

<b>FORMATO</b> <b>ACTA DE APROBACIÓN DEL PLIEGO DE ABSOLUCIÓN DE CONSULTAS Y OBSERVACIONES E INTEGRACIÓN DE BASES</b>																										
1	NÚMERO DE ACTA	009-2025																								
2	<b>SOBRE LA INFORMACIÓN GENERAL</b> En San Borja, a los 16 días del mes de junio del 2025, en la Unidad de Logística del Instituto Geológico, Minero y Metalúrgico, ubicada en Av. Canada N° 1470, San Borja, a las 08:00 horas, se reunieron los miembros del comité de selección designados mediante Resolución Directoral N° 157-2024-INGEMMET/GG-OA de fecha 04 de octubre del 2025, encargado de la preparación, conducción y realización del procedimiento de selección denominado <b>Adjudicación Simplificada N° N° 026-2024-INGEMMET/CS-1</b> , cuyo objeto de convocatoria es la contratación del <b>"Servicio de Internet, Seguridad Gestionada y Telefonía"</b> , a fin de ANALIZAR, DISCUTIR Y APROBAR EL PLIEGO DE ABSOLUCIÓN DE CONSULTAS Y OBSERVACIONES E INTEGRAR LAS BASES.																									
3	<b>SOBRE EL QUÓRUM Y LOS MIEMBROS PARTICIPANTES DE LA SESIÓN</b> El quórum necesario que exige la normativa de contrataciones del Estado se logró con la presencia de los siguientes miembros: <table border="1" style="width: 100%; border-collapse: collapse; margin-top: 5px;"> <tr> <td rowspan="2" style="width: 15%;">Presidente</td> <td rowspan="2" style="width: 35%;">FERNANDO DANIEL DEL POZO BEINGOLEA</td> <td style="width: 10%;">Titular</td> <td style="width: 5%; text-align: center;">X</td> <td rowspan="2" style="width: 35%;">Unidad de Logística</td> </tr> <tr> <td>Suplente</td> <td></td> </tr> <tr> <td rowspan="2">Primer Miembro</td> <td rowspan="2">FRANK CONDORI GONZALES</td> <td>Titular</td> <td style="text-align: center;">X</td> <td rowspan="2">Oficina de Sistemas de Información (área usuaria)</td> </tr> <tr> <td>Suplente</td> <td></td> </tr> <tr> <td rowspan="2">Segundo Miembro</td> <td rowspan="2">GUEILE ROSIO CURAZI YUPANQUI</td> <td>Titular</td> <td style="text-align: center;">X</td> <td rowspan="2">Oficina de Sistemas de Información (área usuaria)</td> </tr> <tr> <td>Suplente</td> <td></td> </tr> </table>					Presidente	FERNANDO DANIEL DEL POZO BEINGOLEA	Titular	X	Unidad de Logística	Suplente		Primer Miembro	FRANK CONDORI GONZALES	Titular	X	Oficina de Sistemas de Información (área usuaria)	Suplente		Segundo Miembro	GUEILE ROSIO CURAZI YUPANQUI	Titular	X	Oficina de Sistemas de Información (área usuaria)	Suplente	
Presidente	FERNANDO DANIEL DEL POZO BEINGOLEA	Titular	X	Unidad de Logística																						
		Suplente																								
Primer Miembro	FRANK CONDORI GONZALES	Titular	X	Oficina de Sistemas de Información (área usuaria)																						
		Suplente																								
Segundo Miembro	GUEILE ROSIO CURAZI YUPANQUI	Titular	X	Oficina de Sistemas de Información (área usuaria)																						
		Suplente																								
4	<b>SOBRE LAS CONSULTAS Y OBSERVACIONES FORMULADAS POR LOS PARTICIPANTES</b> [COMPLETAR CON: "CONSULTAS", "OBSERVACIONES" O "CONSULTAS Y OBSERVACIONES", SEGÚN CORRESPONDA] Los miembros del comité de selección declaran que se presentaron veinticuatro (24) consultas al requerimiento de la presente bases Administrativas. El participante que formulo las consultas fue el siguiente: <table border="1" style="width: 100%; border-collapse: collapse; margin-top: 5px;"> <tr> <th style="width: 5%;">N°</th> <th style="width: 45%;">Nombre o razón social del participante</th> <th style="width: 20%;">N° de Consultas</th> <th style="width: 30%;">N° de Observaciones</th> </tr> <tr> <td style="text-align: center;">1</td> <td>GTD PERÚ S.A</td> <td style="text-align: center;">24</td> <td></td> </tr> </table>					N°	Nombre o razón social del participante	N° de Consultas	N° de Observaciones	1	GTD PERÚ S.A	24														
N°	Nombre o razón social del participante	N° de Consultas	N° de Observaciones																							
1	GTD PERÚ S.A	24																								
5	<b>SOBRE LA ABSOLUCIÓN DE LAS CONSULTAS Y OBSERVACIONES</b> Las consultas relacionadas al requerimiento se remitieron a la Oficina de Sistemas de Información en su calidad de área usuaria mediante Informe N° 004-2025-INGEMMET/CS de fecha 30 de mayo de 2025 para su pronunciamiento. La Oficina de Sistemas de Información en su calidad área usuaria mediante Memorando N° 0524-2025-INGEMMET/OSI, de fecha 13 de junio de 2025 remitió su pronunciamiento adjuntando la absolución de las consultas, los terminos de referencia actualizados y la Autorización de las modificaciones producto de las consultas y/o observaciones .																									
6	DATOS DE LA NUEVA APROBACIÓN DEL EXPEDIENTE DE CONTRATACIÓN		Número																							
			Fecha																							
7	<b>OBSERVACIÓN</b> De la revisión efectuada en aras de continuar con el trámite conforme a lo referido en el Numeral 72.3 del Artículo 72° del Reglamento de la Ley de Contrataciones del Estado, se visualiza que hubo precisiones y ajustes al requerimiento, producto de las consultas y observaciones; Asimismo el Comité de Selección pone en conocimiento de tal hecho a la Oficina de Administración, la cual aprobo el expediente de contratación. En tal sentido el Comité de Selección ve por conveniente proseguir con el trámite correspondiente.																									
8	<b>ACUERDO DEL COMITÉ DE SELECCIÓN</b> En consecuencia, se procede a la INTEGRACION DE BASES de la <b>ADJUDICACION Simplificada N° N° 026-2024-INGEMMET/CS-1</b> , cuyo objeto de convocatoria es la contratación del <b>"Servicio de Internet, Seguridad Gestionada y Telefonía"</b> ; siendo lunes 16 de junio de 2025 a las 10:30 horas, culmina la sesión y en señal de conformidad suscriben la presente los miembros del Comité de Selección, para su publicación en el SEACE.																									
9	<div style="position: absolute; top: 10px; left: 50%; transform: translate(-50%, -50%); font-weight: bold;">FERNANDO DANIEL DEL POZO BEINGOLEA</div> <div style="position: absolute; bottom: 10px; left: 10%; width: 40%;"> <b>FRANK CONDORI GONZALES</b> </div> <div style="position: absolute; bottom: 10px; right: 10%; width: 40%;"> <b>GUEILE ROSIO CURAZI YUPANQUI</b> </div>																									

# BASES ESTÁNDAR DE ADJUDICACIÓN SIMPLIFICADA 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 in blue ink.



### 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> <ul style="list-style-type: none"> <li>• Abc</li> </ul>	Se refiere a consideraciones importantes a tener en cuenta por el órgano encargado de las contrataciones o comité de selección, según corresponda y por los proveedores.
4	<div>Advertencia</div> <ul style="list-style-type: none"> <li>• Abc</li> </ul>	Se refiere a advertencias a tener en cuenta por el órgano encargado de las contrataciones o comité de selección, según corresponda y por los proveedores.
5	<div>Importante para la Entidad</div> <ul style="list-style-type: none"> <li>• Xyz</li> </ul>	Se refiere a consideraciones importantes a tener en cuenta por el órgano encargado de las contrataciones o comité de selección, según corresponda 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 sombreado.
- 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 marzo, junio y diciembre de 2019, julio 2020, julio y diciembre 2021, junio y octubre de 2022

Y P. E.

## **BASES ESTÁNDAR DE ADJUDICACIÓN SIMPLIFICADA PARA LA CONTRATACIÓN DE SERVICIOS EN GENERAL**



### **ADJUDICACIÓN SIMPLIFICADA N°026-2024-INGEMMET/CS**

PRIMERA CONVOCATORIA

Derivada del Concurso Público N° 003-2024-INGEMMET/CS

### **BASES INTEGRADAS**

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





## 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]*

## **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](http://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, así como el literal a) del artículo 89 del Reglamento.

#### Importante

No pueden formularse consultas ni observaciones respecto del contenido de una ficha de homologación aprobada. 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 el numeral 72.4 del artículo 72 del Reglamento y el literal a) del artículo 89 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. FORMA DE PRESENTACIÓN DE OFERTAS

Las ofertas se presentan conforme lo establecido en el artículo 59 y en el artículo 90 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 Digitales<sup>1</sup>). Los demás documentos deben ser visados por el postor. En el caso de persona jurídica, por su representante legal, apoderado o mandatario designado para dicho fin y, en el caso de persona natural, por este o su apoderado. No se acepta el pegado de la imagen de una firma o visto. Las ofertas se presentan foliadas.

#### Importante

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

### 1.7. 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.*

<sup>1</sup> 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>



En la apertura electrónica de la oferta, el órgano encargado de las contrataciones o el comité de selección, según corresponda, 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.

### 1.8. EVALUACIÓN DE LAS OFERTAS

La evaluación de las ofertas se realiza conforme a lo establecido en el numeral 74.1 y el literal a) del numeral 74.2 del artículo 74 del Reglamento.

En el supuesto de que dos (2) o más ofertas empaten, la determinación del orden de prelación de las ofertas empatadas se efectúa siguiendo estrictamente el orden establecido en el numeral 91.1 del artículo 91 del Reglamento.

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

Importante
<i>En el caso de contratación de servicios en general que se presten fuera de la provincia de Lima y Callao, cuyo valor estimado no supere los doscientos mil Soles (S/ 200,000.00), a solicitud del postor se asigna una bonificación equivalente al diez por ciento (10%) sobre el puntaje total obtenido por los postores con domicilio en la provincia donde prestará el servicio, o en las provincias colindantes, sean o no pertenecientes al mismo departamento o región. El domicilio es el consignado en la constancia de inscripción ante el RNP<sup>2</sup>. Lo mismo aplica en el caso de procedimientos de selección por relación de ítems, cuando algún ítem no supera el monto señalado anteriormente.</i>

### 1.9. 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.

### 1.10. 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.

### 1.11. RECHAZO DE LAS OFERTAS

<sup>2</sup> La constancia de inscripción electrónica se visualizará en el portal web del Registro Nacional de Proveedores: [www.rnp.gob.pe](http://www.rnp.gob.pe)

Previo al otorgamiento de la buena pro, el órgano encargado de las contrataciones o el comité de selección, según corresponda, 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 órgano encargado de las contrataciones o el comité de selección, según corresponda, revisa el cumplimiento de los requisitos de calificación de los postores que siguen en el orden de prelación, en caso las hubiere.

#### 1.12. OTORGAMIENTO DE LA BUENA PRO

Definida la oferta ganadora, el órgano encargado de las contrataciones o el comité de selección, según corresponda, 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.

#### 1.13. CONSENTIMIENTO DE LA BUENA PRO

Quando se hayan presentado dos (2) o más ofertas, el consentimiento de la buena pro se produce a los cinco (5) 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 la Entidad convocante, y es conocido y resuelto por su Titular, cuando el valor estimado sea igual o menor a cincuenta (50) UIT. Cuando el valor estimado sea mayor a dicho monto, el recurso de apelación se presenta ante y es resuelto por el Tribunal de Contrataciones del Estado.

En los procedimientos de selección según relación de ítems, el valor estimado total del procedimiento determina ante quién se presenta el recurso de apelación.

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 órgano encargado de las contrataciones o el comité de selección, según corresponda, 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 órgano encargado de las contrataciones o el comité de selección, según corresponda.*

- 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, o en la Unidad de Trámite Documentario de la Entidad, según corresponda.

### 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 cinco (5) 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 cinco (5) 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.

El contrato se perfecciona con la suscripción del documento que lo contiene, salvo en los contratos cuyo monto del valor estimado no supere los doscientos mil Soles (S/ 200,000.00), en los que se puede perfeccionar con la recepción de la orden de servicios, conforme a lo previsto en la sección específica de las bases.

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 valor estimado del ítem corresponda al parámetro establecido en el párrafo anterior.

##### Importante

*El órgano encargado de las contrataciones o el comité de selección, según corresponda, debe consignar en la sección específica de las bases la forma en que se perfeccionará el contrato, sea con la suscripción del contrato o la recepción de la orden de servicios. En caso la Entidad perfeccione el contrato con la recepción de la orden de servicios no debe incluir la proforma del contrato establecida en el Capítulo V de la sección específica de las bases.*

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 cuyos montos sean iguales o menores 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. Dicha excepción también aplica a 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 no superen el monto señalado anteriormente, 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 el 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.

BASES INTEGRADAS

100  
100

## **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.

Descripción	Unidad de medida
Servicio de ciberseguridad: <ul style="list-style-type: none"><li>• Solución de AntiDDoS</li><li>• Solución de Firewall de Aplicaciones Web</li><li>• Solución de Firewall Perimetral</li><li>• Solución de Filtro de Contenidos Web</li><li>• Solución de protección, detección y respuesta automatizada para endpoints (EDR)</li><li>• Solución de almacenamiento de log y reportería</li><li>• Servicio de Ingeniero Dedicado</li></ul>	Servicio

### 1.3. EXPEDIENTE DE CONTRATACIÓN

El expediente de contratación fue aprobado mediante Formato de Aprobación de Expediente de Contratación N° 032-2025 de fecha 22 de mayo del 2025.

### 1.4. FUENTE DE FINANCIAMIENTO

Recursos Ordinarios

#### Importante

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

### 1.5. SISTEMA DE CONTRATACIÓN

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

### 1.6. DISTRIBUCIÓN DE LA BUENA PRO

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 en el plazo de 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, en concordancia con lo establecido en el expediente de contratación.

### 1.9. COSTO DE REPRODUCCIÓN Y ENTREGA DE BASES

Los participantes registrados tienen el derecho de recabar un ejemplar de las bases, para cuyo efecto deben cancelar S/ 4.00 (Cuatro con 00/100 Soles) en la caja de la Entidad, Av. Canadá Nro. 1470 – San Borja.

Importante
------------

<i>El costo de entrega de un ejemplar de las bases no puede exceder el costo de su reproducción.</i>
--

### 1.10. BASE LEGAL

- Ley N° 32185, que aprueba el Presupuesto del Sector Público del año fiscal 2025.
- Ley N° 32186, que aprueba el Equilibrio Financiero del Presupuesto del Sector Público del año fiscal 2025.
- 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 documentos<sup>3</sup>, 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 – PIDE<sup>4</sup> y siempre que el servicio web se encuentre activo en el Catálogo de Servicios de dicha plataforma, no corresponderá exigir el certificado de vigencia de poder y/o documento nacional de identidad.*

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

<sup>3</sup> La omisión del índice no determina la no admisión de la oferta.

<sup>4</sup> Para mayor información de las Entidades usuarias y del Catálogo de Servicios de la Plataforma de Interoperabilidad del Estado – PIDE ingresar al siguiente enlace <https://www.gobiernodigital.gob.pe/interoperabilidad/>

- e) Declaración jurada de plazo de prestación del servicio. **(Anexo N° 4)<sup>5</sup>**
- 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.

**Importante**

- El órgano encargado de las contrataciones o el comité de selección, según corresponda, 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:**

- a) En el caso de microempresas y pequeñas empresas integradas por personas con discapacidad, o en el caso de consorcios conformados en su totalidad por estas empresas, deben presentar la constancia o certificado con el cual acredite su inscripción en el Registro de Empresas Promocionales para Personas con Discapacidad<sup>6</sup>.

**Advertencia**

El órgano encargado de las contrataciones o el comité de selección, según corresponda, no podrá exigir al postor la presentación de documentos que no hayan sido indicados en los acápite "Documentos para la admisión de la oferta", "Requisitos de calificación" y "Factores de evaluación".

**2.3. REQUISITOS PARA PERFECCIONAR EL CONTRATO**

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

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

<sup>5</sup> 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.

<sup>6</sup> Dicho documento se tendrá en consideración en caso de empate, conforme a lo previsto en el artículo 91 del Reglamento.



- cuenta con facultades para perfeccionar el contrato, cuando corresponda.
- f) Copia de DNI del postor en caso de persona natural, o de su representante legal en caso de persona jurídica.

#### Advertencia

*De acuerdo con el artículo 4 del Decreto Legislativo N° 1246, las Entidades están prohibidas de exigir a los administrados o usuarios la información que puedan obtener directamente mediante la interoperabilidad a que se refieren los artículos 2 y 3 de dicho Decreto Legislativo. En esa medida, si la Entidad es usuaria de la Plataforma de Interoperabilidad del Estado – PIDE<sup>7</sup> y siempre que el servicio web se encuentre activo en el Catálogo de Servicios de dicha plataforma, no corresponderá exigir los documentos previstos en los literales e) y f).*

- g) Domicilio para efectos de la notificación durante la ejecución del contrato.
- h) Autorización de notificación de la decisión de la Entidad sobre la solicitud de ampliación de plazo mediante medios electrónicos de comunicación<sup>8</sup>. **(Anexo N° 12)**.
- i) Detalle de los precios unitarios del precio ofertado<sup>9</sup>.
- j) El Postor que se presente debe contar con el servicio de soporte técnico en modalidad telefónica, con una línea gratuita 0800, mediante una empresa de telecomunicaciones, 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. En caso de ser alquilado, se acreditará mediante el contrato con una empresa que cumpla con tener el servicio en las condiciones requeridas.
- k) El Postor que se presente debe 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. En caso de ser alquilado, se acreditará mediante el contrato con una empresa que cumpla con tener el servicio en las condiciones requeridas.
- l) El postor debe presentar el CERTIFICADO O CONSTANCIA de FIRST.
- m) El postor debe presentar una Declaración jurada de poseer un centro de Operaciones y Seguridad (SOC) propio.
- n) El postor debe presentar un Certificado o constancia del nivel de madurez del Centro de Operaciones y Seguridad (SOC), emitido por una entidad auditoria internacional.
- o) El postor debe presentar un Certificado o constancia de ISO/IEC 27001:2013 o 27001:2022<sup>10</sup> del Centro de Operaciones y Seguridad (SOC).
- p) El postor debe tener 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 2021, 2022, 2023 o 2022, 2023, 2024). Se acreditará mediante el ID y la fecha de publicación respectiva.
- q) El postor debe contar con 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

<sup>7</sup> 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/>

<sup>8</sup> En tanto se implemente la funcionalidad en el SEACE, de conformidad con la Primera Disposición Complementaria Transitoria del Decreto Supremo N° 234-2022-EF.

<sup>9</sup> Incluir solo en caso de la contratación bajo el sistema a suma alzada.

<sup>10</sup> CONSULTA N° 05 de la empresa GTD PERÚ S.A



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

**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 en 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 y el 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 cuyos montos sean iguales o menores 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. Dicha excepción también aplica a 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 no supere el monto señalado anteriormente, conforme a lo dispuesto en el literal a) del artículo 152 del Reglamento.*

**Importante**

- *Corresponde a la Entidad verificar que las garantías presentadas por el postor ganador de la buena pro cumplan con los requisitos y condiciones necesarios para su aceptación y eventual ejecución, sin perjuicio de la determinación de las responsabilidades funcionales que correspondan.*
- *De conformidad con el Reglamento Consular del Perú aprobado mediante Decreto Supremo N° 076-2005-RE para que los documentos públicos y privados extendidos en el exterior tengan validez en el Perú, deben estar legalizados por los funcionarios consulares peruanos y refrendados por el Ministerio de Relaciones Exteriores del Perú, salvo que se trate de documentos públicos emitidos en países que formen parte del Convenio de la Apostilla, en cuyo caso bastará con que estos cuenten con la Apostilla de la Haya<sup>11</sup>.*
- *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**

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



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 a través de la plataforma digital del INGEMMET (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.

## 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 a través de la plataforma digital del INGEMMET (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.

el.  
F. P.

### CAPÍTULO III REQUERIMIENTO

#### Importante

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

### 3.1. TERMINOS DE REFERENCIA



#### TÉRMINOS DE REFERENCIA

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

##### ÍTEM 2 "SERVICIO DE CIBERSEGURIDAD"

#### 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 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 conectividad 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 el siguiente ÍTEM:





N°	Descripción	Unidad de medida
ITEM 02	Servicio de ciberseguridad: <ul style="list-style-type: none"> <li>• Solución de AntiDDoS</li> <li>• Solución de Firewall de Aplicaciones Web</li> <li>• Solución de Firewall Perimetral</li> <li>• Solución de Filtro de Contenidos Web</li> <li>• Solución de protección, detección y respuesta automatizada para endpoints (EDR)</li> <li>• Solución de almacenamiento de log y reportería</li> <li>• Servicio de Ingeniero Dedicado</li> </ul>	Servicio

### 5.1. GENERALIDADES DEL SERVICIO DE CIBERSEGURIDAD (ÍTEM 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 Scrapping, 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 importan.
- 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 simultáneo: 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-directorio 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(opcionalmente), 7(opcionalmente), 8, 8.1 y 10<sup>12</sup>.
- La solución propuesta deberá ser compatible mínimo con los siguientes sistemas operativos: Windows Server 2003 R2 SP2 (opcionalmente), 2008 R1 SP2(Opcionalmente), 2008 R2(Opcionalmente), 2012, 2012 R2, 2016 y 2019<sup>13</sup>
- La solución propuesta deberá ser compatible mínimo con los siguientes sistemas operativos: macOS Versiones: Yosemite (10.10) opcionalmente, El Capitan (10.11), Sierra (10.12), High Sierra (10.13), Mojave (10.14) y Catalina (10.15)<sup>14</sup>
- La solución propuesta deberá ser compatible mínimo con los siguientes sistemas operativos: Linux Versiones: RedHat Enterprise Linux y CentOS 6.8 (opcionalmente), 6.9 (opcionalmente), 6.10 (opcionalmente), 7.2, 7.3, 7.4, 7.5, 7.6 y 7.7 y Ubuntu LTS 16.04.5 (opcionalmente), 16.04.6 (opcionalmente), 18.04.1 y 18.04.2 server, 64-bit<sup>15</sup>
  - 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.

<sup>12</sup> CONSULTA N° 016 de la empresa GTD PERÚ S.A.

<sup>13</sup> CONSULTA N° 017 de la empresa GTD PERÚ S.A.

<sup>14</sup> CONSULTA N° 014 y N° 018 de la empresa GTD PERÚ S.A

<sup>15</sup> CONSULTA N° 019 de la empresa GTD PERÚ S.A.



- 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 periodo 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 retorno 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 contra 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 (inundaciones), 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, Freegate, 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 almacenamiento de log y reportería

- La solución de ALMACENAMIENTO DE LOG Y REPORTERÍA deberá estar implementada en la nube del Contratista y en alta disponibilidad, en caso de ocurrir alguna eventualidad esta deberá pasar de un site a otro site y viceversa. La solución deberá almacenar los logs durante un aproximado de noventa (90) días.
- Para dicho fin, el Contratista deberá contar con un diseño de infraestructura, procesos y personal que permitan la continuidad ante un evento de desastre. A nivel de infraestructura se deberá contar al menos con dos (02) Centros de Datos con certificación internacional TIER III (en Diseño como mínimo), estos centros de datos deberán estar interconectados mediante fibras ópticas y equipos DWDM en alta disponibilidad lo cual permitirá que la solución de ALMACENAMIENTO DE LOG Y REPORTERÍA cuente con un esquema de alta disponibilidad, de tal manera que, ante la caída de una, la otra pueda continuar con las funciones requeridas.
- A nivel de procesos y personal, el Contratista deberá contar al menos con dos (02) ubicaciones de Centro de Operaciones de Seguridad (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 de la solución.
- Sobre el equipamiento a considerar en cada uno de los sites que conforman la nube del Contratista se deberá tener en cuenta:
  - Si la solución es virtualizada, debe ser compatible con el ambiente VMware ESXi 5.0/5.1/5.5/6.0/6.5/6.7 o con versiones superiores<sup>16</sup>.
  - Si la solución es virtualizada, debe ser compatible con el ambiente Microsoft Hyper-V 2008 R2 / 2012 / 2012 R2/2016 o con versiones superiores<sup>17</sup>.
  - Si la solución es virtualizada, debe ser compatible con el ambiente Citrix XenServer 6.0+.
  - Si la solución es virtualizada, debe ser compatible con el ambiente Open Source Xen 4.1+.
  - Si la solución es virtualizada, debe ser compatible con el ambiente KVM on Redhat 6.5+ and Ubuntu 17.04.
  - Si la solución es virtualizada, debe ser compatible con el ambiente Nutanix AHV (AOS 5.10.5).

<sup>16</sup> CONSULTA N° 022 de la empresa GTD PERÚ S.A.

<sup>17</sup> CONSULTA N° 023 de la empresa GTD PERÚ S.A.



- Si la solución es virtualizada, debe ser compatible con el ambiente Amazon Web Services (AWS).
- Si la solución es virtualizada, debe ser compatible con el ambiente Microsoft Azure.
- Si la solución es virtualizada, debe ser compatible con el ambiente Google Cloud (GCP).
- Si la solución es virtualizada, debe ser compatible con el ambiente Oracle Cloud Infrastructure (OCI).
- Si la solución es virtualizada, debe ser compatible con el ambiente Alibaba Cloud (AliCloud).
- Si la solución es virtualizada, no debe haber límites a la cantidad de múltiples vCPU.
- Si la solución es virtualizada, no debe haber límites a la expansión de memoria RAM.
- Debe soportar acceso vía SSH, WEB (HTTPS) para la gestión de la solución.
- Contar con comunicación cifrada y autenticación con usuario y contraseña para la obtención de reportes, tanto en interface gráfica (GUI) como vía línea de comandos en consola de gestión.
- Permitir acceso simultáneo de administración, así como permitir crear por lo menos 2 (dos) perfiles para administración y monitoreo.
- Soporte SNMP versión 2 y 3.
- Permitir virtualizar la gestión y administración de los dispositivos, donde cada administrador solo tenga acceso a los equipos autorizados.
- Debe permitir la creación de administrador general, que tenga acceso general a todas las instancias de virtualización de la solución.
- Debe permitir activar y desactivar para cada interface de la plataforma, los permisos de acceso HTTP, HTTPS, SSH.
- Autenticación de usuarios de acceso a la plataforma via LDAP.
- Autenticación de usuarios de acceso a la plataforma via Radius.
- Autenticación de usuarios de acceso a la plataforma via TACACS+.
- Generación de informes en tiempo real de tráfico, en formato de gráfica de mapas geográficos.
- Generación de informes en tiempo real de tráfico, en formato de gráfica de burbuja.
- Generación de informes en tiempo real de tráfico, en formato de gráfica tabla.
- Definición de perfiles de acceso a consola con permiso granulares, tales como: acceso de escritura, de lectura, de creación de nuevos usuarios y cambios en configuraciones generales.
- Debe contar con un asistente gráfico para agregar nuevos dispositivos, usando la dirección IP, usuario y contraseña del mismo.
- Debe ser posible ver la cantidad de logs enviados desde cada dispositivo supervisado.
- Contar con mecanismos de borrado automático de logs antiguos.
- Permitir la importación y exportación de reportes.
- Debe contar con la capacidad de crear informes en formato HTML.
- Debe contar con la capacidad de crear informes en formato PDF.
- Debe contar con la capacidad de crear informes en formato XML.
- Debe contar con la capacidad de crear informes en formato CSV.
- Debe permitir exportar los logs en formato CSV.
- Generación de logs de auditoría, con detalle de la configuración realizada, el administrador que realizó el cambio y hora del mismo.
- Los logs generados por los dispositivos administrados deben ser centralizados en los servidores de la plataforma, pero la solución debe ofrecer también la posibilidad de utilizar un servidor externo de Syslog o similar.
- La solución debe contar con reportes predefinidos.



- Debe poder enviar automáticamente los logs a un servidor FTP externo a la solución.
- Debe ser posible la duplicación de reportes existentes para su posterior edición.
- Debe tener la capacidad de personalizar la portada de los reportes obtenidos.
- Permitir centralmente la visualización de logs recibidos por uno o más dispositivos, incluido la capacidad de uso de filtros para facilitar la búsqueda dentro de los mismos logs.
- Los logs de auditoría de cambios de configuración de reglas y objetos deben ser visualizados en una lista distinta a la de los logs relacionados a tráfico de datos.
- Tener la capacidad de personalización de gráficas en los reportes, tales como barras, líneas y tablas.
- Debe poseer mecanismo de "Drill-Down" para navegar en los reportes de tiempo real.
- Debe permitir descargar de la plataforma los archivos de logs para uso externo.
- Tener la capacidad de generar y enviar reportes periódicos automáticamente.
- Permitir la personalización de cualquier reporte preestablecido por la solución, exclusivamente por el Administrador, para adoptarlo a sus necesidades.
- Permitir el envío por email de manera automática de reportes.
- Debe permitir que el reporte a enviar por email sea al destinatario específico.
- Permitir la programación de la generación de reportes, conforme a un calendario definido por el administrador.
- Debe ser posible visualizar gráficamente en tiempo real la tasa de generación de logs por cada dispositivo gestionado.
- Debe permitir el uso de filtros en los reportes.
- Debe permitir definir el diseño de los reportes, incluir gráfico, añadir texto e imágenes, alineación, saltos de página, fuentes, colores, entre otros.
- Permitir especificar el idioma de los reportes creados.
- Generar alertas automáticas vía email, SNMP y Syslog, basado en eventos especiales en logs, severidad del evento, entre otros.
- Debe permitir el envío automático de reportes a un servidor externo SFTP o FTP.
- Debe ser capaz de crear consultas SQL o similar dentro de las bases de datos de logs, para uso en gráficas y tablas en reportes.
- Tener la capacidad de visualizar en GUI de reportes de información del Sistema, como licencias, memoria, disco duro, uso de CPU, tasa de logs por segundo recibidos, total de logs diarios recibidos, alertas del sistema, entre otros.
- Debe contar con una herramienta que permita analizar el rendimiento en la generación de reportes, con el objetivo de detectar y arreglar problemas en generación de los mismos.
- Que la solución sea capaz de importar archivos con logs de dispositivos compatibles conocido y no conocidos por la plataforma, para posterior generación de reportes.
- Debe ser posible poder definir el espacio que cada instancia de virtualización puede utilizar para almacenamiento de logs.
- Debe proporcionar la información de cantidad de logs almacenados y la estadística de tiempo restante de almacenado.
- Debe ser compatible con autenticación de doble factor (token) para usuarios administradores de la plataforma.
- Debe permitir aplicar políticas para el uso de contraseñas para los administradores de la plataforma, como tamaño mínimo y caracteres permitidos.
- Debe permitir visualizar en tiempo real los logs recibidos.
- Debe permitir el reenvío de logs en formato syslog.
- Debe permitir el reenvío de logs en formato CEF (Common Event Format).



- Debe incluir dashboard para operaciones SOC que monitorea las principales amenazas de seguridad para su red
- Debe incluir dashboard para operaciones SOC que monitorea comprometimiento de usuarios y uso sospechoso de la web en su red.
- Debe incluir dashboard para operaciones SOC que monitorea el tráfico en su red.
- Debe incluir dashboard para operaciones SOC que monitorea el tráfico de aplicaciones y sitios web en su red
- Debe incluir dashboard para operaciones SOC que monitorea detecciones de amenazas de día cero en su red (sandboxing).
- Debe incluir dashboard para operaciones SOC que monitorea actividad de endpoints en su red.
- Debe incluir dashboard para operaciones SOC que monitorea actividad VPN en su red.
- Debe incluir dashboard para operaciones SOC que monitorea puntos de acceso WiFi y SSIDs.
- Debe incluir dashboard para operaciones SOC que monitorea rendimiento de recursos local de la solución (CPU, Memoria).
- Debe permitir crear dashboards personalizados para monitoreo de operaciones SOC.
- Debe soportar configuración de alta disponibilidad Master/Slave en la capa 3.
- Debe permitir generar alertas de eventos a partir de logs recibidos.
- Debe permitir crear incidentes a partir de alertas de eventos para endpoint.
- Debe permitir la integración al sistema de tickets ServiceNow.
- Debe soportar servicio de Indicadores de Compromiso (IoC) del mismo fabricante, que muestre las sospechas de comprometimiento de usuarios finales en la web, debiendo informar por lo menos: dirección IP de usuario, hostname, sistema operativo, veredicto (clasificación general de la amenaza), el número de amenazas detectadas.
- Debe permitir respaldar logs en nube publica de Amazon S3.
- Debe permitir respaldar logs en nube publica de Microsoft Azure.
- Debe permitir respaldar logs en nube publica de Google Cloud.
- Debe soportar el estándar SAML para autenticación de usuarios administradores.
- Debe contar con reporte de cumplimiento de PCI DSS.
- Debe contar con reporte de utilización de aplicaciones SaaS.
- Debe contar con reporte de prevención de pérdida de datos (DLP).
- Debe contar con reporte de VPN.
- Debe contar con reporte de Sistema de prevención de intrusos (IPS).
- Debe contar con reporte de reputación de cliente.
- Debe contar con reporte de análisis de seguridad de usuario.
- Debe contar con reporte de análisis de amenaza cibernética.
- Debe contar con reporte de breve resumen diario de eventos e incidentes de seguridad.
- Debe contar con reporte de tráfico DNS.
- Debe contar con reporte tráfico de correo electrónico.
- Debe contar con reporte de Top 10 de Aplicaciones utilizadas en la red.
- Debe contar con reporte de Top 10 de Websites utilizadas en la red.
- Debe contar con reporte de uso de redes sociales.
- Debe contar con reporte de evaluación de riesgo para correo electrónico.
- Debe contar con reporte de cumplimiento PCI de Wireless.
- Debe contar con reporte de AP's y SSID's autorizados, así como clientes WIFI.
- Debe contar con reporte de vulnerabilidades de solución gestionada de seguridad de equipo terminal.
- Debe contar con reporte de aplicaciones web, si se cuenta con plataforma de seguridad web.



- EL PROVEEDOR deberá entregar los siguientes reportes:
  - a. Un reporte mensual con el resumen ejecutivo.
  - b. Un reporte detallado del consumo de tráfico, aplicaciones, servicios web entre otros de los equipos de seguridad informática en comodato.

**g) 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 siempre y cuando se cuente con la confirmación del fabricante de que la nueva versión de firmware ya es estable<sup>18</sup>.
  - 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

<sup>18</sup> CONSULTA N° 024 de la empresa GTD PERÚ S.A



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), sea propio o tercerizado, 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.

**Importante:** El postor deberá presentar una Declaración jurada de contar con un Centro de Operaciones y Seguridad (SOC), para la suscripción del contrato.

- El Contratista deberá contar con un equipo de respuesta ante incidentes (sea propio o tercerizado), el cual 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 de su partner o socio estratégico para la suscripción del contrato.

- 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 4.7, 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 suscripción del contrato.

- El Contratista deberá operar bajo las mejores prácticas y estándares en seguridad de la información, para lo cual deberá acreditar que ha logrado obtener una certificación de estándares internacionales como el ISO 27001 que cubra el alcance la prestación de servicios relacionados como "Servicios TI" en el territorio nacional.

**Importante:** El Postor debe presentar un Certificado o constancia de ISO/IEC 27001:2013 o 27001:2022 del Centro de Operaciones y Seguridad (SOC) para la suscripción del contrato <sup>19</sup>.

<sup>19</sup> CONSULTA N° 05 de la empresa GTD PERÚ S.A.

- 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 Centro de Operaciones y Seguridad (SOC) tiene como alcance el monitoreo las plataformas de seguridad incluidas en este ITEM.
- El SOC brindará una primera respuesta o comunicación a todos los incidentes críticos en un plazo de 30 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.
- 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/o v4 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.
- Al momento de la solución de una incidencia o avería, el Contratista deberá presentar un reporte preliminar, en un plazo máximo de veinticuatro (24) 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.

**REQUERIMIENTO DE LA MESA DE AYUDA DEL CONTRATISTA**

- a) El Postor deberá contar con el servicio de soporte técnico en modalidad telefónica, con una línea gratuita 0800, mediante una empresa de telecomunicaciones, 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 suscripción del contrato.

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 suscripción del contrato.

- 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 suscripción del contrato.

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, por ende, cumplir con las buenas prácticas usadas para la gestión de servicios de tecnologías de la información, su inclusión en el cuadrante de Gartner, 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 suscripción del contrato.

- 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. 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 suscripción del contrato.

#### 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.

BA

Handwritten signature and stamp in the bottom right corner.



**REQUISITOS DE CALIFICACIÓN**

B	CAPACIDAD TÉCNICA Y PROFESIONAL
B.3	CALIFICACIONES DEL PERSONAL CLAVE
B.3.1	FORMACIÓN ACADÉMICA
	<u>Ítem 02</u>
	<u>Requisitos:</u>
	Un (1) jefe del Proyecto
	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 o Ingeniería de Telecomunicaciones o Ingeniería de Sistemas e Informática y/o Ingeniería de Computación y Sistemas <sup>20</sup> .
	Un (1) Ingeniero Especialista en Seguridad
	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 o Ingeniería de Telecomunicaciones o Ingeniería de Sistemas e Informática y/o Ingeniería de Computación y Sistemas <sup>21</sup> .
	Un (1) Jefe de Ciberseguridad

32

<sup>20</sup> CONSULTA N° 08 de la empresa GTD PERÚ S.A

<sup>21</sup> CONSULTA N° 08 de la empresa GTD PERÚ S.A

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 o Ingeniería de Sistemas e Informática y/o Ingeniería de Computación y Sistemas<sup>22</sup>.

**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 y/o Ingeniería de Sistemas e Informática y/o Ingeniería de Computación y Sistemas<sup>23</sup>.

**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.4 EXPERIENCIA DEL PERSONAL CLAVE**

**Un (1) Jefe del Proyecto**

Experiencia mínima de cinco (5) años en la gestión y/o planificación y/o entrega en producción y/o coordinación, de la implementación de Proyectos de TI y/o Seguridad Gestionada y/o Servicios de Telecomunicaciones, como Jefe o Gestor o Coordinador o Encargado o Gerente o Subgerente del personal requerido como Jefe del Proyecto.

**Un (1) Ingeniero Especialista en Seguridad**

Experiencia mínima de cuatro (4) años en configuración y/o implementación y/o soporte y/o administración y/o monitoreo en proyectos de plataformas de Seguridad y/o CyberSOC y/o Ciberseguridad y/o Seguridad Gestionada y/o Servicio de Respuesta ante Incidentes.

**Un (1) Jefe de Ciberseguridad**

Experiencia mínima de cinco (5) años en configuración y/o implementación y/o análisis y/o soporte y/o administración y/o monitoreo y/o auditoría en proyectos de Ciberseguridad y/o CyberSOC y/o Security Advisor y/o Ciberinteligencia como Especialista o Analista Técnico o Jefe o Líder.

**Un (01) Especialista Help Desk**

Experiencia mínima de tres (03) años de experiencia en la supervisión y/o soporte en proyectos de Soporte Técnico y/o mesa de ayuda y/o su equivalente en inglés Help Desk<sup>24</sup>

**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.

<sup>22</sup> CONSULTA N° 08 de la empresa GTD PERÚ S.A

<sup>23</sup> CONSULTA N° 08 de la empresa GTD PERÚ S.A

<sup>24</sup> CONSULTA N° 10 de la empresa GTD PERÚ S.A



C	<b>EXPERIENCIA DEL POSTOR EN LA ESPECIALIDAD</b>
	<p><u>Item 02</u> <u>Requisitos:</u></p> <p>El postor debe acreditar un monto facturado acumulado equivalente a S/ 7,000,000.00 (siete 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"> <li>- Servicio de Licencias o Servicio de CYBERSOC o Administración y Monitoreo de Plataformas de Seguridad y Correlación Inteligente de Eventos de Seguridad</li> <li>- Servicio de soporte de mantenimiento, monitoreo y administración de plataformas de seguridad TI</li> <li>- Servicio de monitoreo de eventos de seguridad (SOC)</li> <li>- Servicio de CyberSOC o Cyber Defense Center</li> <li>- Soporte, gestión, mantenimiento o monitoreo de equipamiento o plataformas de seguridad</li> <li>- Servicio de seguridad Gestionada, Solución Integral Tecnológica de Ciberseguridad— SIEM</li> <li>- Servicio de soporte de plataforma de seguridad y correlación, servicio de protección de tráfico web, sistema de correlación de eventos-SIEM</li> <li>- Servicio de Seguridad Gestionada</li> <li>- Servicio de housing y/o centro de datos tercerizado y/o servicios gestionados especializados en seguridad e infraestructura TI.</li> <li>- Servicio de acceso a internet de alta disponibilidad y seguridad y/o servicio de telecomunicaciones.</li> </ul> <p><u>Acreditación:</u></p> <p>La experiencia del contratista en la especialidad se acreditará con copia simple de (i) contratos u órdenes de servicios, y su respectiva conformidad o constancia de prestación; o (ii) comprobantes de pago cuya cancelación se acredite documental y fehacientemente, con voucher de depósito, nota de abono, reporte de estado de cuenta, cualquier otro documento emitido por Entidad del sistema financiero que acredite el abono o mediante cancelación en el mismo comprobante de pago<sup>78</sup>, correspondientes a un máximo de veinte (20) contrataciones.</p> <p>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.</p> <p>En el caso de servicios de ejecución periódica o continuada, solo se considera como experiencia la parte del contrato que haya sido ejecutada durante los ocho (8) años anteriores a la fecha de presentación de ofertas, debiendo adjuntarse copia de las conformidades correspondientes a tal parte o los respectivos comprobantes de pago cancelados.</p> <p>En los casos que se acredite experiencia adquirida en consorcio, debe presentarse la promesa de consorcio o el contrato de consorcio del cual se</p>

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.

BA

Handwritten signature and initials in blue ink.



**Importante**

Para determinar que los postores cuentan con las capacidades necesarias para ejecutar el contrato, el órgano encargado de las contrataciones o el comité de selección, según corresponda, 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**

<b>B</b>	<b>CAPACIDAD TÉCNICA Y PROFESIONAL</b>
<b>B.3</b>	<b>CALIFICACIONES DEL PERSONAL CLAVE</b>
<b>B.3.1</b>	<b>FORMACIÓN ACADÉMICA</b>
	<p><u>Requisitos:</u></p> <p><b>Un (01) Jefe de Proyecto</b></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 o Ingeniería de telecomunicaciones o Ingeniería de Sistemas e Informática y/o Ingeniería de Computación y Sistemas<sup>25</sup>.</p> <p><b>Un (01) Ingeniero Especialista en Seguridad</b></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 o Ingeniería de Telecomunicaciones o Ingeniería de Sistemas e Informática y/o Ingeniería de Computación y Sistemas<sup>26</sup>.</p> <p><b>Un (01) Jefe de Ciberseguridad</b></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 o Ingeniería de Sistemas e Informática y/o Ingeniería de Computación y Sistemas<sup>27</sup>.</p> <p><b>Un (01) Especialista Help Desk</b></p> <p>Profesional Titulado y/o Bachiller en Ingeniería Electrónica y/o en Telecomunicaciones y/o Ingeniería de Sistemas y/o Ingeniería Mecatrónica y/o Ingeniería Informática y/o Ingeniería de computación y/o Ingeniería de Sistemas e Informática y/o Ingeniería de Computación y Sistemas<sup>28</sup>.</p> <p><u>Acreditación:</u></p> <p>El título Profesional 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: <a href="https://enlinea.sunedu.gob.pe/">https://enlinea.sunedu.gob.pe/</a> o en el Registro Nacional de Certificados, Grados y Títulos a cargo del Ministerio de Educación a través del siguiente link: <a href="https://titulosinstitutos.minedu.gob.pe/">https://titulosinstitutos.minedu.gob.pe/</a>, 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>B.4</b>	<b>EXPERIENCIA DEL PERSONAL CLAVE</b>

<sup>25</sup> CONSULTA N° 08 de la empresa GTD PERÚ S.A<sup>26</sup> CONSULTA N° 08 de la empresa GTD PERÚ S.A<sup>27</sup> CONSULTA N° 08 de la empresa GTD PERÚ S.A<sup>28</sup> CONSULTA N° 08 de la empresa GTD PERÚ S.A

	<p><b>Requisitos:</b></p> <p><b>Un (1) Jefe del Proyecto</b></p> <p>Experiencia mínima de cinco (5) años en la gestión y/o planificación y/o entrega en producción y/o coordinación, de la implementación de Proyectos de TI y/o Seguridad Gestionada y/o Servicios de Telecomunicaciones, como Jefe o Gestor o Coordinador o Encargado o Gerente o Subgerente del personal requerido como Jefe del Proyecto.</p> <p><b>Un (1) Ingeniero Especialista en Seguridad</b></p> <p>Experiencia mínima de cuatro (4) años en configuración y/o implementación y/o soporte y/o administración y/o monitoreo en proyectos de plataformas de Seguridad y/o CyberSOC y/o Ciberseguridad y/o Seguridad Gestionada y/o Servicio de Respuesta ante Incidentes.</p> <p><b>Un (1) Jefe de Ciberseguridad</b></p> <p>Experiencia mínima de cinco (5) años en configuración y/o implementación y/o análisis y/o soporte y/o administración y/o monitoreo y/o auditoría en proyectos de Ciberseguridad y/o CyberSOC y/o Security Advisor y/o Ciberinteligencia como Especialista o Analista Técnico o Jefe o Líder.</p> <p><b>Un (01) Especialista Help Desk</b></p> <p>Experiencia mínima de tres (03) años de experiencia en la supervisión y/o soporte en proyectos de Soporte Técnico y/o mesa de ayuda y/o su equivalente en inglés Help Desk<sup>29</sup></p> <p><u>De presentarse experiencia ejecutada paralelamente (traslape), para el cómputo del tiempo de dicha experiencia sólo se considerará una vez el periodo traslapado.</u></p> <p><b>Acreditación:</b></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> <table><tr><th>Importante</th></tr><tr><td><ul style="list-style-type: none"><li>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.</li><li>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.</li><li>Se considerará aquella experiencia que no tenga una antigüedad mayor a veinticinco (25) años anteriores a la fecha de la presentación de ofertas.</li><li>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.</li></ul></td></tr></table>	Importante	<ul style="list-style-type: none"><li>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.</li><li>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.</li><li>Se considerará aquella experiencia que no tenga una antigüedad mayor a veinticinco (25) años anteriores a la fecha de la presentación de ofertas.</li><li>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.</li></ul>
Importante			
<ul style="list-style-type: none"><li>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.</li><li>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.</li><li>Se considerará aquella experiencia que no tenga una antigüedad mayor a veinticinco (25) años anteriores a la fecha de la presentación de ofertas.</li><li>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.</li></ul>			
C	EXPERIENCIA DEL POSTOR EN LA ESPECIALIDAD		

<sup>29</sup> CONSULTA N° 10 de la empresa GTD PERÚ S.A



Requisitos:

El postor debe acreditar un monto facturado acumulado equivalente a **S/ 7,000,000.00 (siete 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
- Servicio de housing y/o centro de datos tercerizado y/o servicios gestionados especializados en seguridad e infraestructura TI.
- Servicio de acceso a internet de alta disponibilidad y seguridad y/o servicio de telecomunicaciones.

Acreditación:

La experiencia del postor en la especialidad se acreditará con copia simple de (i) contratos u órdenes de servicios, y su respectiva conformidad o constancia de prestación; o (ii) comprobantes de pago cuya cancelación se acredite documental y fehacientemente, con voucher de depósito, nota de abono, reporte de estado de cuenta, cualquier otro documento emitido por Entidad del sistema financiero que acredite el abono o mediante cancelación en el mismo comprobante de pago<sup>30</sup>, 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

<sup>30</sup> 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".

o los respectivos comprobantes de pago cancelados.

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

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

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

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

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

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

#### Importante

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



**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
<b>A. PRECIO</b>	
<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 ( <b>Anexo N° 6</b> ).	<p>La evaluación consistirá en otorgar el máximo puntaje a la oferta de precio más bajo y otorgar a las demás ofertas puntajes inversamente proporcionales a sus respectivos precios, según la siguiente fórmula:</p> $P_i = \frac{O_m \times PMP}{O_i}$ <p>i= Oferta Pi= Puntaje de la oferta a evaluar Oi=Precio i Om= Precio de la oferta más baja PMP=Puntaje máximo del precio</p> <p style="text-align: right;"><b>100 puntos</b></p>

**Importante**

*Los factores de evaluación elaborados por el órgano encargado de las contrataciones o el comité de selección, según corresponda, 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 órgano encargado de las contrataciones o el comité de selección, según corresponda, adjudicó la buena pro de la **ADJUDICACIÓN SIMPLIFICADA N° 026-2024-INGEMMET/CS-1** para la contratación del 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 la contratación del 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 PAGO<sup>31</sup>**

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

En caso de retraso en el pago por parte de LA ENTIDAD, salvo que se deba a caso fortuito o fuerza

<sup>31</sup> En cada caso concreto, dependiendo de la naturaleza del contrato, podrá adicionarse la información que resulte pertinente a efectos de generar el pago.



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:

##### **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

De conformidad con el artículo 152 del Reglamento, no se constituirá garantía de fiel cumplimiento del contrato ni garantía de fiel cumplimiento por prestaciones accesorias, en contratos cuyos montos sean iguales o menores a doscientos mil Soles (S/ 200,000.00). Dicha excepción también aplica a 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 no supere el monto señalado anteriormente.

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

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

#### **CLÁUSULA 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.*

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 CONTROVERSIAS<sup>32</sup>**

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.

El arbitraje será institucional y resuelto por TRIBUNAL ARBITRAL. LA ENTIDAD propone las siguientes instituciones arbitrales:

Razón Social	RUC	Página Web
CENTRO DE ANÁLISIS Y RESOLUCIÓN DE CONFLICTOS DE LA PONTIFICIA UNIVERSIDAD CATÓLICA DEL PERÚ	20155945860	<a href="https://carc.pucp.edu.pe/">https://carc.pucp.edu.pe/</a>
CAMARA DE COMERCIO DE LIMA	20101266819	<a href="https://www.arbitrajeccl.com.pe/">https://www.arbitrajeccl.com.pe/</a>
CENTRO INTERNACIONAL DE ARBITRAJE DE LA CAMARA DE COMERCIO AMERICANA DEL PERU - AMCHAM PERU	20101917003	<a href="http://www.amcham.org.pe">www.amcham.org.pe</a>

La parte que inicie el arbitraje optará por una de las instituciones rigiendo a 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: [.....]

<sup>32</sup> 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).



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"

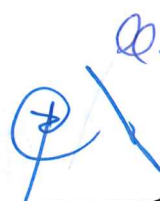
**Importante**

*Este documento puede firmarse digitalmente si ambas partes cuentan con firma digital, según la Ley N° 27269, Ley de Firmas y Certificados Digitales<sup>33</sup>.*

<sup>33</sup> 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

BASES INTEGRADAS





## ANEXO N° 1

### DECLARACIÓN JURADA DE DATOS DEL POSTOR

Señores

**ÓRGANO ENCARGADO DE LAS CONTRATACIONES**

**ADJUDICACIÓN SIMPLIFICADA N° 026-2024-INGEMMET/CS-1**

Presente.-

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

Nombre, Denominación o Razón Social :			
Domicilio Legal :			
RUC :	Teléfono(s) :		
MYPE <sup>34</sup>	Sí	No	
Correo electrónico :			

#### Autorización de notificación por correo electrónico:

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

1. Solicitud de la descripción a detalle de todos los elementos constitutivos de la oferta.
2. Solicitud de reducción de la oferta económica.
3. Solicitud de subsanación de los requisitos para perfeccionar el contrato.
4. Solicitud para presentar los documentos para perfeccionar el contrato, según orden de prelación, de conformidad con lo previsto en el artículo 141 del Reglamento.
5. Respuesta a la solicitud de acceso al expediente de contratación.
6. Notificación de la orden de servicios<sup>35</sup>

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.*

<sup>34</sup> 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. Asimismo, dicha información se tendrá en cuenta en caso de empate, conforme a lo previsto en el artículo 91 del Reglamento.

<sup>35</sup> Cuando el monto del valor estimado del procedimiento o del ítem no supere los doscientos mil Soles (S/ 200,000.00), en caso 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

ÓRGANO ENCARGADO DE LAS CONTRATACIONES

ADJUDICACIÓN SIMPLIFICADA N° 026-2024-INGEMMET/CS-1

Presente.-

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

Datos del consorciado 1			
Nombre, Denominación o Razón Social :			
Domicilio Legal :			
RUC :	Teléfono(s) :		
MYPE <sup>36</sup>	Sí	No	
Correo electrónico :			

Datos del consorciado 2			
Nombre, Denominación o Razón Social :			
Domicilio Legal :			
RUC :	Teléfono(s) :		
MYPE <sup>37</sup>	Sí	No	
Correo electrónico :			

Datos del consorciado ...			
Nombre, Denominación o Razón Social :			
Domicilio Legal :			
RUC :	Teléfono(s) :		
MYPE <sup>38</sup>	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:

<sup>36</sup> 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. Asimismo, dicha información se tendrá en cuenta en caso de empate, conforme a lo previsto en el artículo 91 del Reglamento. Para dichos efectos, todos los integrantes del consorcio deben acreditar la condición de micro o pequeña empresa.

<sup>37</sup> Ibídem.

<sup>38</sup> Ibídem.



1. Solicitud de la descripción a detalle de todos los elementos constitutivos de la oferta.
2. Solicitud de reducción de la oferta económica.
3. Solicitud de subsanación de los requisitos para perfeccionar el contrato.
4. Solicitud para presentar los documentos para perfeccionar el contrato, según orden de prelación, de conformidad con lo previsto en el artículo 141 del Reglamento.
5. Respuesta a la solicitud de acceso al expediente de contratación.
6. Notificación de la orden de servicios<sup>39</sup>

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.*

<sup>39</sup> Cuando el monto del valor estimado del procedimiento o del ítem no supere los doscientos mil Soles (S/ 200,000.00), en caso 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

**ÓRGANO ENCARGADO DE LAS CONTRATACIONES**

**ADJUDICACIÓN SIMPLIFICADA N° 026-2024-INGEMMET/CS-1**

Presente.-

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

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

[CONSIGNAR CIUDAD Y FECHA]

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

**Importante**

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



### ANEXO N° 3

#### DECLARACIÓN JURADA DE CUMPLIMIENTO DE LOS TÉRMINOS DE REFERENCIA

Señores

**ÓRGANO ENCARGADO DE LAS CONTRATACIONES**

**ADJUDICACIÓN SIMPLIFICADA N° 026-2024-INGEMMET/CS-1**

Presente.-

Es grato dirigirme a usted, para hacer de su conocimiento que luego de haber examinado las bases y demás documentos del procedimiento de la referencia y, conociendo todos los alcances y las condiciones detalladas en dichos documentos, el postor que suscribe ofrece el Servicio de Internet, Seguridad Gestionada y Telefonía - **SERVICIO DE CIBERSEGURIDAD**, 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

**ÓRGANO ENCARGADO DE LAS CONTRATACIONES**

**ADJUDICACIÓN SIMPLIFICADA N° 026-2024-INGEMMET/CS-1**

Presente.-

Mediante el presente, con pleno conocimiento de las condiciones que se exigen en las bases del procedimiento de la referencia, me comprometo a prestar el servicio objeto del presente procedimiento de acuerdo al siguiente detalle:

##### 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

[CONSIGNAR CIUDAD Y FECHA]

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



## ANEXO N° 5

### PROMESA DE CONSORCIO

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

Señores

**ÓRGANO ENCARGADO DE LAS CONTRATACIONES**

**ADJUDICACIÓN SIMPLIFICADA N° 026-2024-INGEMMET/CS-1**

Presente.-

Los suscritos declaramos expresamente que hemos convenido en forma irrevocable, durante el lapso que dure el procedimiento de selección, para presentar una oferta conjunta a la **ADJUDICACIÓN SIMPLIFICADA N° 026-2024-INGEMMET/CS-1**

Asimismo, en caso de obtener la buena pro, nos comprometemos a formalizar el contrato de consorcio, de conformidad con lo establecido por el artículo 140 del Reglamento de la Ley de Contrataciones del Estado, bajo las siguientes condiciones:

a) Integrantes del consorcio

1. [NOMBRE, DENOMINACIÓN O RAZÓN SOCIAL DEL CONSORCIADO 1].
2. [NOMBRE, DENOMINACIÓN O RAZÓN SOCIAL DEL CONSORCIADO 2].

b) Designamos a [CONSIGNAR NOMBRES Y APELLIDOS DEL REPRESENTANTE COMÚN], identificado con [CONSIGNAR TIPO DE DOCUMENTO DE IDENTIDAD] N° [CONSIGNAR NÚMERO DE DOCUMENTO DE IDENTIDAD], como representante común del consorcio para efectos de participar en todos los actos referidos al procedimiento de selección, suscripción y ejecución del contrato correspondiente con [CONSIGNAR NOMBRE DE LA ENTIDAD].

Asimismo, declaramos que el representante común del consorcio no se encuentra impedido, inhabilitado ni suspendido para contratar con el Estado.

c) Fijamos nuestro domicilio legal común en [.....].

d) Las obligaciones que corresponden a cada uno de los integrantes del consorcio son las siguientes:

1. OBLIGACIONES DE [NOMBRE, DENOMINACIÓN O RAZÓN SOCIAL DEL CONSORCIADO 1] [ % ]<sup>40</sup>

[DESCRIBIR LAS OBLIGACIONES DEL CONSORCIADO 1]

2. OBLIGACIONES DE [NOMBRE, DENOMINACIÓN O RAZÓN SOCIAL DEL CONSORCIADO 2] [ % ]<sup>41</sup>

[DESCRIBIR LAS OBLIGACIONES DEL CONSORCIADO 2]

TOTAL OBLIGACIONES 100%<sup>42</sup>

<sup>40</sup> Consignar únicamente el porcentaje total de las obligaciones, el cual debe ser expresado en número entero, sin decimales.

<sup>41</sup> Consignar únicamente el porcentaje total de las obligaciones, el cual debe ser expresado en número entero, sin decimales.

<sup>42</sup> Este porcentaje corresponde a la sumatoria de los porcentajes de las obligaciones de cada uno de los integrantes del consorcio.

[CONSIGNAR CIUDAD Y FECHA]

.....  
**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.*

BASES INTEGRADAS

Handwritten signature and initials in blue ink.



## ANEXO N° 6

### PRECIO DE LA OFERTA

Señores

**ÓRGANO ENCARGADO DE LAS CONTRATACIONES**

**ADJUDICACIÓN SIMPLIFICADA N° 026-2024-INGEMMET/CS-1**

Presente.-

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

CONCEPTO	PRECIO TOTAL
Servicio de Internet Seguridad Gestionada y Telefónica – <b>SERVICIO DE CIBERSEGURIDAD</b>	
<b>TOTAL</b>	

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.*
- *En caso que el postor reduzca su oferta, según lo previsto en el artículo 68 del Reglamento, debe presentar nuevamente este Anexo.*

ANEXO N° 8

EXPERIENCIA DEL POSTOR EN LA ESPECIALIDAD

Señores  
ÓRGANO ENCARGADO DE LAS CONTRATACIONES  
ADJUDICACIÓN SIMPLIFICADA N° 026-2024-INGEMMET/CS-1  
Presente.-

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

N°	CLIENTE	OBJETO DEL CONTRATO	N° CONTRATO / O/S / COMPROBANTE DE PAGO	FECHA DEL CONTRATO O CP <sup>43</sup>	FECHA DE LA CONFORMIDAD DE SER EL CASO <sup>44</sup>	EXPERIENCIA PROVENIENTE <sup>45</sup> DE:	MONEDA	IMPORTE <sup>46</sup>	TIPO DE CAMBIO VENTA <sup>47</sup>	MONTO FACTURADO ACUMULADO <sup>48</sup>
1										
2										
3										

<sup>43</sup> 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.

<sup>44</sup> Únicamente, cuando la fecha del perfeccionamiento del contrato, sea previa a los ocho (8) años anteriores a la fecha de presentación de ofertas, caso en el cual el postor debe acreditar que la conformidad se emitió dentro de dicho período.

<sup>45</sup> 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".

<sup>46</sup> Se refiere al monto del contrato ejecutado incluido adicionales y reducciones, de ser el caso.

<sup>47</sup> 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.

<sup>48</sup> 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 <sup>43</sup>	FECHA DE LA CONFORMIDAD DE SER EL CASO <sup>44</sup>	EXPERIENCIA PROVENIENTE <sup>45</sup> DE:	MONEDA	IMPORTE <sup>46</sup>	TIPO DE CAMBIO VENTA <sup>47</sup>	MONTO FACTURADO ACUMULADO <sup>48</sup>
4										
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

**ÓRGANO ENCARGADO DE LAS CONTRATACIONES**

**ADJUDICACIÓN SIMPLIFICADA N° 026-2024-INGEMMET/CS-1**

Presente.-

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

[CONSIGNAR CIUDAD Y FECHA]

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

**Importante**

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



## ANEXO N° 12

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

(DOCUMENTO A PRESENTAR EN EL PERFECCIONAMIENTO DEL CONTRATO)

Señores

**ÓRGANO ENCARGADO DE LAS CONTRATACIONES**

**ADJUDICACIÓN SIMPLIFICADA N° 026-2024-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.*