementa estrategias tecnológicas distintas, solicitamos la revisión de este requerimiento para que no dependa exclusivamente de la creación de firmas en tiempo real, sino que permitan también otras estrategias de defensa como la implementación de algoritmos adaptativos en múltiples capas (de L3 a L7) que trabajen en conjunto e incluyan la inteligencia del fabricante. Esta metodología permite una mitigación dinámica y eficaz contra ataques emergentes y multivectoriales, respondiendo de forma efectiva a amenazas complejas sin recurrir a la generación de firmas, que en el caso de ataques multivector suele incrementar la tasa de falsos positivos.		2025-04-16 23:48:07.0	2025-04-16 23:38:08.0	Enviado	No se confirma, según TDR la solución de protección Anti DDoS permitira proteger mínimamente contra ataques de inundación del tipo TCP SYN, TCP RST, UDP, ICMP y otros tipos de ataques de denegación de servicio. Asimismo, tiene un modulo de IPS (Sistema de Prevención de Intrusos) que actua en multiples capas.	
86	20421780472	GTD PERÚ S.A	Consulta	Específico	5.2	b	33	Dice: La solución deberá tener integrado un módulo de IPS (Sistema de Prevención de Intrusos). Consulta: Teniendo en cuenta que la funcionalidad de IPS no es parte esencial de una solución dedicada a protección contra ataques de DDoS y su implementación puede comprometer las características stateless del appliance, solicitamos que se ponga este punto como opcional o sea removido. Los Firewall, IPSs y WAF son componentes stateful. Esto significa que, una vez establecida una sesión, el dispositivo mantiene información del estado de todas las conexiones que lo atraviesan incluso para protocolos sin estado como UDP o ICMP, y lo hace desde que comienza la conexión hasta que termina. Esta información se guarda en tablas de sesión. Necesita esta información para determinar si el siguiente paquete es válido o no. El número de conexiones en la tabla de sesión tiene un límite y una vez se ha alcanzado este, el dispositivo entra en un estado en el que no puede aceptar más conexiones y empieza a denegar el servicio. Los atacantes lo saben y generan múltiples conexiones para forzar este límite generando una denegación del servicio.		2025-04-16 23:48:07.0	2025-04-16 23:38:41.0	Enviado	No se confirma, debido a que el IPS permite la prevención de intrusos en la red de SUNAFIL, asimismo la solución debe bloquear la denegación de servicio contra ataques de inundación del tipo TCP SYN, TCP RST, UDP, ICMP y otros tipos de ataques de denegación de servicio.	
87	20421780472	GTD PERÚ S.A	Consulta	Específico	5.2	b	33	Dice: La solución deberá soportar un incremento del tráfico originado por ataques de Denegación de Servicios del tipo volumétricos desde hasta un máximo del 100% del ancho de banda contratado. Consulta: Considerando que el Servicio de Internet es de 1,340Mbps, se solicita a la entidad confirmar que se aceptarán soluciones AntiDDoS cuya capacidad de protección se encuentre licenciado para cubrir el incremento de 100%, es decir, 2.6Gbps ~ 3Gbps.		2025-04-16 23:48:07.0	2025-04-16 23:39:13.0	Enviado	No se confirma. Teniendo en consideración que el servicio AntiDdos debe estar en la nube local del proveedor donde el trafico de Internet del proveedor es mayor y por ello la plataforma de mitigación debe tener capacidad de Throughput de 25Gbps. Se precisa que, de acuerdo con la indagacion a traves del estudio de mercado, existe pluralidad de postores y fabricantes que cumplen con dicho requerimiento.	
88	20421780472	GTD PERÚ S.A	Consulta	Específico	5.2	b	33	Dice: La solución deberá proteger frente a ataques de denegación de servicios en una arquitectura "always on", también denominada en línea o siempre activa. No se aceptarán soluciones de mitigación de ataques de denegación de servicios bajo una arquitectura de derivación de tráfico.		2025-04-16 23:48:07.0	2025-04-16 23:39:50.0	Enviado	El participante no plantea una consulta.	
89	20421780472	GTD PERÚ S.A	Consulta	Específico	5.2	b	33	Dice: El proveedor deberá brindar acceso a la plataforma (usuario de lectura) para la revisión de estadísticas por parte de la Entidad. Consulta: Siendo el Postor el especialista en la solución AntiDDoS a ofertar, sirvase la entidad confirmar y/o modifcar este parrafo para que sea un requerimiento deseable más no obligatorio, considerando el siguiente texto: "El proveedor podrá brindar acceso a la plataforma (usuario de lectura) para la revisión de estadísticas por parte de la Entidad".		2025-04-16 23:48:07.0	2025-04-16 23:40:27.0	Enviado	Se confirma, el proveedor podrá brindar acceso a la plataforma (usuario de lectura) para la revisión de estadísticas por parte de la Entidad.	5.2. Equipamiento de Gestión y Seguridad de Internet: En B. Solución de Protección AntiDDos. Se suprimira: (…) deberá Se agregará (…) podrá
90	20421780472	GTD PERÚ S.A	Consulta	Específico	5.2	c	34	Dice: Rendimiento en NGFW - Next Generation Firewall: Rendimiento (throughput) de 30 Gbps (medido con Capacidades habilitadas de: Firewall, Control de Aplicaciones e IPS). Consulta: Se debe tener en cuenta que la seguridad que ofrece un firewall de siguiente generación debe ser con todos los módulos activos (lo que comunmente se le denomida rendimiento de prevención de amenazas, debido a que con esta medición se puede establecer el nivel de impacto que tendrá el equipo al activar todas las funciones de seguridad que son vitales para prevenir amenazas conocidas y desconocidas, por lo cual, se siguiere que este punto no sea consdierado porque no transmite el verdadero rendimiento que debe tener el equipo frente a un ambiente de producción, debido a que no solo se activarán IPS, Firewall y control de aplicaciones.		2025-04-16 23:48:07.0	2025-04-16 23:40:53.0	Enviado	No se confirma, la solución de seguridad next generation firewall, debe garantizar unas capacidades minimas para asegurar un optimo funcionamiento del servicio de internet para la Sede Central y las sedes interconectadas a nivel nacional.	

91	20421780472	GTD PERÚ S.A	Consulta	Específico	5.2	c	34	Dice: Sesiones Concurrentes: 16'000,000 conexiones o sesiones concurrentes Consulta: Es importante tener en consideración que existen diversos modos de medir el rendimiento de las sesiones concurrentes, con el módulo de control de aplicaciones utilizando tráfico HTTP (capa 7, y lo que corresponde a un firewall de siguiente generación) y las sesiones utilizando tráfico TCP (capa 4). El tráfico HTTP es es un protocolo de aplicación web mientras que el TCP es un protocolo de transporte capa 4, por lo cual, el rendimiento en cada uno de ellos difiere y en haras de garantizar el rendimiento de los equipos solicitados, se deberá diferenciar las mediciones de sesiones concurrentes y por segundo tanto para fabricantes que utilicen tráfico HTTP (capa 7) y TCP (Capa 4), por lo cual, el punto deberá estar de la siguiente manera: La plataforma de hardware debe soportar como mínimo 2.2 millones sesiones/conexiones concurrentes y 220 mil nuevas sesiones/conexiones por segundo, medidos en capa 7 (con paquetes HTTP); o en su defecto, soportar 16 millones de sesiones/conexiones concurrentes y 850 mil nuevas sesiones/conexiones por segundo, medidos en capa 4 (con paquetes TCP).		2025-04-16 23:48:07.0	2025-04-16 23:41:25.0	Enviado	No se confirma, se mantiene el numero de sesiones concurrentes solicitados, teniendo en consideración que el firewall tiene que soportar el trafico de internet de la Sede Central y el proveniente de la interconexión de las sedes regionales de SUNAFIL, a nivel nacional.	
92	20421780472	GTD PERÚ S.A	Consulta	Específico	5.2	c	34	Dice: Conexiones por segundo: 350,000 conexiones a sesiones por segundo Consulta: Es importante tener en consideración que existen diversos modos de medir el rendimiento de las sesiones nuevas por segundo, con el módulo de control de aplicaciones utilizando tráfico HTTP (capa 7, y lo que corresponde a un Firewall de siguiente generación) y las sesiones utilizando tráfico TCP (capa 4). El tráfico HTTP es es un protocolo de aplicación web mientras que el TCP es un protocolo de transporte capa 4, por lo cual, el rendimiento en cada uno de ellos difiere y en haras de garantizar el rendimiento de los equipos solicitados, se deberá diferenciar las mediciones de sesiones concurrentes y por segundo tanto para fabricantes que utilicen tráfico HTTP (capa 7) y TCP (Capa 4), por lo cual, el punto deberá estar de la siguiente manera: La plataforma de hardware debe soportar como mínimo 2.2 millones sesiones/conexiones concurrentes y 220 mil nuevas sesiones/conexiones por segundo, medidos en capa 7 (con paquetes HTTP); o en su defecto, soportar 16 millones de sesiones/conexiones concurrentes y 850 mil nuevas sesiones/conexiones por segundo, medidos en capa 4 (con paquetes TCP).		2025-04-16 23:48:07.0	2025-04-16 23:41:59.0	Enviado	No se confirma, se mantiene el numero de conexiones por segundo solicitados, teniendo en consideración que el firewall tiene que soportar el trafico de internet de la Sede Central y el proveniente de la interconexión de las sedes regionales de SUNAFIL, a nivel nacional.	
93	20421780472	GTD PERÚ S.A	Consulta	Específico	5.2	c	34	Dice: El fabricante de la solución de seguridad debe tener un porcentaje igual o superior al 98% de ratio de protección, en la última evaluación de Enterprise Firewall Report de CyberRatings para el año 2024. Consulta: Con la finalidad de aperturar las Bases y no apuntar a un solo vendor, sirvase confirmar que el puntaje mínimo será del 96%, llevando esto a modificar el texto indicando: .."porcentaje igual o superior al 96%.		2025-04-16 23:48:07.0	2025-04-16 23:42:37.0	Enviado	No se confirma lo indicado por el postor, se requiere una solución de seguridad robusta para la protección de información de la entidad. Se precisa que, de acuerdo con la indagacion a traves del estudio de mercado, existe pluralidad de postores y fabricantes que cumplen con dicho requerimiento.	
94	20421780472	GTD PERÚ S.A	Consulta	Específico	5.2	c	34	Dice: El fabricante de la solución de seguridad debe tener un porcentaje igual o superior al 98% de ratio de protección, en la última evaluación de Enterprise Firewall Report de CyberRatings para el año 2024. Consulta: Sirvase confirmar que para garantizar la pluralidad de postores, esta evaluación será considerada como opcional.		2025-04-16 23:48:07.0	2025-04-16 23:43:08.0	Enviado	No se confirma lo indicado por el postor. Se requiere una solución de seguridad robusta para la protección de información de la entidad. Se precisa que, de acuerdo con la indagacion a traves del estudio de mercado, existe pluralidad de postores y fabricantes que cumplen con dicho requerimiento. Por lo tanto este requerimiento no sea considerado como opcional.	
95	20421780472	GTD PERÚ S.A	Consulta	Específico	5.2	c	34	Dice: Los sistemas operativos y/o firmware que operan en los equipos de seguridad firewall ofertados, no deberán tener más de diez (10) vulnerabilidades (CVE) anunciadas y/o publicadas, acumuladas en sus diferentes versiones durante los últimos 12 meses antenoresa la fecha de presentación de propuestas. Consulta: Teniendo en cuenta que las vulnerabilidades publicadas por los fabricantes son de diversas severidades y estos se catalogan por score CVSS (Common Vulnerability Scoring System), y para garantizar la pluralidad de postores, se solicita que el punto pueda modificarse de la siguiente forma: Los sistemas operativos y/o firmware que operan en los equipos de seguridad firewall ofertados, no deberán tener más de diez (10) vulnerabilidades (CVE) o contar con un CVSS superior a 9 anunciadas y/o publicadas, acumuladas en sus diferentes versiones durante los últimos 12 meses antenores a la fecha de presentación de propuestas.		2025-04-16 23:48:07.0	2025-04-16 23:43:40.0	Enviado	No confirma lo indicado por el postor. Se precisa que, en la Finalidad Publica del presente proceso se establece: ."…seguridad gestionada basasa en tecnologia Next Generation Firewall (NGFW), garantizando una conexion confiable, segura y de alta disponibilidad.", asi mismo en el Objetivo General del presente proceso se establece: "Este servicio debe garantizar alta disponibilidad, confiabilidad y seguridad en el intercambio de informacion,...". En tal sentido, los compontes NGFW que se pretenden contratar deben de ofrecer la capacidad para brindar seguridad en las comunicaciones y servicios de le entidad, por lo cual estos no deberían ser inseguros (vulnerables) de manera expresa o en su defecto haber contado con un numero elevado de vulnerabilidades de público conocimiento que puedan ser explotadas por los atacantes (ciberdelincuentes). Es por ello, que se ha considerado una cantidad máxima prudente de 10 vulnerabilidades presentes en sus diferentes versiones de sistema operativo durante los últimos 12 meses. Entendemos que, si bien pueden existir vulnerabilidades en los productos de seguridad, el hecho de contratar productos de seguridad que expresamente ha sido vulnerados en reiteradas ocasiones de manera sistemática por los ciberdelincuentes, va en contra de los objetivos y la finalidad del presente este proceso, por lo cual este requerimiento resulta indispensable.	
96	20421780472	GTD PERÚ S.A	Consulta	Específico	5.2	c	34	Dice: La herramienta debe ser capaz de realizar backup/restore de la configuración, permitiendo al administrador programar la realización de los backups en períodos diario, semanal y mensual. Consulta: Sirvase confirmar que se aceptarán soluciones que almacenen los archivos de configuración al momento de ejecutar y/o compilar cambios y/o modificaciones de la configuración de los firewalls, asimismo, sirvase confirmar que para mantener la disponibilización de estos archivos puedan almacenarse tanto en los firewalls como en la consola de gestión.		2025-04-16 23:48:07.0	2025-04-16 23:44:06.0	Enviado	No se confirma lo indicado por el postor. Se precisa que, el requerimiento del backup/restore de la configuracion, se refiere al respaldo y restauracion de la configuracion en caso de falla en los equipos, y que este respaldo pueda ser programado en periodos establecidos (diario, semanal y mensual). Los archivos de respaldo deben almacenarse en el equipo o en las en plataformas externas al equipo de seguridad (consola de gestión).	5.2. Equipamiento de Gestión y Seguridad de Internet: C. Solución de Seguridad Next Generation Firewall (NGFW): 2) Funcionalidades requeridas: Se agregará: (…) Asimismo, estos archivos pueden almacenarse tanto en los firewalls o en la consola de gestión.
97	20421780472	GTD PERÚ S.A	Consulta	Específico	5.2	c	35	Dice: Los backups pueden ser generados transferidos vía SFTP, SCP, FTP y localmente. El backup debe tener capacidad de ser cifrado. Consulta: Sirvase confirmar que se aceptarán soluciones que permitan exportar manualmente la configuración de los equipos vis XML desde la misma consola de gestión del Firewall.		2025-04-16 23:48:07.0	2025-04-16 23:45:07.0	Enviado	No se confirma lo indicado por el postor. Se precisa que, los procesos de respaldo (backup) de configuracion deben realizarse enviando los archivos de manera programada (automatica), y no de manera manual.	

98	20421780472	GTD PERÚ S.A	Consulta	Específico	5.2	c	35	Dice: Soporte de rutas estáticas, IPSec Routing, RIP, OSPFv2 y OSPFV3(IPv6), IGMP, PIM SM, PIM DM PIM SSM, BGP, EBGP, Multihop y IPv6 BGP-4. Consulta: Sirvase confirmar que para garantizar la pluralidad de postores el protocolo de ruteo BGP-4 será considerado como opcional.		2025-04-16 23:48:07.0	2025-04-16 23:45:32.0	Enviado	Se aclara al participante que, el protocolo de ruteo IPv6 BGP-4 sera opcional.	5.2. Equipamiento de Gestión y Seguridad de Internet: C. Solución de Seguridad Next Generation Firewall (NGFW): 3) Funcionalidades de red: Se agregará: (…) (opcional)
99	20421780472	GTD PERÚ S.A	Consulta	Específico	5.2	c	35	Dice: Soporte de rutas estáticas, IPSec Routing, RIP, OSPFv2 y OSPFV3(IPv6), IGMP, PIM SM, PIM DM PIM SSM, BGP, EBGP, Multihop y IPv6 BGP-4. Consulta:Sirvase confirmar que para garantizar la pluralidad de postores el protocolo de ruteo BGP Multihop será considerado como opcional.		2025-04-16 23:48:07.0	2025-04-16 23:45:57.0	Enviado	Se aclara al participante que, el protocolo de ruteo EBGP Multihop sera opcional.	5.2. Equipamiento de Gestión y Seguridad de Internet: C. Solución de Seguridad Next Generation Firewall (NGFW): 3) Funcionalidades de red: Se agregará: (…) (opcional)
100	20421780472	GTD PERÚ S.A	Consulta	Específico	5.2	c	35	Dice: Debe soportar redundancia de hasta 10 enlaces ISP (Internet Service Provider) redundantes, sin la necesidad de una licencia adicional o software/hardware de terceros. Consulta: Sirvase confirmar que se aceptarán soluciones que permitan el balanceo de por lo menos 02 enlaces de internet.		2025-04-16 23:48:07.0	2025-04-16 23:46:27.0	Enviado	Se aclara al participante, que el requerimiento de hasta 10 enlaces de ISP se modificara y se consideraran como requerimiento minimo 02 enlaces de ISP.	5.2. Equipamiento de Gestión y Seguridad de Internet: C. Solución de Seguridad Next Generation Firewall (NGFW): 3) Funcionalidades de red: Se suprimira: (…) de hasta 10 Se modificara: (…) como minimo **02**
101	20421780472	GTD PERÚ S.A	Consulta	Específico	5.2	c	36	Dice: Sobre la base de las políticas creadas debe tener capacidad de habilitar diversas acciones tales como: Accept, Drop. Reject, Limit (limitar ancho de banda) y habilitar autenticación de usuario final. Consulta: Sirvase confirmar que las acciones Limit y habilitar autenticación del usuarios final serán considerados como opcionales para garantizar pluralidad de postores.		2025-04-16 23:48:07.0	2025-04-16 23:46:54.0	Enviado	No se confirma lo indicado por el postor Se precisa que la accion de Limit tiene como objetivo limitar el ancho de banda en uso aplicaciones especificas para optimizar el consumo del servicio de Internet, y la autenticacion de usuario final, tiene como objetivo la habilitacion de acceso a recursos internos o de Internet mediante un control de autenticacion en el momento del acceso, para validacion de usuario final. Se requiere las caracteristicas indicadas para una mayor seguridad y control de acceso a la red.	
102	20421780472	GTD PERÚ S.A	Consulta	Específico	5.2	c	36	Dice: El equipo debe permitir la creación de políticas de acceso y de prevención de amenazas, con capacidad de seleccionar campos como: Redes y Grupos de Redes, Host, Zonas, Objetos Dinámicos, Dominios FQDN, Usuarios, Grupos de Usuarios, Clientes Remotos VPN. Servicios y Aplicaciones Web y Comunidad de VPN. Consulta: Sirvase confirmar que se aceptarán soluciones que puedan manejar en una sola política las capacidades de acceso como: redes, grupos de redes, zonas de seguridad, objetos, dominios, usuarios, grupos de usuarios, aplicaciones, servicios (puertos) y la acción. Asimismo, en la misma política poder configurar los perfiles de prevención. Con la finalidad de garantizar la pluralidad de postores, se solicita que la comunidad de VPN pueda ser considerada como opcional como componente de la política de seguridad debido a que existen soluciones en el mercado que tienen un apartado exclusivo para la configuración de la VPN Site-to-Site y VPN Site-to-Client para manatener un orden.		2025-04-16 23:48:07.0	2025-04-16 23:47:15.0	Enviado	No se confirma lo indicado por el postor. Se precisa que las reglas creadas para las politicas de acceso, deben tambien gestionar las politcas a los accesos de VPN de los usuarios remotos, de manera que se tenga una politica unificada para los controles de acceso de todos los usuarios, se encuentren dentro o fuera de la red. Adicionalmente, se precisa que, de acuerdo con la indagacion a traves del estudio de mercado, existe pluralidad de postores y fabricantes que cumplen con dicho requerimiento.	
103	20421780472	GTD PERÚ S.A	Consulta	Específico	5.2	c	36	Dice: El equipo debe permitir la creación de políticas de acceso y de prevención de amenazas, con capacidad de seleccionar campos como: Redes y Grupos de Redes, Host, Zonas, Objetos Dinámicos, Dominios FQDN, Usuarios, Grupos de Usuarios, Clientes Remotos VPN. Servicios y Aplicaciones Web y Comunidad de VPN. Consulta: Sirvase confirmar que por aplicaciones web hace referencia a que la solucion deberá controlar aplicaciones de sitios web conocidos, tales como: facebook, X, instagram, O365, GSuite.		2025-04-16 23:48:07.0	2025-04-16 23:48:00.0	Enviado	Se aclara al participante, que en el termino de "Sevicios y Aplicaciones Web" se refieren a los servicios y aplicaciones web que esten disponibles en los servicios web Internos de la entidad y/o de diversos consumos en aplicaciones terceras en Internet, tales como: facebook, X, instagram, entre otros..	
104	20421780472	GTD PERÚ S.A	Consulta	Específico	5.2	c	36	Dice: Las reglas deben permitir manejo de ancho de banda de distintos protocolos y aplicaciones web, permitiendo la limitación del uso ancho de banda, tanto para carga (upload) y descarga (download) por cada regla. Consulta: Debido a que existen otros fabricantes que cuentan con un orden en la creación de políticas de administración de ancho de banda, sirvase confirmar que se aceptará que esta capacidad pueda ser brindada bajo un menu distinto al de las politicas de seguridad.		2025-04-16 23:54:43.0	2025-04-16 23:48:31.0	Enviado	Se precisa que el requerimiento de "reglas deben permitir manejo de ancho de banda de distintos protocolos y aplicaciones web" podra ser empleando las politcas de control de acceso u otra seccion similar, siempre y cuando realicen las tareas de limitación del uso ancho de banda, tanto para carga (upload) y descarga (download) basado en usuario o grupos de usuarios, para aplicaciones web, tales como Facebook, X, Instragram, Youtube, etc.	
105	20421780472	GTD PERÚ S.A	Consulta	Específico	5.2	c	36	Dice: Debe poder analizar la utilización de las reglas, con niveles de indicador: muy alto. alto, medio. bajo y cero. este último indicador permitirá identificar que dicha regla no ha tenido conexiones (sin uso). El uso también debe poder Identificarse numéricamente en miles. millones, gigas y teras de hits por regla. El contacor de uso de la regla podrá configurase en ventanas de tiempo de dia, semana, mes y total. Consulta: Con la finalidad de garantizar pluralidad de postores, y teniendo en consideración que otros fabricantes cuentan con otras capacidades al momento de evidenciar el uso de reglas, se solicita que se acepten soluciones que puedan realizar lo siguiente: Nuevas aplicaciones vistas en las politicas permisivas, reglas que no esten adoptando aplicaciones, aplicaciones no utilizadas, reglas no utilizadas, marcar reglas que se encuentren incluidas en otras, contador de uso de reglas, primera vez que se uso la regla, ultima vez que se uso la regla, fecha en la cual se creo la regla y se modifico.		2025-04-16 23:54:43.0	2025-04-16 23:49:13.0	Enviado	No se confirma lo indicado por el postor. Se precisa que el objetivo de analizar la utilizacion de la reglas, es principalmente ver a lo largo del tiempo cuales son las reglas que estan en desuso o reglas que tienen mayor o menor uso que otras, y por ende requerian una mayor prioridad o tratamiento que el resto de reglas de acceso. Adicionalmente, se precisa que, de acuerdo con la indagacion a traves del estudio de mercado, existe pluralidad de postores y fabricantes que cumplen con dicho requerimiento.	

106	20421780472	GTD PERÚ S.A	Consulta	Específico	5.2	c	36	Dice: Capacidad de crear reglas de firewall en base fuentes dinámicos externas, los cuales serán basados en fuentes de URL externas (HTTP/HTTPs) que contengan archivos planos (CSV) y JSON. En el caso de archivos planos se debe poder el tipo de dato y los delimitadores. En caso de JSON debe emplear sintaxis JQ. Consulta: Sirvase confirmar que se aceptará que los firewalls a proponer cuenten con la capacidad de configurar listas dinámicas externas sobre las cuales puedan ser consumida direcciones IP, dominios y URLs.		2025-04-16 23:54:43.0	2025-04-16 23:49:33.0	Enviado	Se confirma lo indicado por el postor, se precisa que el requerimiento para un mayor entendimiento de la siguiente manera: Capacidad de crear reglas de firewall en base fuentes dinámicos externas, los cuales serán basados en fuentes de URL externas (HTTP/HTTPs) que contengan archivos planos (CSV) y/o JSON y/o (lista de direcciones IP, Dominios y/o URL). Se suprimira: (…) Las reglas de firewall en base fuentes dinámicos externas deben soportar como mínimo Dirección IP, Rango de Red, IP y mascara de red y dominio FQDN.	5.2. Equipamiento de Gestión y Seguridad de Internet: C. Solución de Seguridad Next Generation Firewall (NGFW): 3)Gestión de politicas, Se suprimira: (…) Las reglas de firewall en base fuentes dinámicos externas deben soportar como mínimo Dirección IP, Rango de Red, IP y mascara de red y dominio FQDN. Se modificara: (…) **y/o JSON y/o (lista de direcciones IP, Dominios y/o URL)**.
107	20421780472	GTD PERÚ S.A	Consulta	Específico	5.2	c	36	Dice: Las reglas de firewall en base fuentes dinámicos externas deben soportar como mínimo Dirección IP. Rango de Red, IP y mascara de red y dominio FQDN. Estas fuentes deberán ser efectivas en reglas de aoceso tanto en origen como destino. Consulta: Sirvase confirmar que se aceptará que los firewalls a proponer cuenten con la capacidad de configurar listas dinámicas externas sobre las cuales puedan ser consumida direcciones IP, dominios y URLs.		2025-04-16 23:54:43.0	2025-04-16 23:49:54.0	Enviado	Se confirma lo indicado por el postor, se precisa que el requerimiento para un mayor entendimiento de la siguiente manera: Capacidad de crear reglas de firewall en base fuentes dinámicos externas, los cuales serán basados en fuentes de URL externas (HTTP/HTTPs) que contengan archivos planos (CSV) y/o JSON y/o (lista de direcciones IP, Dominios y/o URL). Se suprimira: (…) Las reglas de firewall en base fuentes dinámicos externas deben soportar como mínimo Dirección IP, Rango de Red, IP y mascara de red y dominio FQDN.	5.2. Equipamiento de Gestión y Seguridad de Internet: C. Solución de Seguridad Next Generation Firewall (NGFW): 3)Gestión de politicas, Se suprimira: (…) Las reglas de firewall en base fuentes dinámicos externas deben soportar como mínimo Dirección IP, Rango de Red, IP y mascara de red y dominio FQDN. Se modificara: (…) **y/o JSON y/o (lista de direcciones IP, Dominios y/o URL)**.
108	20421780472	GTD PERÚ S.A	Consulta	Específico	5.2	c	36	Dice: En el caso de navegación en internet, debe tener capacidad de crear políticas con acciones de interacción al usuario final, tales como: ¿ Preguntar al usuario si desea continuar o no, y deben indicar una razón para continuar. ¿ Informar al usuario, ellos pueden continuar a la aplicación o cancelar el requerimiento. ¿ Bloquear indicando al usuario final un mensaje de bloque a la aplicación. Consulta: Sobre el punto "Informar al usuario, ellos pueden continuar a la aplicación o cancelar el requerimiento", la solicitud en cuestion hace referencia a la navegación (http, https) y este punto hace referencia a "aplicación", por lo cual, se solicita que el punto quede de la siguiente forma: ¿ Informar al usuario, ellos pueden continuar a la aplicación y/o pagina web o cancelar el requerimiento.		2025-04-16 23:54:43.0	2025-04-16 23:50:17.0	Enviado	Se aclara al participante y se precisa que, sobre las politicas con acciones de interacción al usuario final, sera así: Informar al usuario,ellos pueden continuar a la aplicación y/o pagina web o cancelar el requerimiento.	5.2. Equipamiento de Gestión y Seguridad de Internet: C. Solución de Seguridad Next Generation Firewall (NGFW): 4) Gestión de politicas: Se agregará: (…) y/o página web
109	20421780472	GTD PERÚ S.A	Consulta	Específico	5.2	c	36	Dice: En el caso de navegación en internet, debe tener capacidad de crear políticas con acciones de interacción al usuario final, tales como: ¿ Preguntar al usuario si desea continuar o no, y deben indicar una razón para continuar. ¿ Informar al usuario, ellos pueden continuar a la aplicación o cancelar el requerimiento. ¿ Bloquear indicando al usuario final un mensaje de bloque a la aplicación. Consulta: Sobre el punto "Bloquear indicando al usuario final un mensaje de bloque a la aplicación.", la solicitud en cuestion hace referencia a la navegación (http, https) y este punto hace referencia a "aplicación", por lo cual, se solicita que el punto quede de la siguiente forma: ¿ Bloquear indicando al usuario final un mensaje de bloque a la aplicación y/o página web.		2025-04-16 23:54:43.0	2025-04-16 23:50:36.0	Enviado	Se aclara y precisa al participante que, sobre las politicas con acciones de interacción al usuario final, sera así: Bloquear indicando al usuario final un mensaje de bloqueo a la aplicación y/o página web.	5.2. Equipamiento de Gestión y Seguridad de Internet: C. Solución de Seguridad Next Generation Firewall (NGFW): 4) Gestión de politicas: Se agregará: (…) y/o página web
110	20421780472	GTD PERÚ S.A	Consulta	Específico	5.2	c	37	Dice: Debe tener capacidad de controlar el tipo de contenido para el tráfico entrante y saliente. Consulta: Sirvase confirmar que este punto hace referencia a que la solución a proponer deba tener la capacidad de identificar y bloquear extensiones de archivo, tales como: EXE, MSI, PE, Office, ZIP, 7Z, PDF, entre otros.		2025-04-16 23:54:43.0	2025-04-16 23:50:54.0	Enviado	Se aclara y precisa al participante, que el requerimiento de control de contenido para trafico entrante y saliente, y se encuentra especificado los formatos minimos a ser controlados, tales como: PDF, Ejectutables (EXE, COM, DLL, DRV, SCR, VBX,SYS), Microsoft (Power Point, Excel, Word), archivos comprimidos (ZIP, 7Z, RAR, TAR, GZIP) y Base de Datos (Microft Access, DB y DBF).	
111	20421780472	GTD PERÚ S.A	Consulta	Específico	5.2	c	37	Dice: El control se debe realizar por tipo de dato en tránsito, por lo menos de dos maneras: mediante el tipo de contenido, clasificado analizando el contenido del archivo, y mediante el tipo de archivo, analizando el ID o metadato del archivo. Consulta: Con la finalidad de garantizar la pluralidad de postores, se solicita confirmar se aceptarán soluciones que controlen el transito de los archivos por lo menos por el tipo de extensión.		2025-04-16 23:54:43.0	2025-04-16 23:51:14.0	Enviado	No se confirma lo indicado por el postor. Se precisa que el objetivo es que ciertos tipos de archivos no ingresen y salgan de la entidad sin ser analizados, en ese sentido si solo se analiza la extension y no el tipo de archivo via ID o metadato, los usuarios podrian facilmente reemplazar la extension y burlar este control de seguridad. Adicionalmente, se precisa que, de acuerdo con la indagacion a traves del estudio de mercado, existe pluralidad de postores y fabricantes que cumplen con dicho requerimiento.	
112	20421780472	GTD PERÚ S.A	Consulta	Específico	5.2	c	37	Dice: Los formatos de tipo de archivo a restringir deben ser como mínimo: PDF, Ejecutables (EXE, COM, DLL, DRV, SCR, VBX, SYS), Microsoft (Power Point, Excel, Word), archivos comprimidos (ZIP, 7Z, RAR, TAR, GZIP) y Bases de Datos (Microsoft Access, DB y DBF).		2025-04-16 23:54:43.0	2025-04-16 23:51:49.0	Enviado	El participante no plantea una consulta.	
113	20421780472	GTD PERÚ S.A	Consulta	Específico	5.2	c	37	Dice: El IPS debe contar con mecanismo de detección de amenazas de múltiples métodos: detección por firmas, validación de protocolo, detección anómala y analisis de comportamiento. Consulta: Sirvase confirmar que se aceptarán soluciones que basen la identificación de amenazas basado en heuristica y/o analisis de comportamiento.		2025-04-16 23:54:43.0	2025-04-16 23:52:14.0	Enviado	Se confirma lo indicado por el postor, se precisa que el requerimiento para un mayor entendimiento de la siguiente manera: El IPS debe contar con mecanismo de detección de amenazas de múltiples métodos: detección por firmas, validación de protocolo, detección anómala, heurística y/o analisis de comportamiento.	5.2. Equipamiento de Gestión y Seguridad de Internet: C. Solución de Seguridad Next Generation Firewall (NGFW): 5)Prevención de intrusos – ips: Se agregará: (…) heurística y/o
114	20421780472	GTD PERÚ S.A	Consulta	Específico	5.2	c	37	Dice: EL IPS debe contar con motor de identificación de patrones, que le permita diferenciar entre paquetes inofensivos y paquetes maliciosos, detectando expresiones regulares en los flujos de como un segundo nivel de analisis, para reducir la tasa de falsos positivos		2025-04-16 23:54:43.0	2025-04-16 23:52:38.0	Enviado	El particpante no plantea una consulta.	

115	20421780472	GTD PERÚ S.A	Consulta	Especifico	5.2	c	37	Dice: El IPS debe poder detectar evasiones en la retransmisión de paquetes o el envio de paquetes maliciosos en la retransmisión, proveyendo capacidad de reensamblaje de flujo para conexiones TCP y reordenamiento de paquetes. Consulta: Con la finalidad de garantizar la pluralidad de postores, se solicita confirmar que se aceptarán soluciones que sean capaces de detectar tráfico relacionado con comando y control, metodo por el cual realizan retransmision de paquetes sospechosos.		2025-04-16 23:54:43.0	2025-04-16 23:53:00.0	Enviado	No se confirma lo indicado por el postor. Se precisa que las caracteristicas de "detectar evasiones en la retransmisión de paquetes o el envio de paquetes maliciosos en la retransmisión, proveyendo capacidad de reensamblaje de flujo para conexiones TCP y reordenamiento de paquetes" se refieren a tipo de ataques basado en fragmentacion de paquetes TCP/IP. El metodo de comando y control es otro tipo de ataque, no solicitado en esta caracteristica de la consulta. Adicionalmente, se precisa que, de acuerdo con la indagacion a traves del estudio de mercado, existe pluralidad de postores y fabricantes que cumplen con dicho requerimiento.	
116	20421780472	GTD PERÚ S.A	Consulta	Especifico	5.2	c	37	Dice: Detección y prevención de vulnerabilidades, incluidas herramientas de explotación conocidas y desconocidas, y protección contra CVE específicos. Consulta: Con la finalidad de garantizar la pluralidad de postores, se solicita que la detección y prevención del uso de herramientas de explotación conocidas y desconocidas sea considerado como opcional.		2025-04-16 23:54:43.0	2025-04-16 23:53:18.0	Enviado	No se confirma lo indicado por el postor. Se precisa que una de las funcionalidades basicas del motor IPS es la proteccion sobre vulnerabilidades (CVE) conocidas que deberan ser protegidas en la red y servicios de la entidad para evitar su explotacion por parte de los atacantes. Se requiere esta caracteristica para una mayor seguridad. Adicionalmente, se precisa que, de acuerdo con la indagacion a traves del estudio de mercado, existe pluralidad de postores y fabricantes que cumplen con dicho requerimiento.	
117	20421780472	GTD PERÚ S.A	Consulta	Especifico	5.2	c	38	Dice: Las politicas de protección de IPS deben poder establecerse en base a parámetros tales como: número del CVE. nivel de severidad y nivel de efectividad (confianza). Consulta: Con la finalidad de garantizar la pluralidad de postores, se solicita que "el nivel de efectividad" sea considerado como opcional.		2025-04-16 23:54:43.0	2025-04-16 23:53:41.0	Enviado	Se confirma lo indicado por el postor, se precisa que el requerimiento para un mayor entendimiento de la siguiente manera: Las politicas de protección de IPS deben poder establecerse en base a parámetros tales como: número del CVE y nivel de severidad.	5.2. Equipamiento de Gestión y Seguridad de Internet: C. Solución de Seguridad Next Generation Firewall (NGFW): 5)Prevención de intrusos – ips: Se suprimira: (…) y nivel de efectividad (confianza). Se modificara: (…) número del CVE y nivel de severidad
118	20421780472	GTD PERÚ S.A	Consulta	Especifico	5.2	c	38	Dice: Se requiere que capacidad de detección de 10,000 aplicaciones en la base de datos de control de aplicaciones para la aplicación de politicas. Consulta: Con la finalidad de garantizar la pluralidad de postores, se solicita confirmar que se aceptarán soluciones que cuenten con 5000 aplicaciones como mínimo.		2025-04-16 23:54:43.0	2025-04-16 23:54:01.0	Enviado	Se confirma lo indicado por el postor, se precisa que el requerimiento para un mayor entendimiento de la siguiente manera: Se requiere la capacidad de detección de 5,000 aplicaciones en la base de datos de control de aplicaciones para la aplicación de politicas.	5.2. Equipamiento de Gestión y Seguridad de Internet: C. Solución de Seguridad Next Generation Firewall (NGFW): 7) Control de aplicaciones y url filtering: Se suprimira: (…) 10,000 Se modificara: (…) 5,000
119	20421780472	GTD PERÚ S.A	Consulta	Especifico	5.2	c	39	Dice: Solución debe soportar como mínimo 70 categorías de URL Filtering, que incluya categorías para protección de riesgo informático, tales como: Phishing, SPAM, Botnets, Anonymizer, Artificial Intelligence (AI) Hacking, Inactive Sites y Spyware/ Malicious Sites. Consulta: Sirvase confirmar que en caso la solución a proponer no cuente con uno o más categorias de las indicadas, se podrán realizar categorias personalizadas en las cuales se puedan colocar manualmente las URLs de los sitios más conocidos por cada uno.		2025-04-16 23:54:43.0	2025-04-16 23:54:21.0	Enviado	No se confirma lo indicado por el postor. Se precisa que las categorizaciones es un servicio provisto por el fabricante y de actualizacion automatizada por parte de los NGFW, proceso en el cual no intervienen la entidad o los administradores. Por lo cual la tarea de colocar URLs de manera manual, no solo crea una carga adicionalmente sino que ademas no garantiza que este proceso sea eficiente en terminos de seguridad par la restriccion de acceso a esas categorias especificas.	
120	20421780472	GTD PERÚ S.A	Consulta	Especifico	5.2	c	40	Dice: Deberá realizar análisis de malware y bloquearlos en al menos los siguientes protocolos: Web (HTTP. HTTPS). Mail (SMTP o POP3), SMB y FTP Consulta: Sirvase confirmar que se aceptarán soluciones que sean capaces de bloquear malware en el protocolo HTTPS y/o HTTP2.		2025-04-16 23:54:43.0	2025-04-16 23:54:41.0	Enviado	No se confirma lo indicado por el postor. Se precisa que cuando se requiere el bloqueo de malware en protocolo Web se refiere al protocolo no cifrado HTTP y el cifrado HTTPS, siendo este ultimo el de mayor utilizacion en la actualidad, por lo cual no es opcional que el bloqueo de malware no se logre realizar sobre HTTPS.	
121	20421780472	GTD PERÚ S.A	Consulta	Especifico	5.2	c	40	Dice: Prevenir el uso de criptografia vulnerable en el canal SSH. Consulta: Con la finalidad de garantizar la pluralidad de postores, se solicita confirmar este requerimiento será considerado como opcional.		2025-04-16 23:57:43.0	2025-04-16 23:55:12.0	Enviado	No se confirma lo indicado por el postor. Se precisa que el componente de seguridad NGFW debe evitar el uso de protocolo SSH vulnerable, el cual es comunmente explotado por los ciberdelincuentes. En tal sentido el NGFW tiene por finalidad proteger las comunicaciones e informacion enviada y recibida por la entidad, tal como se describe en los objetivos y finalidad publica.	
122	20421780472	GTD PERÚ S.A	Consulta	Especifico	5.2	c	40	Dice: Prevenir el uso de clientes y servidores SSH vulnerables. Consulta: Sirvase confirmar que este punto hace referencia a que se debe complementar con el módulo de IPS y la solución a proponer deberá detectar intento de explotación de vulnerabilidades a nivel de red.		2025-04-16 23:57:43.0	2025-04-16 23:55:32.0	Enviado	No se confirma lo indicado por el postor. Se precisa que el componente de seguridad NGFW debe evitar el uso de protocolo SSH vulnerable, el cual es comunmente explotado por los ciberdelincuentes. En tal sentido el NGFW tiene por finalidad proteger las comunicaciones e informacion enviada y recibida por la entidad, tal como se describe en los objetivos y finalidad publica.	
123	20421780472	GTD PERÚ S.A	Consulta	Especifico	5.2	c	40	Dice: Debe soportar para la alimentación de IoC (indicadores de Compromiso) desde fuentes extemas, en formato CSV y STIX XML (Structured Threat Information Expression) para la prevención de amenazas. Consulta: Sirvase confirmar que se aceptarán soluciones que sean capaces de ingestar información mediante listas dinamicas externas (EDL)		2025-04-16 23:57:43.0	2025-04-16 23:55:57.0	Enviado	Se confirma lo indicado por el participante, se precisa que el requerimiento para un mayor entendimiento de la siguiente manera: Debe soportar para la alimentación de IoC (Indicadores de Compromiso) desde fuentes extemas, en formato CSV y/o STIX XML (Structured Threat Information Expression) y/o listas dinamicas externas (EDL) para la prevención de amenazas.	5.2. Equipamiento de Gestión y Seguridad de Internet: C. Solución de Seguridad Next Generation Firewall (NGFW): 8) Prevención de amenazas: Se modificará: (…) y/o STIX XML Se agregará: (…) y/o listas dinámicas externas (EDL).
124	20421780472	GTD PERÚ S.A	Consulta	Especifico	5.2	c	40	Dice: Los IoC definidos en las fuentes extemas deberán poder ser como mínimo: URL. Dominio, IP, Rango de IP, Hash (MD5, SHA1, SHA256) y campos de correo (Mail From, To, CC, Subject). Consulta: Sirvase confirmar que se aceptarán soluciones que sean capaces de ingestar información mediante listas dinamicas externas (EDL) y que pueda ingestar como mínimo: IP, dominio y URL.		2025-04-16 23:57:43.0	2025-04-16 23:56:15.0	Enviado	No se confirma lo indicado por el postor. Se precisa que el termino IoC se refiere a los Indicadores de Compromiso, y por lo tanto debe cubrir la gran mayoria de amenazas, entre ellas una de las principales son los Hash de malware mediante MD5 y SHA (SH1 y SH256) para evitar el ingreso de malware a la red de la entidad.	
125	20421780472	GTD PERÚ S.A	Consulta	Especifico	5.2	c	41	Dice: La solución debe proveer prevención en tiempo real de malware desconocido en las descargas web y canal de correo electrónico. Consulta: Con la finalidad de garantizar la pluralidad de postores, se solicita confirmar este requerimiento será considerado como opcional.		2025-04-16 23:57:43.0	2025-04-16 23:56:37.0	Enviado	No se confirma lo indicado por el postor. Se precisa que la proteccion de malware en la descargas web y el canal de correo electronico, es un requerimiento de seguridad minimo elemental para proteger la información y la continuidad operativa de los servicios informaticos de la entidad. Adicionalmente, se precisa que, de acuerdo con la indagacion a traves del estudio de mercado, existe pluralidad de postores y fabricantes que cumplen con dicho requerimiento.	

126	20421780472	GTD PERÚ S.A	Consulta	Específico	5.2	c	41	Dice: La solución deberá poder emular archivos para la identificación de malware que viajan en los protocolos: HTTP, HTTPS, SMTP, IMAP, CIFS, SMBv3, SMBv3 multi-channel y FTP. Consulta: Con la finalidad de garantizar la pluralidad de postores, se solicita la emulacion enc SMBv3 Multi-channel sea considerado como opcional.		2025-04-16 23:57:43.0	2025-04-16 23:57:00.0	Enviado	No se confirma lo indicado por el postor. Se precisa que el protocolo SMBv3 es el protocolo actualmente utilizado en redes que emplean sistemas operativos Windows vigentes, para la compartición de archivos en red (carpetas compartidas) y es un canal de la entidad debe proteger para evitar la proliferacion de malware en dicho servicio. Adicionalmente, se precisa que, de acuerdo con la indagacion a traves del estudio de mercado, existe pluralidad de postores y fabricantes que cumplen con dicho requerimiento.	
127	20421780472	GTD PERÚ S.A	Consulta	Específico	5.2	c	41	Dice: La solución deberá poder emular al menos los siguientes tipos de archivos: Adobe PDF, Microsoft Office (documentos y plantillas), DLL, Java, Flash, Scripts, archivos comprimidos (ZIP, 7Z, RAR, GZ, TGZ, TAR, TAR.GZ y JAR), ejecutables (EXE, COM, LNK, DLL, DRV, SYS, SCR, VBX) y archivos de Macos (APP, DMG, PKG). Consulta: Con la finalidad de garantizar la pluralidad de postores, se solicita confirmar que los tipos de archivo APP de macOS, TGZ, TAR.GZ, COM, DRV, SYS, SCR y VBX serán considerados como opcional.		2025-04-16 23:57:43.0	2025-04-16 23:57:13.0	Enviado	No se confirma lo indicado por el postor. Se precisa que actualmente el malware esta presente en multiplos tipos de archivos, especificamente en archivos que puedan ocultar el malware, tales como archivos comprimidos de diversos formatos y archivos de ejecucion tales como scr o scripts (vbx), en los cuales el atacante anida sus archivos e instrucciones de malware para que estos no sean analizados e ingresen a la red de la entidad, comprometiendo la informacion. Adicionalmente, se precisa que, de acuerdo con la indagacion a traves del estudio de mercado, existe pluralidad de postores y fabricantes que cumplen con dicho requerimiento.	
128	20421780472	GTD PERÚ S.A	Consulta	Específico	5.2	c	41	Dice: Cada archivo emulado en el SandBox debe generar un reporte detallado que incluya información forense sobre la actividad maliciosa originada por el archivo. Este reporte debe mostrar una matriz grafica con las técnicas y tácticas empleadas por el malware sobre la base del framework de ciberseguridad MITRE ATT&CK. Consulta: Con la finalidad de garantizar la pluralidad de postores, se solicita confirmar que la visualizacion de las tecnicas y tacticas de MITRE deberán ser considerados como opcional.		2025-04-16 23:57:43.0	2025-04-16 23:57:38.0	Enviado	No se confirma lo indicado por el postor. Se precisa que actualmente las acciones que el atacante intenta o realiza mediante el empleo del malware, estan definidas en un framework de ciberseguridad con secciones especificas y etapas incrementales que evidencian la actividad que realizo o pudo realizar el ciberdelincuente a traves del malware. Estas etapas y secciones denominadas tecnicas y tacticas de MITRE, las cuales resultan de utlidad a la entidad en el analisis de los ataques que fueron o pudieron ser realizados. Adicionalmente, se precisa que, de acuerdo con la indagacion a traves del estudio de mercado, existe pluralidad de postores y fabricantes que cumplen con dicho requerimiento.	