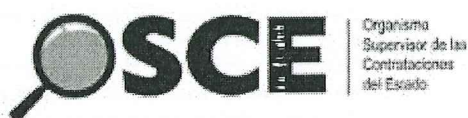


BASES ESTÁNDAR DE CONCURSO PÚBLICO PARA LA CONTRATACIÓN DE SERVICIOS EN GENERAL

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



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

[Handwritten signature]

SIMBOLOGÍA UTILIZADA:

Nº	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	<div>Importante</div> <div>• Abc</div>	Se refiere a consideraciones importantes a tener en cuenta por el comité de selección y por los proveedores.
4	<div>Advertencia</div> <div>• Abc</div>	Se refiere a advertencias a tener en cuenta por el comité de selección y por los proveedores.
5	<div>Importante para la Entidad</div> <div>• Xyz</div>	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:

Nº	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:

- 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.
- 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**



CONCURSO PÚBLICO N°003-2024-INGEMMET/CS

**CONTRATACIÓN DE SERVICIO DE INTERNET, SEGURIDAD
GESTIONADA Y TELEFONIA**

Handwritten signature and initials in blue ink.

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.

Handwritten signature and initials in blue ink.

SECCIÓN GENERAL

DISPOSICIONES COMUNES DEL PROCEDIMIENTO DE SELECCIÓN

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

CAPÍTULO I ETAPAS DEL PROCEDIMIENTO DE SELECCIÓN

1.1. REFERENCIAS

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

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

1.2. CONVOCATORIA

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

1.3. REGISTRO DE PARTICIPANTES

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

Importante

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

1.4. FORMULACIÓN DE CONSULTAS Y OBSERVACIONES A LAS BASES

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

Importante

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

1.5. ABSOLUCIÓN DE CONSULTAS, OBSERVACIONES E INTEGRACIÓN DE BASES

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

Importante

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

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

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

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

Advertencia

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

Importante

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

1.7. FORMA DE PRESENTACIÓN DE OFERTAS

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

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

Importante

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

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

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

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

1.8. PRESENTACIÓN Y APERTURA DE OFERTAS

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

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

Importante

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

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

1.9. EVALUACIÓN DE LAS OFERTAS

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

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

1.10. CALIFICACIÓN DE OFERTAS

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

1.11. SUBSANACIÓN DE LAS OFERTAS

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

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

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

1.12. RECHAZO DE LAS OFERTAS

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

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

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

1.13. OTORGAMIENTO DE LA BUENA PRO

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

1.14. CONSENTIMIENTO DE LA BUENA PRO

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

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

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

Importante

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

CAPÍTULO II SOLUCIÓN DE CONTROVERSIAS DURANTE EL PROCEDIMIENTO DE SELECCIÓN

2.1. RECURSO DE APELACIÓN

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

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

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

Importante

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

2.2. PLAZOS DE INTERPOSICIÓN DEL RECURSO DE APELACIÓN

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

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

CAPÍTULO III DEL CONTRATO

3.1. PERFECCIONAMIENTO DEL CONTRATO

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

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

3.2. GARANTÍAS

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

3.2.1. GARANTÍA DE FIEL CUMPLIMIENTO

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

3.2.2. GARANTÍA DE FIEL CUMPLIMIENTO POR PRESTACIONES ACCESORIAS

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

Importante

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

3.2.3. GARANTÍA POR ADELANTO

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

3.3. REQUISITOS DE LAS GARANTÍAS

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

Importante

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

Advertencia

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

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

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

De otro lado, además de cumplir con el requisito referido a la clasificación de riesgo, a efectos de verificar si la empresa emisora se encuentra autorizada por la SBS para emitir garantías, debe revisarse el portal web de dicha Entidad (<http://www.sbs.gob.pe/sistema-financiero/relacion-de-empresas-que-se-encuentran-autorizadas-a-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 : INSTITUTO GEOLÓGICO, MINERO Y METALÚRGICO –
INGEMMET
RUC N° : 20112919377
Domicilio legal : Av. CANADA Nro 1470 – SAN BORJA
Teléfono: : 6189800 anexo 427
Correo electrónico: : fdelpozo@ingemmet.gob.pe

1.2. OBJETO DE LA CONVOCATORIA

El presente procedimiento de selección tiene por objeto la contratación del Servicio de Internet, Seguridad Gestionada y Telefonía

ITEM	DESCRIPCIÓN	UNIDAD DE MEDIDA
1	SERVICIO DE INTERNET CORPORATIVO PARA LA SEDE PRINCIPAL DEL INGEMMET: <ul style="list-style-type: none">• Optimizador de ancho de banda• AntiDDoS en nube	Servicio
2	SERVICIO DE CIBERSEGURIDAD: <ul style="list-style-type: none">• Solución de AntiDDoS• Solución de Firewall de Aplicaciones Web• Solución de Firewall Perimetral• Solución de Filtro de Contenidos Web• Solución de protección, detección y respuesta automatizada para endpoints (EDR)• Solución de Sistema de Gestión de Información y Eventos de Seguridad Informática (SIEM)• Servicio de Respuesta ante Incidentes• Servicio de Análisis de Vulnerabilidades• Servicio de Inteligencia de Amenazas• Servicio de Mejora Continua • Servicio de Ingeniero Dedicado	Servicio
3	SERVICIO DE TELEFONÍA.	Servicio

1.3. EXPEDIENTE DE CONTRATACIÓN

El expediente de contratación fue aprobado mediante Formato de Aprobación de Expediente de Contratación N° 042-2024 de fecha 04 de octubre del 2024.

1.4. FUENTE DE FINANCIAMIENTO

Recursos Ordinarios

Importante

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

1.5. SISTEMA DE CONTRATACIÓN

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

1.6. DISTRIBUCIÓN DE LA BUENA PRO

De la indagación de mercado se ha podido determinar que para la presente contratación no existe posibilidad de distribuir la Buena Pro, toda vez que la contratación puede ser satisfecha por un solo proveedor.

1.7. ALCANCES DEL REQUERIMIENTO

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

1.8. PLAZO DE PRESTACIÓN DEL SERVICIO

Los servicios materia de la presente convocatoria se prestarán de acuerdo al siguiente detalle:

Para el Ítem N° 01 y 03:

El plazo de treinta y seis (36) meses se iniciará terminada la etapa de la implementación de todas las comunicaciones de la Sede Principal (Av. Canadá 1470, Lima-Perú), para lo cual se suscribirá un Acta de implementación del servicio. Se aclara que el servicio comenzará a ser contabilizado a partir del día siguiente de suscrita el Acta de Conformidad del Servicio.

Para el Ítem N° 02

El plazo de ejecución del servicio será por treinta y seis (36) meses, contabilizados a partir del día siguiente de finalizado los trabajos para la implementación del servicio, para lo cual se firmará el Acta de Inicio del Servicio, el mismo que será suscrito entre un (01) representante propuesto por el Contratista y un (01) representante de la Oficina de Sistemas de Información.

1.9. COSTO DE REPRODUCCIÓN Y ENTREGA DE BASES

Los participantes registrados tienen el derecho de recabar un ejemplar de las bases, para cuyo efecto deben cancelar S/ 4.50 (Cuatro con 50/100 Soles) en la caja de la Entidad, Av. Canadá Nro. 1470 – San Borja.

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° 31953, que aprueba el Presupuesto del Sector Público del año fiscal 2024.
- Ley N° 31954, que aprueba el Equilibrio Financiero del Presupuesto del Sector Público del año fiscal 2024.
- Decreto Supremo N° 082-2019-EF, Texto Único Ordenado de la Ley N° 30225, Ley de Contrataciones del Estado.
- Decreto Supremo N° 344-2018-EF, que aprueba el Reglamento de la Ley de Contrataciones del Estado.
- Directivas y Comunicados emitidos por el Organismo Supervisor de las Contrataciones del Estado – OSCE y demás normas aplicables.
- Decreto Legislativo N° 1071, Ley de Arbitraje, modificado por Decreto Urgencia N° 020-2020.
- Ley N° 27444, Ley del Procedimiento Administrativo General.
- Ley N° 27806, Ley de Transparencia y de Acceso a la Información Pública.
- Directivas, Pronunciamientos y Opiniones del OSCE.
- Demás normas complementarias y conexas con el objeto del procedimiento de selección.

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

CAPÍTULO II DEL PROCEDIMIENTO DE SELECCIÓN

2.1. CALENDARIO DEL PROCEDIMIENTO DE SELECCIÓN

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

Importante

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

2.2. CONTENIDO DE LAS OFERTAS

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

2.2.1. Documentación de presentación obligatoria

2.2.1.1. Documentos para la admisión de la oferta

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

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

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

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

Advertencia

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

- c) Declaración jurada de acuerdo con el literal b) del artículo 52 del Reglamento. (**Anexo N° 2**)

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/>

- d) Declaración jurada de cumplimiento de los Términos de Referencia contenidos en el numeral 3.1 del Capítulo III de la presente sección. (**Anexo N° 3**)
- e) Declaración jurada de plazo de prestación del servicio. (**Anexo N° 4**)⁴
- f) Promesa de consorcio con firmas legalizadas, de ser el caso, en la que se consigne los integrantes, el representante común, el domicilio común y las obligaciones a las que se compromete cada uno de los integrantes del consorcio así como el porcentaje equivalente a dichas obligaciones. (**Anexo N° 5**)
- g) El precio de la oferta en SOLES. Adjuntar obligatoriamente el **Anexo N° 6**.
- El precio total de la oferta y los subtotales que lo componen son expresados con dos (2) decimales.
- h) El postor que se presenten al **ITEM N° 02** (Servicio de Ciberseguridad) deberán presentar el CERTIFICADO O CONSTANCIA de FIRST.
- i) El postor que se presenten al **ITEM N° 02** (Servicio de Ciberseguridad) deberán presentar una Declaración jurada de poseer un centro de Operaciones y Seguridad (SOC) propio.
- j) El postor que se presenten al **ITEM N° 02** (Servicio de Ciberseguridad) deberán presentar un Certificado o constancia del nivel de madurez del Centro de Operaciones y Seguridad (SOC).
- k) El postor que se presenten al **ITEM N° 02** (Servicio de Ciberseguridad) deberán presentar un Certificado o constancia del nivel de madurez del Centro de Operaciones y Seguridad (SOC).
- l) El postor que se presenten al **ITEM N° 02** (Servicio de Ciberseguridad) deberán presentar un Certificado o constancia de ISO/IEC 27001:2013 del Centro de Operaciones y Seguridad (SOC).

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.

2.2.2. Documentación de presentación facultativa:

Ítem N° 03

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

Advertencia

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

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.
- 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 ⁵ (**Anexo N° 12**).
- i) Detalle de los precios unitarios del precio ofertado ⁶.
- j) **Para el Ítem N° 01** Se deberá adjuntar los equipos propuestos podrá estar listados en el sitio web del fabricante en el estado de end-of-life o end-of-sale o end-of-support.
- k) **Para el Ítem N° 01** Se deberá presentar una declaración jurada que se cuenta conexión al Backbone internacional de internet a través de 2 proveedores TIER I como mínimo, ambas serán redundantes, al menos una deberá tener una capacidad mínima de 100Gbps.

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.*

⁵ En tanto se implemente la funcionalidad en el SEACE, de conformidad con la Primera Disposición Complementaria Transitoria del Decreto Supremo N° 234-2022-EF.

⁶ Incluir solo en caso de la contratación bajo el sistema a suma alzada.

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 Haya⁷.
- La Entidad no puede exigir documentación o información adicional a la consignada en el presente numeral para el perfeccionamiento del contrato.

2.4. PERFECCIONAMIENTO DEL CONTRATO

El contrato se perfecciona con la suscripción del documento que lo contiene para dicho efecto el postor ganador de la buena pro, dentro del plazo previsto en el artículo 141 del Reglamento, debe presentar la documentación requerida en el horario establecido en la página web del INGEMMET, a través de la ventanilla virtual del INGEMMET (<https://srvstd.ingemmet.gob.pe/vvirtual/#/login>) o presencialmente mesa de partes del INGEMMET ubicado en la Av. Canadá N° 1470, San Borja, Lima.

Importante

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

2.5. FORMA DE PAGO

La Entidad realizará el pago de la contraprestación pactada a favor del contratista en PAGOS PERIODICOS.

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 Sistemas de Información emitiendo la conformidad de la prestación efectuada.
- Comprobante de pago.
- Entregable mensual del servicio.

Dicha documentación se debe presentar en el horario establecido en la página web del INGEMMET, a través de la ventanilla virtual del INGEMMET (<https://srvstd.ingemmet.gob.pe/vvirtual/#/login>) o presencialmente mesa de partes del INGEMMET ubicado en la Av. Canadá N° 1470, San Borja, Lima.

⁷ 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.

3.1. TERMINOS DE REFERENCIA

Firmado digitalmente por JULCA VELAZCO Lora Osorio PAU 20112812377
Método: Firma de documento
Fecha: 2024/10/13 12:01:42-0500

Firmado digitalmente por GIL MIRANDA
Mauricio Elvandro TAU 20112812377
Método: Firma de documento
Fecha: 2024/10/10 11:03:42-0500

TÉRMINOS DE REFERENCIA

"CONTRATACIÓN DEL SERVICIO DE INTERNET, SEGURIDAD GESTIONADA Y TELEFONÍA"

1. DENOMINACIÓN DE LA CONTRATACIÓN

Contratación del Servicio de Internet Corporativo, Seguridad Gestionada y Transmisión de Voz y Datos para el Instituto Geológico, Minero y Metalúrgico – INGEMMET.

2. FINALIDAD PÚBLICA

La implementación de la contratación del servicio de Internet Corporativo, Seguridad Gestionada y Transmisión de Voz y Datos para el INGEMMET que permitirá a todas las dependencias a nivel institucional, interconectarse a los principales servicios y aplicaciones de TI de manera continua y segura, asimismo garantizará la disponibilidad de la información, para el cumplimiento de las funciones y actividades propias del INGEMMET en beneficio del público usuario y supervisados.

El Instituto Geológico, Minero y Metalúrgico requiere mantener la seguridad informática perimetral para los usuarios del Instituto Geológico, Minero y Metalúrgico, a fin de mitigar ciberataques que atenten contra la continuidad operativa de la entidad, permitiendo así la disponibilidad, integridad y confidencialidad de la información, que es procesada, almacenada y transmitida en la infraestructura tecnológica de la institución.

3. OBJETIVOS DE LA CONTRATACIÓN

El INGEMMET, para soportar sus procesos críticos de negocio, requiere un servicio de Internet Corporativo, Seguridad Gestionada y Transmisión de Voz y Datos que permita realizar adecuadamente las comunicaciones desde la sede principal, en términos de acceso seguro a los sistemas de información, acceso a Internet, comunicaciones de voz y telefonía, así como también un servicio de ciberseguridad que permita proteger adecuadamente la infraestructura, la información y datos del Instituto Geológico, Minero y Metalúrgico.

4. BASE LEGAL

- Ley N° 29956 - Ley que establece el derecho de Portabilidad Numérica en los servicios de telefonía fija.
- Decreto Legislativo N° 1017 - Ley de Contrataciones del Estado, en adelante la Ley.
- Decreto Supremo N° 184-2008-EF - Reglamento de la Ley de Contrataciones del Estado, en adelante el Reglamento.
- Resolución del Consejo Directivo N° 138-2014-CD/OSIPTEL Texto Único Ordenado de las Condiciones de Uso de los Servicios Públicos de Telecomunicaciones, exceptuando los artículos 15° y 16°.

5. CARACTERÍSTICAS Y CONDICIONES DEL SERVICIO A CONTRATAR

Éste se encuentra conformado por los siguientes ITEM:

N°	Descripción	Unidad de medida
----	-------------	------------------

ITEM 01	Servicio de Internet Corporativo para la Sede Principal del INGEMMET <ul style="list-style-type: none">• Optimizador de ancho de banda• AntiDDoS en nube	Servicio
ITEM 02	Servicio de ciberseguridad: <ul style="list-style-type: none">• Solución de AntiDDoS• Solución de Firewall de Aplicaciones Web• Solución de Firewall Perimetral• Solución de Filtro de Contenidos Web• Solución de protección, detección y respuesta automatizada para endpoints (EDR)• Solución de Sistema de Gestión de Información y Eventos de Seguridad Informática (SIEM)• Servicio de Respuesta ante Incidentes• Servicio de Análisis de Vulnerabilidades• Servicio de Inteligencia de Amenazas• Servicio de Mejora Continua• Servicio de Ingeniero Dedicado	Servicio
ITEM 03	Servicio de Telefonía.	Servicio

5.1. SERVICIO DE INTERNET CORPORATIVO PARA LA SEDE PRINCIPAL DEL INGEMMET

La Oficina Principal se ubica en la Avenida Canadá N° 1470, San Borja, Lima - Perú.

6. CONSIDERACIONES GENERALES

6.1. GENERALIDADES DEL SERVICIO DE INTERNET CORPORATIVO (ITEM 01)

1. El backbone del servicio de transmisión de datos para la interconexión de redes y las últimas millas deberá ser de propiedad del contratista del servicio de internet y no rentado a terceros.
2. El backbone del contratista para el servicio de internet de interconexión de redes debe estar implementado con fibra óptica.
3. El contratista del servicio deberá contar con capacidad de 2x100Gbps al NAP Perú.
4. Los nodos del backbone del Internet del contratista del servicio deberán estar interconectados por fibra óptica.
5. El backbone de la red del postor, debe contar con al menos un NODO de nivel CORE (el más alto nivel de la jerarquía de la red, cuya infraestructura desempeña un papel fundamental y debido a su naturaleza crítica, es esencial para mantener la continuidad del servicio y prevenir interrupciones significativas, asegurando así su correcto funcionamiento) el cual deberá estar ubicado dentro de un centro de datos con certificación TIER-3 del Uptime Institute como mínimo en instalaciones construidas y/u operación. Se deberá presentar el mencionado certificado en la etapa de presentación de oferta.
6. El INGEMMET brindará los ambientes adecuados con la infraestructura necesaria (pozo a tierra, UPS, aire acondicionado, energía estabilizada, etc.) para el servicio a ser instalado por el Contratista.
7. Para la realización de trabajos de implementación dentro de las instalaciones de la entidad, se le brindará al contratista todos los accesos necesarios y facilidades, siendo la Entidad responsable de las autorizaciones de ingreso, desocupar los espacios, oficinas, pasillos y demás ambientes donde se realizarán los trabajos de instalación siempre y cuando las coordinaciones sean efectuadas con anticipación

y acorde a lo indicado en el Plan de Trabajo. La Entidad velará por el cumplimiento de dicho Plan de Trabajo para su realización sin contratiempos.

8. El contratista deberá garantizar una disponibilidad del 99.5% de continuidad del servicio.

INTERNET CORPORATIVO

1. Acceso a Internet requerido deberá tener dos circuitos digitales en configuración de activo-pasivo, cada uno con un ancho de banda a 300 Mbps, overbooking 1:1 en cada circuito digital, garantizado al 100% (overbooking considerado hasta el acceso al NAP Perú y la salida internacional).
2. Se requiere una conexión al NAP Perú de mínimo 2 x 100Gbps de capacidad. El cual deberá ser acreditador a través de un documento oficial de NAP Perú.
3. Cada enlace de última milla debe ir a un nodo distinto en la red del contratista, se considerará como Nodo/PoP distinto a un local del Contratista donde se encuentran sus equipos activos que permiten a los clientes el acceso a la red del Contratista para la conexión a los servicios de transmisión/interconexión de datos y/o internet. El INGEMMET solicitará dicha información en la Etapa de Perfeccionamiento del Contrato, se deberá adjuntar un plano o un KMZ en digital, donde se muestre la ruta a seguir por ambos enlaces y el nombre de los POP a los que se conectan. Los enlaces de fibra óptica deben tener recorridos (rutas) distintas (no compartir tramos en común) desde cada PoP/Nodo del Contratista hasta llegar al punto de acceso de la Oficina Principal (Av. Canadá N° 1470, San Borja, Lima, Lima, Perú).
4. Ambos circuitos digitales a Internet deberán funcionar de manera automática; es decir, ante la caída de cualquiera de los circuitos, todo el tráfico pasara por el otro circuito sin intervención manual. El contratista deberá configurar ambos equipos de enrutamiento para este fin. El caso que se requieren de switches o puertos adicionales para el funcionamiento, estos deberán ser provistos por el contratista como parte de su oferta y sin costo para la entidad.
5. El contratista deberá de estar en la capacidad de aumentar el ancho de banda hasta un 30% de la capacidad contratada a solicitud de la entidad.
6. El contratista debe de disponer de equipos y hacer uso para la implementación los cuales deben de soportar protocolos IPV4 e IPV6, la red del contratista debe de soportar IPV4 e IPV6.
7. El contratista debe brindar dos (02) pool de 64 direcciones o (01) pool de 96 direcciones IP Publicas versión 4 de distintos rangos. Se aclara que de las 64 IP's se incluye la IP de red, IP de gateway e IP de broadcast. Se aclara que se puede brindar dichas IPs mediante más de 1 segmento no continuos.
8. El contratista debe brindar pool de 64 direcciones IP Publicas versión 6, se aclara que de las 64 IP's se incluye la IP de red, IP de gateway e IP de broadcast.
9. El contratista deberá de realizar todas las re-configuraciones (adicionales a las ejecutadas al inicio de la instalación) sin costo alguno para el INGEMMET durante todo el periodo del servicio, a solicitud de la entidad. Se aclara que las reconfiguraciones serán según sea requerido por la entidad, el cual será cubierto por el contratista y no implicaría costo alguno para la entidad.
10. El Contratista deberá brindar un portal web donde el personal autorizado del INGEMMET pueda visualizar reportes de tráfico en forma gráfica y hasta para el periodo contratado. Se aclara que el sistema de monitoreo solicitado debe almacenar el historial de tráfico de los enlaces de los últimos doce (12) meses, desde la fecha de emisión del reporte.
11. Para la provisión del servicio, el contratista deberá proponer equipos router, los cuales deberán contar con soporte por parte del fabricante, es decir que los equipos router que implemente el Contratista deben ser de tecnología vigente (no encontrarse en el estado de End of Support y/o End of Service y/o End of Life por parte del fabricante), se aclara que los equipos deben ser nuevos y/o de primer uso.

12. El contratista deberá proveer el acceso total a los servicios de Internet sin restricción de protocolo, puerto o aplicación.
13. Ninguno de los equipos propuestos podrá estar listados en el sitio web del fabricante en el estado de end-of-life o end-of-sale o end-of-support, se deberá adjuntar, para la suscripción de contrato, el enlace público del fabricante que verifique que los modelos propuestos no están listados en ese estado. Se aclara que se aceptará carta de fabricante indicando que los equipos propuestos, al momento de la presentación de la oferta, no se encuentran en el estado de End Of Life o End Of Sale o End of Support.
14. El contratista deberá de etiquetar todos los equipos de comunicación y los medios físicos de conexión que utilizará para brindar el servicio dentro de las instalaciones del INGEMMET. El etiquetado debe ser descripto en un diagrama, el cual permita la identificación de todos los componentes de la implementación.
15. El Contratista deberá brindar el servicio de Servidores DNS para el registro de los dominios del INGEMMET, los cuales deben soportar IPv4 e IPv6.
16. El contratista debe ofrecer el acceso a una página de los DNS, de modo que se pueda visualizar las configuraciones relaciones a la entidad y a cualquier tipo de registro DNS, se aceptará opcionalmente que el contratista brinde una herramienta para autogestionar sus dominios en el DNS del contratista. Se aclara que se aceptará que las modificaciones de los DNS serán atendidas como requerimiento por el contratista, siempre y cuando estas sean atendidas dentro de las 24hrs de solicitadas.
17. El postor deberá contar con conexión al Backbone internacional de internet a través de 2 proveedores TIER I como mínimo, ambas serán redundantes, al menos una deberá tener una capacidad mínima de 100Gbps. Se deberá presentar una declaración jurada como documentación para la suscripción del contrato, que garantice la conexión internacional para ambas rutas, para garantizar la mayor disponibilidad en cuanto al servicio. Adicionalmente se debe presentar una gráfica relacionada indicando los TIER-1.
18. El medio de acceso de la última milla deberá ser de fibra óptica (canalizada y subterránea, o aérea o canalizada, en lo que respecta a planta externa y totalmente canalizada en los interiores del INGEMMET con ruta hasta el Data Center del INGEMMET) un solo canalizado, los cables de fibra óptica deberán ser independientes de los enlaces SIP TRUNK de telefonía. Se aclara que se podrá usar la misma fibra con diversos hilos, siempre y cuando se cumpla con el SLA requerido. Se aclara que el servicio de Telefonía deberá provisionar en un equipo distinto al equipo del servicio de Internet (diferente router).
19. Las averías causadas por terceros, caso fortuito o fuerza mayor, no se deben considerar para el cálculo de la disponibilidad del servicio, siempre y cuando se verifique la veracidad de dicha información.
20. Ante cualquier modificación en el servicio de telecomunicaciones normado por MTC, OSIPTEL, INDECOPI, etc., ésta se deberá aplicar en el contrato con el INGEMMET (mediante adenda u otro que corresponda), en beneficio de la Entidad.
21. Los trabajos de instalación deberán ser coordinados con la Oficina de Sistemas de Información de INGEMMET, de modo que los trabajos se planifiquen en horarios en los que no se afecte el normal funcionamiento de la red de datos a nivel institucional.
22. El Contratista deberá proveer el acceso total a los servicios de Internet sin restricción de protocolo, puerto o aplicación.

OPTIMIZACION DE ANCHO DE BANDA

CARACTERISTICAS MINIMAS

La solución permite auditar, controlar y optimizar el ancho de banda contratado por la entidad, con la capacidad de identificar un mínimo de 5000 firmas de tráfico de capa 7 con la utilización de técnicas de clasificación como DPI que permita cumplir con los siguientes requerimientos como mínimo:

1. La solución debe ser de propósito específico y no una funcionalidad dentro de alguna solución de seguridad o infraestructura IT, como también de ser una solución totalmente integrada y soportada directamente por el mismo fabricante a fin de garantizar un soporte integral.
2. La solución ofertada debe estar licenciada para realizar su labor de monitoreo y gestión de ancho de banda como mínimo de 300 Mbps Full Duplex como capacidad de ancho de banda total.
3. La solución ofertada debe estar en capacidad de soportar un mínimo de 3,000,000 de flujos concurrentes que permita hacer el monitoreo y gestión del ancho de banda.
4. La consola de gestión de la solución debe ser totalmente gráfica 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 específico; estos mecanismos deben permitir filtrar o buscar basado al menos por dirección IP, número de puerto y nombre aplicación.
5. La solución debe trabajar con un modelo de licenciamiento de tipo perpetuo o de forma que garantice que todas las funcionalidades de monitoreo y gestión de tráfico seguirán en funcionamiento aun cuando el soporte de la solución se encuentra expirada al menos por 6 meses a posterior de esa fecha de expiración.
6. 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 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.
7. Las opciones de conexión de red de la solución deben ser flexibles a fin de adaptarse fácilmente a la infraestructura actual y evitar futuras incompatibilidades por crecimientos de la red, por lo tanto, las interfaces con funcionalidad de bypass deben poder soportar simultáneamente interfaces de cobre y de diferentes tipos de fibra como también diferentes tipos de velocidades como son 1G y 10G como mínimo.
8. La solución debe otorgar como mínimo la capacidad para gestionar 02 enlaces físicos de la entidad por medio de 02 bridge o segmentos físicos dispuestos para soportar la conectividad actual de tipo entidad de tipo cobre con velocidad de interface de 1G, pero además debe ofrecer la capacidad de soportar el crecimiento de interfaces de al menos 01 bridge o segmento físico adicional para cualquier crecimiento a futuro y esta expansión deberá soportar los requerimientos de conectividad a los actuales que serían conexión cobre 1G como mínimo.
9. La solución debe permitir la configuración por cada bridge o segmento de bypass de forma independiente, es decir, de forma visual se debe poder seleccionar un bridge/segmento y configurarlo en modo activo o modo bypass independientemente del resto de bridges/segmentos.
10. 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 mínimos los siguientes:

- Aplicación (capa 7)
 - Grupo de aplicaciones
 - Protocolo
 - Puerto
 - Rango de puertos
 - Dirección IP
 - Rango de direcciones IPs
 - Subred
 - VLAN
 - Nombre de host
11. La solución debe permitir la generación de firmas para detectar/reconocer las aplicaciones corporativas, especialmente aquellas que no son estándar o de desarrollo propio.
12. 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 en los enlaces gestionados, permitiendo realizar operaciones matemáticas para el cálculo de las métricas requeridas.
13. La solución debe permitir la gestión 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 del mismo tipo, por lo cual se debe soportar como mínimo hasta 10 niveles de configuración.
14. 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.
15. La consola de la solución debe ser de tipo web que permita el acceso desde los navegadores web convencionales para evitar dependencias en aplicaciones específicas y/u obsoletas que afecta el fácil acceso para los administradores.
16. 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.
17. 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
18. La solución debe 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.
19. 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 la entidad y del espacio disponible en el almacenamiento.
20. La solución debe tener capacidad de realizar capturas de tráfico en forma de sniffer y con la opción de establecer filtros específicos que permitan definir direcciones IP, VLAN, subredes y rango de tiempo para analizar.

21. La capacidad de captura de paquetes del tráfico debe permitir una captura de al menos 12 horas, de tal forma que permita una analítica extendida y se aceptan la inclusión de elementos externos que garanticen esta capacidad de almacenamiento siempre y cuando hagan parte de toda la solución sin costos adicionales hacia la entidad.
22. La solución debe estar en capacidad de identificar el tráfico de un mismo flujo que pueda estar duplicado y pueda afectar la monitorización y la captura de paquetes.
23. La consola de la solución debe permitir capacidades de analítica y monitoreo, como también de gestión del ancho de banda que cumpla 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
 - Creación de cuadros de mandos o dashboards personalizados según las necesidades de la entidad
 - Los cuadros de mandos deben poder crearse interactuando con las múltiples métricas que se han recolectado del tráfico y que vayan en función de la persona que requiere la información
 - El acceso a la información y acciones de configuración debe permitir establecer múltiples roles, al menos 3 que vayan en función con los diferentes niveles de acceso que regularmente se pueden requerir en una entidad, como pueden ser el de administrado, operador o monitoreo y Auditor
 - Capacidad de generación de informes automatizados que se puedan programar y generar automáticamente en formato PDF, imagen (JPG) y CSV, con capacidad de personalización como puede ser el logotipo con el de la entidad.
 - Capacidad de creación de alarmas y notificaciones.
 - Capacidad de interrelacionar alarmas de modo que active una notificación si sucede la combinación de varios eventos que permita determinar mejor una situación y evitar falsos positivos.
 - Notificación de alarmas debe ser posible de emitir en al menos dos tipos de medios de comunicación, siendo uno de ellos el correo electrónico (email) y otro tipo de medio como puede ser mensajería instantánea (ej: WhatsApp, Telegram o similares) que permita la rápida interacción con los funcionarios responsables de la entidad
 - Capacidad de generar múltiples reportes ya sea en formato tabla, series temporales, diagramas, gráficos de barras, gráficos de agregación como por ejemplo tipo "pie" y otros tipos según a la necesidad de la entidad
 - Capacidad en cada reporte o cuadro de mando de profundizar en los datos desde una vista superior a otra vista más específica que permita análisis más detallados.
 - Posibilidad de crear botones de búsqueda personalizados que permita seleccionar múltiples criterios de los posibles filtros o identificadores de tráfico a fin de facilitar la búsqueda de información relevante para la entidad.

ANTIDENEGACION DEL SERVICIO

CARACTERISTICAS MÍNIMAS

1. El contratista debe brindar el servicio de tráfico limpio en la nube local (territorio nacional) desde un Centro de Datos propio o tercerizado, infraestructura crítica del tipo concurrentemente mantenible, certificada con nivel TIER III en Diseño y/o Construcción y/u Operación (por el Uptime Institute), esto con el fin de garantizar la continuidad del servicio.
2. La plataforma de mitigación de ataques DDoS deberá estar en capacidad de detectar ataques volumétricos en los routers de peer del ISP hacia clientes del servicio antiDDoS, clientes de servicio de internet e infraestructura propia del operador. Lo cual garantizará que el proveedor se encuentra en capacidad de evitar que la entidad (Cliente) se convierta en víctima de daño colateral producto de un ataque de DDoS hacia terceros
3. La plataforma deberá incluir la protección contra ataques de denegación de servicio a nivel de aplicación sin estados (stateless) por lo que no deberá tener límite de conexiones ni sesiones concurrentes para el tráfico total (incluyendo tráfico atacante). Es decir, el componente de mitigación no debe estar limitado por el número de sesiones simultáneas que atraviesan el dispositivo, trátese de tráfico legítimo o malicioso
4. El equipamiento deberá estar licenciado de tal manera que pueda mitigar como mínimo un throughput de 1 Gbps de ataque.
5. El equipamiento en la Red del Postor deberá ser de propósito específico, no se aceptarán soluciones basadas en funcionalidades adicionales de equipos como Firewalls, NGFW, UTM, Balanceadores, etc.
6. El fabricante de la solución ofertada deberá encontrarse en el Top 8 Distributed Denial of Service (DDoS) Protection Tools de PeerSpot 2022 o Líder en el Forrester Wave 2021 DDoS Mitigations Solutions lo cual garantiza la madurez y eficiencia de la solución.

CONDICIONES DEL SERVICIO

1. El servicio deberá incluir la gestión de las soluciones ofertadas, para lo cual el Contratista deberá monitorizar, administrar y configurar los componentes que conforman su solución propuesta.
2. Deberá contar con un SOC local (en Perú) y contar con estándares avanzados de procesos, tecnología, personal, gestión y mejora continua en ciberseguridad, lo cual permitirá garantizar una adecuada gestión del servicio de seguridad. Para acreditarlo, el postor deberá presentar un certificado vigente emitido por una entidad reconocida que acredite que el Centro de Operaciones de Seguridad (SOC) ha alcanzado mínimo un nivel de madurez de 4 según el modelo de referencia SOC-CMM (Security Operations Center - Capability Maturity Model).
3. El servicio deberá ser configurado por el contratista y es responsable de las licencias por los treinta y seis (36) meses.
4. El contratista deberá brindar el servicio de monitoreo, control, atención de requerimientos y/o incidentes, supervisión de la solución ofertada será del tipo 24x7x365 desde el SOC durante la vigencia del plazo de ejecución del contrato.
5. El contratista deberá contar con un sólido equipo de trabajo continuamente capacitados que puedan brindar asistencia de soporte para atender incidentes o problemas reportados de una manera eficaz.
6. Gestión de incidentes y problemas, relacionados al software, hardware,

herramientas, funciones de las soluciones ofertadas, de las cuales se contempla los escenarios más relevantes:

- Corrección de errores o fallas.
 - Solución de anomalías de las funciones.
 - Atención y mitigación de eventos de distintas severidades.
 - Resolución de advertencias.
 - Mantenimientos correctivos en sitio y remoto programados.
7. Gestión de solicitudes, de configuraciones a demanda o a recomendación de la entidad.
8. Prevención de indisponibilidad de la plataforma con la asistencia de mantenimientos preventivo que contempla lo físico, lógico y revisión preventiva anual.
- Revisión los componentes lógicos y físicos de la plataforma.
 - Informe de estado.
 - Recomendaciones.
 - Ejecución de trabajos en sitio o remoto.
9. Seguimiento para cierre de incidentes. Se debe realizar el seguimiento de los incidentes para garantizar su atención por parte del personal del contratista y la entidad, de ser el caso. Los medios de apertura, seguimiento y cierre de incidentes serán por correo electrónico o llamada telefónica.

ACUERDOS DE NIVEL DE SERVICIO- SLA

1. El Contratista, ante una avería o falla técnica de los equipos propuestos por el contratista deberá garantizar una disponibilidad del 99.5% de continuidad del servicio, se aclara que la reposición de equipos en caso de que requiera su reemplazo será como máximo 4 horas de confirmada la misma.
2. En caso de pérdida del servicio por avería de planta externa (responsabilidad del contratista), la solución podría tomar hasta 4 horas. En caso la avería de planta externa sea sólo en uno de los enlaces de fibra óptica el tiempo máximo de reparación será de ocho (08) horas, contabilizadas desde la generación del ticket de atención.
3. El servicio deberá estar disponible las veinticuatro (24) horas del día, los siete (07) días de la semana, los 12 meses del año, mientras dure la ejecución del servicio. La disponibilidad del servicio ofrecido deberá de ser de 99.5% mensual, caso contrario el INGEMMET considerara caída del servicio y aplicará las penalidades y sanciones correspondientes, siempre y cuando éstas sean imputables al contratista, este exime a causas ajenas al mismo siempre y cuando se demuestre previa verificación por la entidad.
4. El contratista del servicio solicitado deberá coordinar con el contratista actual, a fin de que el tiempo de interrupción de dichos servicios sea mínimo (desconexión lógica y/o retiro de equipos alquilados). El INGEMMET necesita que los servicios de Internet y telefonía no sean interrumpidos, o que la interrupción sea la mínima posible, contabilizado en unidades de tiempo de minutos solamente (inferior a una hora efectiva) fuera de horario de oficina. Se aclara que se requiere que los servicios de las sedes remotas no se vean afectados o se brinde el soporte necesario con la migración del servicio de Internet y de los equipos propuestos tal que los servicios se mantengan operativos.
5. Toda actividad o provisión de bienes que tenga que ejecutar el contratista del servicio para subsanar una avería será sin costo alguno para el INGEMMET, siempre y cuando no sea responsabilidad de la entidad.

6. La gestión de los equipos que son parte de la solución ofertada será realizada por el contratista.
7. El servicio deberá incluir el costo de todo el licenciamiento y/o suscripción de software que se necesite para la implementación, puesta en marcha y operación de la solución.

INSTALACIÓN, PRUEBAS

1. El contratista deberá ejecutar la instalación de los equipos, materiales, accesorios y todo lo necesario, a fin de dejar completamente habilitado la prestación del servicio a entera satisfacción del INGEMMET.
2. Cualquier trabajo de cableado estructurado (puntos de red), Puertos RJ45 disponibles y habilitados en sus equipos de la red LAN para la conexión con los equipos que implementará El Contratista, el cual debe de usar categoría 6 y certificada, colocando los equipos en un mismo gabinete, y debe considerar todos los patch cords necesarios para la interconexión de sus equipos.
3. El INGEMMET, para la realización de trabajos de implementación dentro de las instalaciones de la entidad, brindará al contratista todos los accesos necesarios, siendo la Entidad responsable de las autorizaciones de ingreso, desocupar los espacios, oficinas, pasillos y demás ambientes donde se realizarán los trabajos de instalación siempre y cuando las coordinaciones sean efectuadas con anticipación y acorde a lo indicado en el Plan de Trabajo. La Entidad velará por el cumplimiento de dicho Plan de Trabajo para su realización sin contratiempos.
4. El contratista y el INGEMMET realizarán de manera conjunta los procedimientos de inspección y pruebas de desempeño del servicio en la sede central antes que el servicio sea aceptado en forma definitiva.

OBLIGACIONES QUE DEBE CUMPLIR EL PROVEEDOR

1. Se aclara que el personal del contratista que realizará la implementación deberá tener seguro SCTR, equipamiento de seguridad (Según Norma G.050 —Seguridad durante la Construcción) y certificado médico para trabajo en altura de ser necesario, esta documentación deberá ser presentada al inicio de la implementación del servicio.
2. El periodo de garantía para TODO el servicio será de treinta y seis (36) meses y se cuenta a partir del día siguiente de la fecha de recepción y aceptación de la implementación.
3. Será de total y exclusiva responsabilidad del contratista contemplar todas las actividades, dispositivos, componentes, accesorios y materiales para la correcta instalación de los elementos necesarios para brindar el servicio.
4. El soporte y licencias de los equipos ofrecidos por el contratista tienen que tener vigencia por el tiempo de operatividad desde la puesta en marcha hasta el final del plazo de ejecución del contrato.

REQUERIMIENTOS DEL CONTRATISTA

Empresa natural o jurídica dedicada a servicios en telecomunicaciones y/o transmisión de voz y datos.

- a) El Postor deberá contar con el servicio de soporte técnico en modalidad telefónica, el alcance será de tráfico local y de larga distancia nacional y líneas móviles que permitan a los usuarios, llamar al postor sin limitación alguna.

En caso de ser propio, se acreditará mediante el contrato con una empresa de telecomunicaciones del servicio ofertado, con una antigüedad por un periodo no

menor a tres (03) años consecutivos, donde se evidencie el alcance de llamadas de tráfico local y de larga distancia nacional, sin restricción de líneas tups y líneas móviles, para la presentación de la oferta.

En caso de ser alquilado, se acreditará mediante el contrato con una empresa que cumpla con tener el servicio en las condiciones requeridas, para la presentación de la oferta.

- b) El Postor deberá contar con una mesa de ayuda en línea o software de administración de soporte de servicios de TI basado en ITIL, cumpliendo de esa manera con el conjunto de conceptos y buenas prácticas usadas para la gestión de servicios de tecnologías de la información, asimismo, el software de gestión del servicio deberá ser CLOUD (servicio en la nube), además evidenciará el uso del software de mesa de ayuda propuesta por un periodo no menor a tres (03) años (podrá ser propio o alquilado).

En caso de ser propio, se acreditará mediante carta del propietario del software donde se evidencie la fecha de inicio de autorización del uso del software de la plataforma ofertada y la renovación anual para acreditar la continuidad del uso del software de mesa de ayuda, para la presentación de la oferta.

En caso de ser alquilado, se acreditará mediante el contrato con una empresa que cumpla con tener el servicio en las condiciones requeridas, para la presentación de la oferta.

- c) La mesa de ayuda en línea o software de administración de soporte de servicios de TI basado en ITIL ofertada por el Postor, y, por ende, cumplir con las buenas prácticas usadas para la gestión de servicios de tecnologías de la información, su inclusión deberá ser por tres (03) años de manera consecutiva (2019, 2020, 2021 o 2020, 2021, 2022 o 2021, 2022, 2023 o 2022, 2023, 2024).

Se acreditará mediante el ID y la fecha de publicación respectiva, para la presentación de la oferta.

- d) La mesa de ayuda en línea o software de administración de soporte de servicios de TI basado en ITIL ofertada por el Postor, deberá facilitar los métodos para migrar datos y servicios de o desde la nube, de forma automática o manualmente por el usuario. Deberá cumplir como mínimo con la opción de las siguientes funcionalidades o servicios disponibles:

- Compatible con Sistemas Operativos: Windows, Linux.
- Escritorio remoto compartido.
- Aplicación móvil para Android y iOS
- Compatible con bases de datos: PostgreSQL, MySQL, MS SQL.
- Informes Personalizables: Exportar como CSV, XLS, PDF.
- Gestión de incidentes, Gestión de SLA.
- Envío automático de tickets.
- Conversión automática de email a ticket.
- Integración con Active Director.
- Importación desde archivos CSV.
- Historial completo de solicitudes.
- Soporte multi sitio.

Se acreditará mediante el link que permita validar los servicios disponibles, para la presentación de la oferta

PERSONAL CLAVE

Se podrá utilizar el mismo personal clave para el ITEM 1 y el ITEM 3.

UN (01) COORDINADOR DE PROYECTO	
Funciones	Será el encargado de llevar la gestión del proyecto y/o la implementación, configuración, mantenimiento soporte y gestión de las soluciones propuestas para el INGEMMET, además coordinará con el personal de la Oficina de Sistemas de Información.
Perfil Profesional	El Coordinador de Proyecto para la provisión del servicio deberá ser un profesional titulado en las carreras de Ingeniería Electrónica y/o Eléctrica y/o Sistemas y/o Telecomunicaciones y/o Ingeniería Informática y/o Computación y sistemas y/o Redes y Comunicaciones y/o Ingeniería de software y/o Ingeniería de Sistemas y Computo.
Capacitación	Certificado PMP y/o Curso y/o Taller y/o Diplomado en Gestión o Gerencia de Proyectos y/o bajo enfoque PMI y/o Diplomatura de Especialización Avanzada en Gerencia de Proyectos y Calidad. En el caso de los cursos y/ Taller y/o diplomado y/o diplomaturas deberá ser con una duración mínima de 32 horas lectivas o académicas.
UN (01) ESPECIALISTA TI: ENCARGADO DE LA INSTALACIÓN Y CONFIGURACIÓN	
Funciones	Encargado de la instalación y puesta en producción de la solución requerida que contempla la migración de la información de los equipos que tiene la Institución.
Perfil Profesional	Profesional Técnico y/o bachiller Titulado en Ing. de Sistemas y/o Electrónico y/o Redes y Comunicaciones y/o Empresarial y de Sistemas y/o Computación y de Sistemas y/o Telecomunicaciones y Redes y/o Estadística e Informática.
Capacitación	Certificación técnica en solución de routers o conectividad o telefonía o en centro de datos
UN (01) ESPECIALISTA HELP DESK	
Funciones	Encargado de la supervisión y correcto flujo de la asistencia técnica de los tickets generados para soporte técnico.
Perfil Profesional	Profesional titulado y/o Bachiller en Ingeniería Electrónica y/o Ingeniería de Telecomunicaciones y/o Ingeniería de Sistemas y/o Ingeniería Mecatrónica y/o Ingeniería Informática y/o Ingeniería de computación.
Capacitación	Deberá contar con certificación de gestión ITIL® 4, con una duración mínima de 30 horas.

ENTREGABLES

PRIMER ENTREGABLE- PLAN DE TRABAJO:

El contratista deberá de presentar un plan de trabajo que contemple la estrategia para cumplir con lo solicitado en los términos de referencia. Este plan deberá ser presentado por el contratista adjudicado con la buena pro como máximo a los diez (10) días calendario de firmado el contrato y deberá de contener lo siguiente puntos:

- a) Topología de la red.
- b) Listado general de equipos a utilizarse en la solución
- c) La distribución de las direcciones IP en la solución.
- d) Cronograma de las actividades.
- e) Esquema de seguridad que contemple las soluciones requeridas y las soluciones pre-existentes en la entidad.
- f) Diagrama referencial de la arquitectura de los enlaces de Internet, donde se precise la conexión del equipamiento a implementar, la interconexión a los backbone internacional de Internet y sus enlaces al NAP, indicando velocidades de interconexión.

SEGUNDO ENTREGABLE- FIN DE LA IMPLEMENTACION:

El contratista deberá entregar al INGEMMET, el informe final del proyecto donde se indique todo lo realizado, configuraciones y deberá presentarse al final de la configuración del servicio. Dicho informe deberá ser firmado por el Coordinador de Proyecto y deberá contener como mínimo lo siguiente:

- a) Descripción de la arquitectura implementada y diagrama de la Topología de la red.
- b) Inventario de los equipos instalados, con su número de serie
- c) Configuración de equipos instalados (parámetros de configuración).
- d) El etiquetado debe ser descrito en un diagrama, el cual permita la identificación de todos los componentes de la implementación.
- e) Información de contactos para el reporte, atención de averías y escalamiento de solicitudes para el cumplimiento de los SLAs (Acuerdo de Niveles de Servicio), el cual debe incluir como mínimo: números de central telefónica y correo electrónico. Se aclara que la información de contactos debe hacer mención o indicar las áreas correspondientes con sus respectivos números telefónicos para su atención.
- f) Check list del etiquetado de los equipos de comunicación.

El informe final del contratista que posteriormente permitirá al INGEMMET emitir la conformidad del servicio.

ENTREGABLE MENSUAL

El contratista deberá entregar un Informe mensual reportando las incidencias y consumos mensuales, estadísticas de uso y otros indicadores de gestión. Este informe deberá ser presentado por el contratista adjudicado con la buena pro como máximo a los diez (10) días calendario de culminado el mes del servicio y debe contener como mínimo la siguiente documentación:

- a) ANCHO DE BANDA: Consumo de ancho de banda
- b) DDOS:
 - Reporte mensual de la actividad de seguridad relacionada a los ataques de

- denegación de servicios detectados y mitigados.
- c) Reporte del consumo del ancho de banda de la WAN en comparación al contratado.

PLAZO DE EJECUCIÓN

IMPLEMENTACIÓN

Para la implementación de la puesta en operación de los servicios requeridos (obras civiles, canalización y/o tendido aéreo del cableado de fibra óptica en planta externa, canalización interna de la fibra óptica, conectorización de los hilos de fibra óptica, instalación de equipos especializados de comunicación propiedad del contratista, así como pruebas de conectividad física y lógica, el tiempo máximo estimado será de sesenta (60) días calendario, a partir del día siguiente de la aceptación del plan de trabajo.

N°	CONCEPTO	PLAZO
1	Plan de trabajo y cronograma de las actividades de la implementación del servicio	Hasta los diez (10) días calendarios contados a partir del día siguiente de la firma del contrato
2	Informe sobre la implementación del servicio	Hasta los sesenta (60) días calendarios contados a partir del día siguiente de la aceptación del plan de trabajo

PRESTACIÓN DEL SERVICIO

Se establece que el plazo contractual de la prestación será treinta y seis (36) meses, se iniciará terminada la etapa de la implementación de todas las comunicaciones de la Sede Principal (Av. Canadá 1470, Lima-Perú), para lo cual se suscribirá un Acta de implementación del servicio. Se aclara que el servicio comenzará a ser contabilizado a partir del día siguiente de suscrita el Acta de Conformidad del Servicio.

N°	CONCEPTO	PLAZO
1	Informe mensual de Operación de servicio contratado	Hasta los siete (07) días calendarios de culminado el servicio de cada mes. Se contabilizará a partir del día siguiente de la firma del Acta de implementación del servicio, durante el periodo de tiempo contratado.

LUGAR DE LA PRESTACIÓN

El servicio se llevará a cabo en las instalaciones del INGEMMET en su Sede Canadá (sito en Av. Canadá N° 1470 – San Borja, Lima-Perú)

FORMA DE PAGO

Se realizará en treinta y seis (36) pagos periódicos mensual, y será efectuada previa Conformidad, con una facturación diferenciada por cada ítem mencionado. El pago del servicio es a todo costo e incluye todos los impuestos de ley. Los costos de la implementación deberán ser considerados dentro de los pagos del servicio mensual. No se realizarán pagos por la implementación.

La empresa contratista deberá emitir factura por un monto fijo mensual durante todo el período del servicio. La Entidad no reconocerá pagos adicionales por consumos realizados fuera de la bolsa contratada. Para efectos del pago de las contraprestaciones ejecutadas por el contratista, la Entidad debe contar con la siguiente documentación:

- Entregable mensual de internet corporativo
- Comprobante de pago.

Dicha documentación se debe presentar mediante los siguientes canales en el horario establecido en la página web del INGEMMET:

- ✓ Mesa de Partes de la Sede Canadá del INGEMMET, ubicada en la Av. Canadá N° 1470 -San Borja- en el horario de 8:00 a 16:30.
- ✓ Ventanilla Virtual a través del siguiente link (<https://www.gob.pe/12519-acceder-a-laventanilla-virtual-del-ingemmet>). En el horario de 00.00 hasta las 23.59 horas

CONFORMIDAD

La conformidad del Servicio será otorgada por la Oficina de Sistemas de Información, la misma que deberá ser otorgada en un plazo máximo de siete (07) días calendarios, de acuerdo con lo indicado en el Artículo 168 del Reglamento de la Ley de Contrataciones del Estado.

PENALIDADES

PENALIDAD POR MORA

Si el contratista no cumple con las actividades encomendadas dentro del plazo estipulado, la Entidad le aplicará una penalidad por cada día de atraso hasta por un monto máximo equivalente al 10% del monto del contrato. La penalidad se aplicará automáticamente y se calculará de acuerdo a la siguiente fórmula:

$$\text{Penalidad diaria} = \frac{0.10 \times \text{Monto}}{F \times \text{Plazo en días}}$$

- Para plazos menores o iguales a 60 días $F=0.40$
- Para plazos mayores a 60 días $F=0.25$

La Entidad tiene derecho para exigir, además de la penalidad, el cumplimiento de la obligación.

OTRAS PENALIDADES

Serán evaluadas durante cada mes de la prestación del servicio y aplicadas según el caso cuando el contratista incurra en falta, se utilizará lo establecido en el siguiente cuadro.

N°	Supuestos de aplicación de penalidad	Forma de calculo
1	Cuando el contratista supera los 7 días para una configuración y/o reconfiguración solicitada por la entidad,	3 % del monto de la facturación mensual del servicio contratado

N°	Supuestos de aplicación de penalidad	Forma de calculo
	se aclara que se refiera a horas de configuración y/o configuración solicitada para la entidad para cambios simples.	
2	Cuando el contratista supere las 12 horas para restablecer la disponibilidad de los routers ante una caída de la misma.	3 % del monto de la facturación mensual del servicio contratado
3	Cuando la no disponibilidad del internet supere las seis (06) horas	5 % del monto de la facturación mensual del servicio contratado

Procedimiento

- Informe a la Oficina de Sistemas de Información, indicando la ocurrencia, desde reportado el incidente.
- La Oficina de Sistemas de Información tendrá el informe del proveedor sobre la incidencia y en base a ello evaluará la responsabilidad.
- Enviar documento a la Unidad de Logística indicando la ocurrencia y el incidente para que sea notificado al proveedor.

PLAZO DE RESPONSABILIDAD DEL CONTRATISTA

La conformidad del servicio por parte del INGEMMET no enerva su derecho a reclamar posteriormente por defectos o vicios ocultos, conforme a lo dispuesto por el artículo 40° de la Ley de Contrataciones del Estado. En tal sentido el plazo de responsabilidad del contratista es no menor de tres (03) años, computado un día después de otorgada la conformidad por parte de la entidad.

6.2. GENERALIDADES DEL SERVICIO DE CIBERSEGURIDAD (ITEM 02)

La administración de los equipos de seguridad en su totalidad será administrada por el proveedor en coordinación con la Oficina de Sistemas de Información de la ENTIDAD. Las licencias y el soporte de fábrica deberá ser parte del servicio por el tiempo que se estipule en el contrato.

El servicio deberá cumplir con las siguientes características mínimas:

a) Solución de Firewall de Aplicaciones Web

El Contratista deberá proveer dos (2) appliance o equipamiento de propósito específico de protección a las aplicaciones web para la Entidad frente a las amenazas externas, realizando detección de amenazas mediante reglas que puedan ser personalizables y/o algoritmos de inteligencia artificial. Deberá contar con alta disponibilidad a nivel de hardware y debe ser de tecnología vigente (No debe encontrarse en "Fin de Vida" (End of Life) o "Fin de Venta" (End of Sale). Asimismo, la solución deberá contar con las siguientes características mínimas:

- La solución deberá proteger un Throughput de 500 Mbps como mínimo
- La solución deberá contar con 4 interfaces GE RJ45 y 4 interfaces SFP como mínimo.
- La solución deberá contar un disco de 400 GB como mínimo
- La solución deberá contar las certificaciones FCC Class A Part 15, RCM, VCCI, CE como mínimo.
- La solución deberá proteger 20 aplicaciones web y/o dominios administrativos como mínimo.
- La solución deberá estar conformada por una solución en hardware que proporcione las funcionalidades WAAP y una consola de gestión, sin necesidad de la instalación de software y/o hardware en algún equipo adicional que no forme parte de la solución.
- La solución deberá proveer la posibilidad de bloquear las transacciones WEB en forma preventiva, antes de que estas lleguen vía red al servidor.
- El servicio deberá de ser capaz de identificar y bloquear ataques a través de una base de datos de firmas de virus y reputación IP, la cual se deberá actualizar automáticamente y de manera periódica.
- Deberá contar con algoritmos para detección de amenazas avanzadas basados en aprendizaje de máquina con Inteligencia Artificial (AI).
- Deberá incluir el servicio de verificación de vulnerabilidades dentro de la misma solución.
- Deberá tener la funcionalidad de antivirus integrada para inspección de tráfico y archivos, sin la necesidad de instalación de otro equipo.
- El servicio deberá permitir crear reglas para filtrar el tráfico web en función de condiciones como la dirección IP, los encabezados y cuerpos HTTP o los URI personalizados.
- El servicio deberá permitir crear reglas que bloqueen ataques comunes como la inyección SQL o el scripting entre sitios.
- El servicio deberá poderse implementar y aprovisionarse automáticamente con plantillas de muestra
- El servicio deberá proporcionar métricas en tiempo real y registra solicitudes sin procesar que incluyen detalles sobre direcciones IP, geolocalización, URI y agentes de usuario.

- El servicio deberá integrarse con servicios de API gestionados.
- El servicio deberá permitir descargar los logs para integrarlos a herramientas de terceros.
- Deberá poder correlacionar eventos o violaciones a las políticas.
- La solución deberá detectar, alertar y opcionalmente bloquear, en tiempo real, cualquier comportamiento malicioso conocido y/o desconocido.
- La solución deberá contar con un conjunto de patrones correspondientes a los ataques conocidos. Esta base de datos de patrones deberá poder actualizarse periódicamente en forma automática y no asistida.
- La solución deberá permitir definir para las reglas y las alarmas, condiciones lógicas en las cuales la alarma o bloqueo no se dispare si no ha ocurrido por lo menos una cantidad de veces definida.
- Se deberá poder implementar en forma nativa controles anti-scraping, permitiendo bloquear intentos reiterados sobre un mismo URL, o parte de un URL.
- Se deberá poder proporcionar protección para todas las vulnerabilidades expresadas en OWASP.
- La solución deberá validar que el contenido y longitud del protocolo http, incluyendo los encabezados, cuerpo y cookies sea correcto. A su vez, deberá poder restringir los métodos http utilizados en una aplicación Web (GET, POST, PUT, etc.).
- La solución deberá permitir tomar acciones y alertar ante violaciones de protocolos inferiores al aplicativo, incluyendo inspección de paquetes IP, TCP, UDP y sus encabezados.
- La solución deberá proteger las aplicaciones Web contra ataques comunes como: SQL Injection, LDAP Injection, OS Commanding, SSI Injection, Remote File Inclusion, Mail Command Injection, XML injection, XPath injection y XQuery injection, Cross Site Scripting (XSS), Cross Site Request Forgery (CSRF), Web Scraping, Forceful Browsing y protección de modificación de campos ocultos.
- La solución deberá soportar la definición de diferentes políticas que podrán asociarse a cada aplicación de forma individual.
- Por cada aplicación protegida, el administrador deberá poder configurar en qué momento se hace solo detección (log) de los ataques recibidos y en qué momento previenen (bloqueo) los ataques.
- Por cada aplicación Web deberá ser posible deshabilitar la prevención de ataques (bloqueo) y dejar habilitado solo la detección (log) de forma granular con el fin de facilitar el troubleshooting por tipos de ataque.
- Ante un bloqueo, dependiendo del modo de operación, la respuesta (página) que se le envía al usuario deberá tener la posibilidad de personalizarse.
- La solución deberá permitir que hosts o clientes confiables puedan ser excluidos de las medidas de protección.
- La solución deberá soportar la identificación de IP origen en caso de que este pase por proxy, interpretando el campo X-forwarded-for del encabezado http.
- Deberá ayudar a separar las amenazas reales de las alertas informativas y los falsos positivos y a centrarse en las amenazas que importantes.
- Los eventos de ataque se deberán agregar y luego se agrupar en incidentes por características comunes. De este modo, poder averiguar rápidamente qué tipos de ataque se producen con frecuencia, las direcciones IP de origen más maliciosas, etc.
- Deberá permitir marcar un incidente como Reconocido o Falso Positivo, y así mostrarse en la columna de Estado del incidente.
- La solución deberá contar con un módulo de exploración de vulnerabilidades del mismo fabricante para ayudar a identificar los 10 defectos principales de OWASP en las aplicaciones web. Destaca las vulnerabilidades que aún están expuestas a los atacantes dada la configuración existente, de modo que pueda ajustar las configuraciones para reforzar la seguridad.

- La solución deberá tener una garantía/soporte del fabricante por 3 años, lo cual incluye actualizaciones de la plataforma.
- Cada componente deberá ser otorgado en calidad de alquiler, formando parte del servicio ofertado.

b) Solución de Firewall Perimetral

El Contratista deberá proveer dos (2) appliance o equipamiento de propósito específico del tipo NGFW configurados en alta disponibilidad (Activo/Standby) a nivel de hardware y debe ser de tecnología vigente (No debe encontrarse en "Fin de Vida" (End of Life) o "Fin de Venta" (End of Sale).

La plataforma de NGFW debe demostrar liderazgo en la industria, para ello debe haber alcanzado el nivel de "Leaders" en el reporte (indicador) de Forrester para Enterprise Firewalls del Q4 de 2022.

Los componentes para los NGFW deberán contar con las siguientes características mínimas:

- Deberá estar licenciado y habilitado en simultaneo las funcionalidades de: Firewall, IPS, Antivirus de red, Filtrado URL, Control de aplicaciones, identificación de usuarios a través de directorio activo, prevención de Bots y Sandboxing en nube.
- La plataforma propuesta deberá permitir utilizar las capacidades de Firewall e IPS en IPv4 e IPv6.
- Protección para protocolos y tráfico anómalos, y deberá tener habilitado mínimamente los siguientes: RIP, BGP, OSPF v2 y v3, IGMP v2 y v3, PIMSM, PIM-DM.
- Deberá ser capaz de operar en los modos Capa 3 (con capacidades completas de Ruteo y NAT), Capa 2, Transparente y Sniffer, de forma simultánea mediante el uso de sus interfaces físicas sin necesidad de tener que hacer uso de contextos o dominios virtuales.
- Deberá soportar redundancia a enlaces. La solución deberá incluir capacidades de SD-WAN durante la vigencia del contrato, permitiendo mejorar la conectividad con las sedes remotas. Se aceptarán componentes adicionales para cumplir el requerimiento.
- Deberá ser capaz de inspeccionar el tráfico cifrado, incluyendo el protocolo TLS 1.3.
- Deberá reconocer por lo menos 2200 aplicaciones diferentes, incluyendo, más no limitando: el tráfico relacionado a peer-to-peer, redes sociales, acceso remoto, actualización de software, protocolos de red, voip, audio, video, proxy, mensajería instantánea, email.

Capacidad

- Deberá tener un rendimiento de NGFW (que soporte en simultaneo: Control de Aplicaciones, Firewall, IPS): 9.5 Gbps mínimo, medido en condiciones de prueba o mixtura empresarial o en transacciones HTTP de 64KB.
- Deberá tener un rendimiento de Threat Prevention o Threat Protection (cuando opera en simultáneo: Control de Aplicaciones, Firewall, IPS, Antivirus/Antimalware/Anti-Bot/Antispyware) de 8.5 Gbps mínimo, medido en condiciones de prueba o mixtura empresarial o en transacciones HTTP de 64KB.
- El equipo deberá soportar como mínimo 7.5 millones de sesiones o conexiones concurrentes y como mínimo 450 mil nuevas sesiones por segundo o conexiones por segundo.

- Deberá contar con fuente de poder redundante con capacidad de cambio en caliente.
- El Firewall deberá soportar como mínimo 15 interfaces 10/100/1000Mbps RJ-45, 6 interfaces y 6 interfaces de 10GbE. No se deberá tomar en cuenta interfaces de gestión.
- Deberá incluir capacidad de trabajar con firewalls virtualizados dentro del mismo equipo, al menos 6 sistemas virtuales.

VPN

- La plataforma deberá tener la capacidad de soportar al menos 1000 conexiones VPN IPSec concurrentes desde dispositivos endpoint y móviles.
- El agente de VPN SSL o VPN IPSEC cliente-a-sitio deberá permitir ser instalado al menos en Windows, Mac OS, Linux y Android.
- El agente de VPN deberá validar la configuración del dispositivo cliente antes de otorgar el acceso a la red. Deberá soportar como mínimo los siguientes criterios de evaluación antes de brindar el acceso a la red: detectar un proceso específico en ejecución, detectar un registro específico, protección activa del antivirus, firewall de host y versión de sistema operativo, así como una combinación de estos criterios.

Identificación de Usuarios

- Se deberá incluir la capacidad de crear políticas basadas en la visibilidad y el control de quién está usando dichas aplicaciones a través de la integración con los servicios de directorio, a través de la autenticación LDAP, Active Directory, E-directory y base de datos local.
- Deberá tener integración con RADIUS para identificar a los usuarios y grupos que permiten las políticas de granularidad/controles basados en usuarios y grupos de usuarios.
- Deberá permitir el control de navegación sin necesidad de instalación de software de cliente, a través del uso portal cautivo.

QoS

- Deberá soportar la creación de políticas de QoS y Traffic Shaping por dirección de origen, dirección de destino, por usuario y grupo.
- Deberá soportar la creación de políticas de calidad de servicio y Traffic Shaping por puerto.
- En QoS deberá permitir la definición de tráfico con ancho de banda garantizado, con máximo ancho de banda y colas de prioridad.

Filtro de Datos

- Deberá permitir realizar la detección y bloqueo de archivos por su extensión.
- Deberá soportar la identificación de archivos comprimidos.
- Deberá soportar la identificación de archivos cifrados.

Prevención de amenazas

- La tecnología adquirida deberá ser parte de la agrupación internacional Cyber Threat Alliance (CTA) para compartir indicadores de compromiso (IoC) con otros fabricantes líderes de ciberseguridad en base al framework de MITRE ATT&CK,

con el fin de mejorar la protección de los clientes a través de la detección de contenido malicioso como: archivos, nombres de dominio, direcciones IP y URI's.

- Las características de IPS y antivirus deberán funcionar de forma permanente, pudiendo utilizarlas de forma indefinida, aunque no exista el derecho a recibir actualizaciones o no exista un contrato de garantía del software con el fabricante.
- Deberá tener los siguientes mecanismos de inspección IPS: Análisis de decodificación de protocolo, análisis para detectar anomalías de protocolo, desfragmentación IP, reensamblado de paquetes TCP y bloqueo de paquetes con formato incorrecto (malformed packets).
- Deberá identificar y bloquear la comunicación con redes de botnet.
- Deberá incluir capacidad de filtro DNS alimentada por un servicio de inteligencia de amenazas de la propia marca.
- Deberá soportar Threat Feeds mediante cualquier de los siguientes métodos: STIX, servicios web, archivos o texto.
- Deberá soportar proteger contra ataques de día cero y malware desconocido a través de un servicio de sandboxing del fabricante.
- Deberá tener habilitado la protección que al hacer una descarga por http/https, deberá soportar modificar archivos (reconstruido durante su análisis) eliminando componentes riesgosos (código, link)

Filtro Web

- Deberá soportar la capacidad de crear políticas basadas en control por URL y categoría de URL.
- Deberá tener capacidad de actualizar la base de datos de URLs y categorías desde el servicio de inteligencia del fabricante.
- Deberá tener la base de datos de URLs en caché en el equipo o en la nube del fabricante, evitando retrasos de comunicación/validación de direcciones URL.
- Deberá tener por lo menos 60 categorías de URL.
- Deberá permitir el bloqueo y continuación (que permita al usuario acceder a un sitio potencialmente bloqueado, informándole en pantalla del bloqueo y permitiendo el uso de un botón Continuar para que el usuario pueda seguir teniendo acceso al sitio).

Garantía

- La solución deberá tener una garantía/soporte del fabricante por 3 años, lo cual incluye actualizaciones de la plataforma.
- Cada componente deberá ser otorgado en calidad de alquiler, formando parte del servicio ofertado.

c) Solución de protección, detección y respuesta automatizada para endpoints (EDR)

La solución propuesta deberá estar licenciado para 825 endpoints por un periodo de 03 años. La solución debe ser de tecnología vigente (No debe encontrarse en "Fin de Vida" (End of Life) o "Fin de Venta" (End of Sale). Esta solución deberá incluir las siguientes características:

Requerimiento del Agente

- La solución propuesta deberá ser compatible mínimo con los siguientes sistemas operativos: Windows (32-bit & 64-bit versiones) XP SP2/SP3, 7, 8, 8.1 y 10

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

Detección de Malware

- La solución deberá incluir la capacidad de compartir inteligencia de amenazas de endpoints con soluciones NGFW, además de generar acciones de respuesta mejoradas en el NGFW u otras plataformas que cuenta con REST API, como suspender o bloquear una dirección IP luego de un ataque de infiltración.
- La solución propuesta deberá poder funcionar en caso el agente no se encuentre conectado a la red empresarial.
- La solución propuesta deberá poder detectar, eliminar y volver a su valor inicial cambios realizados por procesos maliciosos en el registro de las PC.
- La solución propuesta deberá tener la capacidad para realizar la búsqueda de amenazas en las estaciones Windows utilizando indicadores de compromisos (IOC) tales como: Nombre de archivo y hash de archivo, acciones relacionadas a archivos (Creación, Eliminación o Renombrar), acciones relacionadas a los procesos (Terminación de Proceso o Creación de Proceso o Carga de Ejecutable)
- La solución propuesta deberá tener la capacidad de categorizar los eventos detectados en diferentes categorías según la criticidad del evento.
- La solución propuesta deberá incluir capacidades de Threat Hunting, a fin de permitir realizar búsquedas globales en todos los agentes para detectar actividad de malware identificado.
- La solución deberá tener la capacidad de descubrir dispositivos IoT

Prevención de Malware

- La solución propuesta deberá tener la capacidad de prevención de ejecución de archivos maliciosos.
- La solución propuesta deberá incorporar un motor de antivirus de última generación (NGAV) basado en el kernel con capacidad de "Machine Learning".
- La solución propuesta deberá tener capacidad de controlar dispositivos USB y crear excepciones a los dispositivos USB basado en: nombre del dispositivo o vendor o número serial.
- La solución propuesta deberá poder bloquear tráfico malicioso de exfiltración de datos y comunicación hacia C&C (Command & Control)
- La solución propuesta deberá evitar cifrados de disco causado por ransomware y modificación de archivos o registro de los dispositivos.

- La solución propuesta deberá poder ser configurada en modo de monitoreo, donde no se realice ningún bloqueo, pero toda actividad maliciosa sea registrada.
- La solución deberá tener una prevención automatizada en tiempo real del cifrado de ransomware

Post-Infección

- La solución propuesta deberá permitir el aislamiento automático del tráfico de red de un dispositivo donde se ha encontrado una actividad causada por malware.
- La solución propuesta deberá permitir el bloqueo de las actividades realizadas por parte de archivos maliciosos.
- La solución propuesta deberá tener la capacidad de crear excepciones para los falsos positivos.
- La solución propuesta deberá tener la capacidad de recalificar automáticamente la actividad como falso positivo y evitar que ocurran detecciones similares.

Respuesta a Incidentes

- La solución propuesta deberá almacenar meta-data generada por los dispositivos para que la misma sea usada en investigaciones forenses.
- La solución propuesta deberá permitir la integración con plataformas SIEM (Security Information and Event Management) a través de syslog.
- La solución propuesta deberá tener la capacidad de obtener capturas instantáneas de memoria o "dumps" de memoria que permitan la realización de procesos forenses.
- La solución propuesta deberá permitir la integración a través de API donde el mismo tenga la capacidad de entregar información generada en un evento tales como: Dirección IP, nombre de host, usuario, fecha / hora ocurrida, actividad sospechosa, etc.) para permitir la integración vía API REST con otras soluciones de ciberseguridad.
- La solución propuesta deberá permitir el envío de ejecutables para su análisis a un sandbox, con la finalidad de determinar si son maliciosos o inofensivos.
- La solución deberá revertir los cambios realizados por una actividad maliciosa contenida de forma manual o automática.

Control de Vulnerabilidades y Comunicación

- La solución deberá tener la capacidad de remediar las vulnerabilidades encontradas en los dispositivos
- La solución propuesta deberá poder visualizar y entregar información sobre el uso de aplicaciones en red mostrando información como los IP destinos del tráfico generado por la aplicación.
- La solución propuesta deberá permitir utilizar políticas de bloqueo de comunicaciones basadas en el riesgo de acuerdo al código CVE y la calificación o reputación que puede tener una aplicación.
- La solución deberá permitir bloquear la ejecución de aplicaciones a fin de evitar el uso de aplicaciones no deseadas en la organización.

Consola de Administración

- La consola de administración de la solución propuesta deberá permitir la gestión a través de Restful API.
- La solución propuesta deberá poder ser gestionada completamente en nube.
- La consola de administración de la solución propuesta deberá permitir la visualización de salud de los agentes instalados.

- La solución propuesta deberá permitir agregar automáticamente direcciones IP maliciosas detectadas en uno o más firewalls remotos integrados, ya sea a través de API u otro método de integración.
- Se deberá incluir como mínimo 04 horas de asesoramiento del área de servicios profesionales del fabricante. No se aceptará que sea realizado por partners, ni ingenieros comerciales o de soporte.
- Se deberá incluir como mínimo 25 días de monitoreo de eventos realizado por un analista de la solución ofrecida por el mismo fabricante. No se aceptará que sea realizado por partners, ni ingenieros comerciales o de soporte.
- El servicio del fabricante deberá incluir acompañamiento del fabricante para hacer upgrade de versión de software de la consola de la solución ofrecida. No se aceptará que sea realizado por partners, ni ingenieros comerciales o de soporte.

Garantía

- La solución deberá tener una garantía/soporte del fabricante por 3 años, lo cual incluye actualizaciones de la plataforma.
- Cada componente deberá ser otorgado en calidad de alquiler, formando parte del servicio ofertado.
- Para la implementación de la solución EDR se podrá coordinar entre el Contratista y la Entidad para que se puedan desplegar una cantidad de agentes en la etapa de implementación y el resto en la etapa de soporte en caso haya limitantes que impidan un despliegue masivo y rápido desde la consola centralizada y se tenga que realizar la instalación de los agentes de manera manual.

d) Solución de AntiDDoS

El Contratista deberá proveer Un (1) Appliance o Equipamiento de protección ante ataques DDoS, de tipo volumétrico, y de capa de aplicaciones, de propósito específico y debe ser de tecnología vigente (No debe encontrarse en "Fin de Vida" (End of Life) o "Fin de Venta" (End of Sale). Esta solución deberá incluir las siguientes características:

Especificaciones

- Interfaces LAN de cobre GbE con bypass embebido: 4 como mínimo
- Interfaces WAN de cobre GbE con bypass embebido: 4 como mínimo
- Interfaces LAN SFP GbE: 2 como mínimo
- Interfaces WAN SFP GbE: 2 como mínimo
- Disco [GB]: 480 SSD como mínimo
- Throughput [Gbps]: 8 como mínimo
- Tiempo de respuesta para mitigación de ataques DDoS (max) [s]: 1
- Latencia Máxima [us]: 70

Características

- La solución deberá estar basada 100% en hardware para identificar y mitigar ataques DDoS en las capas 3, 4 y 7, no se aceptará soluciones basadas en software
- La detección deberá ser basada en el análisis del comportamiento de los patrones de tráfico de ataques (No dependerá de actualizaciones de firmas digitales)
- El equipo deberá colocarse en línea dentro de la topología de la red y deberá tener una latencia de menos de 70ms
- El equipo deberá detectar y mitigar los ataques de día cero

- La detección y mitigación de ataques deberán ser realizados en un CHIP específico para el procesamiento del tráfico, no se le permitirá el análisis en los procesadores de propósito general
- La solución deberá de realizar a cabo una evaluación continua, cuando se encuentre bajo un ataque, para minimizar los falsos positivos, lo que garantiza que el tráfico real no sufrirá ningún tipo de interrupción
- El dispositivo deberá crear automáticamente los límites para el comportamiento del tráfico de red
- Deberá contar con un modo de aprendizaje para permitir crear perfiles detallados del tráfico de la red
- Deberá contar un modo de prevención, donde los límites de tráfico aprendido se pueden utilizar para mejorar los perfiles de tráfico.
- Deberá tener la capacidad de segmentar los perfiles de seguridad, proporcionando al menos 8 perfiles de seguridad completamente independientes uno del otro.
- Los puertos de cobre deberán tener un mecanismo de derivación incorporado que permitirá que el tráfico continúe cruzando por el equipo en caso de fallo del mismo.
- Deberá tener un período de tiempo configurable para el bloqueo de direcciones IP que se identificaron como la fuente de los ataques de inundación
- Deberá ser capaz de proteger a los segmentos de red IPv6
- Deberá ser capaz de configurar los puertos no estándar para escuchar el protocolo HTTP
- Deberá ser capaz de configurar direcciones IP para el lanzamiento de las contramedidas
- Deberá contar con un ajuste de emergencia para la protección contra ataques comunes
- Deberá soportar una configuración del sistema en alta disponibilidad

Inspección

- El equipo propuesto deberá tener tecnología de inspección de paquetes para el monitoreo del estado para vectores de ataque específicos
- El equipo propuesto deberá tener tecnología de inspección de paquetes para el continuo ajuste de los valores para limitar la velocidad de transferencia
- El equipamiento propuesto deberá contar con una tecnología de inspección de paquetes detallada de cada uno de los paquetes que cruza por el equipo.
- El equipo propuesto deberá tener tecnología de inspección de paquetes por análisis heurístico
- El equipo propuesto deberá tener la tecnología de inspección de paquetes por análisis del comportamiento predictivo
- El equipo propuesto deberá tener la tecnología de Inspección profunda de paquetes
- El equipo propuesto deberá tener la tecnología de procesamiento masivo paralelo para detectar múltiples vectores de ataques simultáneos
- El equipo propuesto deberá tener la tecnología de soporte completo de IPv4 / IPv6 para direcciones IP individuales

Verificación

- El equipo propuesto deberá tener procesos de verificación con la capacidad de realizar filtros dinámicos
- El equipo propuesto deberá tener procesos de verificación activa
- El equipo propuesto deberá tener procesos de verificación con el reconocimiento de anomalías
- El equipo propuesto deberá tener procesos de verificación con el análisis de todos los protocolos válidos

- El equipo propuesto deberá tener procesos de verificación con definición de los límites de tasa de transferencia
- El equipo propuesto deberá tener procesos de verificación para crear listas blancas y listas negras
- El equipo propuesto deberá tener procesos de verificación con reconocimiento del estado de la anomalía
- El equipo propuesto deberá tener procesos de verificación con filtrado de ataques del tipo Stealth
- El equipo propuesto deberá tener procedimientos de verificación para prevenir ataques de suplantación de direcciones locales, cumpliendo con las mejores prácticas actuales (BCP-38)
- El equipo propuesto deberá tener procesos de verificación con rastreo de direcciones origen
- El equipo propuesto deberá tener procesos de verificación de legitimidad para comprobar la dirección IP correspondiente (anti-spoofing)

Prevención

- El equipo propuesto deberá tener mecanismos de prevención contra grandes volúmenes de (inundaciones), que limita el número de conexiones simultáneas y nuevas conexiones por origen
- El equipo propuesto deberá tener mecanismos de prevención contra grandes volúmenes de tráfico (inundaciones), utilizando técnicas para detectar, bloquear, rastrear y reiniciar las conexiones TCP inactivas
- El equipo propuesto deberá tener mecanismos de prevención contra grandes volúmenes de (inundaciones), con la verificación de la legitimidad de la dirección IP
- El equipo propuesto deberá tener mecanismos de prevención contra grandes volúmenes de tráfico (inundaciones), que limite la tasa de paquetes por dirección de origen
- El equipo propuesto deberá tener mecanismos de prevención contra grandes volúmenes de tráfico (inundación), con rastreo de direcciones de origen
- El equipo propuesto deberá tener mecanismos de prevención contra grandes volúmenes de tráfico (inundación) contando con un mecanismo granular de limitación de la tasa de transferencia, teniendo en cuenta las características específicas de cada paquete (SYN, FIN, ACK) por el destino / fuente.
- El equipo propuesto deberá tener mecanismos de prevención contra grandes volúmenes de tráfico (inundaciones) contando con mecanismos de mitigación SYN Cookie, ACK Cookie, Retransmisiones SYN, DNS y retomo de las respuestas de DNS al cliente cuando el bit de truncamiento es igual a 1.

Mitigación de Ataques

- El equipo propuesto deberá tener mecanismos de mitigación de ataques de falsificación de direcciones
- El equipo propuesto deberá tener mecanismos de mitigación de ataques de ataques lento
- El equipo propuesto deberá tener mecanismos de mitigación de ataques de manera direccional. Por lo tanto, un ataque en una dirección no deberá afectar a la otra.
- El equipo propuesto deberá tener mecanismos de mitigación de ataques en la capa 3, contra grandes volúmenes de tráfico (floods)

- El equipo propuesto deberá tener mecanismos de mitigación de ataques en la capa 3 en contra de grandes volúmenes de tráfico (inundación) para prevenir las inundaciones protocolos fragmentados
- El equipo propuesto deberá tener mecanismos de mitigación de ataques en la capa 3 en contra de grandes volúmenes de tráfico (inundación) para evitar inundaciones fuente y destino
- El equipo propuesto deberá tener mecanismos de mitigación de ataques en la capa 3 en contra de grandes volúmenes de tráfico (inundación) para prevenir ataques de suplantación de direcciones locales, cumpliendo con las mejores prácticas actuales (BCP-38)
- El equipo propuesto deberá tener mecanismos de mitigación de ataques en la capa 3 en contra de grandes volúmenes de tráfico (inundación), permitiendo creación de políticas de control en la ubicación geográfica y la inclusión de la reputación de la dirección IP
- El equipo propuesto deberá tener mecanismos de mitigación de ataques en la capa 4 en contra de grandes volúmenes de tráfico (inundación), con la prevención en todos los puertos TCP
- El equipo propuesto deberá tener mecanismos de mitigación de ataques en la capa 4 en contra de grandes volúmenes de tráfico (inundación), con la prevención en todos los puertos UDP
- El equipo propuesto deberá tener mecanismos de mitigación de ataques en la capa 4 en contra de grandes volúmenes de tráfico (inundación), con la prevención de todos los tipos y códigos ICMP
- El equipo propuesto deberá tener mecanismos de mitigación de ataques en la capa 4 en contra de grandes volúmenes de tráfico (inundación), para evitar la gran cantidad de conexiones en la capa 4, tanto de origen y destino
- El equipo propuesto deberá tener mecanismos de mitigación de ataques en la capa 4 en contra de grandes volúmenes de tráfico (inundación), para prevenir ataques SYN, ACK, RST y FIN
- El equipo propuesto deberá tener mecanismos de mitigación de ataques en la capa 4 en contra de grandes volúmenes de tráfico (inundación), para impedir el establecimiento de conexiones excesivas por origen
- El equipo propuesto deberá tener mecanismos de mitigación de ataques en la capa 4 en contra de grandes volúmenes de tráfico (inundación), para prevenir los ataques enviados por redes de ordenadores zombis
- El equipo propuesto deberá tener mecanismos de mitigación de ataques en la capa 4 en contra de grandes volúmenes de tráfico (inundación), para prevenir los ataques utilizando código ICMP
- El equipo propuesto deberá tener mecanismos de mitigación de ataques en la capa 4 en contra de grandes volúmenes de tráfico (inundación), con prevención contra inundaciones que violen el estado de las conexiones TCP
- El equipo propuesto deberá tener mecanismos de mitigación de ataques en la capa 7 en contra de grandes volúmenes de tráfico (inundación), para HTTP URL, HTTP METHOD: GET, HEAD, OPTIONS, TRACE, POST, PUT, DELETE, CONNECT
- El equipo propuesto deberá tener mecanismos de mitigación de ataques en la capa 7 en contra de grandes volúmenes de tráfico (inundación), para Floods de User Agent
- El equipo propuesto deberá tener mecanismos de mitigación de ataques en la capa 7 en contra de grandes volúmenes de tráfico (inundación), para Floods de Referrer
- El equipo propuesto deberá tener mecanismos de mitigación de ataques en la capa 7 en contra de grandes volúmenes de tráfico (inundación), para Floods de Cookie
- El equipo propuesto deberá tener mecanismos de mitigación de ataques en la capa 7 en contra de grandes volúmenes de tráfico (inundación), para Floods de hosts

- El equipo propuesto deberá tener mecanismos de mitigación de ataques en la capa 7 en contra de grandes volúmenes de tráfico (inundación), validando parámetros obligatorios del encabezado HTTP
- El equipo propuesto deberá tener mecanismos de mitigación de ataques en la capa 7 en contra de grandes volúmenes de tráfico (inundación), validando accesos secuenciales de HTTP
- El equipo propuesto deberá tener mecanismos de mitigación de ataques en la capa 7 en contra de grandes volúmenes de tráfico (inundación), validando solicitudes SIP por origen
- El equipo propuesto deberá tener mecanismos de mitigación de ataques en la capa 7 de renegociación SSL
- El equipo propuesto deberá tener mecanismos de análisis de reputación de la dirección IP
- Se deberá tener análisis dinámico de la reputación de la dirección de IP
- Tener las actualizaciones automáticas de bases de datos de reputación de direcciones IP
- DNS Attack Mitigation
- Deberá tener mecanismos avanzados de mitigación de ataques de anomalías en el encabezado de DNS
- Deberá tener mecanismos avanzados de mitigación de ataques de DNS Query-response
- Deberá tener mecanismos avanzados de mitigación de ataques del tipo Flood de Query DNS
- Deberá tener mecanismos avanzados de mitigación de ataques del tipo Query-DNS inesperada
- Deberá tener mecanismos avanzados de mitigación de ataques del tipo DNS-Response no solicitado
- Deberá tener mecanismos avanzados de mitigación de ataques de Cache de DNS response sobre flood
- Deberá tener mecanismos avanzados de mitigación de ataques de Flood de DNS Query por origen dentro del TTL
- El equipo propuesto deberá tener mecanismos de análisis de reputación de dominio
- Management
- Deberá contar con una interface gráfica vía WEB basada en SSL (HTTPS) para la administración del equipo
- Contar con una línea de comandos
- Contar con una administración a través de RESTful API
- Se deberá permitir la creación de rutas estáticas para que pueda configurarse de forma remota desde cualquier punto de la red
- El acceso administrativo deberá tener la opción de estar limitado a equipos específicos
- El equipo deberá ser capaz de enviar los registros de logs a un servidor remoto
- El equipo deberá ser capaz de ser supervisado por SNMP para obtener información sobre el sistema
- El equipo deberá ser capaz de enviar correos electrónicos para las alertas del sistema
- La base de datos de las estadísticas de los ataques de deberá ser accesible a través de SQL
- Deberá ser capaz de autenticar a los usuarios administradores a través de RADIUS
- Deberá ser capaz de crear administradores con acceso total o de sólo lectura

Monitoreo

- Deberá contar con métricas de monitoreo de tráfico por dirección de origen (paquetes por segundo)
- Deberá contar con métricas de monitoreo de tráfico por TCP SYN (paquetes por segundo)
- Deberá contar con métricas de monitoreo de tráfico por conexiones establecidas (paquetes por segundo)
- Deberá contar con métricas de monitoreo de tráfico por TCP SYN por origen (paquetes por segundo)
- Deberá contar con métricas de monitoreo de tráfico por cantidad de conexiones por segundo
- Deberá contar con métricas de monitoreo de tráfico por conexiones concurrentes (por destino)
- Deberá contar con métricas de monitoreo de tráfico por puerto TCP o UDP (paquetes por segundo)
- Deberá contar con métricas de monitoreo de tráfico por paquetes fragmentados por segundo
- Deberá contar con métricas de monitoreo de tráfico por cantidad de accesos a URL (por segundo)
- Deberá contar con métricas de monitoreo de tráfico por el mismo user-agent, Cookie o Host por segundo
- Deberá contar con métricas de monitoreo de tráfico por verificación de anti-spoofing
- Deberá contar con métricas de monitoreo de tráfico de URL asociadas

Reportes

- Deberá contar con reportes de estadísticas por puertos (Paquetes, Bits)
- Deberá contar con reportes de estadísticas de los recursos protegidos (Paquetes, Bits)
- Deberá contar con reportes de estadísticas del número total de paquetes descartados
- Deberá contar con reportes de estadísticas de paquetes descartados por inundaciones (Total, capa 3, capa4 y capa 7)
- Deberá contar con reportes de estadísticas de paquetes descartados en la capa 7 (HTTP y DNS)
- Deberá contar con reportes de estadísticas de paquetes descartados por listas de control de acceso (Total, capa 3, capa4 y capa 7)
- Deberá contar con reportes de estadísticas de paquetes descartados por anomalías (Total, capa 3, capa4 y capa 7)
- Deberá contar con reportes de estadísticas de capa 3 (origen más activo, destino más activo, contabilidad de orígenes únicas, paquetes fragmentados, direcciones bloqueadas y por protocolos)
- Deberá contar con reportes de estadísticas de paquetes descartados de ataques de HASH
- Deberá contar con reportes de estadísticas de la capa 4 (paquetes SYN, SYN por origen, SYN por destino, conexiones por origen, conexiones por destino, conexiones establecidas por destino, nuevas conexiones, puertos TCP, UDP, tipos y códigos ICMP)
- Deberá contar con reportes de estadísticas de la capa 7 (HTTP: Métodos, URLs, Hosts, Referers, Cookies y User Agents)
- Deberá contar con reportes de estadísticas de la capa 7 (DNS: Consultas, Consultar por Origen, Orígenes sospechosos, Contar consultas, Contar por tipo de consultas MX, Consultas totales, Consultas de tipo transferencia de Zona, Consultas Fragmentadas, Respuestas no solicitadas, Consultas no solicitadas,

Descartes LQ, Descartes TTL, Descartes por cache, Descartes por IP Forjados, DNS Rcodes)

- Deberá contar con un monitoreo gráfico que muestra las estadísticas del rendimiento para cada uno de los puertos de los equipos en paquetes y bits por segundo
- Deberá contar con un monitoreo gráfico que muestra las estadísticas del rendimiento de todos los paquetes descartados por inundaciones, ACL, anomalías y ataques tabla hash.
- Los gráficos de monitoreo de paquetes descartados se deberán mostrar al menos en la capa 3, capa 4 y capa 7.

Garantía

- La solución deberá tener una garantía/soporte del fabricante por 3 años, lo cual incluye actualizaciones de la plataforma.
- Cada componente deberá ser otorgado en calidad de alquiler, formando parte del servicio ofertado.

e) Solución de Filtro de Contenidos Web

El Contratista deberá proveer dos (2) appliance o equipamiento de propósito específico configurados en alta disponibilidad (Activo/Standby) a nivel de hardware y debe ser de tecnología vigente (No debe encontrarse en "Fin de Vida" (End of Life) o "Fin de Venta" (End of Sale). Esta solución deberá incluir las siguientes características:

Especificaciones

- Capacidad de Licencia: Hasta 800 usuarios
- Memoria: 16 GB
- Cantidad de Disco: 2
- Capacidad de Almacenamiento: 4 TB
- Doble fuente de poder
- Interfaces 1Gbps RJ45: 4

Características

- La solución deberá consistir en una plataforma de protección para los usuarios en Internet, basada en un dispositivo con funcionalidades de Proxy explícito, así como consola de gestión y monitoreo.
- La plataforma deberá estar optimizada para análisis de contenido de aplicaciones en capa 7.
- Todo el equipo proporcionado deberá ser adecuado para montaje en rack de 19", incluyendo un rail kit (si sea necesario) y los cables de alimentación.
- La gestión del equipo deberá ser compatible a través de la interfaz de administración Web en el mismo dispositivo de protección de la red.
- Los dispositivos de protección de red deberán soportar agregación de enlaces 802.3ad y LACP.
- Los dispositivos de protección de red deberán soportar enrutamiento estático.
- Los dispositivos de protección de red deberán soportar ECMP.
- Los dispositivos de protección de red deberán soportar DHCP Relay.
- Los dispositivos de protección de red deberán soportar DHCP Server.
- Deberá ser compatible con NAT dinámica (varios-a-1).
- Deberá ser compatible con NAT dinámica (muchos-a-muchos).
- Deberá ser compatible con NAT Origen.

- Deberá permitir el monitoreo por SNMP de fallas de hardware, uso de recursos, estado del clúster, ataques y estadísticas de uso de las interfaces de red.
- Enviar logs a sistemas de gestión externos simultáneamente.
- Deberá tener la opción de enviar logs a los sistemas de control externo a través de TCP y SSL.
- Deberá implementar la optimización del tráfico entre dos dispositivos.
- Deberá soportar trabajar en modo transparente, en modo proxy explícito y en modo WCCP
- Deberá soportar la configuración de alta disponibilidad activo / pasivo
- Deberá soportar la configuración de alta disponibilidad activo / activo con configuración de configuración
- Deberá permitir la integración con soluciones de la misma marca para logging y reporting, así como para detección de amenazas persistentes

Políticas

- La política de firewall deberá especificar las condiciones de IP origen, destino y puerto para hacer caché
- Se deberá poder especificar interfaz de origen e interfaz de destino
- Se deberá poder especificar usuario o IP de origen
- Se deberá poder especificar la aplicación utilizada por el usuario
- Se deberá poder especificar el destino IP del tráfico
- Para cada regla se deberá poder especificar si se hará web caché
- Para cada regla se deberá poder especificar los controles de seguridad a utilizar
- Mínimamente se deberá soportar Antivirus, Filtro de categorías web, Filtro de categorías DNS, Filtro de aplicaciones, IPS, DLP y Análisis de contenido
- Se deberá permitir generar log del tráfico y de la transacción HTTP

Control de Aplicaciones

- Los dispositivos de protección de red deberán tener la capacidad de reconocer las aplicaciones, independientemente del puerto y protocolo.
- Deberá ser posible liberar y bloquear aplicaciones sin necesidad de abrir o cerrar puertos y protocolos.
- Deberá reconocer al menos 1.700 aplicaciones diferentes, incluyendo, pero no limitado a: El tráfico relacionado peer-to-peer, redes sociales, acceso remoto, actualización de software, protocolos de red, VoIP, audio, vídeo, Proxy, mensajería instantánea, compartición de archivos, correo electrónico.
- Deberá reconocer al menos las siguientes aplicaciones: BitTorrent, Gnutella, skype, facebook, linked-in, twitter, citrix, logmein, teamviewer, ms-rdp, vnc, gmail, youtube, http-proxy, http-tunnel, facebook chat, gmail chat, whatsapp, 4shared, dropbox, google drive, skydrive, db2, mysql, oracle, active directory, kerberos, ldap, radius, itunes, dhcp, ftp, dns, wins, msrpc, ntp, snmp, rpc over http, gotomeeting, webex, evernote, google-docs.
- Deberá inspeccionar el payload del paquete de datos con el fin de detectar las firmas de las aplicaciones conocidas por el fabricante independiente de puerto y protocolo.
- Deberá detectar aplicaciones a través del análisis del comportamiento del tráfico observado, incluyendo, pero no limitado a las aplicaciones de VoIP que utilizan cifrado propietario y BitTorrent.
- Para tráfico cifrado SSL, deberá poder descifrarlo a fin de posibilitar la lectura de payload para permitir la identificación de firmas de la aplicación conocidas por el fabricante.
- Deberá hacer decodificación de protocolos con el fin de detectar aplicaciones encapsuladas dentro del protocolo y validar que el tráfico corresponde a la

especificación del protocolo, incluyendo, pero no limitado a Yahoo Instant Messenger utilizando HTTP. La decodificación de protocolo también deberá identificar las características específicas dentro de una aplicación, incluyendo, pero no limitado al intercambio de ficheros dentro de Webex.

- Actualización de la base de firmas de la aplicación de forma automática.
- Los dispositivos de protección de red deberán tener la capacidad de identificar al usuario de la red con la integración de Microsoft Active Directory sin necesidad de instalación del agente en el controlador de dominio, o en estaciones de trabajo de usuario.
- Deberá ser posible añadir múltiples reglas de control de aplicaciones, es decir, no deberá limitar habilitar el control de aplicaciones de control solamente en algunas reglas.
- Deberá ser compatible con múltiples métodos de identificación y clasificación de las aplicaciones, al menos verificar firmas y protocolos de decodificación.
- Para mantener la seguridad de red eficiente deberá soportar el control de las aplicaciones desconocidas y no sólo en aplicaciones conocidas.
- Permitir la creación de forma nativa de firmas personalizadas para el reconocimiento de aplicaciones propietarias en su propia interfaz gráfica, sin la necesidad de la acción del fabricante.
- La creación de firmas personalizadas deberá permitir el uso de expresiones regulares, el contexto (sesiones o transacciones), utilizando la posición en el payload de paquetes TCP y UDP.
- El fabricante deberá permitir solicitar la inclusión de aplicaciones en su base de datos.
- Deberá alertar al usuario cuando sea bloqueada una aplicación.
- Deberá permitir la diferenciación de tráfico Peer2Peer (Bittorrent, eMule, etc) permitiendo granularidad de control/reglas para el mismo.
- Deberá permitir la diferenciación de tráfico de mensajería instantánea (AIM, Hangouts, Facebook Chat, etc.) permitiendo granularidad de control/reglas para el mismo.
- Deberá permitir la diferenciación y manejo de las aplicaciones de chat; por ejemplo permitir a Hangouts el chat pero impedir la llamada de video.
- Deberá permitir la diferenciación de aplicaciones Proxies (psiphon, Freerate, etc.) permitiendo granularidad de control/reglas para el mismo.
- Deberá ser posible la creación de grupos dinámicos de aplicaciones, basado en las características de las mismas, tales como: Tecnología utilizada en las aplicaciones (Client-Server, Browse Based, Network Protocol, etc).
- Deberá ser posible crear grupos dinámicos de aplicaciones basados en características de las mismas, tales como: Nivel de riesgo de la aplicación.
- Deberá ser posible crear grupos estáticos de aplicaciones basadas en características de las mismas, tales como: Categoría de Aplicación.
- Deberá ser posible configurar Application Override seleccionando las aplicaciones individualmente.

Prevención de Amenazas

- Para proteger el entorno contra los ataques, deberán tener módulo IPS y antivirus integrado en el propio equipo.
- Deberá incluir firmas de prevención de intrusiones y el bloqueo de archivos maliciosos.
- Las firmas deberán ser capaces de ser activadas o desactivadas, o activadas sólo en el modo de monitoreo.
- Deberá ser posible crear políticas para usuarios, grupos de usuarios, IP, redes o zonas de seguridad.

- Excepciones por IP de origen o destino deberán ser posibles en las reglas o en cada una de las firmas.
- Deberá soportar granularidad en las políticas de IPS y Antivirus, permitiendo la creación de diferentes políticas por zona de seguridad, dirección de origen, dirección de destino, servicio y la combinación de todos estos elementos.
- Deber permitir el bloqueo de vulnerabilidades.
- Deberá permitir el bloqueo de exploits conocidos.
- Deberá incluir la protección contra ataques de denegación de servicio.
- Detectar y bloquear los escaneos de puertos de origen.
- Bloquear ataques realizados por gusanos (worms) conocidos.
- Contar con firmas para bloquear ataques de desbordamiento de memoria intermedia (buffer overflow).
- Deberá poder crear firmas personalizadas en la interfaz gráfica del producto.
- Deberá permitir utilizar operadores de negación en la creación de firmas personalizadas de IPS o anti-spyware, permitiendo la creación de excepciones con granularidad en la configuración.
- Permitir bloqueo de virus y software espía en por lo menos los siguientes protocolos: HTTP, FTP.
- Soportar el bloqueo de archivos por tipo.
- Identificar y bloquear la comunicación con redes de bots.
- Registrar en la consola de supervisión la siguiente información sobre amenazas concretas: El nombre de la firma o el ataque, la aplicación, el usuario, el origen y destino de las comunicaciones, además de las medidas adoptadas por el dispositivo.
- Deberá ser compatible con la captura de paquetes (PCAP), mediante la firma de IPS o control de aplicación.
- Deberá permitir la captura de paquetes por tipo de firma IPS y definir el número de paquetes capturados o permitir la captura del paquete que dio lugar a la alerta, así como su contexto, facilitando el análisis forense y la identificación de falsos positivos.
- Deberá tener la función de protección a través de la resolución de direcciones DNS, la identificación de nombres de resolución de las solicitudes a los dominios maliciosos de botnets conocidos.
- Deberá incluir protección contra virus en contenido HTML y Javascript, software espía (spyware) y gusanos (worms).
- Deberá permitir la configuración de diferentes políticas de control de amenazas y ataques basados en políticas de firewall considerando usuarios, grupos de usuarios, origen, destino, zonas de seguridad, etc., es decir, cada política de firewall puede tener una configuración diferente de IPS basada en usuario, grupos de usuarios, origen, destino, zonas de seguridad.
- Proporcionan protección contra ataques de día cero a través de una estrecha integración con Sandbox (en las instalaciones y en la nube).

Filtro URL

- Deberá permitir especificar la política por tiempo, es decir, la definición de reglas para un tiempo o período determinado (día, mes, año, día de la semana y hora).
- Deberá ser posible crear políticas para usuarios, IPs, redes, o zonas de seguridad.
- Deberá tener la capacidad de crear políticas basadas en la visibilidad y el control de quién está utilizando las URL esto mediante la integración con los servicios de directorio activo y la base de datos local.
- Deberá soportar la capacidad de crear políticas basadas en control por URL y categoría de URL.
- Tener por lo menos 60 categorías de URL.

- Deberá tener la funcionalidad de exclusión de URLs por categoría.
- Permitir página de bloqueo personalizada.
- Permitir bloqueo y continuación (que permita al usuario acceder a un sitio potencialmente bloqueado, informándole en pantalla del bloqueo y permitiendo el uso de un botón Continuar para que el usuario pueda seguir teniendo acceso al sitio).
- Además del Explicit Web Proxy, soportar proxy web transparente.

Identidad de Usuarios

- Se deberá incluir la capacidad de crear políticas basadas en la visibilidad y el control de quién está usando dichas aplicaciones a través de la integración con los servicios de directorio, a través de la autenticación LDAP, Directorio Activo, E-directorio y base de datos local.
- Deberá soportar hacer caching de las consultas de grupos de LDAP para hacer más eficiente la búsqueda en el directorio.
- Deberá tener integración con Microsoft Active Directory para identificar a los usuarios y grupos, permitiendo granularidad a las políticas / controles basados en usuarios y grupos de usuarios.
- Deberá tener integración con RADIUS para identificar a los usuarios y grupos que permiten las políticas de granularidad / controles basados en usuarios y grupos de usuarios.
- Deberá tener la integración LDAP para la identificación de los usuarios y grupos que permiten granularidad en las políticas/controles basados en usuarios y grupos de usuarios.
- Deberá permitir el control sin necesidad de instalación de software de cliente, el equipo que solicita salida a Internet, antes de iniciar la navegación, entre a un portal de autenticación residente en el equipo de seguridad (portal cautivo).
- Deberá de implementar la creación de grupos de usuarios en el firewall, basada atributos de LDAP / AD.
- Permitir la integración con tokens para la autenticación de usuarios, incluyendo, pero no limitado a, acceso a Internet y gestión de la plataforma.

QoS

- Con el fin de controlar el tráfico y aplicaciones cuyo consumo puede ser excesivo (como YouTube, Ustream, etc.) y que tienen un alto consumo de ancho de banda, se requiere de la solución que, además de permitir o denegar dichas solicitudes, deberá tener la capacidad de controlar el ancho de banda máximo cuando son solicitados por los diferentes usuarios o aplicaciones, tanto de audio como de video streaming.
- Soportar la creación de políticas de QoS y Traffic Shaping por dirección de origen.
- Soportar la creación de políticas de QoS y Traffic Shaping por dirección de destino.
- Soportar la creación de políticas de QoS y Traffic Shaping por usuario y grupo.
- Soportar la creación de políticas de QoS y Traffic Shaping para aplicaciones incluyendo, pero no limitado a Skype, BitTorrent y YouTube.
- Soportar la creación de políticas de calidad de servicio y Traffic Shaping por puerto.
- En QoS deberá permitir la definición de tráfico con ancho de banda garantizado.
- En QoS deberá permitir la definición de tráfico con máximo ancho de banda.
- En QoS deberá permitir la definición de colas de prioridad.
- Soportar la priorización de protocolo en tiempo real de voz (VoIP) como H.323, SIP, SCCP, MGCP y aplicaciones como Skype.

VPN

- Soporte VPN de sitio-a-sitio y cliente-a-sitio.
- Soportar VPN IPsec.
- Soportar VPN SSL.
- La VPN IPsec deberá ser compatible con 3DES, AES128, AES192, AES256.
- La VPN IPsec deberá ser compatible con la autenticación SHA-1, SHA-256, SHA-384, SHA-512.
- La VPN IPsec deberá ser compatible con Diffie-Hellman Grupo 1, 2, 5, 14, 15, 16, 17, 18, 19, 20, 21, 27, 28, 29, 30.
- La VPN IPsec deberá ser compatible con Internet Key Exchange (IKEv1 y v2).
- La VPN IPsec deberá ser compatible con la autenticación a través de certificados IKE PKI.
- La VPN SSL deberá soportar que el usuario pueda realizar la conexión a través de cliente instalado en el sistema operativo de su máquina o a través de la interfaz web.
- Las características de VPN SSL se deberán cumplir con o sin el uso de agentes.
- Deberá permitir que todo el tráfico de los usuarios VPN remotos fluya hacia el túnel VPN, previniendo la comunicación directa con dispositivos locales como un proxy.
- Asignación de DNS en la VPN de cliente remoto.
- Soportar autenticación vía AD/LDAP, Secure id, certificado y base de usuarios local.
- Soportar lectura y revisión de CRL (lista de revocación de certificados).
- Permitir la aplicación de políticas de seguridad y visibilidad para las aplicaciones que circulan dentro de túneles SSL.
- Deberá permitir que la conexión a la VPN se establezca de la siguiente manera: Antes de que el usuario se autentique en su estación.
- Deberá permitir que la conexión a la VPN se establezca de la siguiente manera: Después de la autenticación de usuario en la estación.
- Deberá permitir que la conexión a la VPN se establezca de la siguiente manera: Bajo demanda de los usuarios.
- El agente de VPN SSL o IPSEC cliente-a-sitio deberá ser compatible con al menos Windows 7 (32 y 64 bits), Windows 8 (32 y 64 bits), Windows 10 (32 y 64 bits) y Mac OS X (v10.10 o superior).

f) Solución de Sistema de Gestión de Información y Eventos de Seguridad Informática (SIEM)

- EL SIEM deberá siempre estar disponible en modalidad 24x7x365, las 24 horas del día, los 365 días del año ininterrumpidamente, incluyendo domingos y feriados. El plazo del servicio será de treinta y seis (36) meses.
- EL PROVEEDOR deberá considerar el desarrollo de 20 casos de uso sobre el SIEM, 10 para la etapa de implementación y el resto durante el servicio.
- La solución deberá definir el acceso basado en roles, por dispositivo, grupo de dispositivos, rangos de red. También deberá restringir a los usuarios y/o grupos acceso solo a la información de dispositivos, grupos de dispositivos y rangos de red respectivos. Esto incluye ser capaz de restringir el acceso de un usuario a funciones específicas de la solución que no está dentro del alcance de un papel usuarios incluyendo, pero no limitados a la administración, presentación de informes, el filtrado de eventos, de correlación, y/o la visualización de Dashboard.
- La solución deberá contar con el módulo de UBA (user behavior analytics) para el monitoreo de comportamiento de usuarios.
- La solución deberá contar con Machine Learning para el aprendizaje automático del comportamiento de usuarios de la ENTIDAD.
- La solución SIEM deberá proporcionar una gestión centralizada de todos los componentes y funciones administrativas desde una única interfaz basada en web

(Actividad de logs, flujos de red, base de activos, vulnerabilidades, reportes y paneles de administración).

- La solución deberá contar con una interfaz de trabajo (Dashboard) totalmente configurable, debe permitir la separación de los Dashboard predefinidos de la Interfaz del usuario para ser utilizados en Dashboard personalizados.
- La solución deberá proveer los mecanismos para la encriptación de la comunicación entre los componentes. Deberá poder integrarse con sistemas de Directorios como método de autenticación, como mínimo el Directorio Activo.
- La solución deberá contar con un repositorio de aplicaciones (plug-ins) y contenidos adicionales para la incorporación de paquetes de reportes y funcionalidades de terceros (integraciones avanzadas).
- La solución deberá encontrarse como "Challenger"
- La solución deberá poseer una interfaz gráfica de usuario basada en web para la gestión, el análisis y presentación de informes.
- La solución deberá contar con un proceso de copia de seguridad / recuperación automatizada.
- La solución deberá en forma automática realizar Health Check y notificar en el caso de que se detecte algún inconveniente.
- La solución deberá permitir implementaciones como software, virtual y appliance físico.
- La solución deberá poseer una base de datos distribuida para los eventos y actividad de la red de tal manera que toda la información se puede acceder desde una única interfaz de usuario.
- La solución deberá garantizar la integridad de la información recogida a través de hashing SHA-1, SHA2 y MD5. Además, deberá contar con mecanismos de control y comprobación de integridad, que deberá informar y advertir la manipulación de archivos.
- La solución deberá ofrecer widgets del Dashboard personalizables que pueden presentar información de seguridad relevante para los usuarios del sistema (es decir, puntos de vista de eventos, vistas de actividad de red, puntos de vista de incidentes, etc)
- La solución deberá proporcionar mecanismos intuitivos para la solución de problemas, tales como notificaciones proactivas, utilidades de línea de comandos o aplicaciones (plugins) desarrollados por el fabricante.
- La solución deberá tener una arquitectura de recopilación de registros y archivo que admita almacenamiento de eventos a corto plazo (en línea) y largo plazo (sin conexión).
- La solución deberá contar con una base de datos diseñada específicamente para el almacenamiento y procesamiento de eventos de seguridad.
- La solución deberá poseer una taxonomía de eventos y campos. El usuario deberá ser capaz de añadir sus propios nombres de eventos únicos (es decir, la posibilidad de añadir nuevos campos que no forman parte del esquema por defecto).
- La solución deberá permitir el etiquetado personalizada de eventos, deberá proporcionar la recuperación transparente, la agregación, clasificación, filtrado y análisis de datos a través de todos los componentes distribuidos.
- La solución deberá ser compatible con los métodos de recopilación de logs de la industria (syslog, WMI, JDBC, SNMP, Checkpoint LEA, OPSEC, ALE, registros de FTP, SCP, SFTP).
- La solución propuesta deberá integrarse de forma nativa con Exchange on-premise.
- La solución deberá proporcionar recopilación sin agentes de los registros de eventos siempre que sea posible.
- La solución deberá proporcionar la capacidad de distribuir tanto el almacenamiento y el procesamiento de eventos a través de toda su arquitectura de colección y correlación.

- La solución deberá ser compatible con el acceso a largo plazo a los eventos de seguridad detallada. El sistema deberá ser capaz de proporcionar el acceso al menos por 12 meses de información teniendo en cuenta el escenario de máxima utilización de EPS disponibles.
- La solución SIEM deberá soportar como mínimo 2,000 EPS, que en caso se superen se deberá revisar y afinar la solución (plataformas y eventos) para calzar dentro de lo soportado por la licencia.
- La solución deberá proporcionar la capacidad de normalizar campos de eventos globales que no están representados por los campos normalizados por defecto.
- La solución deberá proporcionar la capacidad de almacenar y conservar tanto los eventos normalizados como el original en bruto para fines forenses, dentro del tiempo proporcionado como almacenamiento.
- La solución deberá poder agregar y analizar eventos basados en filtros específicos definidos por el usuario.
- La solución deberá proporcionar una vista de "streaming" en tiempo real que soporte las capacidades de filtrado completo.
- La solución deberá realizar un análisis en tiempo real de los eventos.
- La solución deberá proporcionar la capacidad de hacer un análisis en profundidad de los eventos.
- La solución deberá apoyar y mantener un historial de la actividad de autenticación de usuario en función de cada activo.
- La solución deberá proporcionar reportes, sobre todos los elementos disponibles para la gestión a través de la interfaz gráfica de usuario.
- La solución deberá proporcionar un motor de informes configurable para la creación de informes personalizados.
- La solución deberá realizar reportes programados, por hora, día, semana o mes.
- La solución deberá poseer plantillas para la creación y entrega de informes en múltiples niveles que van desde operaciones a actividades específicas de la entidad.
- La solución deberá poder proporcionar informes out-of-the-box, para las cuestiones operativas típicas del negocio, como reportes de:
 - a. Autenticación
 - b. Identidad
 - c. Actividad del usuario
 - d. Cumplimiento de normativas
 - e. Gestión de configuraciones y cambios
 - f. Gestión de red
 - g. Seguridad
 - h. Monitoreo de uso
 - i. Actividad de las aplicaciones
 - j. Informes específicos por dispositivos (sistema operativos, base de datos, etc)
 - k. Gerenciales / Ejecutivos
- La solución deberá proporcionar reportes out-of-the-box de cumplimiento de las regulaciones específicas (PCI, SOX, FISMA) y marcos de control (NIST, COBIT, ISO).
- La solución deberá poder realizar la distribución automática de informes, en los siguientes formatos:
 - a. HTML
 - b. PDF
 - c. XML
 - d. Excel/CSV
 - e. Word/RTF
- La solución deberá realizar y entregar informes de activos.

- La solución deberá proporcionar alertas en base a las amenazas de seguridad observados en los dispositivos monitoreados.
- La solución deberá proporcionar la capacidad de correlacionar la información a través de dispositivos de distintos fabricantes.
- La solución deberá proporcionar alertas en base a la política establecida
- La solución deberá generar alertas basados en criticidad, para tener en cuenta las prioridades. La criticidad deberá poder asignarse sobre la base de múltiples características, como el tipo de activos, el protocolo, la aplicación, etc.
- La solución deberá proporcionar la capacidad de transmitir alertas usando múltiples protocolos y mecanismos a otras soluciones de gestión.
- La solución deberá poseer la capacidad de tomar medidas tras haber recibido una alerta. Por ejemplo, la solución deberá poder iniciar scripts, generar un incidente o enviar un mensaje de correo electrónico.
- La solución deberá vigilar y alertar cuando hay una interrupción en la recopilación de registros de un dispositivo. En otras palabras, si los registros no son vistos desde un servidor en una cantidad determinada de minutos, generar una alerta.
- La solución deberá proporcionar un mecanismo out-of-the-box para descubrir y clasificar los activos por tipo de sistema (es decir, servidores de correo frente a servidores de bases de datos) para minimizar los falsos positivos asociados a una mala clasificación de los activos.
- La solución deberá realizar la correlación de valores aditivos a través del tiempo.
- La solución deberá realizar la correlación de una secuencia fallida.
- La solución deberá proporcionar un mecanismo, para optimizar el "tuning" de las reglas, que permite la agrupación de valores de entrada similares de una regla de correlación que puede ser utilizado por varias reglas. Este mecanismo de agrupación deberá permitir tanto para grupos estáticos, como grupos dinámicos creados por otras reglas de correlación.
- La solución deberá proporcionar capacidad de enviar notificación de alertas correlacionadas a través de procedimientos bien definidos (es decir, traps SNMP, correo electrónico, etc)
- La solución deberá poseer un mecanismo para capturar todos los aspectos relevantes de un incidente de seguridad en una sola vista. Esta visión deberá incluir hechos relevantes, datos de actividad de la red, alertas correlacionadas, datos de vulnerabilidades, etc.
- La solución deberá proporcionar un mecanismo para marcar un incidente de seguridad para poder darle seguimiento con el personal de operaciones de seguridad.
- La solución deberá proporcionar un mecanismo para el seguimiento de los incidentes de seguridad a través de una amplia gama de atributos relevantes (es decir, direcciones IP, nombres de usuario, dirección MAC, de registro de origen, reglas de correlación, definido por el usuario, etc.). El usuario deberá ser capaz de filtrar los incidentes utilizándolos atributos definidos
- La solución deberá poder descubrir automáticamente las fuentes de eventos, y con solo recibirlos deberá poder catalogarlos automáticamente.
- La solución deberá tener documentada y pública la lista de integraciones nativas soportadas, con al menos 200 módulos de integración, y el procedimiento con el cual se integra cada una de las fuentes.
- La solución deberá contar con un agente de Windows capaz de realizar recolección de eventos locales o utilizando el protocolo RPC. Estos agentes deberán tener la capacidad de ser gestionados de manera centralizada desde la solución y contar con la posibilidad de almacenar eventos localmente en caso de interrupciones de conexión, enviando los eventos recolectados al SIEM una vez restablecida la comunicación.

- La solución deberá contar con un asistente basado en web que permita el desarrollo de conectores de recolección personalizados sin la necesidad de editar archivos de configuración o xml.
- La solución deberá poseer la capacidad de contextualizar la actividad de las aplicaciones en la red con los eventos de seguridad de los dispositivos monitoreados.
- La solución deberá incluir Analíticos de Comportamiento de Usuario (User Behavior Analytics) que permitan detectar aquellos usuarios cuyo patrón de comportamiento es anómalo, y hacer un seguimiento de las actividades de los sospechosos sin requerir una solución adicional.
- La solución deberá poseer la capacidad de priorizar en forma automática los sucesos de seguridad, notificados de acuerdo con la importancia relativa del dispositivo monitoreado.
- La solución deberá poseer la capacidad de asignar calificaciones de credibilidad a los dispositivos de seguridad monitoreados.
- La solución deberá proporcionar una vista de eventos en tiempo real de la información monitorizada en el formato original y normalizado.
- Ante una amenaza, la solución deberá ser capaz de mostrar en una única pantalla los eventos y la información de contexto relacionada.
- El postor deberá brindar soporte y administración del SIEM propuesto.

g) Monitoreo de eventos de seguridad

- Monitoreo en horario 24x7x365 de eventos de seguridad a través de la tecnología Security Information and Event Management (SIEM) propuesto a la ENTIDAD.
- Contará con una base de conocimiento en los procesos de gestión de eventos de seguridad.
- Detección y tratamiento de ataques, desde las tecnologías de seguridad de la ENTIDAD.
- Detección de alertas o incidentes de seguridad en tiempo real, utilizando tecnología SIEM para identificarlos. Se considera que como parte del análisis se realice la notificación y triaje en el tiempo esperado.
- Detección de anomalías e incidentes de seguridad. Es preciso que la ENTIDAD tome acción en el tiempo oportuno.
- EL PROVEEDOR deberá contar con un diseño de infraestructura, procesos y personal que permitan la continuidad ante un evento de desastre. Esta infraestructura deberá contar al menos con 2 ubicaciones de SOC en diferentes países y que tengan un esquema de alta disponibilidad, de tal manera que, ante la caída de una, la otra pueda continuar las labores de monitoreo.
- Las alertas y los incidentes deberán calificarse por su gravedad y prioridad de tratamiento, entendiéndose que puede haber incidentes de baja gravedad, pero cuyo tratamiento puede ser prioritario.
- EL PROVEEDOR deberá contar con un portal de gestión del servicio al cual la ENTIDAD pueda acceder para hacer seguimiento a los incidentes identificados y sus acciones de respuesta. Asimismo, este portal deberá mostrar un dashboard ejecutivo con los principales indicadores del servicio para dos usuarios.
- EL PROVEEDOR deberá entregar los siguientes reportes:
 - a. Un reporte mensual con el resumen ejecutivo y el detalle de las alertas atendidas
 - b. Un reporte detallado de cada incidente confirmado.
- El postor deberá monitorear la disponibilidad, recursos, interfaces de las tecnologías/soluciones listadas en el alcance.

- Se tiene como alcance de monitoreo las plataformas de seguridad incluidas en este ITEM, además de los 2 controladores de dominio, 2 servidores Exchange y 1 antispam de propiedad de la ENTIDAD.
- El SOC brindará una primera respuesta o comunicación a todos los incidentes críticos en un plazo de 15 minutos desde su detección.
- El SOC deberá retener registros de incidentes por un mínimo de 01 año y proporcionará acceso a estos registros a la ENTIDAD bajo una solicitud vía correo, teniendo el PROVEEDOR un plazo de 24 horas para brindar la información.

h) Servicio de inteligencia de amenazas

- EL servicio de inteligencia de amenazas de ciberseguridad deberá ser proporcionada en tiempo real de manera continua (24x7x365) y actualizada con la finalidad de mantener informado a la ENTIDAD sobre Ciber amenazas orientadas, atacantes, sus tácticas, herramientas y prácticas.
- El PROVEEDOR del servicio deberá contar con la funcionalidad de Inteligencia de amenazas, para ello, el PROVEEDOR deberá contar con por lo menos una (01) suscripción global y reconocida mundialmente dentro del rubro para obtener fuentes de inteligencia especializada. Los servicios de suscripción para la función de inteligencia de amenazas deberán estar licenciados y/o contratados para ser usados por el Contratista. Estas fuentes de inteligencia de tipo suscripción no deberán ser gratuitas.
- El servicio de inteligencia de amenazas deberá brindar información especializada en tiempo real, con la finalidad de obtener, de forma periódica, informes globales de nivel de amenazas en internet (detectadas a nivel mundial).
- El servicio de inteligencia de amenazas deberá de integrarse con el servicio de Gestión de Eventos (SIEM).
- El servicio de inteligencia de amenazas deberá operar conjuntamente con el SIEM ofertado, de manera tal que permita complementar la información del SIEM para detectar y analizar actividades anormales en las plataforma tecnológicas de la ENTIDAD con una mayor precisión, y así identificar vectores de ataques, signos de compromiso, intrusión o fuga de información de una manera integral, contrastando la información de las fuentes de inteligencia de amenazas con los eventos relacionados a amenazas y/o incidentes obtenidos por el SIEM.

i) Servicio de Respuesta ante Incidentes

- El PROVEEDOR deberá brindar la atención de respuesta de incidentes de seguridad por parte de sus especialistas, liderando cualquier acción sobre el resto de los proveedores que administren las tecnologías.
 - a. Incidente: Suceso o problema que ocurre de forma inesperada que puede afectar el servicio o continuidad del negocio.
- El alcance de este servicio deberá llevar a cabo tareas forenses digitales y de respuesta a incidentes, para ayudar en el análisis, respuesta, contención y recomendaciones para la remediación de incidentes de seguridad.
- Los servicios se deberán subdividir en por lo menos las siguientes fases:
 - a. Fase 1 - Una fase inicial de recopilación de información para delimitar el alcance y definir los entregables cubiertos por el servicio.
 - b. Fase 2 - Actividades de respuesta ante incidentes en las etapas de detección, análisis, contención, erradicación y recuperación.
 - c. Fase 3 - Redacción y entrega de un informe en el que se detallan los resultados de la investigación y se documenta todo el proceso de respuesta ante incidentes. El Contratista deberá indicar la ubicación del CSIRT, así

como describir las instalaciones y el personal integrante, el mismo que deberá ser de su propiedad.

- Las fases del servicio deberán contar como mínimo la siguiente distribución:

Fase	Tipo	Dueño	Contribuidor	Lugar
Fase 1: Validación de Requerimientos.				
Formulario de Incidente	Actividad	Proveedor	Entidad	Remoto
Presentación de Kick-Off (Reunión Inicial)	Actividad	Proveedor	Entidad	Remoto
Fase 2: Actividades de Respuesta ante Incidentes				
(A) Detección y Análisis	Actividad	Proveedor	Entidad	Remoto
(B) Plan de contención y erradicación	Actividad	Proveedor	Entidad	Remoto
(C) Plan de Recuperación	Actividad	Proveedor	Entidad	Remoto
Fase 3: Post-Incidente				
(D) Elaboración de informes finales	Actividad	Proveedor	Entidad	Remoto

- El objetivo de la Fase 1 deberá ser: (a) acordar el alcance y el calendario de los servicios; y (b) recopilar la información de la ENTIDAD necesaria para llevar a cabo con éxito el servicio.

En esta fase, el PROVEEDOR:

- Deberá proporcionar a la ENTIDAD un Formulario de Incidencias o un correo electrónico, describiendo la información de la ENTIDAD requerida por el PROVEEDOR para poder delimitar el alcance de los servicios descritos en las Fases 2 y 3.
- Deberá organizar una conferencia telefónica inicial para discutir el Formulario de Incidencias completado
- Deberá designar un Incident Responder para este servicio; seleccionar y asignar recursos técnicos, a su discreción, para realizar las actividades de las Fases 2 y 3.
- La Fase 2 deberá subdividirse en por lo menos tres subconjuntos de actividades de respuesta a incidentes:
 - Detección y análisis
 - El PROVEEDOR deberá utilizar tecnología para recopilar la información necesaria para detectar y analizar las amenazas de seguridad. A su discreción razonable, el PROVEEDOR podrá realizar análisis como parte de esta Fase, incluyendo el análisis de logs disponibles y relevantes de herramientas como

firewall/NetFlow, VPN, proxy web, IDS/IPS, SIEM, entre otros artefactos forenses adicionales que tenga la ENTIDAD, así como análisis detallados de archivos y memoria para el descubrimiento de payloads maliciosos.

b. Contención y Erradicación

- i. Una vez identificados los hosts comprometidos, El PROVEEDOR sugerirá opciones de contención tácticas iniciales para que la ENTIDAD las considere según su criterio y responsabilidad con el objetivo de aislar la amenaza. Además, el PROVEEDOR deberá sugerir opciones de remediación para que la ENTIDAD considere a su discreción y responsabilidad, tales como terminar un proceso, eliminar un archivo o eliminar la persistencia del registro. La ENTIDAD podrá aplicar estas opciones de corrección de forma manual o automática. Basándose en los resultados del análisis de amenazas, el PROVEEDOR también podrá proporcionar orientación sobre las mejores prácticas para opciones de corrección adicionales tanto a corto como a largo plazo.
- ii. En esta fase, el PROVEEDOR deberá:
 - Realizar actividades de análisis como las descritas anteriormente y emitir recomendaciones de seguridad sobre contención y remediación.
 - Proporcionar actualizaciones periódicas del proceso según lo acordado.
 - Proporcionar un portal compartido para cargar y almacenar artefactos forenses y diversos documentos relacionados con la investigación.
 - Entregar un informe de análisis inicial de los servidores infectados.
 - Entregar un informe de análisis forense para los equipos pacientes cero
 - En caso se identifique el paciente cero el PROVEEDOR propondrá realizar el análisis forense.

c. Recuperación

- i. El PROVEEDOR deberá presentar un plan de recuperación basado en los hallazgos identificados asegurando que todos los controles de erradicación se apliquen de forma correcta asociado a la causa raíz, este plan deberá ser presentando a la ENTIDAD quien aprobará y definirá las actividades declaradas por EL PROVEEDOR, las actividades serán lideradas por el PROVEEDOR, LA ENTIDAD contactará con todos sus proveedores para asegurar el cumplimiento de las actividades declaradas, se presentará un plan basado en los conceptos de Hardenización y Aseguración de los activos afectados. El servicio de recuperación puede recomendar configuraciones sobre los equipos de ciberseguridad Firewall, IDS, IPS, Proxy, EDR, WAF, DAM, entre otros; para los servicios asociados las configuraciones de Servidores con los sistemas operativos (Microsoft, Linux, entre otros) o equipos de redes (Switches, Router o HUB), el PROVEEDOR deberá brindar acompañamiento, pero la responsabilidad de configuración y recuperación será de la ENTIDAD mediante sus especialistas de servidores y redes, o proveedores relacionados.

- Plan de Recuperación del Servicio
- Diagrama de arquitectura de red asegurada.
- Informe de análisis de vulnerabilidades pre y post Incidente.
- Tras la finalización completa de las fases 1 y 2, el PROVEEDOR, a menos que se indique lo contrario, elaborará y entregará a la ENTIDAD un informe final de respuesta ante incidentes que constará de: (a) todos los hallazgos del incidente de seguridad sobre la cual se presentarán basado en la metodología de respuesta ante incidentes dentro de las etapas de preparación, detección y análisis, contención y erradicación y (b) un conjunto de mejoras recomendadas (lecciones aprendidas) para que la ENTIDAD las considere a su discreción y responsabilidad con vistas a mejorar la postura de seguridad actual de la ENTIDAD. La ENTIDAD dispondrá de siete (7) días laborables para proporcionar comentarios sobre el informe, tras los cuales el informe se considerará aprobado y aceptado por la ENTIDAD.
- La ENTIDAD aceptará y confirmará la finalización de cada fase antes del comienzo de la siguiente fase. Cualquier entregable (o, en general, cualquier documento) no objetado por escrito por la ENTIDAD dentro de los siete (7) días hábiles se podrá considerar como aceptado.
- El servicio remoto de respuesta ante incidentes y análisis forense será en su conjunto 100 horas anuales.
- La ENTIDAD proporcionará toda la información, apoyo, aprobaciones y recursos pertinentes y razonablemente solicitados que necesite el equipo del PROVEEDOR de manera oportuna para completar con éxito el servicio. Más concretamente, pero sin limitar lo anterior, la ENTIDAD deberá ser responsable de:
 - a. Durante toda la duración de los servicios, garantizar que el PROVEEDOR reciba puntualmente toda la información, datos y documentación actualizados y precisos que el PROVEEDOR requiera razonablemente para prestar los servicios y cumplir con las responsabilidades del PROVEEDOR. Esta información incluirá, a título meramente enunciativo y no limitativo (i) información relativa a la seguridad y red de la ENTIDAD, diseño, negocio y otros requisitos aplicables; (ii) documentación funcional y/o técnica relativa a dichos requisitos; y (iii) mapas de topología, información de configuración e infraestructura de red existente.
 - b. A lo largo de la duración de los servicios, garantizará que todo el personal necesario de la ENTIDAD (como personal de operaciones de seguridad y operaciones de red, arquitectura e ingeniería de red) esté disponible para proporcionar información y participar en sesiones de revisión de proyectos, reuniones o conferencias telefónicas según sea necesario para que el PROVEEDOR preste los servicios.
 - c. Mientras duren los servicios, proporcionará acceso remoto a sistemas, redes o información y manos remotas según sea necesario.
 - d. Nombrará a un focal point y proporcionará al Incident Responder una lista de las funciones y responsabilidades del personal designado de la ENTIDAD, según requiera el PROVEEDOR para realizar los servicios como parte de la Fase 1.
 - e. Proporcionará puntualmente a el PROVEEDOR un formulario de incidencias completado y firmado como parte de la Fase 1 que permitirá al PROVEEDOR determinar el alcance de los servicios descritos en las Fases 2 y 3.
 - f. La ENTIDAD y el PROVEEDOR acordarán, como parte de la Fase 1, las fechas y horas específicas para la realización de los servicios descritos en las Fases 2 y 3; y la ENTIDAD y el PROVEEDOR acordarán, como parte de la Fase 1, el método de acceso remoto, si lo hubiera, a los Puntos Finales Cubiertos.

- g. La ENTIDAD y el PROVEEDOR acordarán, como parte de la Fase 1, una lista de equipos de punto final que estarían sujetos a la instalación de alguna herramienta de seguridad.
- Las dependencias del PROVEEDOR y de la ENTIDAD deberán incluir lo siguiente:
 - a. Proporcionar la información requerida para que el PROVEEDOR complete los entregables y las fases relevantes.
 - b. Proporcionar simultáneamente a todos los recursos del PROVEEDOR acceso al equipo o información relevante dentro de los plazos acordados.
 - c. Todos los recursos requeridos por la ENTIDAD estarán disponibles a solicitud del PROVEEDOR y, en particular, cuando se lleven a cabo las fases 2 y 3.
- El equipo de respuesta ante incidentes del proveedor deberá estar registrado como miembro del FIRST (Forum of Incident Response and Security Teams).
Importante: El postor deberá presentar el certificado o constancia de FIRST para la presentación de ofertas.
- El PROVEEDOR deberá crear una matriz de escalamiento en conjunto con la ENTIDAD, en la cual se determine cuándo un incidente deba ser escalado al CSIRT y quienes son los roles autorizados del escalamiento de los tickets.

j) Servicio de Análisis de Vulnerabilidades

- La ENTIDAD requiere de un servicio para el análisis y la gestión de vulnerabilidades que pueda identificar, analizar, clasificar e informar de las vulnerabilidades y sus riesgos. Con la finalidad de corregir debilidades y aplicar controles para garantizar una protección continua. Para ello, el servicio deberá contemplar lo siguiente:
- El servicio deberá poder cubrir el análisis y la gestión de vulnerabilidades de activos On-premise.
- El servicio de análisis y gestión de vulnerabilidades deberá cubrir 100 activos.
- El servicio deberá contemplar como mínimo el escaneo trimestral de vulnerabilidades de los activos a escanear.
- El servicio de análisis y gestión de vulnerabilidades deberá de:
 - a. Evaluar los activos para poder reducir los riesgos de nuevas vulnerabilidades descubiertas.
 - b. Brindar una vista unificada de toda la información de hallazgos de vulnerabilidades.
 - c. Contar con capacidades de análisis de cumplimiento de políticas. El PROVEEDOR deberá revisar las líneas base de seguridad (hardening) a ser analizadas en los activos de la ENTIDAD.
- El PROVEEDOR deberá ser responsable de:
 - a. La evaluación de las vulnerabilidades y la entrega del informe de recomendaciones para la remediación.
 - b. La evaluación del nivel de preparación ante el riesgo de explotación de vulnerabilidades.
 - c. Seguimiento a la corrección/remediación de vulnerabilidades con las áreas respectivas de la ENTIDAD.
 - d. Ejecutar la remediación de vulnerabilidades de las Tecnologías y servicios gestionados por el PROVEEDOR.
 - e. Brindar asesoramiento en la remediación de vulnerabilidades de infraestructura, Tecnologías y aplicaciones no gestionadas por el PROVEEDOR.
- El servicio propuesto deberá cubrir los siguientes beneficios de seguridad:
 - a. Mapeo visual de todos los dispositivos, servicios, recursos y aplicaciones en la red.

- b. Detalle de cada dispositivo, servicios, recursos y aplicaciones por el sistema operativo, los puertos, certificados, etc.
- c. Monitoreo, capacidad de seguimiento y control de la gestión de vulnerabilidades
- Entregables:
 - a. Se entregarán reportes trimestrales del seguimiento del servicio y recomendaciones, como:
 - i. Reportes de hallazgos de vulnerabilidades y recomendaciones de priorización y mitigaciones entregadas por la herramienta, de acuerdo con la criticidad de los activos de la ENTIDAD.
 - ii. Informe ejecutivo del estado de vulnerabilidades.
 - iii. Informe de seguimiento a la remediación de vulnerabilidades.

k) Servicio de Mejora continua

El PROVEEDOR deberá asignar un gestor del servicio quien será responsable de:

- Coordinar los comités internos (técnicos y de gestión).
- Realizar la presentación del servicio mensual.
- Realizar el informe integral del servicio.
- Del procesamiento y análisis de la data (Tickets, Informes, otros).
- Elaborar, proporcionar y darle seguimiento a los KPIs que la ENTIDAD solicite y además el PROVEEDOR deberá facilitar su catálogo de KPI/KRI para su adopción en caso se requiera.

l) Servicio de Ingeniero Dedicado

- El PROVEEDOR deberá brindar un ingeniero dedicado para la ENTIDAD, quien iniciará funciones en el inicio del servicio post-implementación, atendiendo de manera remota cinco (5) días a la semana, desde las 08:30 hasta las 17:30 horas.
- Actividades a Desarrollar: tomará nota de los requerimientos técnicos que se encuentren vinculados a las soluciones de seguridad (Hardware, Software y funcionalidades) y que sean planteados por parte del personal técnico designado por la Oficina de Sistemas de la Información; evaluando su viabilidad técnica, definiendo los parámetros y alcances de las configuraciones requeridas que proporcionen la funcionalidad deseada.
- En caso de ausencia del personal clave por vacaciones, descanso médico o fuerza mayor, que imposibilite la continuidad de sus labores o a solicitud de la ENTIDAD, el PROVEEDOR deberá garantizar que el personal reemplazante tenga el mismo o mayor nivel de estudios, preparación, conocimientos requeridos. La designación del nuevo personal técnico estará sujeta a la previa aceptación por parte de la ENTIDAD.

Consideraciones Adicionales del Servicio

Las siguientes consideraciones aplican a todo el servicio solicitado:

- El Contratista será responsable del levantamiento de la información (actuales políticas y reglas de seguridad) y traslado o adaptación de políticas del equipamiento existente, y en caso aplique proponer mejoras previa evaluación de la Oficina de Sistemas de Información.
- La ENTIDAD podrá solicitar información histórica del servicio con una antigüedad máxima de un (01) año, Esto hace referencia a la información que

se almacenará en el Sistema de Gestión de Información y Eventos de Seguridad informática.

- La ENTIDAD podrá solicitar que se generen los reportes personalizados de cada solución, y estos se remitan de manera periódica a cuentas de correo electrónico que defina la ENTIDAD.
- El Contratista deberá contar para todos los componentes o appliance para la ejecución del servicio con las licencias y soporte respectivo de los fabricantes durante toda la vigencia del contrato.

Instalación y Configuración

- Para la realización de trabajos de implementación del servicio, la Entidad brindará al Contratista las facilidades y accesos necesarios de las instalaciones involucradas para la presente contratación. En ese sentido; el Contratista deberá coordinar con la Entidad los horarios de accesos y trabajos de migración.
- La implementación se realizará en forma paralela al actual servicio para mantener así su continuidad, para dicho fin la Entidad brindará al contratista las facilidades técnicas. Asimismo; el Contratista realizará las configuraciones necesarias en los equipos propuestos a fin de mantener o mejorar el nivel de seguridad existente, con el menor impacto posible.
- El Contratista será responsable de la migración, instalación, configuración y puesta en marcha de las soluciones solicitadas; así mismo, el Contratista deberá asegurar que los equipos a proveer sean compatibles entre sí.
- Todos los componentes o equipos, con sus respectivos accesorios, provistos por el Contratista deberán ser otorgados en calidad de alquiler, formando parte del servicio ofertado durante el tiempo de vigencia del contrato.

Nota:

- La ENTIDAD brindará al contratista toda la información necesaria para realizar las configuraciones de red, perfiles de seguridad, reglas u objetos en general, para poder implementar correctamente la solución ofertada.
- La ENTIDAD asegurará las conexiones eléctricas de todos los equipamientos que se instalen en el Data Center de la ENTIDAD, contando con tomas de energía de tipo C14 para PDU, entre otras.
- La ENTIDAD será responsable de la supervisión, control y custodia de los equipamientos físicos y ambientes virtuales, que provea para la ejecución y funcionamiento de las soluciones de seguridad ofertadas por el CONTRATISTA.
- La ENTIDAD brindará toda información técnica y necesaria para la ejecución y/o implementación de las soluciones de seguridad ofertadas por el CONTRATISTA.

Operación del Servicio

- El CONTRATISTA deberá efectuar las siguientes actividades durante el servicio gestionado (plataformas gestionadas):
 - Trabajos preventivos, correctivos y bajo demanda las 24 horas del día y los 7 días a la semana, el mismo que consistirá en lo siguiente:
 - ✓ Configuraciones a nivel de red.
 - ✓ Configuraciones en las funcionalidades de seguridad.

- ✓ Configuraciones a nivel de seguridad
- ✓ Actualizaciones de Firmware de los equipos propuestos.
- El CONTRATISTA deberá efectuar los Mantenimientos Preventivos que estime conveniente a fin de garantizar el correcto funcionamiento de cada equipo o componente que permita el óptimo desarrollo del servicio requerido.
- El CONTRATISTA deberá contar con equipos a modo de "spare" en los casos que el equipamiento instalado en la entidad no cuente con alta disponibilidad, para su reposición en caso de que se determine una falla que imposibilite su operación. El plazo final para devolver la operatividad con un equipo de reemplazo no deberá exceder las treinta y seis (36) horas de notificada la avería.
- Si uno de los equipos de la solución que se encuentra en alta disponibilidad presenta una avería que imposibilite su operación, el CONTRATISTA deberá considerar una reposición en un plazo máximo de 60 días calendario, en caso de que se presente una situación externa fuera del alcance del CONTRATISTA que imposibilite la entrega del equipo en el periodo indicado, esto se deberá justificar con un sustento del fabricante o del mayorista indicando el nuevo plazo de entrega.
- De ser el caso, y durante la etapa de operación del servicio, el CONTRATISTA deberá remitir a la Oficina de Sistemas de Información una relación del personal técnico o profesional autorizado, para realizar labores de reparación de los appliance o componentes en calidad de alquiler, así como de sus conexiones, instalaciones y configuraciones. La relación del personal antes mencionado deberá ser actualizada cuando se produzcan cambios.

Supervisión

- El servicio estará bajo la supervisión de la Oficina de Sistemas de Información, en su calidad de área usuaria y técnica.
- El CONTRATISTA mantendrá el control y supervisión permanente de todos los aspectos relacionados al servicio.

Calidad del Servicio

- El Contratista deberá contar con un Centro de Operaciones y Seguridad (SOC), donde se encuentren monitoreando las 24 horas del día, los 7 días a la semana y los 365 los días del año durante la vigencia del contrato, este Centro de Operaciones y Seguridad deberá estar dentro del territorio nacional, el cual deberá contar con alta disponibilidad; (el ganador de la buena pro deberá acreditar fehacientemente la pertenencia de este para disponibilidad de la ENTIDAD). Así mismo el Centro de Operaciones y Seguridad (SOC) deberá contar con un sistema de gestión ON LINE el cual mediante un Dashboard personalizable (el cual se podrá mostrar en un Pc, laptop, u teléfono inteligente) permitirá al INGEMMET hacer un seguimiento de los eventos, indicadores de gestión para cumplimiento del SLA, reportes de fallas, atención a nuevas solicitudes o tratamiento de reclamos, así como también la atención y solución de averías, y solicitudes derivadas del servicio sin necesidad de cursar comunicación al proveedor. La ENTIDAD deberá contar con acceso para al menos tres (3) usuarios al sistema de gestión ON LINE.

Importante: El postor deberá presentar una Declaración jurada de poseer un Centro de Operaciones y Seguridad (SOC) propio, para la presentación de ofertas.

- Asimismo, el contratista será responsable de la actualización oportuna de parches y de hacer las copias de respaldo de la configuración y políticas de los productos propuestos, para esto deberá demostrar que el Centro de Operaciones y Seguridad (SOC) cuenta con procedimientos que han logrado un nivel de madurez mínimo de nivel 3 o más, hasta un máximo de 5, los cual deberá acreditar con documento emitido por una entidad auditora internacional.

Importante: El postor deberá presentar el certificado o constancia del nivel de madurez del Centro de Operaciones y Seguridad (SOC) para la presentación de ofertas.

- El Centro de Operación y Seguridad (SOC) deberá operar bajo las mejores prácticas y estándares en seguridad de la información y/o ciberseguridad, a su vez deberán poder operar bajo el concepto de resiliencia tecnológica, para esto el ganador de la buena pro deberá acreditar que el Centro de Operación y Seguridad (SOC) ha logrado obtener una certificación de estándares internacionales que cubra el alcance como "Centro de Operaciones de Seguridad (SOC o CYBERSOC)" en el territorio nacional.
- El Centro de Operación y Seguridad (SOC) deberá operar bajo las mejores prácticas y estándares en seguridad de la información y/o ciberseguridad, a su vez deberán poder operar bajo el concepto de resiliencia tecnológica, para esto el ganador de la buena pro deberá acreditar que el Centro de Operación y Seguridad (SOC) ha logrado obtener una certificación de estándares internacionales que cubra el alcance como "Centro de Operaciones de Seguridad (SOC o CYBERSOC)" en el territorio nacional. También se aceptará el documento emitido por entidad auditora internacional o que el SOC cuenta con certificación internacional ISO 27001 opcional.

Importante: El postor deberá presentar el certificado o constancia de ISO/IEC 27001:2013 del Centro de Operaciones y Seguridad (SOC) para la presentación de ofertas opcional.

- El Centro de Operaciones y Seguridad (SOC) deberá tener la capacidad de escalamiento interno a otros niveles de servicio sin la necesidad de que El Instituto Geológico, Minero y Metalúrgico informe sobre la demora o falta de atención de un evento o incidente informado por cualquier canal de atención (atención telefónica, correo electrónico, etc.).
- El Contratista deberá ofrecer un centro de atención mediante vía telefónica, utilizando un número (0800 o similar), correo electrónico y un teléfono fijo para los escalamientos a nivel nacional, a fin de reportar cualquier incidencia que pueda presentarse durante la ejecución del servicio. El servicio del centro de atención deberá estar alineado a ITIL v3 y deberá contar con personal especializado. La atención será las 24 horas del día, los 7 días a la semana y los 365 los días del año, y deberá incluir los siguientes servicios:
 - ✓ La atención de las incidencias de avería de manera remota y/o en sitio (Gestión de Incidentes).
 - ✓ La atención de los cambios en sitio y/o remoto (Gestión de Cambios).
 - ✓ La atención e identificación de incidentes repetitivos (Gestión de Problemas).

✓ La atención de reportes bajo demanda de la Entidad.

- Ante una contingencia (interrupción parcial o total del servicio, así como a un decremento en la calidad del mismo) comunicada por la Entidad, el tiempo de respuesta por parte del Contratista deberá ser no mayor a treinta (30) minutos de lunes a viernes, las 24 horas del día y no mayor de cuarenta y cinco (45) minutos en los días no laborables, ello no exceptúa que el inicio de plazo para la solución de la contingencia o avería se establece a partir de la comunicación vía telefónica por parte de la Entidad.
- El tiempo máximo de subsanación de un evento o incidente, y que corresponde al tiempo transcurrido desde que El Instituto Geológico, Minero y Metalúrgico reporta la incidencia al Centro de Operaciones y Seguridad (SOC), que parte desde la asignación un ticket de atención a la Entidad, hasta la subsanación del evento a satisfacción del Instituto Geológico, Minero y Metalúrgico, será de cuatro (4) horas.
- En caso el Contratista tenga que escalar al fabricante algún evento o incidente que no puedan solucionar por tratarse de problemas que afecten al servicio, no aplicará el tiempo de subsanación de 4 horas y se esperará una propuesta de solución por el fabricante, debiendo el contratista informar periódicamente los avances de cada caso escalado con el fabricante.

PLAN DE TRABAJO

El Contratista deberá presentar un Plan de Trabajo y cronograma de actividades que se desarrollarán durante la ejecución del servicio, el mismo que deberá contener lo siguiente:

- Diseño y el cronograma detallado de las actividades que se realizarán para la implantación del servicio. El Contratista podrá realizar visitas técnicas in-situ antes de la presentación del diseño; las fechas y el horario para la visita in-situ será previa coordinación con la Oficina de Sistemas de Información.
- El Contratista deberá describir el detalle de las labores y procesos que empleará en la implementación, configuración, programación y puesta en marcha del servicio de seguridad gestionada. Así como también; el plan de trabajo deberá incluir la relación del personal técnico o profesional autorizado, la misma que de ser el caso deberá ser actualizada cuando se produzcan cambios y comunicada a la Entidad. Asimismo; el horario de labores en las instalaciones del Instituto Geológico, Minero y Metalúrgico, previa coordinación con la Oficina de Sistemas de Información.
- El Plan de Trabajo deberá ser remitido en un plazo máximo de diez (10) días calendario, contabilizados a partir del día siguiente de suscrita el Acta de Implementación del Servicio. El Plan de Trabajo será aprobado por la Oficina de Sistemas de Información en un plazo máximo de cinco (5) días calendario, que será contabilizado a partir del día siguiente de haber sido recepcionado el plan de trabajo en mesa de partes.

INFORMES TÉCNICOS

Informes de Implementación del Servicio

- El contratista deberá remitir tres (3) informes técnicos de implementación del servicio, cada treinta (30) días calendario, a mesa de partes del Instituto Geológico, Minero y Metalúrgico, dirigido a la Oficina de Sistemas de Información. El cual será contabilizado a partir del día siguiente de suscrita el Acta de Implementación del Servicio.
- El Primer y el Segundo Informe deberán contener los avances respectivos de las actividades relacionadas a la implementación del servicio. Es importante mencionar que; el Primer Informe deberá contener el levantamiento de la información inicial, el cual contendrá la arquitectura inicial, el inventario actualizado, los backups y/o snapshot de las configuraciones realizadas de las soluciones de seguridad del Instituto Geológico, Minero y Metalúrgico, la cual deberá ser entregada en formato impreso y/o digital.
- El Tercer Informe deberá contener el detalle final de los trabajos de diseño, instalación, configuración, incluyendo el sistema de atención y escalamiento de comunicaciones, así como también la puesta en marcha del servicio de seguridad gestionada, con la descripción del funcionamiento y consideraciones para la operatividad de los componentes y equipamiento de seguridad que forma parte de la contratación.
- Los informes técnicos de la implementación del servicio deberán ser remitidos en un plazo máximo de cinco (5) días calendario, una vez concluido el plazo para cada informe técnico de implementación (treinta (30) días calendario).

Informe Mensual

- El Contratista deberá remitir un (1) informe mensual del servicio vía mesa de partes del Instituto Geológico, Minero y Metalúrgico, dirigido a la Oficina de Sistemas de Información.
- Los informes mensuales del servicio de seguridad gestionada, deberá incluir como mínimo lo siguiente:
 - ✓ Presentación del consolidado del mes de eventos, incidentes y requerimientos del servicio de seguridad gestionada.
 - ✓ Presentación de la disponibilidad del servicio de seguridad gestionada durante el mes.
 - ✓ Presentación de incidentes y eventos, con la respectiva solución efectuada de todos los equipos que contempla el servicio de seguridad gestionada durante el mes.
 - ✓ Presentación en los informes mensuales sobre los respaldos realizados a las soluciones ofertadas.
 - ✓ Detalles de cambios en las configuraciones y políticas de los equipos efectuados en el mes.
 - ✓ Conclusiones y Recomendaciones.
- Previa coordinación con la Oficina de Sistemas de Información, se efectuará una reunión mensual de revisión del informe mensual, entre el Contratista y personal de la OSI.
- En caso de que el área usuaria solicite documentación adicional a los informes mensuales, el Contratista deberá remitir.
 - ✓ Información estadística de rendimiento de la atención de las solicitudes de cambios, las incidencias de averías y de la capacidad, el cual deberá ser entregado a solicitud del área usuaria.

- ✓ Informe Anual completo del Servicio Integral.
- ✓ Cualquier otro aspecto relacionado al servicio que sea solicitado por el área usuaria.
- Los informes técnicos mensuales, deberán ser remitidos en un plazo máximo de diez (10) días calendario, una vez finalizado el mes.
- Reunión mensual de seguimiento al servicio.

Informe de Incidencias

En caso de que el área usuaria solicite de forma particular un informe de incidencia, este deberá contener lo siguiente:

- Reportes de incidencias, ataques y fallas de la solución. Estos reportes deberán ser a nivel técnico y también a nivel ejecutivo.
- Reporte de la gestión realizada por cada incidente que se produzca que incluya: las medidas de contención y respuesta implementadas y el estado de recuperación de los servicios o activos.
- Reporte de análisis forense del incidente significativo adverso que identifique las causas y las medidas para su gestión si este fuera necesario.
- Al momento de la solución de una incidencia o avería, el Contratista deberá presentar un reporte preliminar, en un plazo máximo de cuatro (4) horas de ocurrido el incidente. El reporte preliminar deberá especificar el motivo que causó la avería y la solución ejecutada. El reporte preliminar será enviado vía correo electrónico al responsable de las coordinaciones, y deberá ser incluido en el informe mensual del servicio. Posterior a ello, y de ser solicitado por el área usuaria, el Contratista deberá presentar un informe detallado de la avería vía mesa de partes, el cual no deberá exceder las noventa y seis (96) horas luego de remitida la solicitud. Reportes de incidencias, ataques y fallas de la solución. Estos reportes deberán ser a nivel técnico y también a nivel ejecutivo.

Informe de estado de copias de respaldo de las soluciones

- El Contratista deberá contar con una copia de respaldo de la configuración de todos los equipos con una antigüedad mínima de quince (15) días calendarios, a fin de utilizarlos en caso de contingencia.

PLAZO DE EJECUCIÓN

Implementación del Servicio

El plazo máximo para la implementación del servicio será por sesenta (60) días calendario, contabilizados a partir del día siguiente de la firma del Acta de Implementación del Servicio, previa suscripción del Contrato, el mismo que será suscrito entre un (01) representante propuesto por el Contratista y un (01) representante de la Oficina de Sistemas de Información.

Ejecución del Servicio

El plazo de ejecución del servicio será por treinta y seis (36) meses, contabilizados a partir del día siguiente de finalizado los trabajos para la implementación del servicio, para lo cual se firmará el Acta de Inicio del Servicio, el mismo que será suscrito entre un (01) representante propuesto por el Contratista y un (01) representante de la Oficina de Sistemas de Información.

CONSIDERACIONES ESPECÍFICAS

DEL PERSONAL CLAVE

El personal clave que se requiere para la implementación y ejecución del servicio son los siguientes:

Un (1) Jefe del Proyecto

Formación Académica:

Un (1) Profesional Titulado en Ingeniería Electrónica o Ingeniería de Sistemas o Ingeniería Informática y de Sistemas o en Ingeniería de Cómputo y Sistemas o Ingeniería Informática o Ingeniería de Sistemas de Información o Ingeniería de Software, del personal clave requerido como Jefe de Proyecto.

Certificaciones:

El Jefe de Proyecto deberá contar con certificación de Project Management Professional (PMP) vigente e ITIL.

Importante: El ganador de la buena pro deberá presentar para la presentación de ofertas la certificación Project Management Professional (PMP) e ITIL en idioma español, o en su defecto acompañado de la traducción respectiva, emitido por traductor público juramentado o traductor colegiado certificado, según corresponda.

Experiencia:

Deberá contar con experiencia mínima de seis (6) años en Gestión de Proyectos de TI y/o Seguridad Gestionada, como Jefe o Gestor o Coordinador o Encargado o Gerente o Subgerente del personal requerido como Jefe del Proyecto.

Actividades a Desarrollar: Encargado de liderar, planificar, dirigir y realizar un seguimiento integral de los trabajos y actividades relacionadas a la implementación del servicio. El Jefe del Proyecto deberá representar al Contratista durante las coordinaciones correspondientes en la etapa de implementación. Será el encargado de la elaboración de los informes de Implementación del Servicio.

Un (1) Líder del CSIRT

Formación Académica:

Un (1) Profesional Titulado o Bachiller en Ingeniería Electrónica o Ingeniería de Sistemas o en Tecnologías de la Información o en Ingeniería de Cómputo y Sistemas o Ingeniería Informática o Ingeniería de Sistemas de Información o Ingeniería de Software, del personal clave requerido como Líder del CSIRT.

Certificaciones:

El Líder del CSIRT deberá contar con certificación de ISO/IEC 27032 Lead Cybersecurity Manager vigente.

Handwritten signature and initials in blue ink.

Importante: El ganador de la buena pro deberá presentar para la presentación de ofertas la certificación de Lead Cybersecurity Manager en idioma español, o en su defecto acompañado de la traducción respectiva, emitido por traductor público juramentado o traductor colegiado certificado, según corresponda.

Experiencia:

Deberá contar con experiencia mínima de cuatro (4) años en proyectos de plataformas de Seguridad, CyberSOC o Ciberseguridad o Servicio de Respuesta ante Incidentes, como Jefe o Líder o Coordinador del personal requerido como Líder del CSIRT.

Actividades a Desarrollar: Encargado de liderar el equipo de respuesta ante incidentes ante una amenaza que se haya detectado en la infraestructura de la entidad y se encargará de liderar las comunicaciones hacia la ENTIDAD en las reuniones de presentación de resultados donde se requiera tomar acciones para mitigar las amenazas.

Un (1) Líder del CyberSOC

Formación Académica:

Un (1) Profesional Titulado o Bachiller en Ingeniería Electrónica o en Telecomunicaciones o en Redes y Comunicaciones o Sistemas o en Tecnologías de la Información o en Cómputo y Sistemas o Informática o de Sistemas de Información o Ingeniería de Seguridad, del personal clave requerido como Líder del CyberSOC.

Certificaciones:

El Líder del CyberSOC deberá contar con certificación de Certified Information Systems Security Professional (CISSP) vigente.

Importante: El ganador de la buena pro deberá presentar para la presentación de ofertas la certificación de Certified Information Systems Security Professional (CISSP) en idioma español, o en su defecto acompañado de la traducción respectiva, emitido por traductor público juramentado o traductor colegiado certificado, según corresponda.

Experiencia:

Deberá contar con experiencia mínima de seis (6) años en servicios especializados de CyberSOC, Security Advisor o Ciberinteligencia como Especialista o Analista Técnico o Jefe o Líder, del personal requerido como Líder del CyberSOC.

Actividades a Desarrollar: Encargado de liderar el equipo de CyberSOC ante los incidentes críticos que se hayan detectado en la infraestructura de la entidad y se encargará de liderar las comunicaciones hacia la ENTIDAD en las reuniones de presentación de resultados donde se requiera tomar acciones para identificar y mitigar las amenazas o vulnerabilidades, así como participará en la presentación de recomendaciones y mejoras del servicio en caso se requiera.

6.3. GENERALIDADES DEL SERVICIO DE TELEFONÍA (ITEM 03)

CARACTERÍSTICAS GENERALES

1. El INGEMMET en su Sede Principal Av. Canadá N° 1470, San Borja, Lima-Perú, requiere contar con dos (02) enlaces SIP Trunk cada uno de 30 canales del tipo VoIP (voz sobre IP) para el servicio básico de telefonía digital que permita la comunicación o transferencia simultánea de voz. Los enlaces SIP Trunk deberán usar canalización y/o tendido aéreo por rutas distintas (no compartir tramos en común) desde cada PoP/Nodo del Contratista hasta llegar al punto de acceso de la Oficina Principal (Av. Canadá N° 1470, San Borja, Lima, Lima, Perú). Se aclara que enlaces SIP Trunk deberán trabajar en alta disponibilidad, considerando solo una cabecera. Adicionalmente, se solicita una bolsa de minutos o tarifa básica plana para llamadas locales, celulares, larga distancia nacional (LDN) y larga distancia internacional (LDI), como se indica en la Tabla N° 1-Bolsa de Minutos por Tipo de Llamadas. Se aclara el canalizado se refiere a la fibra óptica y/o tendido aéreo del contratista desde el nodo más cercano hasta el punto de entrada de la entidad.
2. El número de cabecera (primera línea) deberá permanecer invariable, a fin de no modificar el número telefónico principal del INGEMMET (la entidad solo cuenta con 01 DID (número principal) (01 6189800)) y la documentación impresa y virtual con la que se cuenta en la entidad, apelando a la Ley N° 29956, Ley que establece el derecho de Portabilidad Numérica en los servicios de telefonía fija. Actualmente los trámites de portabilidad se realizan con mayor rapidez, en caso ello sea necesario efectuar. Por ello, la implementación del servicio de telefonía será contabilizada a partir de la confirmación de la factibilidad técnica correspondiente a la portabilidad numérica del contratista, suponiendo que dichos trámites se efectúen con una anticipación razonable.
3. No habrá cobro por establecimiento de llamadas (cobro de minuto por conexión)
4. No habrá cobro por redondeo de llamadas a fijos locales, celulares (local y nacional), larga distancia nacional (fijo y celular) e internacional (fijo y celular). El cobro deberá ser al segundo para fijos locales, celulares (local y nacional), larga distancia nacional (fijo y celular) e internacional (fijo y celular).
5. El postor deberá contar como mínimo con un portal web que permita:
 - o Visualizar gráficamente en línea las llamadas entrantes y salientes, llamadas de entrada sin responder, llamadas entrantes respondidas. La información del dashboard deberá actualizarse al menos cada hora.
 - o Reporte de llamadas entrantes y salientes, detallando como mínimo tipo de llamada (entrante, saliente), origen, destino, fecha y hora, duración de la llamada. Dicho reporte deberá poder extraerse por rango de fechas (incluyendo las llamadas finalizadas al momento de generar el reporte). La información deberá tener un tiempo de permanencia de al menos 3 meses.
 - o Deberá permitir descargar los reportes en formatos compatibles con EXCEL y/o PDF.

6. El INGEMMET administra y cuenta con una central telefónica (AVAYA modelo IP Office 500 Server Edition) que tiene dos (02) enlaces IP SIP. Se aclara que se tiene 337 extensiones.
7. El contratista brindará un sistema de tarificación que mantenga una conversación con nuestra Central Telefónica. El sistema permitirá la identificación de llamadas realizadas por anexo y por código de llamadas, de forma tal que los montos unitarios y globales por llamadas efectuados en el INGEMMET deberán coincidir con el facturado por el contratista que brinde el servicio con una aproximación de un +/- 5%. Ello garantizará que los mencionados cobros se pueden sustentar mediante los respectivos reportes que el sistema de tarificación ofrece. La solución de tarificación será administrada por la entidad.
8. El Sistema de Tarificación deberá ser implementado en un Centro de Datos del tipo TIER III certificado por Uptime Institute, siendo el postor quien provea el hardware con Sistema Operativo necesario para la instalación del sistema de tarificación a ofertar por el contratista. Cabe precisar que el sistema de tarificación es una solución de software, a ser instalado en un hardware y sistema operativo. El dimensionamiento del hardware (servidor físico y/o virtual) así como del sistema operativo necesario será responsabilidad del postor. El software y licencia de base de datos será brindado por el contratista, en caso instale una versión de SQL SERVER EXPRESS, el contratista debe revisar el tamaño de las bases de datos constantemente para evitar que llegue al tamaño máximo y evite la pérdida de información, asimismo debe realizar el mantenimiento y configuración de una nueva base de datos manteniendo la BD Histórica.
9. El sistema de tarificación deberá ser administrado por personal de INGEMMET, permitiendo generación de reportes y consultas.
10. No permitirá la consideración de llamadas efectivas por timbrados o repiques sin respuesta. El costo por los timbrados o repiques deberá siempre ser nulo.
11. No permitirá la consideración de cobro por establecimiento de llamadas.
12. Se permitirá el acceso gratuito a los servicios de emergencia.
13. A continuación, se muestra la bolsa de minutos que se debe considerar como tarifa básica (cargo fijo mensual):

Tabla N° 1 - Bolsa de Minutos Mensual por Tipo de Llamadas

N°	Tipo de Llamadas	Unidad de medida	Cantidad
1	Instalación de 02 enlaces Trunk SIP	Unidad	02
2	Llamadas Fijo - Fijo Local	Minutos	3,000
3	Llamadas Fijo - Fijo Nacional	Minutos	500
4	Llamadas Fijo - Rural Nacional	Minutos	500
5	Llamadas Fijo - Fijo Internacional	Minutos	75
6	Llamadas Fijo - Celular Internacional	Minutos	75
7	Llamadas Fijo - Celular local y nacional	Minutos	4,000

14. Servicio sin restricciones de bloqueo para ningún tipo de destino definido en el cuadro de bolsas a contratar. Caso contrario deberá ser solicitado expresamente por el INGEMMET a través del área responsable del servicio.
15. En caso de superar el consumo de la bolsa de minutos mensual indicada en la Tabla N° 01, durante el tiempo de ejecución del contrato, este excedente no será facturado a INGEMMET.

SERVICIO DE TELEFONÍA LOCAL

El servicio a contratar deberá cumplir con las siguientes características técnicas mínimas:

1. Para las troncales IP el tipo de señalización deberá ser: VOIP (SIP)
2. El medio de acceso de última milla deberá ser a través de fibra óptica (canalizada y subterránea y/o aérea en lo que respecta a planta externa y totalmente canalizada en los interiores del INGEMMET con ruta hasta el Cuarto de Equipos o Datacenter). Cada enlace SIP Trunk deberá tener cable de fibra óptica independiente, los cuales deberán partir de nodos distintos y por rutas distintas.
3. Cabeceras de números colectivos (Hunting), que permita acceder a un grupo de líneas de usuarios (canales de voz), con un sólo número principal,
4. Cada enlace SIP Trunk de 30 canales de 64 Kbps para comunicaciones simultáneas de voz.
5. La cabecera actual deberá permanecer invariable, acorde a lo dispuesto por Ley N° 29956.
6. Se deberá considerar un horario único de 24 horas para el tráfico de llamadas.
7. Permitir la interconexión con otros operadores de telefonía fija y móvil en todo el Perú.
8. Identificación de la llamada entrante.
9. Servicio de facturación detallada de las conexiones o llamadas salientes, así como los minutos reales consumidos en forma mensual, los que deberán llegar por correo electrónico o mediante Ventanilla Virtual a través del siguiente link (<https://www.gob.pe/12519-acceder-a-laventanilla-virtual-del-ingemmet>). En el horario de 00.00 hasta las 23.59 horas, en formato MS Excel, lo que permitirá a la entidad analizar sus consumos de manera detallada por cada DID, donde se detalle sus consumos llamada por llamada. Se aclara que los detalles de consumo se entregarán dentro de los siete (07) días calendario después de su emisión. Se aclara que el plazo de siete días inicia con la "emisión" de la factura. Se aclara que el reporte debe de tener los siguientes campos:
 - Teléfono de Origen y teléfono de Destino, Servicio, Hora Inicial y hora final, Minutos, Tarifa, Monto, Operador
10. Permitir la interconexión con otros operadores telefonía fija a nivel local.
11. Servicio Técnico las 24 horas del día dentro del plazo contractual respectivo, incluyendo días feriados y/o fines de semana.

HACIA LOS SERVICIOS DE TELEFONIA CELULAR

El servicio a contratar deberá cumplir con las siguientes características técnicas mínimas:

1. Se deberá considerar un horario único de 24 horas para el tráfico de llamadas.
2. Permitir la interconexión con otros operadores telefonía móvil en todo el Perú.
3. Servicio de facturación detallada de las conexiones o llamadas salientes, así como los minutos reales consumidos en forma mensual, los que deberán llegar por correo electrónico o Ventanilla Virtual a través del siguiente link (<https://www.gob.pe/12519-acceder-a-laventanilla-virtual-del-ingemmet>). En el horario de 00.00 hasta las 23.59 horas, y en formato MS Excel, lo que permitirá a la entidad analizar sus consumos de manera detallada por cada DID, donde se detalle sus consumos llamada por llamada. Se aclara que los detalles de consumo se entregarán dentro de los siete (07) días calendario después de su emisión.
4. Servicio Técnico las 24 horas del día dentro del plazo contractual respectivo, incluyendo días feriados y/o fines de semana.
5. La propuesta deberá considerar una tarifa única para destinos móviles de todo el Perú.

6. El servicio debe brindar la posibilidad de restringir las llamadas a teléfonos celulares en general (locales, nacionales e internacionales) a petición de la entidad.

SERVICIO DE TELEFONÍA LARGA DISTANCIA NACIONAL, RURAL Y OTROS TIPOS DE LLAMADAS DE TELEFONÍA

El servicio de troncal VoIP a contratar deberá cumplir con las siguientes características técnicas mínimas:

1. Se deberá considerar un horario único de 24 horas para el tráfico de llamadas.
2. Permitir la interconexión con otros operadores de telefonía fija y móvil en todas las provincias del Perú.
3. Servicio de facturación detallada de las conexiones o llamadas salientes, así como los minutos reales consumidos en forma mensual, los que deberán llegar por correo electrónico a Ventanilla Virtual a través del siguiente link (<https://www.gob.pe/12519-acceder-a-laventanilla-virtual-del-ingemmet>). En el horario de 00.00 hasta las 23.59 horas, y en formato MS Excel, lo que permitirá a la entidad analizar sus consumos de manera detallada por cada DID, donde se detalle sus consumos llamada por llamada.
4. Servicio Técnico las 24 horas del día dentro del plazo contractual respectivo, incluyendo días feriados y/o fines de semana.

SERVICIO DE TELEFONÍA LARGA DISTANCIA INTERNACIONAL

El servicio de troncal VoIP a contratar deberá cumplir con las siguientes características técnicas mínimas:

1. Brindará un código de seguridad para efectuar llamadas con destino internacional. Este código será coordinado con la entidad.
2. Bloqueo de las llamadas LDI a pedido de la entidad.
3. Se deberá considerar un horario único de 24 horas para el tráfico de llamadas.
4. Permitir la interconexión con otros operadores de telefonía fija y móvil en otros países.
5. Servicio de facturación detallada de las conexiones o llamadas salientes, así como los minutos reales consumidos en forma mensual, los que deberán llegar por correo electrónico a Ventanilla Virtual a través del siguiente link (<https://www.gob.pe/12519-acceder-a-laventanilla-virtual-del-ingemmet>). En el horario de 00.00 hasta las 23.59 horas, y en formato MS Excel, lo que permitirá a la entidad analizar sus consumos de manera detallada por cada DID, donde se detalle sus consumos llamada por llamada y verificar el cumplimiento del servicio al 100%.
6. Servicio Técnico las 24 horas del día dentro del plazo contractual respectivo, incluyendo días feriados y/o fines de semana.

ACUERDOS DE NIVEL DE SERVICIO- SLA

1. El servicio deberá estar disponible las veinticuatro (24) horas del día, los siete (07) días de la semana, los 12 meses del año, mientras dure la ejecución del servicio. La disponibilidad del servicio ofrecido deberá de ser de 99.5% mensual, caso contrario el INGEMMET considerara caída del servicio y aplicará las penalidades y sanciones correspondientes, siempre y cuando éstas sean imputables al contratista, este exime a causas ajenas al mismo siempre y cuando se demuestre previa verificación por la entidad, se aclara que el tiempo de respuesta será de dos (02) horas desde que la entidad comunica el incidente al NOC del contratista hasta

- la entrega del ticket de atención y se realizara los primeros descartes del incidente y se aclara que el tiempo de solución de un incidente crítico será de cuatro (04) horas contabilizados desde la entrega del ticket de atención. Se aclara que la atención para el tarifador será de cuatro (04) horas para incidentes críticos y de seis (06) horas para las atenciones no críticas.
2. El contratista del servicio solicitado deberá coordinar con el contratista actual, a fin de que el tiempo de interrupción de dichos servicios sea mínimo (desconexión lógica y/o retiro de equipos alquilados). El INGEMMET necesita que los servicios de Internet y telefonía no sean interrumpidos, o que la interrupción sea la mínima posible, contabilizado en unidades de tiempo de minutos solamente (inferior a una hora efectiva) fuera de horario de oficina.
 3. Toda actividad o provisión de bienes que tenga que ejecutar el contratista del servicio para subsanar una avería será sin costo alguno para el INGEMMET, siempre y cuando no sea responsabilidad de la entidad.

INSTALACIÓN, PRUEBAS

5. El contratista deberá ejecutar la instalación de los equipos, materiales, accesorios y todo lo necesario, a fin de dejar completamente habilitado la prestación del servicio a entera satisfacción del INGEMMET.
6. Cualquier trabajo de cableado estructurado (puntos de red), Puertos RJ45 disponibles y habilitados en sus equipos de la red LAN para la conexión con los equipos que implementará El Contratista, el cual debe de usar categoría 6 y certificada, colocando los equipos en un mismo gabinete, y debe considerar todos los patch cords necesarios para la interconexión de sus equipos.
7. El INGEMMET, para la realización de trabajos de implementación dentro de las instalaciones de la entidad, brindará al contratista todos los accesos necesarios, siendo la Entidad responsable de las autorizaciones de ingreso, desocupar los espacios, oficinas, pasillos y demás ambientes donde se realizarán los trabajos de instalación siempre y cuando las coordinaciones sean efectuadas con anticipación y acorde a lo indicado en el Plan de Trabajo. La Entidad velará por el cumplimiento de dicho Plan de Trabajo para su realización sin contratiempos.
8. El contratista y el INGEMMET realizarán de manera conjunta los procedimientos de inspección y pruebas de desempeño del servicio en la sede central antes que el servicio sea aceptado en forma definitiva.

OBLIGACIONES QUE DEBE CUMPLIR EL PROVEEDOR

5. Se aclara que el personal del contratista que realizará la implementación deberá tener seguro SCTR, equipamiento de seguridad (Según Norma G.050 —Seguridad durante la Construcción) y certificado médico para trabajo en altura de ser necesario, esta documentación deberá ser presentada al inicio de la implementación del servicio.
6. El periodo de garantía para TODO el servicio será de treinta y seis (36) meses y se cuenta a partir del día siguiente de la fecha de recepción y aceptación de la implementación.
7. Será de total y exclusiva responsabilidad del contratista contemplar todas las actividades, dispositivos, componentes, accesorios y materiales para la correcta instalación de los elementos necesarios para brindar el servicio.
8. El soporte y licencias de los equipos ofrecidos por el contratista tienen que tener vigencia por el tiempo de operatividad desde la puesta en marcha hasta el final del plazo de ejecución del contrato.

REQUERIMIENTOS DEL CONTRATISTA

Empresa natural o jurídica dedicada a servicios en telecomunicaciones y/o transmisión de voz y datos.

- e) El Postor deberá contar con el servicio de soporte técnico en modalidad telefónica, el alcance será de tráfico local y de larga distancia nacional y líneas móviles que permitan a los usuarios, llamar al postor sin limitación alguna.

En caso de ser propio, se acreditará mediante el contrato con una empresa de telecomunicaciones del servicio ofertado, con una antigüedad por un periodo no menor a tres (03) años consecutivos, donde se evidencie el alcance de llamadas de tráfico local y de larga distancia nacional, sin restricción de líneas tups y líneas móviles, para la presentación de la oferta.

En caso de ser alquilado, se acreditará mediante el contrato con una empresa que cumpla con tener el servicio en las condiciones requeridas, para la presentación de la oferta.

- f) El Postor deberá contar con una mesa de ayuda en línea o software de administración de soporte de servicios de TI basado en ITIL, cumpliendo de esa manera con el conjunto de conceptos y buenas prácticas usadas para la gestión de servicios de tecnologías de la información, asimismo, el software de gestión del servicio deberá ser CLOUD (servicio en la nube), además evidenciará el uso del software de mesa de ayuda propuesta por un periodo no menor a tres (03) años (podrá ser propio o alquilado).

En caso de ser propio, se acreditará mediante carta del propietario del software donde se evidencie la fecha de inicio de autorización del uso del software de la plataforma ofertada y la renovación anual para acreditar la continuidad del uso del software de mesa de ayuda, para la presentación de la oferta.

En caso de ser alquilado, se acreditará mediante el contrato con una empresa que cumpla con tener el servicio en las condiciones requeridas, para la presentación de la oferta.

- g) La mesa de ayuda en línea o software de administración de soporte de servicios de TI basado en ITIL ofertada por el Postor, , por ende, cumplir con las buenas prácticas usadas para la gestión de servicios de tecnologías de la información, su inclusión deberá ser por tres (03) años de manera consecutiva (2019, 2020, 2021 o 2020, 2021, 2022 o 2021, 2022, 2023 o 2022, 2023, 2024).

Se acreditará mediante el ID y la fecha de publicación respectiva, para la presentación de la oferta.

- h) La mesa de ayuda en línea o software de administración de soporte de servicios de TI basado en ITIL ofertada por el Postor, deberá facilitar los métodos para migrar datos y servicios de o desde la nube, de forma automática o manualmente por el usuario. Deberá cumplir como mínimo con la opción de las siguientes funcionalidades o servicios disponibles:

- o Compatible con Sistemas Operativos: Windows, Linux.
- o Escritorio remoto compartido.
- o Aplicación móvil para Android y iOS
- o Compatible con bases de datos: PostgreSQL, MySQL, MS SQL.
- o Informes Personalizables: Exportar como CSV, XLS, PDF.
- o Gestión de incidentes, Gestión de SLA.
- o Envío automático de tickets.
- o Conversión automática de email a ticket.
- o Integración con Active Director.
- o Importación desde archivos CSV.

- Historial completo de solicitudes.
- Soporte multi sitio.

Se acreditará mediante el link que permita validar los servicios disponibles, para la presentación de la oferta

PERSONAL CLAVE

Se podrá utilizar el mismo personal clave para el ITEM 1 y el ITEM 3.

UN (01) COORDINADOR DE PROYECTO	
Funciones	Será el encargado de llevar la gestión del proyecto y/o la implementación, configuración, mantenimiento soporte y gestión de las soluciones propuestas para el INGEMMET, además coordinará con el personal de la Oficina de Sistemas de Información.
Perfil Profesional	El Coordinador de Proyecto para la provisión del servicio deberá ser un profesional titulado en las carreras de Ingeniería Electrónica y/o Eléctrica y/o Sistemas y/o Telecomunicaciones y/o Ingeniería Informática y/o Computación y sistemas y/o Redes y Comunicaciones y/o Ingeniería de software y/o Ingeniería de Sistemas y Computo.
Capacitación	Certificado PMP y/o Curso y/o Taller y/o Diplomado en Gestión o Gerencia de Proyectos y/o bajo enfoque PMI y/o Diplomatura de Especialización Avanzada en Gerencia de Proyectos y Calidad. En el caso de los cursos y/ Taller y/o diplomado y/o diplomaturas deberá ser con una duración mínima de 32 horas lectivas o académicas.
UN (01) ESPECIALISTA TI: ENCARGADO DE LA INSTALACIÓN Y CONFIGURACIÓN	
Funciones	Encargado de la instalación y puesta en producción de la solución requerida que contempla la migración de la información de los equipos que tiene la Institución.
Perfil Profesional	Profesional Técnico y/o bachiller Titulado en Ing. de Sistemas y/o Electrónico y/o Redes y Comunicaciones y/o Empresarial y de Sistemas y/o Computación y de Sistemas y/o Telecomunicaciones y Redes y/o Estadística e Informática.
Capacitación	Certificación técnica en solución de routers o conectividad o telefonía o en centro de datos
UN (01) ESPECIALISTA HELP DESK	
Funciones	Encargado de la supervisión y correcto flujo de la asistencia técnica de los tickets generados para soporte técnico.

Perfil Profesional	Profesional titulado y/o Bachiller en Ingeniería Electrónica y/o Ingeniería de Telecomunicaciones y/o Ingeniería de Sistemas y/o Ingeniería Mecatrónica y/o Ingeniería Informática y/o Ingeniería de computación.
Capacitación	Deberá contar con certificación de gestión ITIL® 4, con una duración mínima de 30 horas.

ENTREGABLES

PRIMER ENTREGABLE- PLAN DE TRABAJO:

El contratista deberá de presentar un plan de trabajo que contemple la estrategia para cumplir con lo solicitado en los términos de referencia. Este plan deberá ser presentado por el contratista adjudicado con la buena pro como máximo a los diez (10) días calendario de firmado el contrato y deberá de contener lo siguiente puntos:

- Listado general de recursos a utilizarse en la solución.
- Diagrama referencial de la arquitectura del servicio de telefonía (Tarificador) con Central Telefónica de la entidad.
- Cronograma de las actividades.

El plan de trabajo deberá ser aprobado mediante correo electrónico máximo 05 días por la Oficina de Sistemas e Información, para dar inicio a la implementación del servicio.

SEGUNDO ENTREGABLE- FIN DE LA IMPLEMENTACION:

El contratista deberá entregar al INGEMMET, el informe final del proyecto donde se indique todo lo realizado, configuraciones y deberá presentarse al final de la configuración del servicio. Dicho informe deberá ser firmado por el Coordinador de Proyecto y deberá contener como mínimo lo siguiente:

- Descripción de la arquitectura implementada y diagrama de la Solución.
- Configuración de equipos instalados (parámetros de configuración).
- Implementación, configuración, integración y pruebas operativas con la Central Telefónica de la Entidad.
- Información de contactos para el reporte, atención de averías y escalamiento de solicitudes para el cumplimiento de los SLAs (Acuerdo de Niveles de Servicio), el cual debe incluir como mínimo: números de central telefónica y correo electrónico. Se aclara que la información de contactos debe hacer mención o indicar las áreas correspondientes con sus respectivos números telefónicos para su atención.

ENTREGABLE MENSUAL

El contratista deberá entregar un Informe mensual reportando las incidencias y consumos mensuales, estadísticas de uso y otros indicadores de gestión, Este informe deberá ser presentado por el contratista adjudicado con la buena pro como máximo a los diez (10) días calendario de culminado el mes del servicio y debe contener como mínimo la siguiente documentación:

- Reporte de llamadas entrantes y salientes, detallando como mínimo tipo de

- llamada (entrante, saliente), origen, destino, fecha y hora, duración de la llamada.
b) Estadísticas de los números más llamados
c) Opcionalmente, estadísticas de los anexos con mayor flujo de llamadas.

PLAZO DE EJECUCIÓN

IMPLEMENTACIÓN

Para la implementación de la puesta en operación de los servicios requeridos (obras civiles, canalización y/o tendido aéreo del cableado de fibra óptica en planta externa, canalización interna de la fibra óptica, conectorización de los hilos de fibra óptica, instalación de equipos especializados de comunicación propiedad del contratista, así como pruebas de conectividad física y lógica, el tiempo máximo estimado será de sesenta (60) días calendario, a partir del día siguiente de la aceptación del plan de trabajo.

N°	CONCEPTO	PLAZO
1	Plan de trabajo y cronograma de las actividades de la implementación del servicio	Hasta los diez (10) días calendarios contados a partir del día siguiente de la firma del contrato
2	Informe sobre la implementación del servicio	Hasta los sesenta (60) días calendarios contados a partir del día siguiente de la aceptación del plan de trabajo

PRESTACIÓN DEL SERVICIO

Se establece que el plazo contractual de la prestación será treinta y seis (36) meses, se iniciará terminada la etapa de la implementación de todas las comunicaciones de la Sede Principal (Av. Canadá 1470, Lima-Perú), para lo cual se suscribirá un Acta de implementación del servicio. Se aclara que el servicio comenzará a ser contabilizado a partir del día siguiente de suscrita el Acta de Conformidad del Servicio.

N°	CONCEPTO	PLAZO
1	Informe mensual de Operación de servicio contratado	Hasta los siete (07) días calendarios de culminado el servicio de cada mes. Se contabilizará a partir del día siguiente de la firma del Acta de implementación del servicio, durante el periodo de tiempo contratado.

LUGAR DE LA PRESTACIÓN

El servicio se llevará a cabo en las instalaciones del INGEMMET en su Sede Canadá (sito en Av. Canadá N° 1470 – San Borja, Lima-Perú)

FORMA DE PAGO

Se realizará en treinta y seis (36) pagos periódicos mensual, y será efectuada previa Conformidad, con una facturación diferenciada por cada ítem mencionado. El pago del servicio es a todo costo e incluye todos los impuestos de ley. Los costos de la

implementación deberán ser considerados dentro de los pagos del servicio mensual. No se realizarán pagos por la implementación.

La empresa contratista deberá emitir factura por un monto fijo mensual durante todo el período del servicio. La Entidad no reconocerá pagos adicionales por consumos realizados fuera de la bolsa contratada. Para efectos del pago de las contraprestaciones ejecutadas por el contratista, la Entidad debe contar con la siguiente documentación:

- Entregable mensual de telefonía
- Comprobante de pago.

Dicha documentación se debe presentar mediante los siguientes canales en el horario establecido en la página web del INGEMMET:

- ✓ Mesa de Partes de la Sede Canadá del INGEMMET, ubicada en la Av. Canadá N° 1470 –San Borja– en el horario de 8:00 a 16:30.
- ✓ Ventanilla Virtual a través del siguiente link (<https://www.gob.pe/12519-acceder-a-laventanilla-virtual-del-ingemmet>). En el horario de 00.00 hasta las 23.59 horas

CONFORMIDAD

La conformidad del Servicio será otorgada por la Oficina de Sistemas de Información, la misma que deberá ser otorgada en un plazo máximo de siete (07) días calendarios, de acuerdo con lo indicado en el Artículo 168 del Reglamento de la Ley de Contrataciones del Estado.

PENALIDADES

PENALIDAD POR MORA

Si el contratista no cumple con las actividades encomendadas dentro del plazo estipulado, la Entidad le aplicará una penalidad por cada día de atraso hasta por un monto máximo equivalente al 10% del monto del contrato. La penalidad se aplicará automáticamente y se calculará de acuerdo a la siguiente fórmula:

$$\text{Penalidad diaria} = \frac{0.10 \times \text{Monto}}{F \times \text{Plazo en días}}$$

- Para plazos menores o iguales a 60 días $F=0.40$
- Para plazos mayores a 60 días $F=0.25$

La Entidad tiene derecho para exigir, además de la penalidad, el cumplimiento de la obligación.

OTRAS PENALIDADES

Serán evaluadas durante cada mes de la prestación del servicio y aplicadas según el caso cuando el contratista incurra en falta, se utilizará lo establecido en el siguiente cuadro.

N°	Supuestos de aplicación de penalidad	Forma de calculo
1	Cuando el contratista supera los 7 días para una configuración y/o reconfiguración solicitada por la entidad, se aclara que se refiera a horas de configuración y/o configuración solicitada para la entidad para cambios simples.	3 % del monto de la facturación mensual del servicio contratado
2	Cuando el contratista supere las 12 horas para restablecer la disponibilidad de la telefonía ante una caída de la misma.	3 % del monto de la facturación mensual del servicio contratado
3	Cuando la no disponibilidad de la telefonía supere las seis (06) horas	5 % del monto de la facturación mensual del servicio contratado

Procedimiento

- Informe a la Oficina de Sistemas de Información, indicando la ocurrencia, desde reportado el incidente.
- La Oficina de Sistemas de Información tendrá el informe del proveedor sobre la incidencia y en base a ello evaluará la responsabilidad.
- Enviar documento a la Unidad de Logística indicando la ocurrencia y el incidente para que sea notificado al proveedor.

PLAZO DE RESPONSABILIDAD DEL CONTRATISTA

La conformidad del servicio por parte del INGEMMET no enerva su derecho a reclamar posteriormente por defectos o vicios ocultos, conforme a lo dispuesto por el artículo 40° de la Ley de Contrataciones del Estado. En tal sentido el plazo de responsabilidad del contratista es no menor de tres (03) años, computado un día después de otorgada la conformidad por parte de la entidad.

REQUISITOS DE CALIFICACIÓN

A	CAPACIDAD LEGAL
	HABILITACIÓN
	<u>Ítem 1 – Servicio de Internet corporativo</u>
	<p><u>Requisitos:</u></p> <p>Deberá contar con la autorización o registro del Ministerio de Transportes y Comunicaciones (MTC) para brindar los servicios de Internet y Transmisión de Datos</p> <hr/> <p>Importante De conformidad con la Opinión N°186-2016/DTN, la habilitación de un contratista, está relacionada con cierta atribución con la cual debe contar el contratista 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</p>

	<p><u>Acreditación:</u></p> <ul style="list-style-type: none"> • El contratista deberá tener autorización emitida por el Ministerio de Transportes y Comunicaciones para brindar servicios de Telecomunicaciones en el Perú, en la modalidad Internet Service Provider – ISP. • El proveedor deberá estar en el registro vigente de empresas prestadoras de servicios de valor añadido del Ministerio de Transportes y Comunicaciones, en el rubro de Conmutación de Datos por Paquetes (Internet). <p><u>Importante</u> 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.</p> <p><u>Ítem 03- Servicio de telefonía</u></p> <p><u>Requisitos:</u></p> <p>El contratista del servicio deberá evidenciar registro y/o autorización y/o concesión del Ministerio de Transportes y Comunicaciones para el servicio de telefonía fija local y/o certificado de inscripción de registro de comercializadores de la concesión general de concesiones, para comercializar el servicio de telefonía fija local y servicio de telefonía larga distancia nacional e internacional a nivel nacional</p> <p><u>Importante</u> De conformidad con la Opinión N°186-2016/DTN, la habilitación de un contratista, está relacionada con cierta atribución con la cual debe contar el contratista 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</p> <p><u>Acreditación:</u></p> <ul style="list-style-type: none"> • El contratista deberá tener autorización emitida por el Ministerio de Transportes y Comunicaciones para brindar servicios de Telecomunicaciones en el Perú, en la modalidad Internet Service Provider – ISP. • El proveedor deberá estar en el registro vigente de empresas prestadoras de servicios de valor añadido del Ministerio de Transportes y Comunicaciones, en el rubro de Conmutación de Datos por Paquetes (Internet). <p><u>Importante</u> 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.</p>
B	CAPACIDAD TÉCNICA Y PROFESIONAL
B.3	CALIFICACIONES DEL PERSONAL CLAVE

B.3. 1	FORMACIÓN ACADÉMICA
	<p><u>Ítem 01</u></p> <p><u>Requisitos:</u></p> <p>Un (01) Coordinador de Proyecto El Coordinador de Proyecto para la provisión del servicio deberá ser un profesional titulado en las carreras de Ingeniería Electrónica y/o Eléctrica y/o Sistemas y/o Telecomunicaciones y/o Ingeniería Informática y/o Computación y sistemas y/o Redes y Comunicaciones y/o Ingeniería de software y/o Ingeniería de Sistemas y Computo.</p> <p>Un (01) Especialista TI: Encargado de la Instalación y Configuración Profesional Técnico y/o bachiller Titulado en Ing. de Sistemas y/o Electrónico y/o Redes y Comunicaciones y/o Empresarial y de Sistemas y/o Computación y de Sistemas y/o Telecomunicaciones y Redes y/o Estadística e Informática.</p> <p>Un (01) Especialista Help Desk Profesional titulado y/o Bachiller en Ingeniería Electrónica y/o Ingeniería de Telecomunicaciones y/o Ingeniería de Sistemas y/o Ingeniería Mecatrónica y/o Ingeniería Informática y/o Ingeniería de computación.</p> <p><u>Acreditación:</u> El título profesional y/o técnico y/o grado de bachiller 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.</p> <p>En caso el título profesional y/o técnico y/o grado de bachiller no se encuentre inscrito en el referido registro, el contratista debe presentar la copia del diploma respectivo a fin de acreditar la formación académica requerida.</p> <p><u>Ítem 02</u></p> <p>DEL PERSONAL CLAVE</p> <p>El personal clave que se requiere para la implementación y ejecución del servicio son los siguientes:</p> <p>Un (1) jefe del Proyecto</p> <p><u>Formación Académica:</u></p> <p>Un (1) Profesional Titulado en Ingeniería Electrónica o Ingeniería de Sistemas o Ingeniería Informática y de Sistemas o en Ingeniería de Cómputo y Sistemas o Ingeniería Informática o Ingeniería de Sistemas de Información o Ingeniería de Software, del personal clave requerido como Jefe de Proyecto</p>

Un (1) Líder del CSIRT

Formación Académica:

Un (1) Profesional Titulado o Bachiller en Ingeniería Electrónica o Ingeniería de Sistemas o en Tecnologías de la Información o en Ingeniería de Cómputo y Sistemas o Ingeniería Informática o Ingeniería de Sistemas de Información o Ingeniería de Software, del personal clave requerido como Líder del CSIRT.

Un (1) Líder del CyberSOC

Formación Académica:

Un (1) Profesional Titulado o Bachiller en Ingeniería Electrónica o en Telecomunicaciones o en Redes y Comunicaciones o Sistemas o en Tecnologías de la Información o en Cómputo y Sistemas o Informática o de Sistemas de Información o Ingeniería de Seguridad, del personal clave requerido como Líder del CyberSOC.

Ítem 03

Requisitos:

Un (01) Coordinador de Proyecto

El Coordinador de Proyecto para la provisión del servicio deberá ser un profesional titulado en las carreras de Ingeniería Electrónica y/o Eléctrica y/o Sistemas y/o Telecomunicaciones y/o Ingeniería Informática y/o Computación y sistemas y/o Redes y Comunicaciones y/o Ingeniería de software y/o Ingeniería de Sistemas y Computo.

Un (01) Especialista TI: Encargado de la Instalación y Configuración
Profesional Técnico y/o bachiller Titulado en Ing. de Sistemas y/o Electrónico y/o Redes y Comunicaciones y/o Empresarial y de Sistemas y/o Computación y de Sistemas y/o Telecomunicaciones y Redes y/o Estadística e Informática.

Un (01) Especialista Help Desk

Profesional titulado y/o Bachiller en Ingeniería Electrónica y/o Ingeniería de Telecomunicaciones y/o Ingeniería de Sistemas y/o Ingeniería Mecatrónica y/o Ingeniería Informática y/o Ingeniería de computación.

Acreditación:

El título profesional y/o técnico y/o grado de bachiller 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 el título profesional y/o técnico y/o grado de bachiller no se encuentre inscrito en el referido registro, el contratista debe presentar la copia del diploma respectivo a fin de acreditar la formación académica requerida.
B.3. 2	CAPACITACIÓN
	<p><u>Ítem 01</u></p> <p><u>Requisitos:</u></p> <p>Un (01) Coordinador de Proyecto Certificado PMP y/o Curso y/o Taller y/o Diplomado en Gestión o Gerencia de Proyectos y/o bajo enfoque PMI y/o Diplomatura de Especialización Avanzada en Gerencia de Proyectos y Calidad. En el caso de los cursos y/o Taller y/o diplomado y/o diplomaturas deberá ser con una duración mínima de 32 horas lectivas o académicas.</p> <p>Un (01) Especialista TI: Encargado de la Instalación y Configuración Certificación técnica en solución de routers o conectividad o telefonía o en centro de datos</p> <p>Un (01) Especialista Help Desk Deberá contar con certificación de gestión ITIL® 4, con una duración mínima de 30 horas.</p> <p><u>Importante:</u> Se acreditará la capacitación mediante certificados de estudios de postgrado, considerando que cada crédito del curso que acredita la capacitación equivale a dieciséis horas lectivas, según la normativa de la materia.</p> <p><u>Ítem 02</u></p> <p>Un (1) jefe del Proyecto</p> <p><u>Certificaciones:</u> El Jefe de Proyecto deberá contar con certificación de Project Management Professional (PMP) vigente e ITIL.</p> <p><i><u>Importante:</u> Se deberá presentar para la presentación de ofertas la certificación Project Management Professional (PMP) e ITIL en idioma español, o en su defecto acompañado de la traducción respectiva, emitido por traductor público juramentado o traductor colegiado certificado, según corresponda.</i></p> <p>Un (1) Líder del CSIRT</p> <p><u>Certificaciones:</u> El Líder del CSIRT deberá contar con certificación de ISO/IEC 27032 Lead Cybersecurity Manager vigente.</p> <p><i><u>Importante:</u> Se deberá presentar para la presentación de ofertas la certificación de Lead Cybersecurity Manager en idioma español, o en su defecto acompañado de la traducción respectiva, emitido por</i></p>

	<p><i>traductor público juramentado o traductor colegiado certificado, según corresponda.</i></p> <p>Un (1) Líder del CyberSOC</p> <p><u>Certificaciones:</u> El Líder del CyberSOC deberá contar con certificación de Certified Information Systems Security Professional (CISSP) vigente.</p> <p><i>Importante: Se deberá presentar para la presentación de ofertas la certificación de Certified Information Systems Security Professional (CISSP) en idioma español, o en su defecto acompañado de la traducción respectiva, emitido por traductor público juramentado o traductor colegiado certificado, según corresponda.</i></p> <p><u>Ítem 03</u></p> <p><u>Requisitos:</u></p> <p>Un (01) Coordinador de Proyecto Certificado PMP y/o Curso y/o Taller y/o Diplomado en Gestión o Gerencia de Proyectos y/o bajo enfoque PMI y/o Diplomatura de Especialización Avanzada en Gerencia de Proyectos y Calidad. En el caso de los cursos y/o Taller y/o diplomado y/o diplomaturas deberá ser con una duración mínima de 32 horas lectivas o académicas.</p> <p>Un (01) Especialista TI: Encargado de la Instalación y Configuración Certificación técnica en solución de routers o conectividad o telefonía o en centro de datos, con una duración mínima de 30 horas.</p> <p>Un (01) Especialista Help Desk Deberá contar con certificación de gestión ITIL® 4, con una duración mínima de 30 horas.</p> <p><u>Importante:</u> Se acreditará la capacitación mediante certificados de estudios de postgrado, considerando que cada crédito del curso que acredita la capacitación equivale a dieciséis horas lectivas, según la normativa de la materia.</p>
B.4	EXPERIENCIA DEL PERSONAL CLAVE
	<p><u>Ítem 01</u></p> <p><u>Requisitos:</u></p> <p>Un (01) coordinador de Proyecto Experiencia mínima de tres (03) años de experiencia en dirección y/o coordinación y/o gestión y/o supervisión y/o implementación de proyectos en tecnologías de información y/o proyectos de telecomunicaciones para los</p>

servicios de acceso a internet y/o transmisión de datos y/o telefonía fija y/o internet, en entidades públicas o privadas.

Un (01) Especialista TI: Encargado de la Instalación y Configuración
Experiencia mínima de un año (01) años en trabajos y/o actividades como especialista técnico brindando servicio de instalación o configuración o administración y soporte en servidores o storage o virtualización o Networking.

Un (01) Especialista Help Desk
Experiencia mínima de tres (03) años de experiencia como supervisor de soporte técnico y/o mesa de ayuda y/o su equivalente en inglés Help Desk.

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.

Ítem 02

DEL PERSONAL CLAVE

El personal clave que se requiere para la implementación y ejecución del servicio son los siguientes:

Un (1) Jefe del Proyecto

Experiencia:

Deberá contar con experiencia mínima de seis (6) años en Gestión de Proyectos de TI y/o Seguridad Gestionada, como Jefe o Gestor o Coordinador o Encargado o Gerente o Subgerente del personal requerido como Jefe del Proyecto.

Actividades a Desarrollar: Encargado de liderar, planificar, dirigir y realizar un seguimiento integral de los trabajos y actividades relacionadas a la implementación del servicio. El Jefe del Proyecto deberá representar al Contratista durante las coordinaciones correspondientes en la etapa de implementación. Será el encargado de la elaboración de los informes de Implementación del Servicio.

Un (1) Líder del CSIRT

Experiencia:

Deberá contar con experiencia mínima de cuatro (4) años en proyectos de plataformas de Seguridad, CyberSOC o Ciberseguridad o Servicio de Respuesta ante Incidentes, como Jefe o Líder o Coordinador del personal requerido como Líder del CSIRT.

Actividades a Desarrollar: Encargado de liderar el equipo de respuesta ante incidentes ante una amenaza que se haya detectado en la infraestructura de la entidad y se encargará de liderar las comunicaciones

	<p>hacia la ENTIDAD en las reuniones de presentación de resultados donde se requiera tomar acciones para mitigar las amenazas.</p> <p>Un (1) Líder del CyberSOC</p> <p>Experiencia:</p> <p>Deberá contar con experiencia mínima de seis (6) años en servicios especializados de CyberSOC, Security Advisor o Ciberinteligencia como Especialista o Analista Técnico o Jefe o Líder, del personal requerido como Líder del CyberSOC.</p> <p>Actividades a Desarrollar: Encargado de liderar el equipo de CyberSOC ante los incidentes críticos que se hayan detectado en la infraestructura de la entidad y se encargará de liderar las comunicaciones hacia la ENTIDAD en las reuniones de presentación de resultados donde se requiera tomar acciones para identificar y mitigar las amenazas o vulnerabilidades, así como participará en la presentación de recomendaciones y mejoras del servicio en caso se requiera.</p> <p>Ítem 03</p> <p>Requisitos:</p> <p>Un (01) coordinador de Proyecto Experiencia mínima de tres (03) años de experiencia en dirección y/o coordinación y/o gestión y/o supervisión y/o implementación de proyectos en tecnologías de información y/o proyectos de telecomunicaciones para los servicios de acceso a internet y/o transmisión de datos y/o telefonía fija y/o internet, en entidades públicas o privadas.</p> <p>Un (01) Especialista TI: Encargado de la Instalación y Configuración Experiencia mínima de un año (01) años en trabajos y/o actividades como especialista técnico brindando servicio de instalación o configuración o administración y soporte en servidores o storage o virtualización o Networking.</p> <p>Un (01) Especialista Help Desk Experiencia mínima de cinco (05) años de experiencia como supervisor de soporte técnico y/o mesa de ayuda y/o su equivalente en inglés Help Desk.</p> <p>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.</p>
C	EXPERIENCIA DEL POSTOR EN LA ESPECIALIDAD

Ítem 01

Requisitos:

El contratista debe acreditar un monto facturado acumulado equivalente a S/ 1'000,000 (Un millón con 00/100 soles, por la contratación de servicios iguales o similares al objeto de la convocatoria, durante los ocho (8) años anteriores a la fecha de la presentación de ofertas que se computarán desde la fecha de la conformidad o emisión del comprobante de pago, según corresponda.

Se consideran servicios similares a los siguientes:

- Servicio de acceso a internet y/o servicio de internet.
- Servicio de internet fijo y/o Servicio de internet dedicado y/o servicios en telecomunicaciones.
- Servicio de transmisión de voz y datos.
- Servicio de Internet y Enlace de Datos y/o Servicio de Internet Dedicado y Enlace de Datos y/o Servicio Integral de Telecomunicaciones.
- Servicios en telecomunicaciones y/o Servicio Integral de Telecomunicaciones.
- Servicio de telefonía móvil y/o telefonía satelital y/o centrales telefónicas
- Servicio de Transmisión- Recepción de Datos a través de Terminales de Conexión Satelital y/o Servicio de Telefonía Fija y/o Servicio de transmisión de datos en general.

Ítem 02

Requisitos:

El postor debe acreditar un monto facturado acumulado equivalente a S/ 8,000,000.00 (ocho millones y 00/100 Soles), por la contratación de servicios iguales o similares al objeto de la convocatoria, durante los ocho (8) años anteriores a la fecha de la presentación de ofertas que se computarán desde la fecha de la conformidad o emisión del comprobante de pago, según corresponda.

Se consideran servicios similares a los siguientes:

- Servicio de Licencias o Servicio de CYBERSOC o Administración y Monitoreo de Plataformas de Seguridad y Correlación Inteligente de Eventos de Seguridad
- Servicio de soporte de mantenimiento, monitoreo y administración de plataformas de seguridad TI
- Servicio de monitoreo de eventos de seguridad (SOC)
- Servicio de CyberSOC o Cyber Defense Center
- Soporte, gestión, mantenimiento o monitoreo de equipamiento o plataformas de seguridad
- Servicio de seguridad Gestionada, Solución Integral Tecnológica de Ciberseguridad – SIEM
- Servicio de soporte de plataforma de seguridad y correlación, servicio de protección de tráfico web, sistema de correlación de eventos-SIEM
- Servicio de Seguridad Gestionada

Ítem 03

Requisitos:

El contratista debe acreditar un monto facturado acumulado equivalente a S/ 300,000.00 (Trescientos mil con 00/100 soles, por la contratación de servicios iguales o similares al objeto de la convocatoria, durante los ocho (8) años anteriores a la fecha de la presentación de ofertas que se computarán desde la fecha de la conformidad o emisión del comprobante de pago, según corresponda.

En el caso de postores que declaren en el Anexo N° 1 tener la condición de micro y pequeña empresa, se acredita una experiencia de S/. 30,000.00 treinta mil con 00/100 soles, por la contratación de servicios iguales o similares al objeto de la convocatoria, durante los ocho (8) años anteriores a la fecha de la presentación de ofertas que se computarán desde la fecha de la conformidad o emisión del comprobante de pago, según corresponda. En el caso de consorcios, todos los integrantes deben contar con la condición de micro y pequeña empresa.

Se consideran servicios similares a los siguientes:

- Servicio de acceso a internet y/o servicio de internet.
- Servicio de internet fijo y/o Servicio de internet dedicado y/o servicios en telecomunicaciones.
- Servicio de transmisión de voz y datos.
- Servicio de Internet y Enlace de Datos y/o Servicio de Internet Dedicado y Enlace de Datos y/o Servicio Integral de Telecomunicaciones.
- Servicios en telecomunicaciones y/o Servicio Integral de Telecomunicaciones.
- Servicio de telefonía móvil y/o telefonía satelital y/o centrales telefónicas
- Servicio de Transmisión- Recepción de Datos a través de Terminales de Conexión Satelital y/o Servicio de Telefonía Fija y/o Servicio de transmisión de datos en general.

Acreditación:

La experiencia del contratista en la especialidad se acreditará con copia simple de (i) contratos u órdenes de servicios, y su respectiva conformidad o constancia de prestación; o (ii) comprobantes de pago cuya cancelación se acredite documental y fehacientemente, con voucher de depósito, nota de abono, reporte de estado de cuenta, cualquier otro documento emitido por Entidad del sistema financiero que acredite el abono o mediante cancelación en el mismo comprobante de pago⁷⁸, correspondientes a un máximo de veinte (20) contrataciones.

En caso el contratista presente varios comprobantes de pago para acreditar una sola contratación, se debe acreditar que corresponden a dicha contratación; de lo contrario, se asumirá que los comprobantes acreditan contrataciones independientes, en cuyo caso solo se considerará, para la evaluación, las veinte (20) primeras contrataciones indicadas en el Anexo N° 8 referido a la Experiencia del Contratista 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 Contratista es 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 de 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 contratista, consignar si dicha experiencia corresponde a la matriz en caso de que el contratista sea sucursal, o fue transmitida por reorganización societaria, debiendo acompañar la documentación sustentatoria correspondiente.

Si el contratista 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 publicada 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, el contratista es deben llenar y presentar el Anexo N° 8 referido a la Experiencia del Contratista en la Especialidad.

Importante

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

3.2. REQUISITOS DE CALIFICACIÓN

Importante para la Entidad

Los requisitos de calificación que la Entidad **debe** adoptar son los siguientes:

Esta nota deberá ser eliminada una vez culminada la elaboración de las bases.

A

CAPACIDAD LEGAL

HABILITACIÓN

Ítem N° 01: Servicio de Internet Corporativo

Requisitos:

Deberá contar con la autorización o registro del Ministerio de Transportes y Comunicaciones (MTC) para brindar los servicios de Internet y Transmisión de Datos

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:

- El contratista deberá tener autorización emitida por el Ministerio de Transportes y Comunicaciones para brindar servicios de Telecomunicaciones en el Perú, en la modalidad Internet Service Provider – ISP.
- El proveedor deberá estar en el registro vigente de empresas prestadoras de servicios de valor añadido del Ministerio de Transportes y Comunicaciones, en el rubro de Conmutación de Datos por Paquetes (Internet).

Ítem N° 03: Servicio de Telefonía

Requisitos:

El contratista del servicio deberá evidenciar registro y/o autorización y/o concesión del Ministerio de Transportes y Comunicaciones para el servicio de telefonía fija local y/o certificado de inscripción de registro de comercializadores de la concesión general de concesiones, para comercializar el servicio de telefonía fija local y servicio de telefonía larga distancia nacional e internacional 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:

- El contratista deberá tener autorización emitida por el Ministerio de Transportes y Comunicaciones para brindar servicios de Telecomunicaciones en el Perú, en la modalidad Internet Service Provider – ISP.
- El proveedor deberá estar en el registro vigente de empresas prestadoras de servicios de valor añadido del Ministerio de Transportes y Comunicaciones, en el rubro de Conmutación de Datos por Paquetes (Internet).

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
	<p><u>Ítem N° 01: Servicio de Internet Corporativo</u></p> <p><u>Requisitos:</u></p> <p>Un (01) Coordinador de Proyecto</p> <p>Profesional titulado en las carreras de Ingeniería Electrónica y/o Eléctrica y/o Sistemas y/o Telecomunicaciones y/o Ingeniería Informática y/o Computación y sistemas y/o Redes y Comunicaciones y/o Ingeniería de software y/o Ingeniería de Sistemas y Computo.</p> <p>Un (01) Especialista TI: Encargado de la Instalación y Configuración</p> <p>Profesional Técnico y/o bachiller Titulado en Ing. de Sistemas y/o Electrónico y/o Redes y Comunicaciones y/o Empresarial y de Sistemas y/o Computación y de Sistemas y/o Telecomunicaciones y Redes y/o Estadística e Informática.</p> <p>Un (01) Especialista Help Desk</p> <p>Profesional titulado y/o Bachiller en Ingeniería Electrónica y/o Ingeniería de Telecomunicaciones y/o Ingeniería de Sistemas y/o Ingeniería Mecatrónica y/o Ingeniería Informática y/o Ingeniería de computación.</p> <p><u>Ítem N° 02: Servicio de Ciberseguridad</u></p> <p><u>Requisitos:</u></p> <p>Un (01) Jefe de Proyecto</p> <p>Profesional Titulado en Ingeniería Electrónica o Ingeniería de Sistemas o Ingeniería Informática y de Sistemas o en Ingeniería de Cómputo y Sistemas o Ingeniería Informática o Ingeniería de Sistemas de Información o Ingeniería de Software.</p> <p>Un (01) Lider del CSIRT</p> <p>Profesional Titulado o Bachiller en Ingeniería Electrónica o Ingeniería de Sistemas o en Tecnologías de la Información o en Ingeniería de Cómputo y Sistemas o Ingeniería Informática o Ingeniería de Sistemas de Información o Ingeniería de Software.</p> <p>Un (01) Lider del CyberSOC</p>

	<p>Profesional Titulado o Bachiller en Ingeniería Electrónica o en Telecomunicaciones o en Redes y Comunicaciones o Sistemas o en Tecnologías de la Información o en Cómputo y Sistemas o Informática o de Sistemas de Información o Ingeniería de Seguridad.</p> <p><u>Ítem N° 03: Servicio de Telefonía</u></p> <p><u>Requisitos:</u></p> <p>Un (01) Coordinador de Proyecto</p> <p>Profesional titulado en las carreras de Ingeniería Electrónica y/o Eléctrica y/o Sistemas y/o Telecomunicaciones y/o Ingeniería Informática y/o Computación y sistemas y/o Redes y Comunicaciones y/o Ingeniería de software y/o Ingeniería de Sistemas y Computo.</p> <p>Un (01) Especialista TI: Encargado de la Instalación y Configuración</p> <p>Profesional Técnico y/o bachiller Titulado en Ing. de Sistemas y/o Electrónico y/o Redes y Comunicaciones y/o Empresarial y de Sistemas y/o Computación y de Sistemas y/o Telecomunicaciones y Redes y/o Estadística e Informática.</p> <p>Un (01) Especialista Help Desk</p> <p>Profesional titulado y/o Bachiller en Ingeniería Electrónica y/o Ingeniería de Telecomunicaciones y/o Ingeniería de Sistemas y/o Ingeniería Mecatrónica y/o Ingeniería Informática y/o Ingeniería de computación.</p> <p><u>Acreditación:</u></p> <p>El título Profesional y/o técnico y /o grado de bachiller será verificado por el comité de selección en el Registro Nacional de Grados Académicos y Títulos Profesionales en el portal web de la Superintendencia Nacional de Educación Superior Universitaria - SUNEDU a través del siguiente link: https://enlinea.sunedu.gob.pe/ o en el Registro Nacional de Certificados, Grados y Títulos a cargo del Ministerio de Educación a través del siguiente link: https://titulosinstitutos.minedu.gob.pe/, según corresponda.</p> <p>En caso el título profesional y/o técnico y/o grado de bachiller no se encuentre inscrito en el referido registro, el postor debe presentar la copia del diploma respectivo a fin de acreditar la formación académica requerida.</p>
B.3.2	CAPACITACIÓN
	<p><u>Ítem N° 01: Servicio de Internet Corporativo</u></p> <p><u>Requisitos:</u></p> <p>Un (01) Coordinador de Proyecto</p> <p>Certificado PMP y/o Curso y/o Taller y/o Diplomado en Gestión o Gerencia de Proyectos y/o bajo enfoque PMI y/o Diplomatura de Especialización Avanzada en Gerencia de Proyectos y Calidad. En el caso de los cursos y/ Taller y/o diplomado y/o diplomaturas deberá ser con una duración mínima de 32 horas lectivas.</p> <p>Un (01) Especialista TI: Encargado de la Instalación y Configuración</p> <p>Certificación técnica en solución de routers o conectividad o telefonía o en centro de datos</p> <p>Un (01) Especialista Help Desk</p> <p>Certificación de gestión ITIL® 4, con una duración mínima de 30 horas lectivas.</p> <p><u>Acreditación:</u></p> <p>Se acreditará con copia simple de constancia, certificado u otro documento, según corresponda.</p> <p><u>Ítem N° 02: Servicio de Ciberseguridad</u></p>

	<p><u>Requisitos:</u></p> <p>Un (01) Jefe de Proyecto</p> <p>Certificación de Project Management Professional (PMP) vigente e ITIL.</p> <p>Un (01) Lider del CSIRT</p> <p>Certificación de ISO/IEC 27032 Lead Cybersecurity Manager vigente.</p> <p>Un (01) Lider del CyberSOC</p> <p>Certificación de Certified Information Systems Security Professional (CISSP) vigente</p> <p><u>Acreditación:</u></p> <p>Se acreditará con copia simple de constancia, certificado u otro documento, según corresponda.</p> <p><u>Ítem N° 03: Servicio de Telefonía</u></p> <p><u>Requisitos:</u></p> <p>Un (01) Coordinador de Proyecto</p> <p>Certificado PMP y/o Curso y/o Taller y/o Diplomado en Gestión o Gerencia de Proyectos y/o bajo enfoque PMI y/o Diplomatura de Especialización Avanzada en Gerencia de Proyectos y Calidad. En el caso de los cursos y/Taller y/o diplomado y/o diplomaturas deberá ser con una duración mínima de 32 horas lectivas.</p> <p>Un (01) Especialista TI: Encargado de la Instalación y Configuración</p> <p>Certificación técnica en solución de routers o conectividad o telefonía o en centro de datos, con una duración mínima de 30 horas lectivas.</p> <p>Un (01) Especialista Help Desk</p> <p>Certificación de gestión ITIL® 4, con una duración mínima de 30 horas lectivas.</p> <p><u>Acreditación:</u></p> <p>Se acreditará con copia simple de constancia, certificado u otro documento, según corresponda.</p> <div style="border: 1px solid black; padding: 5px; margin-top: 10px;"> <p>Importante</p> <p><i>Se podrá acreditar la capacitación mediante certificados de estudios de postgrado, considerando que cada crédito del curso que acredita la capacitación equivale a dieciséis horas lectivas, según la normativa de la materia.</i></p> </div>
B.4	EXPERIENCIA DEL PERSONAL CLAVE

Ítem N° 01: Servicio de Internet Corporativo

Requisitos:

Un (01) Coordinador de Proyecto

Experiencia mínima de tres (03) años de experiencia en dirección y/o coordinación y/o gestión y/o supervisión y/o implementación de proyectos en tecnologías de información y/o proyectos de telecomunicaciones para los servicios de acceso a internet y/o transmisión de datos y/o telefonía fija y/o internet, en entidades públicas o privadas.

Un (01) Especialista TI: Encargado de la Instalación y Configuración

Experiencia mínima de un año (01) año en trabajos y/o actividades como especialista técnico brindando servicio de instalación o configuración o administración y soporte en servidores o storage o virtualización o Networking.

Un (01) Especialista Help Desk

Experiencia mínima de tres (03) años de experiencia como supervisor de soporte técnico y/o mesa de ayuda y/o su equivalente en inglés Help Desk.

Ítem N° 02: Servicio de Ciberseguridad

Requisitos:

Un (01) Jefe de Proyecto

Experiencia mínima de seis (6) años en Gestión de Proyectos de TI y/o Seguridad Gestionada, como Jefe o Gestor o Coordinador o Encargado o Gerente o Subgerente del personal requerido como Jefe del Proyecto.

Un (01) Lider del CSIRT

Experiencia mínima de cuatro (4) años en proyectos de plataformas de Seguridad, CyberSOC o Ciberseguridad o Servicio de Respuesta ante Incidentes, como Jefe o Líder o Coordinador del personal requerido como Líder del CSIRT.

Un (01) Lider del CyberSOC

Experiencia mínima de seis (6) años en servicios especializados de CyberSOC, Security Advisor o Ciberinteligencia como Especialista o Analista Técnico o Jefe o Líder, del personal requerido como Líder del CyberSOC.

Ítem N° 03: Servicio de Telefonía

Requisitos:

Un (01) Coordinador de Proyecto

Experiencia mínima de tres (03) años de experiencia en dirección y/o coordinación y/o gestión y/o supervisión y/o implementación de proyectos en tecnologías de información y/o proyectos de telecomunicaciones para los servicios de acceso a internet y/o transmisión de datos y/o telefonía fija y/o internet, en entidades públicas o privadas.

Un (01) Especialista TI: Encargado de la Instalación y Configuración

Experiencia mínima de un año (01) años en trabajos y/o actividades como especialista técnico brindando servicio de instalación o configuración o administración y soporte en servidores o storage o virtualización o Networking.

Un (01) Especialista Help Desk

Experiencia mínima de cinco (05) años de experiencia como supervisor de soporte técnico y/o mesa de ayuda y/o su equivalente en inglés Help Desk.

De presentarse experiencia ejecutada paralelamente (traslape), para el cómputo del tiempo de dicha

	<p><u>experiencia sólo se considerará una vez el periodo traslapado.</u></p> <p><u>Acreditación:</u></p> <p>La experiencia del personal clave se acreditará con cualquiera de los siguientes documentos: (i) copia simple de contratos y su respectiva conformidad o (ii) constancias o (iii) certificados o (iv) cualquier otra documentación que, de manera fehaciente demuestre la experiencia del personal propuesto.</p> <div style="border: 1px solid black; padding: 5px; margin-top: 10px;"> <p>Importante</p> <ul style="list-style-type: none"> • <i>Los documentos que acreditan la experiencia deben incluir los nombres y apellidos del personal clave, el cargo desempeñado, el plazo de la prestación indicando el día, mes y año de inicio y culminación, el nombre de la Entidad u organización que emite el documento, la fecha de emisión y nombres y apellidos de quien suscribe el documento.</i> • <i>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.</i> • <i>Se considerará aquella experiencia que no tenga una antigüedad mayor a veinticinco (25) años anteriores a la fecha de la presentación de ofertas.</i> • <i>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.</i> </div>
C	<p>EXPERIENCIA DEL POSTOR EN LA ESPECIALIDAD</p> <p><u>Ítem N° 01: Servicio de Internet Corporativo</u></p> <p><u>Requisitos:</u></p> <p>El postor debe acreditar un monto facturado acumulado equivalente a S/ 1'000,000.00 (Un Millón con 00/100 Soles), por la contratación de servicios iguales o similares al objeto de la convocatoria, durante los ocho (8) años anteriores a la fecha de la presentación de ofertas que se computarán desde la fecha de la conformidad o emisión del comprobante de pago, según corresponda.</p> <p>Se consideran servicios similares a los siguientes:</p> <ul style="list-style-type: none"> • Servicio de acceso a internet y/o servicio de internet. • Servicio de internet fijo y/o Servicio de internet dedicado y/o servicios en telecomunicaciones. • Servicio de transmisión de voz y datos. • Servicio de Internet y Enlace de Datos y/o Servicio de Internet Dedicado y Enlace de Datos y/o Servicio Integral de Telecomunicaciones. • Servicios en telecomunicaciones y/o Servicio Integral de Telecomunicaciones. • Servicio de telefonía móvil y/o telefonía satelital y/o centrales telefónicas • Servicio de Transmisión- Recepción de Datos a través de Terminales de Conexión Satelital y/o Servicio de Telefonía Fija y/o Servicio de transmisión de datos en general. <p><u>Ítem N° 02: Servicio de Ciberseguridad</u></p> <p><u>Requisitos:</u></p> <p>El postor debe acreditar un monto facturado acumulado equivalente a S/ 8,000,000.00 (ocho millones y 00/100 Soles), por la contratación de servicios iguales o similares al objeto de la convocatoria, durante los ocho (8) años anteriores a la fecha de la presentación de ofertas que se computarán desde la fecha de la conformidad o emisión del comprobante de pago, según corresponda.</p> <p>Se consideran servicios similares a los siguientes:</p> <ul style="list-style-type: none"> - Servicio de Licencias o Servicio de CYBERSOC o Administración y Monitoreo de Plataformas de Seguridad y Correlación Inteligente de Eventos de Seguridad - Servicio de soporte de mantenimiento, monitoreo y administración de plataformas de seguridad TI

- Servicio de monitoreo de eventos de seguridad (SOC)
- Servicio de CyberSOC o Cyber Defense Center
- Soporte, gestión, mantenimiento o monitoreo de equipamiento o plataformas de seguridad
- Servicio de seguridad Gestionada, Solución Integral Tecnológica de Ciberseguridad – SIEM
- Servicio de soporte de plataforma de seguridad y correlación, servicio de protección de tráfico web, sistema de correlación de eventos-SIEM
- Servicio de Seguridad Gestionada

Ítem N° 03: Servicio de TelefoníaRequisitos:

El contratista debe acreditar un monto facturado acumulado equivalente a **S/ 300,000.00 (Trescientos mil con 00/100 soles)**, por la contratación de servicios iguales o similares al objeto de la convocatoria, durante los ocho (8) años anteriores a la fecha de la presentación de ofertas que se computarán desde la fecha de la conformidad o emisión del comprobante de pago, según corresponda.

En el caso de postores que declaren en el Anexo N° 1 tener la condición de micro y pequeña empresa, se acredita una experiencia de **S/. 30,000.00 (treinta mil con 00/100 soles)**, por la contratación de servicios iguales o similares al objeto de la convocatoria, durante los ocho (8) años anteriores a la fecha de la presentación de ofertas que se computarán desde la fecha de la conformidad o emisión del comprobante de pago, según corresponda. En el caso de consorcios, todos los integrantes deben contar con la condición de micro y pequeña empresa.

Se consideran servicios similares a los siguientes:

- Servicio de acceso a internet y/o servicio de internet.
- Servicio de internet fijo y/o Servicio de internet dedicado y/o servicios en telecomunicaciones.
- Servicio de transmisión de voz y datos.
- Servicio de Internet y Enlace de Datos y/o Servicio de Internet Dedicado y Enlace de Datos y/o Servicio Integral de Telecomunicaciones.
- Servicios en telecomunicaciones y/o Servicio Integral de Telecomunicaciones.
- Servicio de telefonía móvil y/o telefonía satelital y/o centrales telefónicas
- Servicio de Transmisión- Recepción de Datos a través de Terminales de Conexión Satelital y/o Servicio de Telefonía Fija y/o Servicio de transmisión de datos en general.

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 pago⁸, correspondientes a un máximo de veinte (20) contrataciones.

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

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

En los casos que se acredite experiencia adquirida en consorcio, debe presentarse la promesa de consorcio o el contrato de consorcio del cual se desprenda fehacientemente el porcentaje de las

⁸ 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".

obligaciones que se asumió en el contrato presentado; de lo contrario, no se computará la experiencia proveniente de dicho contrato.

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

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

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

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

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

Importante

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

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	
<u>Evaluación:</u> Se evaluará considerando el precio ofertado por el postor. <u>Acreditación:</u> Se acreditará mediante el documento que contiene el precio de la oferta (Anexo N° 6).		La evaluación consistirá en otorgar el máximo puntaje a la oferta de precio más bajo y otorgar a las demás ofertas puntajes inversamente proporcionales a sus respectivos precios, según la siguiente fórmula: $P_i = \frac{O_m \times PMP}{O_i}$ i = Oferta 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 Internet, Seguridad Gestionada y Telefonía, que celebra de una parte [CONSIGNAR EL NOMBRE DE LA ENTIDAD], en adelante LA ENTIDAD, con RUC N° [.....], con domicilio legal en [.....], representada por [.....], identificado con DNI N° [.....], y de otra parte [.....], con RUC N° [.....], con domicilio legal en [.....], inscrita en la Ficha N° [.....] Asiento N° [.....] del Registro de Personas Jurídicas de la ciudad de [.....], debidamente representado por su Representante Legal, [.....], con DNI N° [.....], según poder inscrito en la Ficha N° [.....], Asiento N° [.....] del Registro de Personas Jurídicas de la ciudad de [.....], a quien en adelante se le denominará EL CONTRATISTA en los términos y condiciones siguientes:

CLÁUSULA PRIMERA: ANTECEDENTES

Con fecha [.....], el comité de selección adjudicó la buena pro del **CONCURSO PÚBLICO N° 003-2024-INGEMMET/CS** para la contratación de Servicio de Internet, Seguridad Gestionada y Telefonía, a [INDICAR NOMBRE DEL GANADOR DE LA BUENA PRO], cuyos detalles e importe constan en los documentos integrantes del presente contrato.

CLÁUSULA SEGUNDA: OBJETO

El presente contrato tiene por objeto Servicio de Internet, Seguridad Gestionada y Telefonía.

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 PAGO⁹

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, siempre que se verifiquen las condiciones establecidas en el contrato para ello, bajo responsabilidad del funcionario competente.

⁹ En cada caso concreto, dependiendo de la naturaleza del contrato, podrá adicionarse la información que resulte pertinente a efectos de generar el pago.

En caso de retraso en el pago por parte de LA ENTIDAD, salvo que se deba a caso fortuito o fuerza mayor, EL CONTRATISTA tendrá derecho al pago de intereses legales conforme a lo establecido en el artículo 39 de la Ley de Contrataciones del Estado y en el artículo 171 de su Reglamento, los que se computan desde la oportunidad en que el pago debió efectuarse.

CLÁUSULA QUINTA: DEL PLAZO DE LA EJECUCIÓN DE LA PRESTACIÓN

El plazo de ejecución del presente contrato es de la siguiente manera:

PARA EL ÍTEM N° 01 Y 03**IMPLEMENTACIÓN:**

Para la implementación de la puesta en operación de los servicios requeridos (obras civiles, canalización y/o tendido aéreo del cableado de fibra óptica en planta externa, canalización interna de la fibra óptica, conectorización de los hilos de fibra óptica, instalación de equipos especializados de comunicación propiedad del contratista, así como pruebas de conectividad física y lógica, el tiempo máximo estimado será de sesenta (60) días calendario, a partir del día siguiente de la aceptación del plan de trabajo.

N°	CONCEPTO	PLAZO
1	Plan de trabajo y cronograma de las actividades de la implementación del servicio	Hasta los diez (10) días calendarios contados a partir del día siguiente de la firma del contrato
2	Informe sobre la implementación del servicio	Hasta los sesenta (60) días calendarios contados a partir del día siguiente de la aceptación del plan de trabajo

PRESTACIÓN DEL SERVICIO:

Se establece que el plazo contractual de la prestación será treinta y seis (36) meses, se iniciará terminada la etapa de la implementación de todas las comunicaciones de la Sede Principal (Av. Canadá 1470, Lima-Perú), para lo cual se suscribirá un Acta de implementación del servicio. Se aclara que el servicio comenzará a ser contabilizado a partir del día siguiente de suscrita el Acta de Conformidad del Servicio.

N°	CONCEPTO	PLAZO
1	Informe mensual de Operación de servicio contratado	Hasta los siete (07) días calendarios de culminado el servicio de cada mes. Se contabilizará a partir del día siguiente de la firma del Acta de implementación del servicio, durante el periodo de tiempo contratado.

PARA EL ÍTEM N° 02**IMPLEMENTACIÓN DEL SERVICIO**

El plazo máximo para la implementación del servicio será por sesenta (60) días calendario, contabilizados a partir del día siguiente de la firma del Acta de Implementación del Servicio, previa suscripción del Contrato, el mismo que será suscrito entre un (01) representante propuesto por el Contratista y un (01) representante de la Oficina de Sistemas de Información.

EJECUCIÓN DEL SERVICIO

El plazo de ejecución del servicio será por treinta y seis (36) meses, contabilizados a partir del día siguiente de finalizado los trabajos para la implementación del servicio, para lo cual se firmará el Acta de Inicio del Servicio, el mismo que será suscrito entre un (01) representante propuesto por el Contratista y un (01) representante de la Oficina de Sistemas de Información

CLÁUSULA SEXTA: PARTES INTEGRANTES DEL CONTRATO

El presente contrato está conformado por las bases integradas, la oferta ganadora, así como los documentos derivados del procedimiento de selección que establezcan obligaciones para las partes.

CLÁUSULA SÉTIMA: GARANTÍAS

EL CONTRATISTA entregó al perfeccionamiento del contrato la respectiva garantía incondicional, solidaria, irrevocable, y de realización automática en el país al solo requerimiento, a favor de LA

ENTIDAD, por los conceptos, montos y vigencias siguientes:

- De fiel cumplimiento del contrato: [CONSIGNAR EL MONTO], a través de la [INDICAR EL TIPO DE GARANTÍA PRESENTADA] N° [INDICAR NÚMERO DEL DOCUMENTO] emitida por [SEÑALAR EMPRESA QUE LA EMITE]. Monto que es equivalente al diez por ciento (10%) del monto del contrato original, la misma que debe mantenerse vigente hasta la conformidad de la recepción de la prestación.

Importante

Al amparo de lo dispuesto en el numeral 149.4 del artículo 149 del Reglamento de la Ley de Contrataciones del Estado, en el caso de contratos periódicos de prestación de servicios en general, si el postor ganador de la buena pro solicita la retención del diez por ciento (10%) del monto del contrato original como garantía de fiel cumplimiento de contrato, debe consignarse lo siguiente:

"De fiel cumplimiento del contrato: [CONSIGNAR EL MONTO], a través de la retención que debe efectuar LA ENTIDAD, durante la primera mitad del número total de pagos a realizarse, de forma prorrateada, con cargo a ser devuelto a la finalización del mismo."

En el caso que corresponda, consignar lo siguiente:

- Garantía fiel cumplimiento por prestaciones accesorias: [CONSIGNAR EL MONTO], a través de la [INDICAR EL TIPO DE GARANTÍA PRESENTADA] N° [INDICAR NÚMERO DEL DOCUMENTO] emitida por [SEÑALAR EMPRESA QUE LA EMITE], la misma que debe mantenerse vigente hasta el cumplimiento total de las obligaciones garantizadas.

Importante

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

- "De fiel cumplimiento por prestaciones accesorias: [CONSIGNAR EL MONTO], a través de la retención que debe efectuar LA ENTIDAD, durante la primera mitad del número total de pagos a realizarse, de forma prorrateada, con cargo a ser devuelto a la finalización del mismo."*

Importante

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

CLÁUSULA OCTAVA: EJECUCIÓN DE GARANTÍAS POR FALTA DE RENOVACIÓN

LA ENTIDAD puede solicitar la ejecución de las garantías cuando EL CONTRATISTA no las hubiere renovado antes de la fecha de su vencimiento, conforme a lo dispuesto por el literal a) del numeral 155.1 del artículo 155 del Reglamento de la Ley de Contrataciones del Estado.

CLÁUSULA NOVENA: CONFORMIDAD DE LA PRESTACIÓN DEL SERVICIO

La conformidad de la prestación del servicio se regula por lo dispuesto en el artículo 168 del Reglamento de la Ley de Contrataciones del Estado. La conformidad será otorgada por [CONSIGNAR EL ÁREA O UNIDAD ORGÁNICA QUE OTORGARÁ LA CONFORMIDAD] en el plazo máximo de [CONSIGNAR SIETE (7) DÍAS O MÁXIMO QUINCE (15) DÍAS, EN CASO SE REQUIERA EFECTUAR PRUEBAS QUE PERMITAN VERIFICAR EL CUMPLIMIENTO DE LA OBLIGACIÓN] días de producida la recepción.

De existir observaciones, LA ENTIDAD las comunica al CONTRATISTA, indicando claramente el sentido de estas, otorgándole un plazo para subsanar no menor de dos (2) ni mayor de ocho (8) días. Dependiendo de la complejidad o sofisticación de las subsanaciones a realizar el plazo para

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

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

CLÁUSULA DÉCIMA: DECLARACIÓN JURADA DEL CONTRATISTA

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

CLÁUSULA UNDÉCIMA: RESPONSABILIDAD POR VICIOS OCULTOS

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

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

CLÁUSULA DUODÉCIMA: PENALIDADES

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

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

Donde:

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

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

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

Importante

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

OTRAS PENALIDADES:

Serán evaluadas durante cada mes de la prestación del servicio y aplicadas según el caso cuando el contratista incurra en falta, se utilizará lo establecido en el siguiente cuadro:

N°	SUPUESTOS DE APLICACIÓN DE PENALIDAD	FORMA DE CALCULO
1	Cuando el contratista supera los 7 días para una configuración y/o reconfiguración solicitada por la entidad, se aclara que se refiera a horas de configuración y/o configuración solicitada para la entidad para cambios simples.	3 % del monto de la facturación mensual del servicio contratado

2	Cuando el contratista supere las 12 horas para restablecer la disponibilidad de los routers ante una caída de la misma.	3 % del monto de la facturación mensual del servicio contratado
3	Cuando la no disponibilidad del internet supere las seis (06) horas	5 % del monto de la facturación mensual del servicio contratado

Procedimiento

- Informe a la Oficina de Sistemas de Información, indicando la ocurrencia, desde reportado el incidente.
- La Oficina de Sistemas de Información tendrá el informe del proveedor sobre la incidencia y en base a ello evaluará la responsabilidad.
- Enviar documento a la Unidad de Logística indicando la ocurrencia y el incidente para que sea notificado al proveedor.

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

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

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

CLÁUSULA DÉCIMA TERCERA: RESOLUCIÓN DEL CONTRATO

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

CLÁUSULA DÉCIMA CUARTA: RESPONSABILIDAD DE LAS PARTES

Cuando se resuelva el contrato por causas imputables a algunas de las partes, se debe resarcir los daños y perjuicios ocasionados, a través de la indemnización correspondiente. Ello no obsta la aplicación de las sanciones administrativas, penales y pecuniarias a que dicho incumplimiento diere lugar, en el caso que éstas correspondan.

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

CLÁUSULA DÉCIMA QUINTA: ANTICORRUPCIÓN

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

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

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

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

CLÁUSULA DÉCIMA SEXTA: MARCO LEGAL DEL CONTRATO

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

CLÁUSULA DÉCIMA SÉTIMA: SOLUCIÓN DE CONTROVERSIAS¹⁰

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

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

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

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

CLÁUSULA DÉCIMA OCTAVA: FACULTAD DE ELEVAR A ESCRITURA PÚBLICA

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

CLÁUSULA DÉCIMA NOVENA: DOMICILIO PARA EFECTOS DE LA EJECUCIÓN CONTRACTUAL

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

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

DOMICILIO DEL CONTRATISTA: [CONSIGNAR EL DOMICILIO SEÑALADO POR EL POSTOR GANADOR DE LA BUENA PRO AL PRESENTAR LOS REQUISITOS PARA EL PERFECCIONAMIENTO DEL CONTRATO]

La variación del domicilio aquí declarado de alguna de las partes debe ser comunicada a la otra parte, formalmente y por escrito, con una anticipación no menor de quince (15) días calendario.

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

"LA ENTIDAD"

"EL CONTRATISTA"

Importante

Este documento puede firmarse digitalmente si ambas partes cuentan con firma digital, según la Ley N° 27269, Ley de Firmas y Certificados Digitales¹¹.

¹⁰ 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).

¹¹ 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

108

ANEXO N° 1

DECLARACIÓN JURADA DE DATOS DEL POSTOR

Señores
COMITÉ DE SELECCIÓN
CONCURSO PÚBLICO N° 003-2024-INGEMMET/CS
Presente.-

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

Nombre, Denominación o Razón Social :				
Domicilio Legal :				
RUC :	Teléfono(s) :			
MYPE ¹²		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 servicios¹³

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.

¹² 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.

¹³ Consignar en el caso de procedimientos de selección por relación de ítems, cuando el monto del valor estimado del ítem no supere los doscientos mil Soles (S/ 200 000.00), cuando se haya optado por perfeccionar el contrato con una orden de servicios.

Importante

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

ANEXO N° 1

DECLARACIÓN JURADA DE DATOS DEL POSTOR

Señores

COMITÉ DE SELECCIÓN

CONCURSO PÚBLICO N° 003-2024-INGEMMET/CS

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 ¹⁴		Sí	No	
Correo electrónico :				

Datos del consorciado 2				
Nombre, Denominación o Razón Social :				
Domicilio Legal :				
RUC :	Teléfono(s) :			
MYPE ¹⁵		Sí	No	
Correo electrónico :				

Datos del consorciado ...				
Nombre, Denominación o Razón Social :				
Domicilio Legal :				
RUC :	Teléfono(s) :			
MYPE ¹⁶		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.

¹⁴ 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.

¹⁵ Ibídem.

¹⁶ 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 servicios¹⁷

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.

¹⁷ Consignar en el caso de procedimientos de selección por relación de ítems, cuando el monto del valor estimado del ítem no supere los doscientos mil Soles (S/ 200 000.00), cuando se haya optado por perfeccionar el contrato con una orden de servicios.

ANEXO N° 2

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

Señores
COMITÉ DE SELECCIÓN
CONCURSO PÚBLICO N° 003-2024-INGEMMET/CS
Presente.-

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

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

[CONSIGNAR CIUDAD Y FECHA]

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

Importante

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



ANEXO N° 3

DECLARACIÓN JURADA DE CUMPLIMIENTO DE LOS TÉRMINOS DE REFERENCIA

Señores

COMITÉ DE SELECCIÓN

CONCURSO PÚBLICO N° 003-2024-INGEMMET/CS

Presente.-

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

[CONSIGNAR CIUDAD Y FECHA]

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

Importante

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



ANEXO N° 4

DECLARACIÓN JURADA DE PLAZO DE PRESTACIÓN DEL SERVICIO

Señores
COMITÉ DE SELECCIÓN
CONCURSO PÚBLICO N° 003-2024-INGEMMET/CS
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

18
18

ANEXO N° 5

PROMESA DE CONSORCIO

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

Señores

COMITÉ DE SELECCIÓN

CONCURSO PÚBLICO N° 003-2024-INGEMMET/CS

Presente.-

Los suscritos declaramos expresamente que hemos convenido en forma irrevocable, durante el lapso que dure el procedimiento de selección, para presentar una oferta conjunta al **CONCURSO PÚBLICO N° 003-2024-INGEMMET/CS**

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] [%]¹⁸

[DESCRIBIR LAS OBLIGACIONES DEL CONSORCIADO 1]

2. OBLIGACIONES DE [NOMBRE, DENOMINACIÓN O RAZÓN SOCIAL DEL CONSORCIADO 2] [%]¹⁹

[DESCRIBIR LAS OBLIGACIONES DEL CONSORCIADO 2]

TOTAL OBLIGACIONES

100%²⁰

[CONSIGNAR CIUDAD Y FECHA]

¹⁸ Consignar únicamente el porcentaje total de las obligaciones, el cual debe ser expresado en número entero, sin decimales.

¹⁹ Consignar únicamente el porcentaje total de las obligaciones, el cual debe ser expresado en número entero, sin decimales.

²⁰ Este porcentaje corresponde a la sumatoria de los porcentajes de las obligaciones de cada uno de los integrantes del consorcio.

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

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

Importante

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



ANEXO N° 6

PRECIO DE LA OFERTA

ITEM N°

Señores
COMITÉ DE SELECCIÓN
CONCURSO PÚBLICO N° 003-2024-INGEMMET/CS
Presente.-

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

ITEM	CONCEPTO	PRECIO TOTAL
TOTAL		

El precio de la oferta SOLES 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]"

El postor puede presentar el precio de su oferta en un solo documento o documentos independientes, en los ítems que se presente.

Importante

Cuando se trate de consorcios, esta declaración jurada será presentada por cada uno de los integrantes del consorcio, salvo que se trate de consorcios con contabilidad independiente, en cuyo caso debe ser suscrita por el representante común, debiendo indicar su condición de consorcio con contabilidad independiente y el número de RUC del consorcio.

ANEXO N° 8

EXPERIENCIA DEL POSTOR EN LA ESPECIALIDAD

Señores
COMITÉ DE SELECCIÓN
CONCURSO PÚBLICO N° 003-2024-INGEMMET/CS
Presente.-

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

N°	CLIENTE	OBJETO DEL CONTRATO	N° CONTRATO / O/S / COMPROBANTE DE PAGO	FECHA DEL CONTRATO O CP ²¹	FECHA DE LA CONFORMIDAD DE SER EL CASO ²²	EXPERIENCIA PROVENIENTE ²³ DE:	MONEDA	IMPORTE ²⁴	TIPO DE CAMBIO VENTA ²⁵	MONTO FACTURADO ACUMULADO ²⁶
1										
2										
3										
4										

²¹

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.

²²

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.

²³

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".

²⁴

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

²⁵

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.

²⁶

Consignar en la moneda establecida en las bases.

N°	CLIENTE	OBJETO DEL CONTRATO	N° CONTRATO / O/S / COMPROBANTE DE PAGO	FECHA DEL CONTRATO O CP ²¹	FECHA DE LA CONFORMIDAD DE SER EL CASO ²²	EXPERIENCIA PROVENIENTE ²³ DE:	MONEDA	IMPORTE ²⁴	TIPO DE CAMBIO VENTA ²⁵	MONTO FACTURADO ACUMULADO ²⁶
5										
6										
7										
8										
9										
10										
...										
20										
TOTAL										

[CONSIGNAR CIUDAD Y FECHA]

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

ANEXO N° 9

**DECLARACIÓN JURADA
(NUMERAL 49.4 DEL ARTÍCULO 49 DEL REGLAMENTO)**

Señores
COMITÉ DE SELECCIÓN
CONCURSO PÚBLICO N° 003-2024-INGEMMET/CS
Presente.-

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

[CONSIGNAR CIUDAD Y FECHA]

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

Importante

A efectos de cautelar la veracidad de esta declaración, el postor puede verificar la información de la Relación de Proveedores Sancionados por el Tribunal de Contrataciones del Estado con Sanción Vigente en <http://portal.osce.gob.pe/rnp/content/relación-de-proveedores-sancionados>.

También le asiste dicha facultad al órgano encargado de las contrataciones o al órgano de la Entidad al que se le haya asignado la función de verificación de la oferta presentada por el postor ganador de la buena pro.

ANEXO N° 11

**SOLICITUD DE BONIFICACIÓN DEL CINCO POR CIENTO (5%) POR TENER LA CONDICIÓN DE
MICRO Y PEQUEÑA EMPRESA
ITEM N° 03**

Señores
COMITÉ DE SELECCIÓN
CONCURSO PÚBLICO N° 003-2024-INGEMMET/CS
Presente.-

Mediante el presente el suscrito, postor y/o Representante legal de [CONSIGNAR EN CASO DE SER PERSONA JURÍDICA], solicito la asignación de la bonificación del cinco por ciento (5%) sobre el puntaje total obtenido, debido a que mi representada cuenta con la condición de micro y pequeña empresa.

[CONSIGNAR CIUDAD Y FECHA]

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

Importante

- Para asignar la bonificación, el comité de selección, según corresponda, verifica 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/>.
- Para que un consorcio pueda acceder a la bonificación, cada uno de sus integrantes debe cumplir con la condición de micro y pequeña empresa.

ANEXO N° 12

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

(DOCUMENTO A PRESENTAR EN EL PERFECCIONAMIENTO DEL CONTRATO)

Señores
COMITÉ DE SELECCIÓN
CONCURSO PÚBLICO N° 003-2024-INGEMMET/CS

Presente.-

El que se suscribe, [.....], postor adjudicado y/o Representante Legal de [CONSIGNAR EN CASO DE SER PERSONA JURÍDICA], identificado con [CONSIGNAR TIPO DE DOCUMENTO DE IDENTIDAD] N° [CONSIGNAR NÚMERO DE DOCUMENTO DE IDENTIDAD], autorizo que durante la ejecución del contrato se me notifique al correo electrónico [INDICAR EL CORREO ELECTRÓNICO] lo siguiente:

✓ Notificación de la decisión de la Entidad respecto a la solicitud de ampliación de plazo.

[CONSIGNAR CIUDAD Y FECHA]

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

Importante

La notificación de la decisión de la Entidad respecto a la solicitud de ampliación de plazo se efectúa por medios electrónicos de comunicación, siempre que se cuente con la autorización correspondiente y sea posible obtener un acuse de recibo a través del mecanismo utilizado.

