

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

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



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

### SIMBOLOGÍA UTILIZADA:

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

### CARACTERÍSTICAS DEL DOCUMENTO:

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

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

### INSTRUCCIONES DE USO:

- Una vez registrada la información solicitada dentro de los corchetes sombreados en gris, el texto deberá quedar en letra tamaño 10, con estilo normal, sin formato de negrita y sin sombrear.
- La nota **IMPORTANTE** no puede ser modificada ni eliminada en la Sección General. En el caso de la Sección Específica debe seguirse la instrucción que se indica en dicha nota.

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



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

**CONCURSO PÚBLICO N°  
003-2025-JUS**

**CONTRATACIÓN DE SERVICIO DE  
"SERVICIO DE GESTIÓN DE CIBERSEGURIDAD PERIMETRAL  
PARA EL MINISTERIO DE JUSTICIA Y DERECHOS HUMANOS"**

## DEBER DE COLABORACIÓN

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

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

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

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

## **SECCIÓN GENERAL**

### **DISPOSICIONES COMUNES DEL PROCEDIMIENTO DE SELECCIÓN**

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

## CAPÍTULO I ETAPAS DEL PROCEDIMIENTO DE SELECCIÓN

### 1.1. REFERENCIAS

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

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

### 1.2. CONVOCATORIA

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

### 1.3. REGISTRO DE PARTICIPANTES

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

#### Importante

- *Para registrarse como participante en un procedimiento de selección convocado por las Entidades del Estado Peruano, es necesario que los proveedores cuenten con inscripción vigente y estar habilitados ante el Registro Nacional de Proveedores (RNP) que administra el Organismo Supervisor de las Contrataciones del Estado (OSCE). Para obtener mayor información, se puede ingresar a la siguiente dirección electrónica: [www.rnp.gob.pe](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.

#### Importante

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

### 1.5. ABSOLUCIÓN DE CONSULTAS, OBSERVACIONES E INTEGRACIÓN DE BASES

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

#### Importante

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

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

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

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

#### Advertencia

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

#### Importante

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

### 1.7. FORMA DE PRESENTACIÓN DE OFERTAS

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

Las declaraciones juradas, formatos o formularios previstos en las bases que conforman la oferta deben estar debidamente firmados por el postor (firma manuscrita o digital, según la Ley N° 27269, Ley de Firmas y Certificados 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*

<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>

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

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

## 1.8. PRESENTACIÓN Y APERTURA DE OFERTAS

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

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

### Importante

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

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

## 1.9. EVALUACIÓN DE LAS OFERTAS

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

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

## 1.10. CALIFICACIÓN DE OFERTAS

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

## 1.11. SUBSANACIÓN DE LAS OFERTAS

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

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

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

## 1.12. RECHAZO DE LAS OFERTAS

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

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

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

### **1.13. OTORGAMIENTO DE LA BUENA PRO**

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

### **1.14. CONSENTIMIENTO DE LA BUENA PRO**

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

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

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

#### **Importante**

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

## CAPÍTULO II

### SOLUCIÓN DE CONTROVERSIAS DURANTE EL PROCEDIMIENTO DE SELECCIÓN

#### 2.1. RECURSO DE APELACIÓN

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

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

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

#### Importante

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

#### 2.2. PLAZOS DE INTERPOSICIÓN DEL RECURSO DE APELACIÓN

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

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



## CAPÍTULO III DEL CONTRATO

### 3.1. PERFECCIONAMIENTO DEL CONTRATO

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

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

### 3.2. GARANTÍAS

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

#### 3.2.1. GARANTÍA DE FIEL CUMPLIMIENTO

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

#### 3.2.2. GARANTÍA DE FIEL CUMPLIMIENTO POR PRESTACIONES ACCESORIAS

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

#### Importante

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

#### 3.2.3. GARANTÍA POR ADELANTO

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

### 3.3. REQUISITOS DE LAS GARANTÍAS

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

#### **Importante**

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

#### **Advertencia**

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

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

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

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

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

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

*De otro lado, además de cumplir con el requisito referido a la clasificación de riesgo, a efectos de verificar si la empresa emisora se encuentra autorizada por la SBS para emitir garantías, debe revisarse el portal web de dicha Entidad (<http://www.sbs.gob.pe/sistema-financiero/relacion-de-empresas-que-se-encuentran-autorizadas-a-emitar-cartas-fianza>).*

*Los funcionarios competentes deben verificar la autenticidad de la garantía a través de los mecanismos establecidos (consulta web, teléfono u otros) por la empresa emisora.*

### **3.4. EJECUCIÓN DE GARANTÍAS**

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

### **3.5. ADELANTOS**

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

### **3.6. PENALIDADES**

### 3.6.1. PENALIDAD POR MORA EN LA EJECUCIÓN DE LA PRESTACIÓN

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

### 3.6.2. OTRAS PENALIDADES

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

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

## 3.7. INCUMPLIMIENTO DEL CONTRATO

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

## 3.8. PAGOS

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

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

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

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

#### **Advertencia**

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

## 3.9. DISPOSICIONES FINALES

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

## **SECCIÓN ESPECÍFICA**

### **CONDICIONES ESPECIALES DEL PROCEDIMIENTO DE SELECCIÓN**

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

## CAPÍTULO I GENERALIDADES

### 1.1. ENTIDAD CONVOCANTE

Nombre : MINISTERIO DE JUSTICIA Y DERECHOS HUMANOS  
RUC N° : 20131371617  
Domicilio legal : Calle Scipión Llona N°350 - Miraflores  
Teléfono: : (01) 204-8020  
Correo electrónico: : [oab429@minjus.gob.pe](mailto:oab429@minjus.gob.pe) / [oab419@minjus.gob.pe](mailto:oab419@minjus.gob.pe) /  
[jperez@minjus.gob.pe](mailto:jperez@minjus.gob.pe)

### 1.2. OBJETO DE LA CONVOCATORIA

El presente procedimiento de selección tiene por objeto la contratación del “**Servicio de Gestión de Ciberseguridad Perimetral para el Ministerio de Justicia y Derechos Humanos**”.

### 1.3. EXPEDIENTE DE CONTRATACIÓN

El expediente de contratación fue aprobado mediante Formato N°02 Solicitud y Aprobación de Expediente de Contratación **FORMULARIO 025-2025-JUS/OGA** el 16 de abril de 2025.

### 1.4. FUENTE DE FINANCIAMIENTO

Recursos Ordinarios

#### Importante

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

### 1.5. SISTEMA DE CONTRATACIÓN

El presente procedimiento se rige por el sistema de **Suma Alzada** de acuerdo con lo establecido en el expediente de contratación respectivo.

### 1.6. DISTRIBUCIÓN DE LA BUENA PRO

No corresponde.

### 1.7. ALCANCES DEL REQUERIMIENTO

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

### 1.8. PLAZO DE PRESTACIÓN DEL SERVICIO

Los servicios materia de la presente convocatoria se prestarán en el plazo de:

**Plazo de Prestación Principal:**

- El plazo de entrega del Plan de Trabajo del servicio, es de hasta veinte (20) días calendario contados a partir del día siguiente de la suscripción del contrato.
- El plazo de implementación del servicio será de hasta noventa (90) días calendario contados a partir del día siguiente de aprobado el plan de trabajo.
- El plazo de la prestación del servicio es por treinta y seis (36) meses, contados a partir del día siguiente de la fecha de suscripción del acta de Conformidad por la implementación del servicio.

**Plazo de Prestación Accesorio:**

- Capacitación: la prestación de este servicio es de sesenta días (60) calendarios, contados a partir del día siguiente de la suscripción del acta de Conformidad por la implementación del servicio.

En concordancia con lo establecido en el expediente de contratación.

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

Los participantes registrados tienen el derecho de recabar un ejemplar de las bases, para cuyo efecto deben cancelar **S/ 5.00 (cinco con 00/100 Soles)** en la Caja de la Entidad, sito en Calle Scipión Llona N° 350 - Miraflores. La entrega del ejemplar se realizará en la misma dirección, en la Oficina de Abastecimiento.

**Importante**

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

### 1.10. BASE LEGAL

- Ley N° 32185, Ley de Presupuesto del Sector Público para el Año Fiscal 2025.
- Ley N° 32186, Ley de Equilibrio Financiero del Presupuesto del Sector Público del año fiscal 2025.
- Ley N° 30225, Ley de Contrataciones del Estado y su modificatoria.
- Decreto Supremo N° 082-2019-EF, que aprueba el 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 N° 30225
- Ley de Contrataciones del Estado, modificado por Decreto Supremo N° 377-2019-EF, N° 168-2020-EF, N° 250-2020-EF, N° 162-2021-EF y demás modificatorias.
- Directivas y Opiniones del OSCE.
- Ley N° 27444, Ley del Procedimiento Administrativo General.
- Ley N° 29733, Ley de Protección de Datos Personales o norma que lo sustituya,

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>2</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>3</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>2</sup> La omisión del índice no determina la no admisión de la oferta.

<sup>3</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) La acreditación del cumplimiento de las características técnicas o funcionalidades requeridas por los componentes o soluciones del "Servicio de Ciberseguridad para el MINJUSDH" tales como Seguridad Perimetral, Protección contra ataques a las aplicaciones y servicios web, Ethical Hacking, Protección AntiDDOS perimetral no volumétrico, Antispam y el Centro de Operaciones de Ciberseguridad (CyberSoc), adjuntando la documentación oficial del fabricante en idioma inglés o español, ya sean Hojas de Datos (Datasheets), Brochures, Guía técnica de usuario (link y/o manuales de usuario) indicando el número de página, párrafo y texto que valide el cumplimiento (ANEXO de Características Técnicas). No se aceptarán cartas de fabricante como fundamento para el cumplimiento de las características técnicas o funcionalidades principales (ANEXO de Características Técnicas). En caso se presenten características no documentadas en hojas técnicas oficiales, el postor podrá brindar explicaciones adicionales, pero únicamente a título complementario, debiendo siempre acompañarse de mecanismos objetivos de validación, tales como capturas de pantalla de la interfaz del sistema, enlaces verificables a documentación en línea o referencias técnicas que sean verificables.
- f) Deberá adjuntar carta de fabricante y/o el link público del fabricante que verifique que los modelos propuestos no están en el listado ni anunciado en el sitio web del fabricante como end-of-life, end-of-sale o end-of-support.
- g) El contratista deberá contar con estándares internacionales, por lo que deberá presentar la Certificación vigente del ISO 27001 como mínimo.
- h) Declaración jurada de plazo de prestación del servicio. **(Anexo Nº 4)**<sup>4</sup>
- i) Promesa de consorcio con firmas legalizadas, de ser el caso, en la que se consigne los integrantes, el representante común, el domicilio común y las obligaciones a las que se compromete cada uno de los integrantes del consorcio así como el porcentaje equivalente a dichas obligaciones. **(Anexo Nº 5)**
- j) El precio de la oferta en Soles. Adjuntar obligatoriamente el **Anexo Nº 6**.

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

#### Importante

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

#### 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:

Ninguna.

<sup>4</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.



#### **Advertencia**

*El comité de selección 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:

- Garantía de fiel cumplimiento del contrato.
- Garantía de fiel cumplimiento por prestaciones accesorias, de ser el caso.
- Contrato de consorcio con firmas legalizadas ante Notario de cada uno de los integrantes de ser el caso.
- 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.
- Copia de la vigencia del poder del representante legal de la empresa que acredite que cuenta con facultades para perfeccionar el contrato, cuando corresponda.
- 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>5</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).*

- Domicilio para efectos de la notificación durante la ejecución del contrato.
- Autorización de notificación de la decisión de la Entidad sobre la solicitud de ampliación de plazo mediante medios electrónicos de comunicación <sup>6</sup> (**Anexo N° 12**).
- Detalle de los precios unitarios del precio ofertado<sup>7</sup>.
- Estructura de costos<sup>8</sup>.

#### **Importante**

- En caso que el postor ganador de la buena pro sea un consorcio, las garantías que presente este para el perfeccionamiento del contrato, así como durante la ejecución contractual, de ser el caso, además de cumplir con las condiciones establecidas en el artículo 33 de la Ley y el artículo 148 del Reglamento, deben consignar expresamente el nombre completo o la denominación o razón social de los integrantes del consorcio, en calidad de garantizados, de lo contrario no podrán ser aceptadas por las Entidades. No se cumple el requisito antes indicado si se consigna únicamente la denominación del consorcio, conforme lo dispuesto en la Directiva "Participación de Proveedores en Consorcio en las Contrataciones del Estado".*
- En los contratos periódicos de prestación de servicios en general que celebren las Entidades con las micro y pequeñas empresas, estas últimas pueden otorgar como garantía de fiel cumplimiento el diez por ciento (10%) del monto del contrato, porcentaje que es retenido por la Entidad durante la primera mitad del número total de pagos a realizarse, de forma*

<sup>5</sup> Para mayor información de las Entidades usuarias de la Plataforma de Interoperabilidad del Estado – PIDE ingresar al siguiente enlace <https://www.gobiernodigital.gob.pe/interoperabilidad/>

<sup>6</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>7</sup> Incluir solo en caso de la contratación bajo el sistema a suma alzada.

<sup>8</sup> Incluir solo cuando resulte necesario para la ejecución contractual, identificar los costos de cada uno de los rubros que comprenden la oferta.

prorrataada en cada pago, con cargo a ser devuelto a la finalización del mismo, conforme lo establece el numeral 149.4 del artículo 149 del Reglamento y numeral 151.2 del artículo 151 del Reglamento. Para dicho efecto los postores deben encontrarse registrados en el REMYPE, consignando en la Declaración Jurada de Datos del Postor (Anexo N° 1) o en la solicitud de retención de la garantía durante el perfeccionamiento del contrato, que tienen la condición de MYPE, lo cual será verificado por la Entidad en el link <http://www2.trabajo.gob.pe/servicios-en-linea-2-2> opción consulta de empresas acreditadas en el REMYPE.

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

#### Importante

- Corresponde a la Entidad verificar que las garantías presentadas por el postor ganador de la buena pro cumplan con los requisitos y condiciones necesarios para su aceptación y eventual ejecución, sin perjuicio de la determinación de las responsabilidades funcionales que correspondan.
- De conformidad con el Reglamento Consular del Perú aprobado mediante Decreto Supremo N° 076-2005-RE para que los documentos públicos y privados extendidos en el exterior tengan validez en el Perú, deben estar legalizados por los funcionarios consulares peruanos y refrendados por el Ministerio de Relaciones Exteriores del Perú, salvo que se trate de documentos públicos emitidos en países que formen parte del Convenio de la Apostilla, en cuyo caso bastará con que estos cuenten con la Apostilla de la Haya<sup>9</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

El contrato se perfecciona con la suscripción del documento que lo contiene. Para dicho efecto el postor ganador de la buena pro, dentro del plazo previsto en el artículo 141 del Reglamento, debe presentar la documentación requerida en Mesa de Partes del Ministerio de Justicia y Derechos Humanos, sito en Calle Scipión Llona N° 350 – Miraflores, en el horario de 08:00 a 16:30 pm., de lunes a viernes o Mesa de Partes Virtual, <https://sgd.minjus.gob.pe/sgd-virtual/public/ciudadano/ciudadanoMain.xhtml>. Considerar el envío de la carta fianza de forma física a la dirección de la Entidad antes mencionada.

#### Importante

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

## 2.5. FORMA DE PAGO

La Entidad realizará el pago de la contraprestación pactada a favor del contratista:

#### PRESTACIÓN PRINCIPAL:

El pago de servicio se efectuará en treinta y seis (36) cuotas mensuales iguales, para ello el contratista deberá cumplir con presentar de forma mensual el informe que corresponda al periodo

<sup>9</sup> Según lo previsto en la Opinión N° 009-2016/DTN.

a facturarse, el mismo que deberá ser verificado por la Oficina de Infraestructura y Soporte Tecnológico (OIST) del MINJUSDH para la emisión y suscripción de las actas de conformidad.

**PRESTACIÓN ACCESORIA – ENTRENAMIENTO O CAPACITACIÓN:**

El pago se realizará concluido el adiestramiento o entrenamiento y entrega de certificados dentro de los diez (10) días calendarios, siguientes al otorgamiento de la conformidad respectiva en aplicación al artículo 171° del Reglamento de la Ley de Contrataciones del Estado y la modificación del numeral 171.1 por la Primera Disposición Complementaria Modificatoria del D.S. N° 168-2020-EF

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 Infraestructura y soporte Tecnológico (OIST) de MINJUSDH emitiendo la conformidad de la prestación efectuada.
- Comprobante de pago.

Dicha documentación se debe presentar en la Mesa Partes Presencial en la Sede Central del MINJUSDH ubicado en Scipión Llona N°350 - Miraflores – Lima, o Mesa de Partes Virtual del Ministerio de Justicia y Derechos Humanos. (<https://sgd.minjus.gob.pe/sgd-virtual/public/ciudadano/ciudadanoMain.xhtml>).

## 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



PERÚ

Ministerio  
de Justicia  
y Derechos Humanos

Secretaría  
General

Oficina General de  
Tecnologías de  
Información

Oficina de  
Infraestructura  
y Soporte Tecnológico

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

#### TÉRMINOS DE REFERENCIA N° 0004-2025-JUS/OGTI-OIST

#### 1. DENOMINACIÓN DE LA CONTRATACIÓN

"Servicio de Gestión de Ciberseguridad Perimetral para el Ministerio de Justicia y Derechos Humanos"

#### 2. FINALIDAD PÚBLICA

Contar con el servicio de Gestión de Ciberseguridad Perimetral para el Ministerio de Justicia y Derechos Humanos para la protección de los activos informáticos críticos del Ministerio de Justicia y Derechos Humanos - MINJUSDH, logrando con ello brindar servicios digitales confiables, seguros y de calidad a la ciudadanía.

#### 3. ANTECEDENTES

El MINJUSDH se dedica a promover y proteger los derechos humanos, facilitar el acceso a la justicia, asesorar y defender jurídicamente al Estado, y coordinar políticas públicas en el ámbito de la justicia y los derechos humanos, entre sus funciones principales es aprobar, dirigir, supervisar y evaluar el cumplimiento de la política nacional del sector justicia, en armonía con la política general del Estado y los planes de gobierno. Esto incluye coordinar con otros ministerios y entidades de la administración pública las actividades vinculadas a su ámbito de competencia, encargarse de los centros de reclusión del país y gestionar las relaciones del Estado con las entidades religiosas.

Con fecha 15 de diciembre de 2021, se suscribe el Contrato N° 051-2021-JUS, iniciando la prestación del servicio el 23 de abril de 2022 por el periodo de treinta y seis (36) meses, con el cual se cuenta actualmente con la solución de Seguridad Perimetral informática para la sede Central del MINJUSDH.

#### 4. OBJETIVOS DE LA CONTRATACIÓN

##### Objetivo General.

Contratación de una persona natural o jurídica especializada en seguridad informática y/o información, que provea los servicios de Ciberseguridad requeridos por el Ministerio de Justicia y Derechos Humanos, por el periodo de treinta y seis (36) meses, contados a partir del día siguiente de la fecha de suscripción del acta de Conformidad por la implementación del servicio.

##### Objetivos Específicos.

- Contar con un servicio de seguridad perimetral con tecnologías de Firewalls de Siguiente Generación que detecten y prevengan intrusos hasta la capa de aplicación, con filtrado URL, control de aplicaciones, visibilidad de archivos, con Antispyware y/o Antibot, Antimalware y/o Antivirus, IPS, e integración con el directorio activo. Contar con un servicio de protección con tecnología sandboxing y acceso remoto VPN.

Esta es una copia auténtica imprimible de un documento electrónico archivado por el Ministerio de Justicia y Derechos Humanos, aplicando lo dispuesto por el Art. 25 del D.S. 070-2013-PCM y la tercera Disposición Complementaria final del D.S. 026-2016-PCM. Su autenticidad e integridad pueden ser contrastadas a través de la siguiente dirección web: [https://sgd.minjus.gob.pe/gesdoc\\_web/login.jsp](https://sgd.minjus.gob.pe/gesdoc_web/login.jsp) e ingresando el Tipo de Documento, Número y Rango de Fechas de ser el caso o [https://sgd.minjus.gob.pe/gesdoc\\_web/verifica.jsp](https://sgd.minjus.gob.pe/gesdoc_web/verifica.jsp) e ingresando Tipo de Documento, Número, Remitente y Año, según corresponda.





PERÚ

Ministerio  
de Justicia  
y Derechos Humanos

Secretaría  
General

Oficina General de  
Tecnologías de  
Información

Oficina de  
Infraestructura  
y Soporte Tecnológico

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

- Contar con un Servicio de Ethical Hacking
- Contar con un Servicio de protección contra ataques a las aplicaciones y servicios web.
- Contar con un Servicio de Protección AntiDDoS perimetral no volumétrico
- Contar con un Servicio de Protección de Correo Electrónico (Antispam).
- Contar con un Servicio de un Centro de Operaciones de Ciberseguridad (CyberSOC).

## 5. ALCANCES Y DESCRIPCIÓN DEL SERVICIO

El servicio ofertado debe proporcionar equipamiento de seguridad tecnológica, siendo responsabilidad del contratista garantizar la compatibilidad, integración, interoperabilidad y funcionalidad entre los componentes del servicio solicitado y las soluciones de seguridad preexistente en el MINJUSDH. El contratista implementará la infraestructura tecnológica relacionada al servicio requerido con las capacidades y funcionalidades que le permitan cumplir con los Términos de Referencia y de manera tal que funcionen correctamente durante la vigencia del contrato.

El contratista debe ser una personal natural o jurídica con especialización en Ciberseguridad y como tal debe implementar un servicio de calidad, soportadas por la mejor tecnología disponible en el mercado y con la capacidad de integrar soluciones en entornos multimarca. Además, será responsable de gestionar y administrar todas las soluciones implementadas para garantizar la correcta provisión del servicio, incluyendo proyectos de implementación/migración/integración de sus servicios con otras plataformas, prestando asesoría técnica en materia de tecnología durante el periodo de ejecución del servicio; participando inclusive en los diseños, topologías, en las implementaciones y la gestión de dichos proyectos. Esto no incluye el aprovisionamiento de equipamiento adicional.

El contratista es responsable de los materiales necesarios para la instalación de todos los equipos que conforman las soluciones para brindar el servicio requerido. Antes de la instalación de los equipos debe identificar que el tipo de toma de cada equipo sea compatible con los PDU (del tipo C-13) instalados en los gabinetes del Centro de Datos de la sede central del MINJUSDH, identificar la profundidad y el tipo de ranura de los ejes verticales para el rackeo respectivo. Asimismo, el contratista es responsable de proveer e instalar el cableado necesario para la operatividad de cada uno de los equipos que conforman las soluciones ofertadas y su conectividad e integración con cada uno de los componentes del servicio, en caso de cableado de cobre debe ser CAT6 o superior y en caso de fibra óptica multimodo los conectores deben ser Tipo LC; el Contratista debe proveer todos los transceivers que correspondan para las soluciones que proveerá para el servicio, tanto para el dispositivo origen y dispositivo destino.

Las soluciones de ciberseguridad que se implementaran para el cumplimiento de la prestación del servicio, deben contar con consolas de administración para la gestión

*Esta es una copia auténtica imprimible de un documento electrónico archivado por el Ministerio de Justicia y Derechos Humanos, aplicando lo dispuesto por el Art. 25 del D.S. 070-2013-PCM y la tercera Disposición Complementaria final del D.S. 026-2016-PCM. Su autenticidad e integridad pueden ser contrastadas a través de la siguiente dirección web: [https://sgd.minjus.gob.pe/gesdoc\\_web/login.jsp](https://sgd.minjus.gob.pe/gesdoc_web/login.jsp) e ingresando el Tipo de Documento, Número y Rango de Fechas de ser el caso o [https://sgd.minjus.gob.pe/gesdoc\\_web/verifica.jsp](https://sgd.minjus.gob.pe/gesdoc_web/verifica.jsp) e ingresando Tipo de Documento, Número, Remitente y Año, según corresponda.*





PERÚ

Ministerio  
de Justicia  
y Derechos Humanos

Secretaría  
General

Oficina General de  
Tecnologías de  
Información

Oficina de  
Infraestructura  
y Soporte Tecnológico

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

respectiva. Estas consolas pueden ser dedicadas o virtualizadas (debe incluir todo el licenciamiento necesario para el funcionamiento adecuado), de acuerdo a las soluciones que corresponda, el equipamiento provisto por el contratista se instalara en el Centro de Datos del MINJUSDH ubicado en la Calle Scipión Llona N° 350 - Miraflores - Lima. El contratista debe garantizar la performance y buen rendimiento de todas las consolas de gestión, instaladas como parte del servicio.

El dimensionamiento del equipamiento y licenciamiento, en el caso de las consolas virtualizadas, será de total responsabilidad del contratista, toda vez que esta debe ofrecer un óptimo rendimiento de operación, así como su diseño y topología. En caso estas presenten degradación de performance o rendimiento, el contratista implementará y ejecutará las acciones correctivas correspondientes de forma tal que se restablezcan el óptimo rendimiento. El Contratista debe garantizar durante el periodo de contrato el soporte técnico de hardware y software de estas soluciones de virtualización. Asimismo, el Contratista debe garantizar el almacenamiento de seis (6) meses de logs, para cada solución de ciberseguridad requerido o en su defecto garantizar al menos un (1) mes de logs para analítica de la solución y cinco (5) meses de logs en servidor syslog adicional. Estos logs deben estar disponibles cuando el MINJUSDH lo requiera.

El contratista debe garantizar que el hardware y/o software de cada solución que se implemente para brindar el servicio solicitado sea nuevo, de primer uso y año de fabricación 2024 como mínimo. El hardware y/o software de las soluciones deben tener garantía y soporte del fabricante, por el periodo de vigencia del contrato, ante defectos de fabricación, fallas de los componentes internos, que causen inoperatividad o mal funcionamiento de la solución, para proceder con el reemplazo de hardware correspondiente, el cual no debe exceder de los diez (10) días calendarios contados a partir del día siguiente de recibida la notificación por parte del MINJUSDH, sin costo para la Entidad, esto aplica para el servicio de seguridad perimetral siempre y cuando uno de los dos appliances requeridos en los Términos de Referencia haya presentado fallas. Para el caso de inoperatividad de los dos appliances, el contratista deberá realizar el reemplazo temporal de por lo menos un appliance en un lapso no mayor a dos (02) horas, a fin de recuperar la disponibilidad del servicio, de no cumplir con el tiempo requerido se aplicará la penalidad descrita en el numeral 5.13 de los Términos de referencia.

Además, el contratista deberá garantizar durante el presente servicio la vigencia tecnológica de los equipos o soluciones implementados, en caso el fabricante publique mejoras tecnológicas el contratista deberá aplicarlas en un plazo no mayor a cinco (05) días calendarios luego de notificado a la entidad a través de la mesa de partes presencial o virtual del MINJUSDH, sin costo adicional para la entidad. Asimismo, el contratista realizará las coordinaciones técnicas correspondientes con el personal de la Oficina de Infraestructura y Soporte Tecnológico (OIST) del MINJUSDH.

*Esta es una copia auténtica imprimible de un documento electrónico archivado por el Ministerio de Justicia y Derechos Humanos, aplicando lo dispuesto por el Art. 25 del D.S. 070-2013-PCM y la tercera Disposición Complementaria final del D.S. 026-2016-PCM. Su autenticidad e integridad pueden ser contrastadas a través de la siguiente dirección web: [https://sgd.minjus.gob.pe/gesdoc\\_web/login.jsp](https://sgd.minjus.gob.pe/gesdoc_web/login.jsp) e ingresando el Tipo de Documento, Número y Rango de Fechas de ser el caso o [https://sgd.minjus.gob.pe/gesdoc\\_web/verifica.jsp](https://sgd.minjus.gob.pe/gesdoc_web/verifica.jsp) e ingresando Tipo de Documento, Número, Remitente y Año, según corresponda."*





PERÚ

Ministerio  
de Justicia  
y Derechos Humanos

Secretaría  
General

Oficina General de  
Tecnologías de  
Información

Oficina de  
Infraestructura  
y Soporte Tecnológico

“Decenio de la igualdad de oportunidades para mujeres y hombres”  
“Año de la recuperación y consolidación de la economía peruana”

Durante la vigencia del contrato, el contratista deberá realizar de manera continua medidas preventivas a todas las soluciones implementadas, a fin de asegurar la operatividad de todos los componentes del servicio.

El Contratista será responsable de mantener actualizadas todas las soluciones implementadas con las últimas versiones estables de sus sistemas operativos y en caso corresponda con las últimas firmas de ataque, firmas de virus y/o malwares, bases de datos de aplicaciones, categorización de URLs y todas las nuevas funcionalidades de protección y análisis que correspondan. El contratista debe asegurar y garantizar al MINJUSDH el óptimo funcionamiento y rendimiento de la solución implementada, bajo los parámetros establecidos por el fabricante, debiendo realizar los ajustes de capacidades de hardware/software necesarios si se detecta recurrencia en la degradación de rendimiento de dicha solución; si para la actualización o upgrade de los sistemas operativos implique realizar un mejoramiento de las capacidades de la solución (CPU, Memoria, Disco) o realizar un upgrade de la solución, estas deben ser asumidas por el Contratista sin costo adicional para el MINJUSDH. Además, cuando se identifiquen vulnerabilidades en los sistemas o infraestructura que soporta las soluciones implementadas en este servicio, el Contratista debe ejecutar la remediación correspondiente en coordinación con el personal de la Oficina de Infraestructura y Soporte Tecnológico (OIST) del MINJUSDH.

Desde el CyberSOC (CyberSecurity Operation Center) del Contratista se atenderán los requerimientos de NIVEL 2 y/o NIVEL 3, asignados por el personal de la Oficina de Infraestructura y Soporte Tecnológico (OIST) del MINJUSDH, además de gestionar la operación de todas las soluciones implementadas como parte de la prestación del servicio.

A la presentación de ofertas, el postor debe entregar la siguiente información técnica:

La acreditación del cumplimiento de las características técnicas o funcionalidades requeridas por los componentes o soluciones del “Servicio de Ciberseguridad para el MINJUSDH” tales como Seguridad Perimetral, Protección contra ataques a las aplicaciones y servicios web, Ethical Hacking, Protección AntiDDOS perimetral no volumétrico, Antispam y el Centro de Operaciones de Ciberseguridad (CyberSoc), adjuntando la documentación oficial del fabricante en idioma inglés o español, ya sean Hojas de Datos (Datasheets), Brochures, Guía técnica de usuario (link y/o manuales de usuario) indicando el número de página, párrafo y texto que valide el cumplimiento. (ANEXO de Características Técnicas). No se aceptarán cartas de fabricante como fundamento para el cumplimiento de las características técnicas o funcionalidades principales. En caso se presenten características no documentadas en hojas técnicas oficiales, el postor podrá brindar explicaciones adicionales, pero únicamente a título complementario, debiendo siempre acompañarse de mecanismos objetivos de

*Esta es una copia auténtica imprimible de un documento electrónico archivado por el Ministerio de Justicia y Derechos Humanos, aplicando lo dispuesto por el Art. 25 del D.S. 070-2013-PCM y la tercera Disposición Complementaria final del D.S. 026-2016-PCM. Su autenticidad e integridad pueden ser contrastadas a través de la siguiente dirección web: [https://sgd.minjus.gob.pe/gesdoc\\_web/login.jsp](https://sgd.minjus.gob.pe/gesdoc_web/login.jsp) e ingresando el Tipo de Documento, Número y Rango de Fechas de ser el caso o [https://sgd.minjus.gob.pe/gesdoc\\_web/verifica.jsp](https://sgd.minjus.gob.pe/gesdoc_web/verifica.jsp) e ingresando Tipo de Documento, Número, Remitente y Año, según corresponda.”*



PERÚ

Ministerio  
de Justicia  
y Derechos Humanos

Secretaría  
General

Oficina General de  
Tecnologías de  
Información

Oficina de  
Infraestructura  
y Soporte Tecnológico

“Decenio de la igualdad de oportunidades para mujeres y hombres”  
“Año de la recuperación y consolidación de la economía peruana”

validación, tales como capturas de pantalla de la interfaz del sistema, enlaces verificables a documentación en línea o referencias técnicas que sean verificables.

A continuación, se describen los componentes de “Servicios de Ciberseguridad para el MINJUSDH”:

- A. Servicio de Seguridad perimetral.
  - Seguridad perimetral con tecnologías de Firewalls de siguiente generación.
  - Acceso remoto por Virtual Private Network (VPN),
  - Protección con tecnología sandboxing.
- B. Servicio de Protección contra ataques a las aplicaciones y servicios web.
- C. Servicio de Ethical Hacking.
- D. Servicio de Protección AntiDDoS perimetral no volumétrico.
- E. Servicio de Protección de Correo Electrónico (Antispam).
- F. Servicio de un Centro de Operaciones de Ciberseguridad (CyberSOC).

## A. SERVICIO DE SEGURIDAD PERIMETRAL

### Consideraciones Generales

Para la seguridad perimetral, el Contratista debe proveer el servicio a través de la implementación de las siguientes soluciones:

- Debe ser ofrecida en alta disponibilidad, es decir por lo menos 2 (dos) appliances con las mismas características mínimas mencionadas en estas especificaciones técnicas.
- El fabricante de la solución ofertada deberá ser miembro activo del Cyber Threat Alliance.
- El Postor tiene la libertad de añadir consolas terceras para cumplir con los requerimientos técnicos solicitados, ya sea para capacidades de gestión, reportes y/o seguridad.
- El fabricante puede pertenecer al cuadrante de Líderes de Gartner para “Enterprise Network Firewall” o “Firewalls de Redes Empresariales” en los últimos 8 reportes. (Opcional)
- Una solución de Firewall de siguiente generación (NGFW) compuesta por dos (2) appliances que deberán ser instalados en el Centro de Datos del MINJUSDH. Los equipos Firewall deben estar en alta disponibilidad y deben contar con las siguientes funcionalidades de protección activas: Firewall, VPN, URL filtering, Control de Aplicaciones, visibilidad de archivos, Antispyware y/o Antibot, Antimalware y/o Antivirus, IPS, y debe integrarse con el Directorio Activo de la Institución.
- Una solución sandboxing en la nube, integrada a la solución Firewall de siguiente generación, para la protección contra malware avanzado y de

Esta es una copia auténtica imprimible de un documento electrónico archivado por el Ministerio de Justicia y Derechos Humanos, aplicando lo dispuesto por el Art. 25 del D.S. 070-2013-PCM y la tercera Disposición Complementaria final del D.S. 026-2016-PCM. Su autenticidad e integridad pueden ser contrastadas a través de la siguiente dirección web: [https://sgd.minjus.gob.pe/gesdoc\\_web/login.jsp](https://sgd.minjus.gob.pe/gesdoc_web/login.jsp) e ingresando el Tipo de Documento, Número y Rango de Fechas de ser el caso o [https://sgd.minjus.gob.pe/gesdoc\\_web/verifica.jsp](https://sgd.minjus.gob.pe/gesdoc_web/verifica.jsp) e ingresando Tipo de Documento, Número, Remitente y Año, según corresponda.”





PERÚ

Ministerio  
de Justicia  
y Derechos Humanos

Secretaría  
General

Oficina General de  
Tecnologías de  
Información

Oficina de  
Infraestructura  
y Soporte Tecnológico

“Decenio de la igualdad de oportunidades para mujeres y hombres”  
“Año de la recuperación y consolidación de la economía peruana”

día cero en el perímetro de la red con Internet, en el Centro de Datos del MINJUSDH. La solución que implemente el Contratista debe incluir la protección contra el Ransomware. La solución debe analizar los archivos sospechosos y maliciosos en ambientes virtuales con los siguientes Sistemas Operativos como mínimo: Windows 7, Windows 8 (Opcional), Windows 10 y futuras versiones de sistemas operativos liberados por Microsoft, que se integre perfectamente a los Firewalls perimetrales de acceso a Internet. El contratista debe proveer el licenciamiento necesario y realizar todas las configuraciones que correspondan para el correcto funcionamiento de la solución sandboxing.

Para la integración de las soluciones de seguridad perimetral a proveer con los diferentes servicios preexistentes del MINJUSDH.

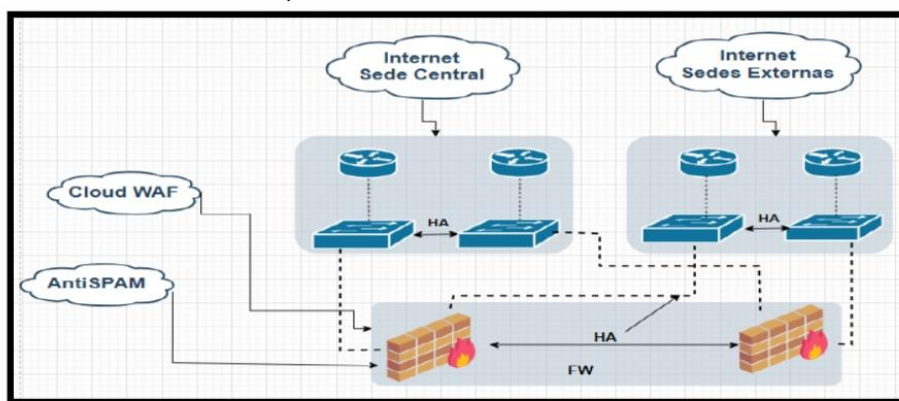


Figura 1: Topología referencial para la seguridad perimetral.

Para el servicio de Acceso Remoto por VPN, se requiere que la solución soporte hasta cinco mil (5000) usuarios con un crecimiento de hasta 30% durante el periodo de servicio, bajo condiciones aceptables de consumo de CPU menor al 40% en promedio y con las funcionalidades de protección activas. La solución debe soportar VPN Site-to-Site y Client-to-Site en protocolo IPSec con una concurrencia mínima de 1800 conexiones. La solución debe soportar autenticación de doble factor, comunicaciones encriptadas, protección de datos y/o prevención de fuga de información y/o subida o descarga de archivos específicos, o con extensiones específicas. Además, debe colocar en cuarentena de forma automática o manual los dispositivos comprometidos que intenten conectarse por VPN. En su defecto, la solución bloqueará la conectividad de los clientes que no entren en cumplimiento.

*Esta es una copia auténtica imprimible de un documento electrónico archivado por el Ministerio de Justicia y Derechos Humanos, aplicando lo dispuesto por el Art. 25 del D.S. 070-2013-PCM y la tercera Disposición Complementaria final del D.S. 026-2016-PCM. Su autenticidad e integridad pueden ser contrastadas a través de la siguiente dirección web: [https://sgd.minjus.gob.pe/gesdoc\\_web/login.jsp](https://sgd.minjus.gob.pe/gesdoc_web/login.jsp) e ingresando el Tipo de Documento, Número y Rango de Fechas de ser el caso o [https://sgd.minjus.gob.pe/gesdoc\\_web/verifica.jsp](https://sgd.minjus.gob.pe/gesdoc_web/verifica.jsp) e ingresando Tipo de Documento, Número, Remitente y Año, según corresponda.”*



PERÚ

Ministerio  
de Justicia  
y Derechos Humanos

Secretaría  
General

Oficina General de  
Tecnologías de  
Información

Oficina de  
Infraestructura  
y Soporte Tecnológico

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

Asimismo, el MINJUSDH brinda servicios de consultas a su base de datos, a Instituciones y Empresas que firman convenios con la Entidad, a través de líneas dedicadas cuyas cabeceras están instaladas en el MINJUSDH.

El soporte técnico que el Contratista contrate al fabricante de las soluciones instaladas para proveer el servicio requerido no debe ser el "standard", debe ser el nivel de soporte inmediato superior a éste, que incluya la atención 24x7, mediante correo, llamadas telefónica, asistencia remota y videoconferencia, durante el periodo de servicio. Se precisa que en caso el fabricante de las soluciones tenga distinta clasificación de soporte a lo mencionado, se aceptará el soporte contratado por el Contratista que incluya la atención 24x7. El contratista debe presentar el contrato que acredite la contratación del soporte requerido, en el entregable "Informa Final de implementación", mas no activar el mismo, el cual será activado finalizado la implementación y con el acta de conformidad de la entidad.

Es responsabilidad del contratista realizar las gestiones correspondientes de manera directa con el fabricante de la solución para garantizar una correcta operación del equipamiento ofertado como parte del servicio desde la apertura de un ticket de soporte hasta el cierre de este. Así mismo, garantizar que el MINJUSDH pueda aperturar casos directamente con el fabricante.

### **Consideraciones Específicas**

***Para el servicio de Firewall de Siguiente Generación de acceso a Internet.***

#### **1. DESCRIPCION**

- ✓ La Solución de Next Generation Firewall (NGFW) para la seguridad de la red/institucional debe ser ofrecida en alta disponibilidad, es decir por lo menos dos (02) appliances con las mismas características mínimas mencionadas en los Términos de Referencia.
- ✓ El Postor tiene la libertad de añadir consolas terceras para cumplir con los requerimientos técnicos solicitados, ya sea para capacidades de gestión, reportes y seguridad.
- ✓ Deber ser miembro del Cyber Threat Alliance.
- ✓ El fabricante debe pertenecer al cuadrante de Líderes de Gartner para "Enterprise Network Firewall" o "Firewalls de Redes Empresariales" en los últimos 8 reportes

#### **2. REQUERIMIENTOS SOPORTE**

- ✓ Ninguno de los modelos ofertados podrá estar listados ni anunciado en el sitio web del fabricante como end-of-life, end-of-sale o end-of-support. a la presentación de ofertas se deberá adjuntar carta de fabricante y/o el link público del fabricante que verifique que los modelos propuestos no están en ese listado.

Esta es una copia auténtica imprimible de un documento electrónico archivado por el Ministerio de Justicia y Derechos Humanos, aplicando lo dispuesto por el Art. 25 del D.S. 070-2013-PCM y la tercera Disposición Complementaria final del D.S. 026-2016-PCM. Su autenticidad e integridad pueden ser contrastadas a través de la siguiente dirección web: [https://sgd.minjus.gob.pe/gesdoc\\_web/login.jsp](https://sgd.minjus.gob.pe/gesdoc_web/login.jsp) e ingresando el Tipo de Documento, Número y Rango de Fechas de ser el caso o [https://sgd.minjus.gob.pe/gesdoc\\_web/verifica.jsp](https://sgd.minjus.gob.pe/gesdoc_web/verifica.jsp) e ingresando Tipo de Documento, Número, Remitente y Año, según corresponda.





PERÚ

Ministerio  
de Justicia  
y Derechos Humanos

Secretaría  
General

Oficina General de  
Tecnologías de  
Información

Oficina de  
Infraestructura  
y Soporte Tecnológico

"Decenio de la igualdad de oportunidades para mujeres y hombres"

"Año de la recuperación y consolidación de la economía peruana"

- ✓ La solución propuesta deberá tener soporte vigente de fábrica durante la vigencia del contrato del servicio, el soporte del fabricante deberá incluir atención de incidentes de software o hardware de la plataforma, reposición de partes o equipo de reemplazo en caso de falla de hardware.
- ✓ El soporte deberá estar disponible 24x7x365, la apertura de casos deberá poder realizarse vía online o vía telefónica.
- ✓ El contratista deberá proporcionar a la entidad, el acceso al portal de soporte del fabricante, donde se tenga la potestad de dar seguimiento a los mismos.

### 3. CAPACIDAD DE RENDIMIENTO

- ✓ Throughput de Prevención de Amenazas de 18 Gbps medido con tráfico productivo real (transacciones usando una mixtura de aplicaciones de capa 7, transacciones medidas en condiciones empresariales o transacciones HTTP 64KB de tamaño), con las siguientes funcionalidades habilitadas simultáneamente: Firewall, Control de aplicaciones, Sistema de Prevención de Intrusos (IPS), Seguridad del tráfico DNS, Antivirus/Antimalware de red, Antispyware, Sandboxing y Logging activo. Si el fabricante tuviese diferentes niveles o modos de inspección de seguridad, el equipo ofertado deberá soportar el throughput requerido con el modo más alto de inspección de seguridad. Se debe garantizar que el equipo no degrade su performance por debajo de lo requerido al habilitar los módulos de seguridad indicados en el modo más alto de inspección.
- ✓ La plataforma de hardware debe soportar como mínimo 3 millones sesiones/conexiones concurrentes y 260 mil nuevas sesiones/conexiones por segundo como mínimo, medidos en capa 7 (con paquetes HTTP); o en su defecto, soportar 18 millones de sesiones/conexiones concurrentes y 850 mil nuevas sesiones/conexiones por segundo, medidos en capa 4 (con paquetes TCP) como mínimo.
- ✓ Debe contar con fuente de poder redundante intercambiable en caliente (HOT SWAP) o fuentes intercambiables.
- ✓ Disco interno de estado sólido de 400GB o superior
- ✓ Contar con una interfaz de cobre RJ45 dedicada para la gestión del equipo
- ✓ Contar con la siguiente cantidad de interfaces para el tráfico de datos como mínimo:
  - 4 interfaces de 25GE SFP28
  - 8 interfaces de 10GE SFP+
  - 8 interfaces de 1GE de Cobre
  - 2 interfaces de 40Gb/100Gb
- ✓ Deberá tener CPU y memoria RAM dedicada para tareas de gestión del equipo, de manera independiente a los recursos para el procesamiento del tráfico. Esta arquitectura podrá estar integrada dentro del NGFW, o en caso no lo soporte, se podrán incluir consolas de gestión externas al NGFW.

### 4. CAPACIDADES DE NETWORKING

- ✓ El dispositivo de seguridad debe soportar VLAN Tags 802.1q, agregación de links 802.3ad, policy based routing o policy based forwarding, ruteo

*Esta es una copia auténtica imprimible de un documento electrónico archivado por el Ministerio de Justicia y Derechos Humanos, aplicando lo dispuesto por el Art. 25 del D.S. 070-2013-PCM y la tercera Disposición Complementaria final del D.S. 026-2016-PCM. Su autenticidad e integridad pueden ser contrastadas a través de la siguiente dirección web: [https://sgd.minjus.gob.pe/gesdoc\\_web/login.jsp](https://sgd.minjus.gob.pe/gesdoc_web/login.jsp) e ingresando el Tipo de Documento, Número y Rango de Fechas de ser el caso o [https://sgd.minjus.gob.pe/gesdoc\\_web/verifica.jsp](https://sgd.minjus.gob.pe/gesdoc_web/verifica.jsp) e ingresando Tipo de Documento, Número, Remitente y Año, según corresponda."*



PERÚ

Ministerio  
de Justicia  
y Derechos Humanos

Secretaría  
General

Oficina General de  
Tecnologías de  
Información

Oficina de  
Infraestructura  
y Soporte Tecnológico

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

multicast, jumbo frames, sub-interfaces ethernet lógicas, NAT de origen y destino.

- ✓ Debe soportar enrutamiento estático y dinámico (RIPv2, BGP y OSPFv2).
- ✓ Soportar diferentes características de networking operando en el protocolo IPv6, como mínimo: ruteo estático OSPFv3, MP-BGP, policy based routing o policy based forwarding, dual-stack (soporte IPv4 e IPv6), QoS, NAT64, BFD, SLAAC y/o DHCPv6 Relay.
- ✓ La plataforma propuesta por el fabricante debe contar con certificación USGv6-r1 para las pruebas de Firewall y/o IDS y/o IPS.

#### 5. ALTA DISPONIBILIDAD

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

#### 6. FUNCIONALIDADES DE FIREWALL

- ✓ Control de políticas puertos, direcciones IP, segmentos y/o rangos de red, región geográfica, usuarios y grupos de usuarios, aplicaciones, grupo de aplicaciones y/o grupos estáticos y/o grupos dinámicos de aplicaciones (basados en sus atributos).
- ✓ Permitir agrupar las políticas y/o reglas de seguridad utilizando etiquetas u otro método.
- ✓ Debe realizar validaciones de la configuración antes de ser aplicada o instalada, esto implica, entre otras cosas, identificar y notificar cuando existan reglas generales superpuestas sobre otras específicas (shadowed rules).
- ✓ Debe mostrar la primera y última vez que se utilizó una regla de seguridad.
- ✓ Debe mostrar la fecha de creación y última fecha de modificación de la regla de seguridad.
- ✓ La solución debe permitir identificar las reglas de seguridad que no han tenido uso en la red desde el último encendido del dispositivo firewall, ya sea mediante un filtro directo o mediante columnas configurables que permitan visualizar el conteo de uso (Hit Count), incluyendo fecha del primer y último uso.
- ✓ Debe permitir tener un registro de auditoría en cada política que permita conocer que cambios se realizó con anterioridad.

#### 7. DESCIFRADO DE TRÁFICO SSL/TLS

Esta es una copia auténtica imprimible de un documento electrónico archivado por el Ministerio de Justicia y Derechos Humanos, aplicando lo dispuesto por el Art. 25 del D.S. 070-2013-PCM y la tercera Disposición Complementaria final del D.S. 026-2016-PCM. Su autenticidad e integridad pueden ser contrastadas a través de la siguiente dirección web: [https://sgd.minjus.gob.pe/gesdoc\\_web/login.jsp](https://sgd.minjus.gob.pe/gesdoc_web/login.jsp) e ingresando el Tipo de Documento, Número y Rango de Fechas de ser el caso o [https://sgd.minjus.gob.pe/gesdoc\\_web/verifica.jsp](https://sgd.minjus.gob.pe/gesdoc_web/verifica.jsp) e ingresando Tipo de Documento, Número, Remitente y Año, según corresponda."







PERÚ

Ministerio  
de Justicia  
y Derechos Humanos

Secretaría  
General

Oficina General de  
Tecnologías de  
Información

Oficina de  
Infraestructura  
y Soporte Tecnológico

"Decenio de la igualdad de oportunidades para mujeres y hombres"

"Año de la recuperación y consolidación de la economía peruana"

- ✓ Debe permitir descifrar el tráfico de navegación de usuarios a internet mediante la instalación de un certificado digital en las estaciones de trabajo.
- ✓ Capacidad de bloquear la conexión hacia sitios web cifrados con protocolos obsoletos y/o no fiables, a pesar de no descifrar el tráfico.
- ✓ Debe soportar certificados que utilicen Subject Alternative Name (SAN) y Server Name Indication (SNI).
- ✓ Permitir el descifrado selectivo de categorías de URLs, por ejemplo, debe ser capaz de especificar excluir del descifrado a páginas con contenido sensible y descifrar el resto de las páginas.
- ✓ Permitir excluir sitios a los cuales no se les aplicará la política de descifrado en base al Common Name del certificado.

#### 8. VISIBILIDAD EN CAPA 7 Y CONTROL DE APLICACIONES

- ✓ La solución debe de reconocer y tener visibilidad como mínimo 4000 aplicaciones y podrá reconocer aplicaciones tipo peer-to-peer, redes sociales, acceso remoto, update de software, protocolos de red, voip, audio, video, proxy, mensajería instantánea, email.
- ✓ Las aplicaciones deberán estar clasificadas en al menos 30 tipos, de tal manera que se puedan configurar políticas en base al tipo de aplicación.
- ✓ Las aplicaciones deberán contar con atributos descriptivos tales como tipo, nivel de riesgo y etiqueta.
- ✓ Para tráfico cifrado (SSL/TLS), debe permitir el descifrado de paquetes con el fin de permitir la lectura del payload de la aplicación cifrada.
- ✓ Debe inspeccionar el payload del paquete de datos con el objetivo de detectar las aplicaciones en capa 7, a través de expresiones regulares, firmas u otro mecanismo. Debe ser capaz de determinar si una aplicación está utilizando su puerto default o no, por ejemplo, RDP en el puerto 80 en vez del 3389.
- ✓ Las políticas de seguridad deben poder definirse netamente en base a aplicaciones, sin necesidad de especificar puertos.
- ✓ Las políticas de seguridad deberán poder definirse 100% en base a aplicaciones pudiendo aplicar reglas específicas a cada aplicación. Es decir, si 2 aplicaciones utilizan el mismo puerto y protocolo, se debe poder crear 2 políticas de seguridad en las cuales se apliquen controles diferentes a cada aplicación.

#### 9. PREVENCIÓN DE AMENAZAS

- ✓ La solución propuesta deberá contar con capacidades de IPS (Intrusion Prevention System), Antivirus/Antimalware, Antispyware/Antibot.
- ✓ Las funcionalidades de IPS, Antivirus y Antispyware/Antibot deberán operar de forma permanente durante la vigencia del contrato y contar con actualizaciones de firmas y mecanismos de protección proporcionados por el fabricante durante el periodo contratado. En caso de culminación del contrato, el proveedor deberá garantizar el cese controlado de los servicios sin generar interrupciones súbitas ni impactos sobre la operación de la entidad, conforme a las buenas prácticas de continuidad de servicios

*Esta es una copia auténtica imprimible de un documento electrónico archivado por el Ministerio de Justicia y Derechos Humanos, aplicando lo dispuesto por el Art. 25 del D.S. 070-2013-PCM y la tercera Disposición Complementaria final del D.S. 026-2016-PCM. Su autenticidad e integridad pueden ser contrastadas a través de la siguiente dirección web: [https://sgd.minjus.gob.pe/gesdoc\\_web/login.jsp](https://sgd.minjus.gob.pe/gesdoc_web/login.jsp) e ingresando el Tipo de Documento, Número y Rango de Fechas de ser el caso o [https://sgd.minjus.gob.pe/gesdoc\\_web/verifica.jsp](https://sgd.minjus.gob.pe/gesdoc_web/verifica.jsp) e ingresando Tipo de Documento, Número, Remitente y Año, según corresponda."*





PERÚ

Ministerio  
de Justicia  
y Derechos Humanos

Secretaría  
General

Oficina General de  
Tecnologías de  
Información

Oficina de  
Infraestructura  
y Soporte Tecnológico

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

- ✓ El equipo deberá soportar el throughput solicitado operando en el máximo nivel o modo de seguridad de inspección de IPS, Antispyware y/o Antibot, Antimalware y/o Antivirus.
- ✓ La solución deberá identificar las consultas que realizan los hosts infectados hacia dominios maliciosos, de tal forma que se pueda bloquear dichas consultas DNS.
- ✓ Deberá contar con un mecanismo que permita identificar los equipos potencialmente infectados en base al análisis de su tráfico DNS, ya sea si el tráfico entre la potencial víctima y su servidor DNS utilizado pasa o no pasa por el NGFW.
- ✓ Deberá ser capaz de identificar amenazas sobre el tráfico DNS encriptado camuflado sobre HTTPS (DNS over HTTPS – DoH), y/o también DNS sobre TLS.
- ✓ El módulo de IPS debe ser capaz de bloquear ataques en base a firmas, heurística y anomalías en el protocolo.
- ✓ El módulo de IPS debe permitir personalizar firmas directamente desde la consola gráfica.
- ✓ Respecto a ataques de malware, las firmas deberán estar basadas en patrones y no únicamente en hashes, con el objetivo de identificar y bloquear el malware polimórfico que pertenezca a una misma familia.
- ✓ Con la finalidad de contar con una protección robusta contra amenazas emergentes a nivel mundial, la solución deberá ser capaz de actualizar su base de firmas de malware en tiempo real o automática.
- ✓ Debe incorporar una plataforma de sandbox basada en nube para el análisis de ejecutables desconocidos.
- ✓ Debe ser capaz de detectar y bloquear el virus y malware en general que se propague en, al menos, los siguientes protocolos: SFTP, HTTP, HTTPS, HTTP/2, FTP, (SMB versión 1opcional), SMB versiones 2 y 3, SMTP, IMAP y POP3..

#### 10. SANDBOXING

- ✓ La plataforma de Sandbox podrá ser ofrecido en Nube (Cloud).
- ✓ Deberá ser capaz de emular o analizar el potencial malware en entornos: Windows, Linux y/o MacOS.
- ✓ El sandbox deberá ser capaz de analizar como mínimo 5 000 archivos por hora realizando análisis dinámico del archivo (entiéndase por análisis dinámico aquel que no está basado en firmas, ni prefiltros, sino en emulación completa del potencial malware). De ser requerido algún hardware adicional para el proceso de análisis de archivo se debe considerar el hardware necesario para cumplir con las especificaciones técnicas
- ✓ También se aceptará soluciones sandbox terceras de otro fabricante distinto al NGFW.
- ✓ El análisis dinámico de los archivos enviados no deberá tomar más de 10 minutos en emitir un veredicto por archivo, bajo condiciones normales de operación, garantizando un tiempo de respuesta adecuado que permita la detección temprana de amenazas.

*Esta es una copia auténtica imprimible de un documento electrónico archivado por el Ministerio de Justicia y Derechos Humanos, aplicando lo dispuesto por el Art. 25 del D.S. 070-2013-PCM y la tercera Disposición Complementaria final del D.S. 026-2016-PCM. Su autenticidad e integridad pueden ser contrastadas a través de la siguiente dirección web: [https://sgd.minjus.gob.pe/gesdoc\\_web/login.jsp](https://sgd.minjus.gob.pe/gesdoc_web/login.jsp) e ingresando el Tipo de Documento, Número y Rango de Fechas de ser el caso o [https://sgd.minjus.gob.pe/gesdoc\\_web/verifica.jsp](https://sgd.minjus.gob.pe/gesdoc_web/verifica.jsp) e ingresando Tipo de Documento, Número, Remitente y Año, según corresponda."*







PERÚ

Ministerio  
de Justicia  
y Derechos Humanos

Secretaría  
General

Oficina General de  
Tecnologías de  
Información

Oficina de  
Infraestructura  
y Soporte Tecnológico

"Decenio de la igualdad de oportunidades para mujeres y hombres"

"Año de la recuperación y consolidación de la economía peruana"

- ✓ La plataforma de Sandbox Cloud, deberá cumplir con los siguientes requerimientos:
  - Deberá tener una disponibilidad de al menos 99.9% contabilizados mensualmente.
  - Deberá garantizar la privacidad y confidencialidad del contenido de los archivos analizados, para lo cual se requiere que el servicio cuente como mínimo con certificaciones SOC2 Tipo II Plus de AICPA, ISO 27001, ISO 27017 e ISO 27018.
- ✓ Deberá generar automáticamente las firmas de malware y bloquear el acceso a las URLs maliciosas utilizadas por el malware.
- ✓ Debe permitir al administrador la descarga del archivo original analizado por el sandbox.
- ✓ La solución deberá contar con un mecanismo de retroalimentación que permita la mejora continua del sistema de detección de amenazas. Este mecanismo puede incluir reportes manuales o automáticos de archivos sospechosos para su análisis posterior por el fabricante o por el equipo técnico de la entidad, con el fin de mejorar la precisión del motor de análisis.
- ✓ Permitir la subida de archivos al sandbox de forma manual y/o vía API, con el objetivo de automatizar las tareas de análisis dinámico.
- ✓ Debe detectar técnicas usadas para evadir herramientas de Sandboxing como detección de hypervisor (debe usar hipervisores hardenizado y personalizados), inyección de código a procesos permitidos y deshabilitación de funcionalidades de seguridad del host.

#### 11. FILTRO DE CONTENIDO WEB

- ✓ Debe poseer al menos 70 categorías de URLs, incluyendo las de malware, command and control, proxy, phishing, redes sociales, páginas de adultos.
- ✓ Debe soportar un cache local de URLs en el dispositivo, evitando el delay de comunicación/validación de las URLs
- ✓ Debe contar con medidas de antievasión como Cloaking y/o Captcha falsos y/o codificación de caracteres HTML; o mecanismos similares que dificulten técnicas de evasión automatizadas por bots o scripts maliciosos.
- ✓ Debe permitir la creación de categorías personalizadas.
- ✓ Debe permitir la personalización de la página de bloqueo.
- ✓ Debe permitir notificar al usuario, mostrándole solo una página de alerta personalizable, pero permitiéndole continuar la navegación al site.
- ✓ Debe ser capaz de registrar el User-agent y/o Client Type, Referer y/o Resource, XFF y/o IP Origen de cada sesión hacia internet.
- ✓ Debe ser capaz de forzar la navegación de los usuarios en el modo Safe Search Enforcement.
- ✓ Debe identificar cuando un usuario envía credenciales corporativas de red a sitios no autorizados y debe poder bloquear dicho envío, previniendo así ataques de robo de credenciales y/o en su defecto cuente con la funcionalidad de prevenir el Phishing a nivel de la navegación de los usuarios de atraviesan el perímetro de red".

#### 12. IDENTIFICACION DE USUARIOS

Esta es una copia auténtica imprimible de un documento electrónico archivado por el Ministerio de Justicia y Derechos Humanos, aplicando lo dispuesto por el Art. 25 del D.S. 070-2013-PCM y la tercera Disposición Complementaria final del D.S. 026-2016-PCM. Su autenticidad e integridad pueden ser contrastadas a través de la siguiente dirección web: [https://sgd.minjus.gob.pe/gesdoc\\_web/login.jsp](https://sgd.minjus.gob.pe/gesdoc_web/login.jsp) e ingresando el Tipo de Documento, Número y Rango de Fechas de ser el caso o [https://sgd.minjus.gob.pe/gesdoc\\_web/verifica.jsp](https://sgd.minjus.gob.pe/gesdoc_web/verifica.jsp) e ingresando Tipo de Documento, Número, Remitente y Año, según corresponda."





PERÚ

Ministerio  
de Justicia  
y Derechos Humanos

Secretaría  
General

Oficina General de  
Tecnologías de  
Información

Oficina de  
Infraestructura  
y Soporte Tecnológico

"Decenio de la igualdad de oportunidades para mujeres y hombres"

"Año de la recuperación y consolidación de la economía peruana"

- ✓ Debe permitir la creación de políticas de seguridad basadas en la identidad del usuario y grupo al cual pertenece, a través de la integración de servicios de autenticación como Active Directory y/o Novell eDirectory y/o Open LDAP y base de datos local.
- ✓ Debe contar con varios mecanismos para la identificación del usuario y la dirección IP del equipo en donde se encuentra autenticado. Como mínimo deberá poder integrarse a las siguientes plataformas para cubrir este requerimiento:
  - Eventos de login gestionados en Domain Controller y/o Microsoft Exchange.
  - Terminal Server de Microsoft o Citrix
  - Consultando directamente a cada estación de trabajo y/o al propio servidor de Active Directory y/o Domain controller a través del protocolo WMI.
- ✓ Deberá contar con un componente que permita integrarse a diversas plataformas de identidades tales como Azure LDAP y/o Microsoft Entra ID, Google Directory y/o Google Workspace, Okta, Cisco Duo, PingID.
- ✓ Debe contar con la funcionalidad de Portal Cautivo (Captive Portal), de tal manera que el NGFW muestre un portal al usuario para que se autentique manualmente. Las cuentas podrán ser definidas localmente en el NGFW o integradas con plataformas terceras.
- ✓ Debe tener integración con plataformas de MFA (Multi Factor Authentication), de tal forma que cuando un dispositivo requiera acceder a recurso, se le solicite el OTP.

### 13. QOS

- ✓ Con la finalidad de controlar aplicaciones y tráfico cuyo consumo pueda ser excesivo, (como YouTube o Netflix), se requiere que la solución tenga la capacidad de controlarlas a través de políticas personalizables.
- ✓ Soportar la creación de políticas de QoS por: dirección de origen y destino, por grupo de usuario de LDAP, por aplicaciones, por puerto.
- ✓ El QoS debe permitir la definición de clases por: ancho de banda garantizado, ancho de banda máximo, prioridad.
- ✓ Soportar marcación de paquetes DSCP y/o clasificar los paquetes entrantes en función de la dirección IP, inclusive por aplicaciones y/o redes y/o grupo de redes
- ✓ Permitir el monitoreo en tiempo real del tráfico gestionado por el QoS.

### 14. FILTRO DE DATOS

- ✓ Los archivos deben ser identificados por extensión y, firmas y/o tipo de dato asegurando la detección precisa de contenido potencialmente riesgoso sin depender únicamente de la nomenclatura del archivo
- ✓ Permite identificar y opcionalmente prevenir la transferencia (subida o bajada) de varios tipos de archivos (incluidos MS Office, PDF, PE, APK, Flash, DLL, BAT, CAB, PIF, REG, archivos comprimidos en RAR, ZIP u otro).
- ✓ Permitir, identificar y opcionalmente prevenir la transferencia de información sensible basados en el contenido del archivo, incluyendo,

Esta es una copia auténtica imprimible de un documento electrónico archivado por el Ministerio de Justicia y Derechos Humanos, aplicando lo dispuesto por el Art. 25 del D.S. 070-2013-PCM y la tercera Disposición Complementaria final del D.S. 026-2016-PCM. Su autenticidad e integridad pueden ser contrastadas a través de la siguiente dirección web: [https://sgd.minjus.gob.pe/gesdoc\\_web/login.jsp](https://sgd.minjus.gob.pe/gesdoc_web/login.jsp) e ingresando el Tipo de Documento, Número y Rango de Fechas de ser el caso o [https://sgd.minjus.gob.pe/gesdoc\\_web/verifica.jsp](https://sgd.minjus.gob.pe/gesdoc_web/verifica.jsp) e ingresando Tipo de Documento, Número, Remitente y Año, según corresponda."





PERÚ

Ministerio  
de Justicia  
y Derechos Humanos

Secretaría  
General

Oficina General de  
Tecnologías de  
Información

Oficina de  
Infraestructura  
y Soporte Tecnológico

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

más no limitando al número de tarjetas de crédito; y permitiendo la creación de nuevos tipos de datos vía expresión regular.

#### 15. VPN

- ✓ Soportar VPN Site-to-Site en protocolo IPSec
- ✓ La VPN site to site debe soportar como mínimo:
  - AES 128 e 256 (Advanced Encryption Standard)
  - Autenticación MD5, SHA-1, SHA-2 y/o SHA-256; como mínimo
  - Diffie-Hellman Group 1, Group 2, Group 5 y Group 14;
  - Algoritmo Internet Key Exchange (IKEv1 & IKEv2);
- ✓ Permitir la aplicación de políticas de seguridad y visibilidad para las aplicaciones que circulan dentro de los túneles VPN.
- ✓ Permitir aplicar QoS dentro de los túneles VPN.
- ✓ Soportar VPN client-to-site pudiendo operar usando el protocolo IPSec o SSL.
- ✓ Permitir la conexión por medio de agente instalado en el sistema operativo.
- ✓ Soportar autenticación vía AD/LDAP, Kerberos, TACACS+, SAML, Certificados Digitales y RADIUS.
- ✓ Capacidad de integrarse con plataformas de Doble Factor de Autenticación (2FA).
- ✓ Debe permitir definir segmentos de red para ser agregadas de forma automática en la tabla de rutas de la interfaz túnel del equipo que tenga instalado el agente de VPN.
- ✓ Debe soportar Split Tunnel para elegir los segmentos de red que serán enrutados por la VPN, incluyendo el soporte de Split DNS.
- ✓ Debe permitir los siguientes tipos de conexión del cliente al túnel VPN:
  - Antes del usuario se autentique en la estación.
  - Después de la autenticación del usuario en la estación usando Single Sign On (SSO).
  - A demanda, de forma manual por parte del usuario.
- ✓ El agente de VPN client-to-site debe ser compatible al menos con: Windows, MacOS X

#### 16. DETECCIÓN Y RESPUESTA EXTENDIDA

- ✓ Cantidad: 200 licencias de endpoints (XDR) para servidores.
- ✓ La solución deber ser compatible con al menos los siguientes sistemas operativos: MS Windows Server 2012 R2, 2016, 2019, 2022 Linux CentOS 7 o superior, Redhat Enterprise 8 o superior sobre arquitectura x86\_64.
- ✓ La solución de seguridad antimalware debe ser basada en gestión y despliegue a través de servicios de nube (SaaS) del propio fabricante, en modalidad de suscripción. Asimismo, deberá contar con un módulo anti exploit el cual deberá identificar y bloquear técnicas de explotación sin necesidad de utilizar firmas y/o heurísticas. La solución no deberá tener ningún componente que requiera actualizar una base de datos de firmas.
- ✓ La solución debe incluir como mínimo las siguientes funcionalidades:
  - Capacidades de Respuesta y Remediación Extendida (XDR).

*Esta es una copia auténtica imprimible de un documento electrónico archivado por el Ministerio de Justicia y Derechos Humanos, aplicando lo dispuesto por el Art. 25 del D.S. 070-2013-PCM y la tercera Disposición Complementaria final del D.S. 026-2016-PCM. Su autenticidad e integridad pueden ser contrastadas a través de la siguiente dirección web: [https://sgd.minjus.gob.pe/gesdoc\\_web/login.jsp](https://sgd.minjus.gob.pe/gesdoc_web/login.jsp) e ingresando el Tipo de Documento, Número y Rango de Fechas de ser el caso o [https://sgd.minjus.gob.pe/gesdoc\\_web/verifica.jsp](https://sgd.minjus.gob.pe/gesdoc_web/verifica.jsp) e ingresando Tipo de Documento, Número, Remitente y Año, según corresponda."*





PERÚ

Ministerio  
de Justicia  
y Derechos Humanos

Secretaría  
General

Oficina General de  
Tecnologías de  
Información

Oficina de  
Infraestructura  
y Soporte Tecnológico

"Decenio de la igualdad de oportunidades para mujeres y hombres"

"Año de la recuperación y consolidación de la economía peruana"

- Mapa de Captura de Amenazas (Threat Hunting).
- Análisis Forense (entiéndase a investigaciones detalladas después de un incidente de seguridad, incluyendo el análisis de logs, tráfico de red, eventos de endpoints esto puede ser recopilado por telemetría o similar).
- Mapa de amenazas basado en MITRE ATT&CK (se aceptarán soluciones que hayan obtenido por lo menos un 98% de efectividad de detección de técnicas de ataques).
- Deberá contar con capacidades de UEBA (User and Entity Behavior Analytics), siendo capaz de retener los eventos recolectados durante al menos 30 días y aprender una línea base o perfil de comportamiento de cada dispositivo y usuario.
- ✓ Mapa de amenazas basado en MITRE ATT&CK.
- ✓ Debe tener capacidades de remediación automáticas y manuales que requieran acción del administrador.
- ✓ Debe tener detección automática temprana y respuesta a eventos de seguridad en los servidores y estaciones finales, y eliminar los falsos positivos.
- ✓ Debe crear incidentes de seguridad, donde un incidente, es una colección de eventos de uno o más productos que juntos representan una historia de ataque. Para ellos, debe utilizar la inteligencia artificial (IA) y aplicar modelos de aprendizaje automático (ML) para correlacionar los eventos de los productos integrados (eventos benignos y de seguridad) en incidentes unificados. Asimismo deberá de incluir una secuencia grafica de incidentes de seguridad.
- ✓ El nivel de prioridad del incidente se debe calcular en función de los artefactos (IoC) del incidente, incluidos los niveles de confianza y gravedad de la detección.
- ✓ Los incidentes de seguridad deben tener los estados de: nuevo, asignado, en proceso y cerrado.
- ✓ Debe mostrar una vista general de línea de tiempo de todos los incidentes de seguridad agrupados e identificados por severidad (crítico, alto, medio, bajo) mediante colores.
- ✓ Cada incidente de seguridad asociado a un analista debe tener la siguiente información:
  - Nivel de prioridad (opcional)
  - Fuente Origen
  - Tácticas de MITRE ATT&CK involucradas.
  - Activos involucrados.
  - Indicadores de compromiso identificados.
  - Acciones de prevención realizadas y/o acciones de prevención recomendadas.
  - Cronología (línea de tiempo) del incidente
- ✓ Las capacidades de análisis de cada incidente deben permitir tener una vista detallada de:
  - Información y análisis forense para ver procesos (entiéndase a investigaciones detalladas después de un incidente de seguridad,

*Esta es una copia auténtica imprimible de un documento electrónico archivado por el Ministerio de Justicia y Derechos Humanos, aplicando lo dispuesto por el Art. 25 del D.S. 070-2013-PCM y la tercera Disposición Complementaria final del D.S. 026-2016-PCM. Su autenticidad e integridad pueden ser contrastadas a través de la siguiente dirección web: [https://sgd.minjus.gob.pe/gesdoc\\_web/login.jsp](https://sgd.minjus.gob.pe/gesdoc_web/login.jsp) e ingresando el Tipo de Documento, Número y Rango de Fechas de ser el caso o [https://sgd.minjus.gob.pe/gesdoc\\_web/verifica.jsp](https://sgd.minjus.gob.pe/gesdoc_web/verifica.jsp) e ingresando Tipo de Documento, Número, Remitente y Año, según corresponda."*



PERÚ

Ministerio  
de Justicia  
y Derechos Humanos

Secretaría  
General

Oficina General de  
Tecnologías de  
Información

Oficina de  
Infraestructura  
y Soporte Tecnológico

“Decenio de la igualdad de oportunidades para mujeres y hombres”  
“Año de la recuperación y consolidación de la economía peruana”

incluyendo el análisis de logs, tráfico de red, eventos de endpoints esto puede ser recopilado por telemetría o similar), archivos, URL, dominios (opcional) y registros involucrados en la información y relacionados con el incidente.

- Indicadores (IoC) y artefactos para ver los indicadores y artefactos relacionados con el incidente.
  - Árbol de ataque para ver una representación gráfica del informe forense generado por la solución de Endpoint para cada detección realizada o una secuencia grafica del incidente de seguridad que correlacione las alertas individuales, ambas con el objetivo de identificar la causa raíz del incidente.
  - Conocer las tácticas MITRE ATT&CK utilizadas en el incidente.
  - Por cada IoC relacionado con el incidente se debe poder buscar este dato en el Mapa de Captura de Amenazas, la consola de Inteligencia de Amenazas y en la búsqueda de Incidentes
- ✓ Debe permitir crear indicadores de compromiso de manera automatizada sobre la base de cada uno de los incidentes, y sobre la base de estos IoC, tomar las siguientes acciones de prevención manera automática o manual:
- Crear el IoC en la gestión de IoC (para prevención o detección).
  - Aislar un Endpoint a través del agente de seguridad ofertado
  - Poner en cuarentena un archivo través del agente de seguridad ofertado
  - Matar un proceso través del agente de seguridad ofertado
  - Aislar direcciones IP (hosts) en los firewalls.
- ✓ Debe contar con un módulo de Inteligencia de Amenazas, que permita brindar contexto a través de la fuente del propio fabricante, así como de una fuente tercera o soportar integrarse con una fuente de terceros como mínimo, con los siguientes datos:
- i. Información del indicador (IoC) en una descripción general de alto nivel del indicador analizado.
    - Para dominios y URL, muestra una captura de pantalla en vivo del sitio web. (opcional)
    - Para los archivos, muestra el detalle del hash del archivo: MD5, SHA1 y SHA256
    - Visto por primera vez: fecha en que se vio el archivo por primera vez.
    - Visto por última vez: fecha en que se vio el archivo por última vez.
  - ii. Información de Research o Búsqueda que muestre para Archivos o información recolectada en la telemetría de los servidores y estaciones finales:
    - Los nombres de archivo observados por el fabricante para este tipo archivo (El research será basado en el hash del archivo).
    - El tráfico de red que creó el archivo durante la emulación de amenazas. (opcional)

*Esta es una copia auténtica imprimible de un documento electrónico archivado por el Ministerio de Justicia y Derechos Humanos, aplicando lo dispuesto por el Art. 25 del D.S. 070-2013-PCM y la tercera Disposición Complementaria final del D.S. 026-2016-PCM. Su autenticidad e integridad pueden ser contrastadas a través de la siguiente dirección web: [https://sgd.minjus.gob.pe/gesdoc\\_web/login.jsp](https://sgd.minjus.gob.pe/gesdoc_web/login.jsp) e ingresando el Tipo de Documento, Número y Rango de Fechas de ser el caso o [https://sgd.minjus.gob.pe/gesdoc\\_web/verifica.jsp](https://sgd.minjus.gob.pe/gesdoc_web/verifica.jsp) e ingresando Tipo de Documento, Número, Remitente y Año, según corresponda.”*







PERÚ

Ministerio  
de Justicia  
y Derechos Humanos

Secretaría  
General

Oficina General de  
Tecnologías de  
Información

Oficina de  
Infraestructura  
y Soporte Tecnológico

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

- Solicitudes DNS del archivo creados durante la emulación de amenazas.
- Proceso principal (parent process) que creó el archivo.
- El hash del archivo.
- URL de origen desde las que se descargó el archivo. (opcional).
- ✓ La caza de amenazas debe permitir:
  - Recopilación y enriquecimiento de datos: todos los eventos se recopilan a través de múltiples sensores en agente, se envían a un repositorio unificado y se complementan con información de inteligencia de amenazas, mapa de MITRE.
  - Consultas predefinidas y un panel de MITRE que mapean toda la actividad y permite el inicio rápido a la búsqueda proactiva de amenazas.
  - Acciones de remediación por cada resultado o de manera masiva, para tomar acciones como la cuarentena de archivos, terminar procesos, iniciar análisis forense y aislar equipos.
  - Los datos del mapa de captura de amenazas se deben almacenar la telemetría del endpoint durante un periodo mínimo de 30 días, con la finalidad de realizar investigaciones durante este periodo de tiempo.
- ✓ Debe poder crear y editar indicadores de compromiso (IoC) que se aplican a todos los productos (estaciones finales y servidores) integrados con la solución de XDR
- ✓ Por cada uno de los IoC se debe tener como mínimo las siguientes capacidades:
  - Debe poder habilitar y deshabilitar cada uno de los IoC
  - Definir tipo: Dominio, IP, URL, Hash (MD5, SHA1, SHA256)
  - Nivel de confianza y nivel de severidad
  - Fecha de expiración del IoC.
  - Debe permitir la carga masiva de IoC de terceros, mediante archivos CSV.
- ✓ La consola de administración deberá estar alojada en nube provista por el fabricante a través de Internet. Opcionalmente la consola de administración podría mostrar una secuencia gráfica del incidente de seguridad, correlacionando automáticamente las alertas individuales mediante inteligencia artificial, con el fin de identificar la causa raíz del incidente.
- ✓ El acceso a consola de administración en nube debe soportar doble factor de autenticación (MFA) a través de Google Authenticator y/o Microsoft Authenticator y/o token enviado por correo electrónico.
- ✓ La solución detección y respuesta extendida debe incluir al menos retención de datos de incidentes y alertas debe ser de al menos de 90 días.

#### 17. CAPACIDADES DE OPTIMIZACIÓN

- ✓ Se deberá incluir una herramienta integrada y/o externa que genere alertas si existen problemas de salud del equipo en materia de hardware

*Esta es una copia auténtica imprimible de un documento electrónico archivado por el Ministerio de Justicia y Derechos Humanos, aplicando lo dispuesto por el Art. 25 del D.S. 070-2013-PCM y la tercera Disposición Complementaria final del D.S. 026-2016-PCM. Su autenticidad e integridad pueden ser contrastadas a través de la siguiente dirección web: [https://sgd.minjus.gob.pe/gesdoc\\_web/login.jsp](https://sgd.minjus.gob.pe/gesdoc_web/login.jsp) e ingresando el Tipo de Documento, Número y Rango de Fechas de ser el caso o [https://sgd.minjus.gob.pe/gesdoc\\_web/verifica.jsp](https://sgd.minjus.gob.pe/gesdoc_web/verifica.jsp) e ingresando Tipo de Documento, Número, Remitente y Año, según corresponda."*



PERÚ

Ministerio  
de Justicia  
y Derechos Humanos

Secretaría  
General

Oficina General de  
Tecnologías de  
Información

Oficina de  
Infraestructura  
y Soporte Tecnológico

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

y software, como mínimo: consumo de memoria, problemas de la alta disponibilidad (HA), problemas de disco duro, expiración de licencias.

- ✓ Con el objetivo de que la Institución cuente con autonomía para evaluar si el NGFW se encuentra configurado acorde a las buenas prácticas y evitar que el postor sea juez y parte del control de calidad de ésta, se deberá incluir una herramienta o servicio del propio fabricante que permita evaluar si el NGFW se encuentra configurado acorde a las buenas prácticas del fabricante en materia de los diferentes módulos de seguridad que se le haya activado. Esto se deberá realizar 2 veces por cada año según la vigencia del contrato para todas las políticas configuradas en los NGFW.
- ✓ Esta herramienta o servicio del propio fabricante deberá consolidar la información de todos los NGFW por adquirir en el presente proyecto.
- ✓ Esta herramienta o servicio debe contar con gráficos ejecutivos que permitan mostrar el nivel de adopción de los módulos de seguridad del NGFW en las políticas de seguridad.
- ✓ Esta herramienta o servicio debe identificar las políticas abiertas que no tengan restricciones de puertos y/o aplicaciones (ANY o ALL), con el objetivo de corregirlas y hacer cumplir el principio de mínimo privilegio.
- ✓ La herramienta o servicio de evaluación del propio fabricante de buenas prácticas deberá ser específica para la configuración de los NGFW implementado, no se aceptarán portales con guías de usuarios genéricas.

#### 18. ADMINISTRACION Y MONITOREO

- ✓ Con la finalidad de no degradar el performance de procesamiento de red y seguridad del NGFW, la administración del equipo, gestión de reportes y gestión de logs deben contar con recursos dedicados de CPU y Disco Duro, ya sea integrado dentro del mismo appliance u otro appliance independiente del mismo fabricante.
- ✓ En caso el postor haya incluido en su propuesta plataformas externas al NGFW, éstas también deberán tener su propia consola de gestión, ya sea de manera integrada, appliance independiente o basadas en nube.
- ✓ La solución debe permitir exportar las reglas de seguridad del NGFW al menos en formato CSV y PDF desde su consola de administración o mediante herramientas integradas del fabricante.
- ✓ Debe contar con un dashboard interactivo y gráfico que permita monitorear el uso de las aplicaciones en capa 7, sitios web visitados, actividad de los usuarios, actividad por IP (origen y destino), países origen y destino del tráfico, uso de las reglas de seguridad, actividad del tráfico malicioso, actividad de los usuarios VPN. Esta información podrá ser vista en base a Bytes y Sesiones, y ser filtrado en base a un rango de tiempo, IP, usuario, país y regla de seguridad.
- ✓ Debe registrar eventos correlacionados a través de patrones y umbrales definidos que coincidan con los patrones de tráfico de la red de la entidad. Se deberá representar de forma gráfica los eventos correlacionados.
- ✓ Debe permitir el control de acceso a la gestión del equipo a través de roles personalizables.
- ✓ Debe permitir la captura de paquetes en formato PCAP para poder ser leídos por una herramienta tercera. La captura de paquetes deberá poder

*Esta es una copia auténtica imprimible de un documento electrónico archivado por el Ministerio de Justicia y Derechos Humanos, aplicando lo dispuesto por el Art. 25 del D.S. 070-2013-PCM y la tercera Disposición Complementaria final del D.S. 026-2016-PCM. Su autenticidad e integridad pueden ser contrastadas a través de la siguiente dirección web: [https://sgd.minjus.gob.pe/gesdoc\\_web/login.jsp](https://sgd.minjus.gob.pe/gesdoc_web/login.jsp) e ingresando el Tipo de Documento, Número y Rango de Fechas de ser el caso o [https://sgd.minjus.gob.pe/gesdoc\\_web/verifica.jsp](https://sgd.minjus.gob.pe/gesdoc_web/verifica.jsp) e ingresando Tipo de Documento, Número, Remitente y Año, según corresponda."*







PERÚ

Ministerio  
de Justicia  
y Derechos Humanos

Secretaría  
General

Oficina General de  
Tecnologías de  
Información

Oficina de  
Infraestructura  
y Soporte Tecnológico

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

ser filtrada antes del proceso de ejecución en base a la interfaz, IP y Puerto (origen y destino)

- ✓ Ante escenarios donde existan dos o más administradores en el equipo, logueados y realizando cambios en simultáneo en la consola de gestión, la solución deberá de ser capaz de solo aplicar los cambios realizados por cada administrador individual, sin afectar o sobrescribir los cambios del otro administrador.
- ✓ Contar con un módulo que permita comparar y que indique específicamente que cambio se hizo a una política de seguridad respecto a una versión anterior de dicha política.
- ✓ Debe poder realizar una copia de seguridad (backup) automática de las configuraciones y rollback de configuración a la última configuración salvada.
- ✓ Deberá soportar la ingesta de 14 000 eventos por segundo para garantizar la recepción de los registros de todas las políticas configuradas, en caso que Next Generation Firewall no cuente con recursos dedicados para la gestión, se deberá proporcionar un equipo adicional del mismo fabricante que cumpla lo solicitado.
- ✓ Debe contar con una capacidad de 16 TB utilizables después de realizado el RAID, en caso que Next Generation Firewall no cuente con recursos dedicados para la gestión, se podrá proporcionar un equipo adicional del mismo fabricante que cumpla con la capacidad solicitada.
- ✓ Debe permitir el monitoreo de eventos basados en SNMP, integración con SIEM a través de Syslog, y envío de alertas por correo electrónico (integrándose a un servidor SMTP).
- ✓ Debe permitir la generación de logs de auditoría detallados, informando de la configuración realizada, el administrador que la realice, su IP y el horario de la alteración.
- ✓ La gestión de NGFW debe permitir la asignación de una cuota de uso de disco para definir una capacidad máxima de almacenamiento de logs de tráfico de datos, amenazas, auditoría de configuraciones, eventos de sistema.
- ✓ Debe soportar la personalización de reportes, permitiendo mostrar información de eventos de Antispyware y/o Antibot, Antimalware y/o Antivirus, IPS, navegación a internet, aplicaciones, malware de día cero, debe permitir seleccionar las columnas a mostrar, filtrar la información en base a usuarios, grupos de usuarios, direcciones IP, el rango de fechas de los datos, deben poder ser exportados en PDF y enviados automáticamente vía correo electrónico.
- ✓ Debe permitir configurar reportes para ver el tiempo de navegación de los usuarios en internet, clasificado por tipo de página web y URL.
- ✓ Debe contar con reportes predeterminados que muestren información y diversas estadísticas sobre el uso de aplicaciones SaaS.
- ✓ La gestión de NGFW debe permitir realizar tareas de gestión a través del API basado en XML y/o JSON.

El servicio de los Firewalls perimetrales de Internet requerido, debe ser capaz de monitorear los archivos salientes desde la red interna hacia internet, con el

*Esta es una copia auténtica imprimible de un documento electrónico archivado por el Ministerio de Justicia y Derechos Humanos, aplicando lo dispuesto por el Art. 25 del D.S. 070-2013-PCM y la tercera Disposición Complementaria final del D.S. 026-2016-PCM. Su autenticidad e integridad pueden ser contrastadas a través de la siguiente dirección web: [https://sgd.minjus.gob.pe/gesdoc\\_web/login.jsp](https://sgd.minjus.gob.pe/gesdoc_web/login.jsp) e ingresando el Tipo de Documento, Número y Rango de Fechas de ser el caso o [https://sgd.minjus.gob.pe/gesdoc\\_web/verifica.jsp](https://sgd.minjus.gob.pe/gesdoc_web/verifica.jsp) e ingresando Tipo de Documento, Número, Remitente y Año, según corresponda."*





PERÚ

Ministerio  
de Justicia  
y Derechos Humanos

Secretaría  
General

Oficina General de  
Tecnologías de  
Información

Oficina de  
Infraestructura  
y Soporte Tecnológico

"Decenio de la igualdad de oportunidades para mujeres y hombres"

"Año de la recuperación y consolidación de la economía peruana"

objetivo de detectar la salida del MINJUSDH. Durante el periodo de contrato, a solicitud de la Oficina de Infraestructura y Soporte Tecnológico (OIST) y sin costo adicional para la Entidad, el servicio debe ser capaz de pasar a modo de prevención bloqueando la salida de archivos confidenciales; para el cumplimiento de este objetivo el Contratista es responsable de realizar todas las configuraciones que sean necesarias en los firewalls perimetrales, de acuerdo a los controles de seguridad relacionadas a la prevención de fuga de información, que será alcanzado por los especialistas de la Oficina de Infraestructura y Soporte Tecnológico (OIST). El Contratista contará con un plazo de diez (10) días calendario, contados a partir del día siguiente de la entrega de los controles mencionados, para realizar las configuraciones correspondientes.

El contratista debe configurar todas las funcionalidades de protección requeridas de acuerdo a las políticas, directivas y lineamientos que proporcionará la Oficina de Infraestructura y Soporte Tecnológico (OIST) durante el proceso de implementación e incluir también la migración de las políticas de los actuales Firewalls hacia los Firewalls que proveerá para el servicio. Además, los Firewalls perimetrales de internet deben tener la funcionalidad de configurarse de tal manera que ante un escenario de contingencia (eventual apagado del centro de datos de contingencia a implementar del MINJUSDH), todo el tráfico de salida hacia Internet y el tráfico de entrada hacia la red interna sea asumido por los Firewalls perimetrales del Centro de Datos Principal, de manera automática; y viceversa: ante un escenario de contingencia (eventual apagado completo del Centro de Datos principal), todo el tráfico de salida hacia Internet y el tráfico de entrada hacia la red interna sea asumido por los Firewalls perimetrales del centro de datos de contingencia que podría tener el MINJUSDH, de manera automática. Asimismo, el contratista debe realizar todas las configuraciones que correspondan en las funcionalidades Antispyware y/o Antibot, Antimalware y/o Antivirus, IPS e IPS hasta conseguir un nivel adecuado de protección de los activos informáticos del MINJUSDH. No se aceptarán que las configuraciones sean básicas, con plantillas predefinidas o precargadas por el fabricante; las políticas de las funcionalidades Antispyware/Antimalware e IPS deben ser personalizadas por el Contratista antes de su puesta a producción.

Todas las funcionalidades de seguridad solicitadas, tales como Antispyware y/o Antibot, Antimalware y/o Antivirus, e IPS, deben estar configuradas en el máximo nivel/modo de inspección de seguridad para garantizar un análisis a profundidad. En caso las plataformas cuenten con más de un nivel de inspección, la solución deberá estar dimensionada para operar en el máximo nivel/modo de inspección seguridad más exigente.

Durante el periodo de servicio, el tuning a todas las funcionalidades de protección, debe ser una actividad frecuente y recurrente por parte del Contratista, conducente a garantizar la mayor precisión en el filtrado del tráfico malicioso para mejorar de manera continua los niveles de protección de los activos informáticos del MINJUSDH, previa coordinación con los especialistas de la Oficina de Infraestructura y Soporte Tecnológico (OIST). Durante los tres (3) primeros meses de la ejecución del servicio, el Contratista y los especialistas de la Oficina de Infraestructura y Soporte Tecnológico (OIST) evaluarán la posibilidad de realizar la inspección en las soluciones perimetrales de acceso a Internet, en el caso se considere viable la inspección HTTPS, el Contratista debe

*Esta es una copia auténtica imprimible de un documento electrónico archivado por el Ministerio de Justicia y Derechos Humanos, aplicando lo dispuesto por el Art. 25 del D.S. 070-2013-PCM y la tercera Disposición Complementaria final del D.S. 026-2016-PCM. Su autenticidad e integridad pueden ser contrastadas a través de la siguiente dirección web: [https://sgd.minjus.gob.pe/gesdoc\\_web/login.jsp](https://sgd.minjus.gob.pe/gesdoc_web/login.jsp) e ingresando el Tipo de Documento, Número y Rango de Fechas de ser el caso o [https://sgd.minjus.gob.pe/gesdoc\\_web/verifica.jsp](https://sgd.minjus.gob.pe/gesdoc_web/verifica.jsp) e ingresando Tipo de Documento, Número, Remitente y Año, según corresponda."*

20







PERÚ

Ministerio  
de Justicia  
y Derechos Humanos

Secretaría  
General

Oficina General de  
Tecnologías de  
Información

Oficina de  
Infraestructura  
y Soporte Tecnológico

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

elaborar un "plan de actividades" para ejecutar la inspección mencionada en coordinación con los especialistas de la Oficina de Infraestructura y Soporte Tecnológico (OIST).

#### ***Para el servicio de protección sandboxing en la nube.***

El servicio requerido con tecnología sandboxing en la nube, debe proveer información forense sobre las acciones realizadas por el malware y generar automáticamente las firmas de malware y bloquear el acceso a las URLs maliciosas utilizadas por el malware. Debe soportar el análisis de archivos ejecutables (EXE), DLLs, archivos comprimidos (ZIP y RAR), archivos office (.doc, .docx, .xls, .xlsx, .ppt, .pptx), archivos java (.jar), archivos de tipos script (.vbs, .ps1, .js), flash y/o swf, opcionalmente para archivos de MacOS (dmg y pkg) y/o Android APKs en el ambiente controlado. Debe permitir la subida de archivos al sandbox de forma manual y/o soportar un servicio adicional que permite vía API enviar muestras a al servicio de Sandboxing del vendor oferente, con ello tener capacidad de detección de malware conocido/desconocido, como también detectar técnicas para evasión de sandboxing.

Debe integrarse perfectamente con la solución de Firewall de Siguierte Generación, debe tener la capacidad de emular los archivos sospechosos en entornos Windows 7, Windows 8 (Opcional), Windows 10 y futuras versiones de sistemas operativos liberados por Microsoft, debe garantizar la privacidad y seguridad del contenido de los archivos analizados, para lo cual se requiere que la plataforma cuente con las certificaciones SOC 2 de tipo 2 de AICPA y/o FedRAMP.

Deberá tener una disponibilidad de al menos 99.9% contabilizados mensualmente.

#### ***Para el servicio de acceso remoto por Virtual Private Network (VPN).***

Para el servicio de Acceso Remoto VPN, la solución debe permitir la aplicación de políticas de seguridad y visibilidad para las aplicaciones que circulan dentro de los túneles VPN. La solución debe tener interoperabilidad con otros fabricantes. El contratista debe realizar todas las configuraciones en la solución e incorporar los mecanismos y soportes necesarios para que el servicio VPN brinde autenticación de doble factor, con certificado digital e integración con el Directorio Activo. La entidad brindará el certificado digital para los usuarios que tengan acceso remoto vía VPN.

Deberá soportar VPN Site-to-Site en protocolo IPSec.

La VPN site to site debe soportar como mínimo:

- DES y 3DES; AES 128, 192 y/o 256 (Advanced Encryption Standard).

Esta es una copia auténtica imprimible de un documento electrónico archivado por el Ministerio de Justicia y Derechos Humanos, aplicando lo dispuesto por el Art. 25 del D.S. 070-2013-PCM y la tercera Disposición Complementaria final del D.S. 026-2016-PCM. Su autenticidad e integridad pueden ser contrastadas a través de la siguiente dirección web: [https://sgd.minjus.gob.pe/gesdoc\\_web/login.jsp](https://sgd.minjus.gob.pe/gesdoc_web/login.jsp) e ingresando el Tipo de Documento, Número y Rango de Fechas de ser el caso o [https://sgd.minjus.gob.pe/gesdoc\\_web/verifica.jsp](https://sgd.minjus.gob.pe/gesdoc_web/verifica.jsp) e ingresando Tipo de Documento, Número, Remitente y Año, según corresponda."







PERÚ

Ministerio  
de Justicia  
y Derechos Humanos

Secretaría  
General

Oficina General de  
Tecnologías de  
Información

Oficina de  
Infraestructura  
y Soporte Tecnológico

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

- Autenticación MD5, SHA-1 y/o SHA-2.
- Diffie-Hellman Group 1, Group 2, Group 5 y Group 14.
- Algoritmo Internet Key Exchange (IKEv1 & IKEv2);

Permitir la aplicación de políticas de seguridad y visibilidad para las aplicaciones que circulan dentro de los túneles VPN.

Permitir aplicar QoS dentro de los túneles VPN site to site.

Soportar VPN client-to-site pudiendo operar usando el protocolo IPSec o SSL.

La plataforma debe ser capaz de colocar en cuarentena equipos con actividad maliciosa identificada, de manera manual y automática. Los equipos en cuarentena no deberán tener conexión con ningún recurso de red protegido por la solución. En su defecto se aceptarán soluciones que cuenten con funcionalidades que aseguren que los clientes VPN cumplan con Política de Seguridad de la Organización

Debe permitir configurar una postura de seguridad del equipo con el cliente VPN instalado, que permita validar determinadas características del equipo y en base al nivel de cumplimiento (compliance) del host permitir, denegar o limitar el acceso a los recursos de la red interna. Por lo menos se deberá poder configurar los siguientes casos de uso y una combinación de ellas:

- Sistema operativo del equipo
- Pertenencia al dominio corporativo
- Software antivirus instalado y habilitado en tiempo real
- Software antivirus con la base de datos de firmas actualizada en un número de días personalizable
- Marca del software antivirus
- Parche de seguridad instalado opcional según su nivel de criticidad.
- Permitir añadir validaciones de aplicaciones personalizadas añadiendo la Clave de Registro (en caso de Windows) o Plist (en caso de MacOS). En su defecto, se aceptarán soluciones que validen la versión del Sistema Operativo en dispositivos Windows
- Este control deberá estar disponible al menos para equipos Windows y MacOS, en al menos 1000 dispositivos.

Asimismo, el servicio VPN ante una eventual caída, debe tener la funcionalidad poder configurar automáticamente en otro centro de datos de contingencia que pueda implementar el MINJUSDH, sin necesidad de realizar configuraciones manuales, post incidente, en los clientes VPN.

El MINJUSDH cuenta con un servicio VPN actual en producción, el cual tiene

*Esta es una copia auténtica imprimible de un documento electrónico archivado por el Ministerio de Justicia y Derechos Humanos, aplicando lo dispuesto por el Art. 25 del D.S. 070-2013-PCM y la tercera Disposición Complementaria final del D.S. 026-2016-PCM. Su autenticidad e integridad pueden ser contrastadas a través de la siguiente dirección web: [https://sgd.minjus.gob.pe/gesdoc\\_web/login.jsp](https://sgd.minjus.gob.pe/gesdoc_web/login.jsp) e ingresando el Tipo de Documento, Número y Rango de Fechas de ser el caso o [https://sgd.minjus.gob.pe/gesdoc\\_web/verifica.jsp](https://sgd.minjus.gob.pe/gesdoc_web/verifica.jsp) e ingresando Tipo de Documento, Número, Remitente y Año, según corresponda."*





Ministerio  
de Justicia  
y Derechos Humanos

Secretaría  
General

Oficina General de  
Tecnologías de  
Información

Oficina de  
Infraestructura  
y Soporte Tecnológico

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

políticas de acceso definidas, las cuales deben ser migradas por el Contratista a la solución requerida.

El Contratista será responsable del soporte y despliegue necesario de los clientes VPN.

***Para las consolas de administración de las soluciones perimetrales.***

El MINJUSDH requiere que las soluciones: Seguridad perimetral con tecnologías de Firewalls de siguiente generación, acceso remoto por Virtual Private Network (VPN.) y Protección con tecnología sandboxing, se gestionen mediante una consola centralizada on-premise que debe ser en formato appliance y debe ser del mismo fabricante, con la finalidad de hacer más eficiente su administración.

La consola debe contar un flujo de aprobación de cambios.

- Esta función debe permitir la opción de revisar y aprobar los cambios de configuración realizados por otros administradores antes de publicarlos ya sea por un super admin o un rango mayor al administrador.
- Se puede definir qué administradores deben enviar sus cambios para su aprobación y qué administradores están autorizados para aprobar los cambios.

O en su defecto brindar soluciones que sean capaces de limitar la ejecución(compilar) de cambios efectuados por usuarios de menor jerarquía.

Esta consola debe ser capaz de gestionar todas las políticas de seguridad de cada uno de los appliances y servidores que conforman las soluciones referidas. Debe ser capaz de brindar una gestión bajo multidominio o agrupando los appliances o servidores de acuerdo a su propósito o función dentro de la red del MINJUSDH. Debe ser capaz de visualizar e identificar los estados de operatividad de los equipos, visualizar consumos de CPU y Memoria, estadísticas de conexiones, servicios y/o aplicaciones, protocolos, usuarios, cantidad de tráfico ya sea en tiempo real y en histórico. Debe ser capaz de concentrar todos los logs y eventos de los equipos que conforman la solución de seguridad perimetral, correlacionar sus eventos y visualizar indicadores de ataques, amenazas, hosts infectados, control de accesos, tráfico, archivos infectados, entre otros. Debe permitir la generación de reportes personalizados y automatizados, con la opción de ser enviados de manera automática vía correo electrónico.

***Acuerdo de niveles de servicio (ANS).***

Esta es una copia auténtica imprimible de un documento electrónico archivado por el Ministerio de Justicia y Derechos Humanos, aplicando lo dispuesto por el Art. 25 del D.S. 070-2013-PCM y la tercera Disposición Complementaria final del D.S. 026-2016-PCM. Su autenticidad e integridad pueden ser contrastadas a través de la siguiente dirección web: [https://sgd.minjus.gob.pe/gesdoc\\_web/login.jsp](https://sgd.minjus.gob.pe/gesdoc_web/login.jsp) e ingresando el Tipo de Documento, Número y Rango de Fechas de ser el caso o [https://sgd.minjus.gob.pe/gesdoc\\_web/verifica.jsp](https://sgd.minjus.gob.pe/gesdoc_web/verifica.jsp) e ingresando Tipo de Documento, Número, Remitente y Año, según corresponda."





PERÚ

Ministerio de Justicia y Derechos Humanos

Secretaría General

Oficina General de Tecnologías de Información

Oficina de Infraestructura y Soporte Tecnológico

“Decenio de la igualdad de oportunidades para mujeres y hombres”  
“Año de la recuperación y consolidación de la economía peruana”

ANS	Descripción	Cálculo de la Medición	Valor Base %	Horario Acordado	Periodicidad
Disponibilidad del servicio de Firewalls perimetrales para el acceso a Internet.	El objetivo de este ANS es medir la disponibilidad de la solución Firewalls perimetrales para el acceso a Internet.	Disponibilidad = $(1 - \text{TIPM} / \text{TTSM}) * 100$	>=99.9	24x7	Mensual
Disponibilidad del servicio de protección con tecnología Sandboxing perimetral.	El objetivo de este ANS es medir la disponibilidad de la solución de sandboxing de la nube.				
Disponibilidad del servicio de acceso remoto VPN.	El objetivo de este ANS es medir la disponibilidad de la solución de acceso remoto VPN.				

Donde TE: Tiempo Total Efectivo = TT – TIP

TT: Tiempo Total al mes en minutos (N° días x 24 x 60)

TIP: Tiempo de interrupciones programadas al servicio (en minutos)

TIPM: Tiempo de interrupción en el mes en minutos.

TTSM: Tiempo total de servicio en el mes en minutos.

Si la disponibilidad de la solución Firewalls perimetral, protección con tecnología Sandboxing perimetral y acceso remoto por VPN es menor al 99.9% en base mensual, en hasta dos (2) oportunidades durante dos (02) meses consecutivos, el Contratista debe reemplazar la solución, por otra solución de iguales o superiores características, sin costo para la Entidad y sin que esto exima las penalidades correspondientes. Para el reemplazo de la solución el contratista tiene un plazo de diez (10) días calendarios contados a partir del día siguiente de recibida la notificación por parte del MINJUSDH. Se precisa que para el reemplazo de las soluciones será previa comprobación de falla y pruebas respectivas.

Asimismo, debe contar con los servicios profesionales de un Ingeniero del fabricante para asegurar el diseño, configuración y puesta en producción de la solución.

## B. SERVICIO DE PROTECCIÓN CONTRA ATAQUES A LAS APLICACIONES Y SERVICIOS WEB.

### Consideraciones Generales:

El servicio debe proteger a nuestras aplicaciones y servicios web publicados a Internet, por el enlace de internet de la sede Central del MINJUSDH, el Contratista debe proveer el servicio con la implementación de una solución de Web Application and API Protection (WAAP) en la nube, contra ataques a nivel de aplicación y que incluya una consola de administración en la nube del mismo fabricante.

*Esta es una copia auténtica imprimible de un documento electrónico archivado por el Ministerio de Justicia y Derechos Humanos, aplicando lo dispuesto por el Art. 25 del D.S. 070-2013-PCM y la tercera Disposición Complementaria final del D.S. 026-2016-PCM. Su autenticidad e integridad pueden ser contrastadas a través de la siguiente dirección web: [https://sgd.minjus.gob.pe/gesdoc\\_web/login.jsp](https://sgd.minjus.gob.pe/gesdoc_web/login.jsp) e ingresando el Tipo de Documento, Número y Rango de Fechas de ser el caso o [https://sgd.minjus.gob.pe/gesdoc\\_web/verifica.jsp](https://sgd.minjus.gob.pe/gesdoc_web/verifica.jsp) e ingresando Tipo de Documento, Número, Remitente y Año, según corresponda.”*







PERÚ

Ministerio  
de Justicia  
y Derechos Humanos

Secretaría  
General

Oficina General de  
Tecnologías de  
Información

Oficina de  
Infraestructura  
y Soporte Tecnológico

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

El soporte técnico que el Contratista contrate al fabricante de la solución WAAP, debe ser un nivel de soporte que incluya la atención 24x7 durante el periodo de servicio.

La solución debe incluir capacidades de protección contra vulnerabilidades descritas en OWASP Top 10, así como funcionalidades de WAF, Bot Manager, API Protection, Client Side Protection y mitigación DDoS para las aplicaciones web expuestas al entorno público. Estas capacidades deberán aplicarse a 25 aplicaciones como mínimo dependiendo de la criticidad que la entidad evalúe y considerando la suma total del ancho de banda a proteger. Se entiende como aplicación al sitio web, o al subdominio web (URL) a proteger.

El flujo actual de enrutamiento de red y aplicaciones no pasa por un balanceador de carga, sin embargo con el fin de asegurar un adecuado tráfico de las aplicaciones que subirán al Servicio de Protección contra Ataques a las Aplicaciones y Servicio Web, se deberá contemplar como mínimo 2 balanceadores en modalidad Activo-Pasivo (Appliance).

#### **Consideraciones Específicas**

La solución a implementar para la provisión del servicio, debe contar con generación y análisis automático de políticas de seguridad, debe contar con capacidad de aprendizaje sin manipulación del administrador y proveer protección de Aplicaciones Web contra amenazas registradas OWASP Top Ten Vulnerabilities vigente, incluyendo SQL Injection, Cross-site Scripting (XSS), Parameter tampering, Manipulación de sesión, Command Injection, Application Buffer Overflow Attacks, Ataques de Fuerza Bruta, Reconocimiento de Web Server, SOAP y Manipulación de Web Service, ataques de día cero, Hidden field manipulation (Opcional si se propone una solución en nube) y Cookie poisoning (Opcional si se propone una solución en nube), debe incluir reputación de IP y geo protección. Debe detectar y mitigar ataques de BOTS. Debe proteger contra ataques DDoS de aplicación.

Para soluciones on-premise se considerará para el resguardo de sesiones la solución debe firmar o encriptar cookies con el fin de poder validar sesiones legítimas y evitar el secuestro de sesiones. Para garantizar la persistencia de sesiones, se requieren métodos como cookie insert, cookie rewrite y cookie passive.

Para soluciones en Cloud WAAP el servicio deberá soportar, para cada aplicación protegida, el balanceo de carga hasta 8 servidores origen, incluyendo métricas de round-robin y least connections, persistencia por IP y Cookie

Esta es una copia auténtica imprimible de un documento electrónico archivado por el Ministerio de Justicia y Derechos Humanos, aplicando lo dispuesto por el Art. 25 del D.S. 070-2013-PCM y la tercera Disposición Complementaria final del D.S. 026-2016-PCM. Su autenticidad e integridad pueden ser contrastadas a través de la siguiente dirección web: [https://sgd.minjus.gob.pe/gesdoc\\_web/login.jsp](https://sgd.minjus.gob.pe/gesdoc_web/login.jsp) e ingresando el Tipo de Documento, Número y Rango de Fechas de ser el caso o [https://sgd.minjus.gob.pe/gesdoc\\_web/verifica.jsp](https://sgd.minjus.gob.pe/gesdoc_web/verifica.jsp) e ingresando Tipo de Documento, Número, Remitente y Año, según corresponda."



PERÚ

Ministerio  
de Justicia  
y Derechos Humanos

Secretaría  
General

Oficina General de  
Tecnologías de  
Información

Oficina de  
Infraestructura  
y Soporte Tecnológico

“Decenio de la igualdad de oportunidades para mujeres y hombres”  
“Año de la recuperación y consolidación de la economía peruana”

La solución debe contar con la posibilidad de poder re escribir u ocultar la localización de paths en la URL, sin necesidad de realizar scripts o tener que modificar el código de la aplicación.

Debe permitir visualizar el tiempo de respuesta de red y las aplicaciones por cada transacción que se realice hacia estas aplicaciones (será opcional en caso de soluciones basadas en nube).

El servicio debe cubrir la protección de subdominios/hosts/aplicaciones/servicios web en protocolos HTTP y HTTPS. Las 25 aplicaciones con capacidades de protección contra vulnerabilidades descritas en OWASP Top 10, así como funcionalidades de WAF, Bot Manager, API Protection, Client Side Protection y mitigación DDoS para las aplicaciones web expuestas al entorno público pueden contar con más de un subdominio en HTTP o HTTPS para cada una de las aplicaciones mencionadas siempre y cuando cumplan con tener valores idénticos de “IP Pública (Origin Server)”, “Puerto(s)”, “Protocolo” y “Certificado Digital SSL

El contratista debe considerar que se podrán incorporar nuevos subdominios durante el periodo del servicio siempre y cuando se cumplan con la condición anterior. Debe garantizar que no se degrade la performance de la solución con todas las características de

Protección activas (será opcional en caso de soluciones basadas en nube) y considerar la posibilidad de habilitar protocolo IPv6 durante el periodo de servicio.

El Contratista es responsable de todas las configuraciones necesarias en la solución WAAP para cumplir a cabalidad con la protección requerida, para ello en la etapa de implementación de la solución se deberá contar con los servicios profesionales de un Ingeniero del fabricante para asegurar el diseño, configuración y puesta en producción de la solución.

#### Requerimientos de Seguridad Web

La política de seguridad no debe ser genérica, ni basada en políticas por defecto o mejores prácticas. Debe ser una política a la medida, ajustada a cada aplicación aprovisionada.

Las aplicaciones aprovisionadas se podrán configurar en modo activo, bloqueando los paquetes de ataques de forma proactiva o en modo monitoreo, simplemente reportando eventos, pero no bloqueándolos.

Las políticas de seguridad deben implementar filtros de seguridad que soporten modelo Requerimientos de Seguridad de Aplicaciones s de seguridad positivos y negativos.

*Esta es una copia auténtica imprimible de un documento electrónico archivado por el Ministerio de Justicia y Derechos Humanos, aplicando lo dispuesto por el Art. 25 del D.S. 070-2013-PCM y la tercera Disposición Complementaria final del D.S. 026-2016-PCM. Su autenticidad e integridad pueden ser contrastadas a través de la siguiente dirección web: [https://sgd.minjus.gob.pe/gesdoc\\_web/login.jsp](https://sgd.minjus.gob.pe/gesdoc_web/login.jsp) e ingresando el Tipo de Documento, Número y Rango de Fechas de ser el caso o [https://sgd.minjus.gob.pe/gesdoc\\_web/verifica.jsp](https://sgd.minjus.gob.pe/gesdoc_web/verifica.jsp) e ingresando Tipo de Documento, Número, Remitente y Año, según corresponda.”*





Ministerio  
de Justicia  
y Derechos Humanos

Secretaría  
General

Oficina General de  
Tecnologías de  
Información

Oficina de  
Infraestructura  
y Soporte Tecnológico

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

El servicio debe proteger contra ataques de tipo SSRF (Server side request forgery) y RFI (Remote File Inclusion)

El servicio debe bloquear conexiones que no sean HTTP RFC Compliance

El servicio a través del portal, debe permitir la configuración del bloqueo de tráfico proveniente de anonymous proxies hacia las aplicaciones desde el portal de servicios.

El servicio debe proveer una protección basada en firmas que protega la aplicación contra vulnerabilidades conocidas.

El servicio debe proveer una protección contra comandos de SQL, comandos de shell y ataques de cross-site scripting, usando un algoritmo de reducción para detectar posibles segmentos de código en los parámetros. La protección debe cubrir al menos las siguientes amenazas: Cross Site Scripting (XSS), SQL Injections, Injection Flaws, Command Execution, Database Sabotage, Stealth Commanding, Backdoor. (Database Sabotage, Stealth Commanding, Backdoor son opcionales si se oferta una solución en nube)

El servicio debe proveer una protección basada en modelo de seguridad positivo que evalúe los requerimientos hacia la aplicación, contra una lista que contenga la URI y métodos permitidos, bloqueando todos aquellos requerimientos que no se encuentren explícitamente definidos.

El servicio debe incluir una protección basada en inteligencia de amenazas que podrá activarse o desactivarse desde el portal y permitirá crear excepciones de IP que deban ser excluidas de dichas listas.

El servicio debe brindar al menos las siguientes opciones de página de bloqueo:

- Proveer una página de bloqueo por defecto la cual es mostrada a usuarios identificados como atacantes que intentan acceder a la aplicación.
- Personalizar la página de bloqueo a través de la redirección a un sitio web específico.

El servicio debe permitir crear reglas de rate limiting definiendo al menos los siguientes parámetros por regla:

- Acción de la regla: Bloqueo y solo reporte como mínimo.
- Identificador de cliente: Mínimo requerido, tracking por IP y tracking a través de una cookie insertada por el servicio como mínimo.
- Método, Path.

*Esta es una copia auténtica imprimible de un documento electrónico archivado por el Ministerio de Justicia y Derechos Humanos, aplicando lo dispuesto por el Art. 25 del D.S. 070-2013-PCM y la tercera Disposición Complementaria final del D.S. 026-2016-PCM. Su autenticidad e integridad pueden ser contrastadas a través de la siguiente dirección web: [https://sgd.minjus.gob.pe/gesdoc\\_web/login.jsp](https://sgd.minjus.gob.pe/gesdoc_web/login.jsp) e ingresando el Tipo de Documento, Número y Rango de Fechas de ser el caso o [https://sgd.minjus.gob.pe/gesdoc\\_web/verifica.jsp](https://sgd.minjus.gob.pe/gesdoc_web/verifica.jsp) e ingresando Tipo de Documento, Número, Remitente y Año, según corresponda."*







PERÚ

Ministerio  
de Justicia  
y Derechos Humanos

Secretaría  
General

Oficina General de  
Tecnologías de  
Información

Oficina de  
Infraestructura  
y Soporte Tecnológico

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

- Límite permitido (Threshold)
- Tiempo de bloqueo.

La solución deberá permitir al administrador, crear firmas custom (Custom Signatures). Mediante este mecanismo el administrador podrá incorporar a las protecciones incluidas en la solución patrones específicos que desee tratar como eventos de seguridad.

La solución debe contar con un mecanismo que permita el bloqueo automático y temporal de direcciones IP de origen (source-blocking), basado en el seguimiento de los ataques que dicho origen a realizado y correlacionado por herramientas de ML

El servicio debe incluir una protección que permita enmascarar o bloquear información confidencial proveniente de la aplicación incluyendo mensajes de errores del servidor y número de tarjetas de crédito.

La solución debe contar con un mecanismo que permita visualizar los subdominios y/o URLs que invocan los scripts de java (JS) desde el navegador de los usuarios que consumen las aplicaciones, así como el nivel de amenaza de los mismos y si es que estos cuentan o no con certificados de seguridad.

La solución debe soportar detección y mitigación de ataques del lado del cliente, para proteger contra al menos las siguientes amenazas formjacking, Megacart, supply chain, e-skimming y DOM based XSS.

La protección del lado del Cliente, debe mostrar los dominios accedidos por los diferentes scripts que se ejecutan del lado del usuario. Dichos dominios deberán categorizarse en base a su reputación generando un indicador de nivel de amenaza potencial

La protección del lado del cliente, debe ser capaz de informar cuando:

- Se detecta comunicación con un nuevo dominio.
- Se detecta una nueva solicitud saliente.
- Se detecta un nuevo origen

La protección del lado del cliente debe tener como mínimo las siguientes funcionalidades:

- Bloquear automáticamente dominios sospechosos según su nivel de amenaza y permitir dominios legítimos con excepciones.
- Evaluación del nivel de amenazas.

*Esta es una copia auténtica imprimible de un documento electrónico archivado por el Ministerio de Justicia y Derechos Humanos, aplicando lo dispuesto por el Art. 25 del D.S. 070-2013-PCM y la tercera Disposición Complementaria final del D.S. 026-2016-PCM. Su autenticidad e integridad pueden ser contrastadas a través de la siguiente dirección web: [https://sgd.minjus.gob.pe/gesdoc\\_web/login.jsp](https://sgd.minjus.gob.pe/gesdoc_web/login.jsp) e ingresando el Tipo de Documento, Número y Rango de Fechas de ser el caso o [https://sgd.minjus.gob.pe/gesdoc\\_web/verifica.jsp](https://sgd.minjus.gob.pe/gesdoc_web/verifica.jsp) e ingresando Tipo de Documento, Número, Remitente y Año, según corresponda."*



PERÚ

Ministerio  
de Justicia  
y Derechos Humanos

Secretaría  
General

Oficina General de  
Tecnologías de  
Información

Oficina de  
Infraestructura  
y Soporte Tecnológico

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

- Notificaciones en tiempo real para cada nuevo descubrimiento y cambios en servicios existentes."

#### Requerimientos de Seguridad de Aplicaciones.

La solución debe soportar descubrimiento de la API a través de machine learning, generando un archivo que se pueda descargar desde el portal del servicio.

El contratista deberá considerar un volumen estimado de llamadas API, tomando como base el tráfico actual de 4 millones de solicitudes HTTP/S por día. Se estima que aproximadamente el 40% de este tráfico corresponde a llamadas API, lo cual representa un volumen aproximado de 1.6 millones de llamadas API diarias, 48 millones mensuales y 584 millones anuales.

La solución debe realizar Schema Enforcement en XML y JSON validando el método, endpoint, query parameters, header parameters, cookie parameters y body parameters.

La solución debe soportar API quota management permitiendo configurar el número de llamadas en un periodo de tiempo configurable, por cada método dentro de los endpoints de API definidos y debe realizar seguimiento a cada origen que realiza el llamado.

El servicio a través del portal, debe permitir añadir o modificar los parámetros de tipo query, header cookies o body de los endpoints.

El servicio a través del portal, debe permitir definir la política para unir la información de un nuevo archivo Open API con la información que ya se encuentra configurada en el portal, dando al operador al menos las siguientes opciones:

- Sobre escribir todo con el nuevo archivo.
- Sobre escribir endpoints duplicados y añadir nuevos endpoints.(opcional).
- Solo añadir nuevos endpoints (opcional).

La solución de protección API debe soportar la configuración de seguridad sobre cada endpoint en modo bloqueo, solo reporte y deshabilitado.

La protección de API debe contar con capacidades avanzadas, que le permita brindar protección contra vulnerabilidades en la lógica de negocios (Requerido por PCIDSS4.0)

*Esta es una copia auténtica imprimible de un documento electrónico archivado por el Ministerio de Justicia y Derechos Humanos, aplicando lo dispuesto por el Art. 25 del D.S. 070-2013-PCM y la tercera Disposición Complementaria final del D.S. 026-2016-PCM. Su autenticidad e integridad pueden ser contrastadas a través de la siguiente dirección web: [https://sgd.minjus.gob.pe/gesdoc\\_web/login.jsp](https://sgd.minjus.gob.pe/gesdoc_web/login.jsp) e ingresando el Tipo de Documento, Número y Rango de Fechas de ser el caso o [https://sgd.minjus.gob.pe/gesdoc\\_web/verifica.jsp](https://sgd.minjus.gob.pe/gesdoc_web/verifica.jsp) e ingresando Tipo de Documento, Número, Remitente y Año, según corresponda."*







PERÚ

Ministerio  
de Justicia  
y Derechos Humanos

Secretaría  
General

Oficina General de  
Tecnologías de  
Información

Oficina de  
Infraestructura  
y Soporte Tecnológico

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

La capacidad de mitigación contra ataques a la lógica de negocios, debe estar basada en AI, empleando aprendizaje continuo, y teniendo la posibilidad de aplicar políticas en tiempo real para mitigar los ataques

Las políticas que se aplican, deben garantizar ser lo suficientemente granulares para bloquear al usuario ofensor, y no a otros usuarios compartiendo la misma dirección IP.

La protección de APIs debe tener un control de autorización de tokens basado en JSON Web Token (JWT) el cual asegure que sólo los usuarios autenticados y autorizados interactúen con las APIs expuestas

#### **Requerimientos de Gestión de Bots.**

El servicio debe incluir protección contra ataques de tipo BOT (ataques automatizados).

El servicio debe clasificar el tráfico hacia las aplicaciones en:

- Tráfico Generado por Humanos
- Tráfico Generado por Bots Buenos
- Tráfico Generado por Bot Malos"

El servicio debe cubrir ataques automatizados listados en OWASP de amenazas automatizadas, como mínimo:

- Account take over
- Web Scrapping
- Denial of Inventory
- Payment Frauds"

La solución debe estar basada en tecnología que permita detectar la intención del tráfico y el comportamiento de los usuarios con el fin de detectar las amenazas automatizadas avanzadas de forma precisa sin impactar el tráfico legítimo de los clientes utilizando al menos las siguientes técnicas:

- Inteligencia de bots compartida entre usuarios del servicio.
- Machine Learning semi-supervisado para identificar patrones de bots emergentes.
- IDBA (Intent Based Deep Behavioral Analysis) o tecnologías equivalentes

El servicio debe detectar y bloquear tráfico de bots en donde existan las siguientes anomalías de User-Agent:

*Esta es una copia auténtica imprimible de un documento electrónico archivado por el Ministerio de Justicia y Derechos Humanos, aplicando lo dispuesto por el Art. 25 del D.S. 070-2013-PCM y la tercera Disposición Complementaria final del D.S. 026-2016-PCM. Su autenticidad e integridad pueden ser contrastadas a través de la siguiente dirección web: [https://sgd.minjus.gob.pe/gesdoc\\_web/login.jsp](https://sgd.minjus.gob.pe/gesdoc_web/login.jsp) e ingresando el Tipo de Documento, Número y Rango de Fechas de ser el caso o [https://sgd.minjus.gob.pe/gesdoc\\_web/verifica.jsp](https://sgd.minjus.gob.pe/gesdoc_web/verifica.jsp) e ingresando Tipo de Documento, Número, Remitente y Año, según corresponda."*



PERÚ

Ministerio  
de Justicia  
y Derechos Humanos

Secretaría  
General

Oficina General de  
Tecnologías de  
Información

Oficina de  
Infraestructura  
y Soporte Tecnológico

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

- User-Agents invalidos.
- Headless Chrome.
- Navegadores Antiguos.

La solución debe ser capaz de proteger contra solicitudes que contengan user-agents generados por herramientas automatizadas.

La solución debe proteger contra las peticiones procedentes de IP proxy que contengan versiones antiguas del navegador mediante la limitación condicional de la velocidad.

La solución debe proteger contra bots que envíen peticiones que contengan claves o valores de cabecera maliciosos.

La solución debe proteger contra bots que envíen peticiones de navegadores antiguos sin los encabezados estándar.

La solución debe proteger contra bots que manipulen las cookies que buscan mantener las sesiones seguras.

La solución debe contar con un módulo de anomalías en los encabezados HTTP basado en aprendizaje automático, que aprenda cuál es el conjunto típico esperado de encabezados estándar para cualquier versión importante del navegador, y si encuentra una anomalía con respecto a eso tome acciones sobre el tráfico.

La solución deberá contar con mecanismos que permitan detectar y mitigar comportamientos automatizados relacionados con la resolución masiva de captchas (captcha farms), mediante análisis de comportamiento. La acción de mitigación podrá incluir, de manera opcional, técnicas como el bucle infinito de captcha u otras equivalentes para detener el avance del tráfico automatizado.

La solución debe contar con mecanismos para identificar BOTS que generan ataques rotando sus direcciones IP e identidades, protegiendo de esta manera todos los activos sobre un mismo dominio raíz.

La solución debe tener la capacidad de construir una línea base de tráfico con el objetivo de identificar bots altamente distribuidos en función de "burst" de tráfico, "burst" de IP distribuidas e identificar el patrón de bot de este ataque e implementar una política automáticamente para mitigar este ataque.

Desde el portal se debe permitir configurar al menos las siguientes acciones de bloqueo para bots:

*Esta es una copia auténtica imprimible de un documento electrónico archivado por el Ministerio de Justicia y Derechos Humanos, aplicando lo dispuesto por el Art. 25 del D.S. 070-2013-PCM y la tercera Disposición Complementaria final del D.S. 026-2016-PCM. Su autenticidad e integridad pueden ser contrastadas a través de la siguiente dirección web: [https://sgd.minjus.gob.pe/gesdoc\\_web/login.jsp](https://sgd.minjus.gob.pe/gesdoc_web/login.jsp) e ingresando el Tipo de Documento, Número y Rango de Fechas de ser el caso o [https://sgd.minjus.gob.pe/gesdoc\\_web/verifica.jsp](https://sgd.minjus.gob.pe/gesdoc_web/verifica.jsp) e ingresando Tipo de Documento, Número, Remitente y Año, según corresponda."*



PERÚ

Ministerio  
de Justicia  
y Derechos Humanos

Secretaría  
General

Oficina General de  
Tecnologías de  
Información

Oficina de  
Infraestructura  
y Soporte Tecnológico

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

- Página de bloqueo.
- Challenge a través de Captcha
- Permitir.

Desde el portal se debe permitir configurar y aplicar desafíos CAPTCHA adecuados al riesgo detectado. La configuración de dificultad podrá ser automática o parametrizable, según la solución ofertada.

La solución debe soportar reto criptográfico, el cual será enviado al origen sospechoso para su validación. La posibilidad de incremento de dificultad podrá considerarse como una funcionalidad adicional.

Desde el portal se debe permitir configurar excepciones por IP para la protección de bots. La posibilidad de establecer una fecha de expiración será opcional, en función de las capacidades de la solución ofertada.

Desde el portal se debe permitir configurar acciones contra los bots en URLs específicas de la aplicación.

Desde el portal se debe permitir personalizar las páginas de bloqueo y de captcha.

El Bot Manager debe integrarse con aplicaciones web que tienen como objetivo recopilar datos del usuario para identificar el patrón de comportamiento, en función de los parámetros recopilados. Estos datos ayudan a los motores de bots a realizar análisis más profundos sobre los tipos de bots que intentan acceder a la aplicación.

El servicio de protección de BOT debe permitir integración nativa con ambientes Android e iPhone, mediante un SDK provisto por el fabricante. (debe incluir para las 25 aplicaciones con capacidades de protección contra vulnerabilidades descritas en OWASP Top 10, así como funcionalidades de WAF, Bot Manager, API Protection, Client Side Protection y mitigación DDoS para las aplicaciones web expuestas al entorno público, las capacidades de protección dependerá de la criticidad que la entidad evalúe y considerando la suma total del ancho de banda a proteger.)

El SDK debe incluir un mecanismo para Android e iOS, que valide la autenticidad del dispositivo móvil y evite que se establezcan conexiones a la app a través de emuladores, aplicaciones modificadas y sistemas operativos modificados.

#### **Para la consola de gestión de la solución WAF.**

El Contratista debe implementar una consola en la nube u on-premise para una

Esta es una copia auténtica imprimible de un documento electrónico archivado por el Ministerio de Justicia y Derechos Humanos, aplicando lo dispuesto por el Art. 25 del D.S. 070-2013-PCM y la tercera Disposición Complementaria final del D.S. 026-2016-PCM. Su autenticidad e integridad pueden ser contrastadas a través de la siguiente dirección web: [https://sgd.minjus.gob.pe/gesdoc\\_web/login.jsp](https://sgd.minjus.gob.pe/gesdoc_web/login.jsp) e ingresando el Tipo de Documento, Número y Rango de Fechas de ser el caso o [https://sgd.minjus.gob.pe/gesdoc\\_web/verifica.jsp](https://sgd.minjus.gob.pe/gesdoc_web/verifica.jsp) e ingresando Tipo de Documento, Número, Remitente y Año, según corresponda."







PERÚ

Ministerio  
de Justicia  
y Derechos Humanos

Secretaría  
General

Oficina General de  
Tecnologías de  
Información

Oficina de  
Infraestructura  
y Soporte Tecnológico

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

mejor visibilidad, monitoreo y generación de reportes de la solución. Debe garantizar el almacenamiento de logs de al menos 1 mes para las aplicaciones a proteger (Aplicaciones con protección para las vulnerabilidades descritas en OWASP Top 10 y aplicaciones con capacidades de protección de WAF, Bot Manager, API Protection, Client Side Protection y mitigación DDoS.). La solución de seguridad web debe soportar integración con soluciones de SIEM o similar para envío de logs de seguridad y almacenamiento de los mismos como mínimo de 6 meses

Esta consola de gestión debe contar con un entorno web para realizar las tareas de configuración de la solución y debe soportar diferentes niveles de autorización para los usuarios administradores de la misma; además debe ser capaz de personalizar el "dashboard" por usuario de acuerdo a políticas definidas, ello significa que debe ser capaz de limitar el alcance de las configuraciones que puedan realizar distintos usuarios de acuerdo a sus roles. Se debe permitir visualizar el tiempo de latencia a nivel de red y aplicación para las aplicaciones protegidas por el WAAP. Se debe visualizar el estado de la solución WAAP, consumo de CPU, memoria, conexiones, ataques, entre otros (Siendo opcional la visualización del consumo de CPU y memoria). La consola de gestión debe incluir todo el licenciamiento necesario para una completa y eficiente gestión de la solución WAF.

#### Acuerdos de nivel de servicio (ANS).

ANS	Descripción	Cálculo de la Medición	Valor Base %	Horario Acordado	Periodicidad
Disponibilidad del servicio de protección contra ataques a las aplicaciones y servicios web	El objetivo de este ANS es medir la disponibilidad de la solución contra ataques a las aplicaciones y servicios web.	$\text{Disponibilidad} = (1 - \text{TIPM} / \text{TTSM}) * 100$	$\geq 99.9$	24x7	Mensual

Donde TIPM: Tiempo de interrupción en el mes en minutos.

TTSM: Tiempo total de servicio en el mes en minutos.

Si la disponibilidad del servicio de protección contra ataques a las aplicaciones y servicios web es menor al 99.9% en base mensual, en hasta dos (2) oportunidades durante dos (02) meses consecutivos, el Contratista debe reemplazar la solución, por otra solución de iguales o superiores características, sin costo para la Entidad y sin que esto exima las penalidades correspondientes. Para el reemplazo de la solución en nube, el Contratista tiene un plazo tres (03) días, contados a partir del día siguiente de recibida la notificación por parte del MINJUSDH.

Esta es una copia auténtica imprimible de un documento electrónico archivado por el Ministerio de Justicia y Derechos Humanos, aplicando lo dispuesto por el Art. 25 del D.S. 070-2013-PCM y la tercera Disposición Complementaria final del D.S. 026-2016-PCM. Su autenticidad e integridad pueden ser contrastadas a través de la siguiente dirección web: [https://sgd.minjus.gob.pe/gesdoc\\_web/login.jsp](https://sgd.minjus.gob.pe/gesdoc_web/login.jsp) e ingresando el Tipo de Documento, Número y Rango de Fechas de ser el caso o [https://sgd.minjus.gob.pe/gesdoc\\_web/verifica.jsp](https://sgd.minjus.gob.pe/gesdoc_web/verifica.jsp) e ingresando Tipo de Documento, Número, Remitente y Año, según corresponda."





PERÚ

Ministerio  
de Justicia  
y Derechos Humanos

Secretaría  
General

Oficina General de  
Tecnologías de  
Información

Oficina de  
Infraestructura  
y Soporte Tecnológico

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

Se precisa que para el reemplazo de la solución será previa comprobación de falla y pruebas respectivas.

### C. ETHICAL HACKING

#### Consideraciones Generales:

El servicio requerido debe proveer análisis de Ethical Hacking externos, realizados con al menos dos (2) herramientas propietarias específicas para el escaneo de aplicaciones mencionado en el cuadro N° 01.

El contratista deberá reunirse previo a cada ejecución con el equipo de seguridad de la Oficina de Infraestructura y Soporte Tecnológico (OIST) para definir los activos de información que serán analizados.

#### Consideraciones Específicas:

##### **Del servicio de Ethical Hacking externo.**

Este servicio se realizará una (01) veces por año, abarcando un total de tres (03) servicios durante los tres (3) años del contrato, previa coordinación con el equipo de seguridad de la Oficina de Infraestructura y Soporte Tecnológico (OIST), en horario que no impacte el funcionamiento de la infraestructura tecnológica del MINJUSDH. El Contratista, dentro de su Plan de Trabajo del Servicio, debe incluir las fechas tentativas para la ejecución del servicio de Ethical Hacking, considerando los siguientes puntos:

- ✓ Ataques de penetración controlados y diagnóstico sobre los aplicativos publicados e internos del MINJUSDH, detallados en el Cuadro N° 01 y la infraestructura que los soporta, dispositivos IPS, Firewalls, Router, switches CORE, Servidor de Correo, Controladores de Dominio, servidores de Colaboración, red WiFi, DNS autoritativo e interfaces de acceso externo, basados en escenarios reales de actividades de hacking hacia la Entidad, tomando como referencia el OWAS Top Ten vigente o usar otras metodologías de evaluación de seguridad.
- ✓ Se debe considerar el análisis para todas las aplicaciones mencionado en el **Cuadro N° 01** y la infraestructura que los soporta, teniendo en cuenta un crecimiento de hasta 10% durante el periodo de servicio, de acuerdo al detalle:
  - Primer año, una (01) ejecución: 35% del total.
  - Segundo año, una (01) ejecución: 35% del total.
  - Tercer año, una (01) ejecución: 30% del total.
- ✓ Con los resultados del análisis, el Contratista debe generar una matriz de riesgos.

Esta es una copia auténtica imprimible de un documento electrónico archivado por el Ministerio de Justicia y Derechos Humanos, aplicando lo dispuesto por el Art. 25 del D.S. 070-2013-PCM y la tercera Disposición Complementaria final del D.S. 026-2016-PCM. Su autenticidad e integridad pueden ser contrastadas a través de la siguiente dirección web: [https://sgd.minjus.gob.pe/gesdoc\\_web/login.jsp](https://sgd.minjus.gob.pe/gesdoc_web/login.jsp) e ingresando el Tipo de Documento, Número y Rango de Fechas de ser el caso o [https://sgd.minjus.gob.pe/gesdoc\\_web/verifica.jsp](https://sgd.minjus.gob.pe/gesdoc_web/verifica.jsp) e ingresando Tipo de Documento, Número, Remitente y Año, según corresponda."





PERÚ

Ministerio  
de Justicia  
y Derechos Humanos

Secretaría  
General

Oficina General de  
Tecnologías de  
Información

Oficina de  
Infraestructura  
y Soporte Tecnológico

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

- ✓ El contratista, posterior a la ejecución de los servicios de Ethical Hacking, tanto externo como interno, debe hacer entrega al MINJUSDH de los informes, en los plazos que se indican y por cada actividad ejecutada, considerando los siguientes entregable:
  - **Informe de diagnóstico:** Se debe presentar el detalle de los hallazgos y oportunidades de mejora identificadas en los dispositivos y Aplicativos publicados por el MINJUSDH, así como también en los aplicativos internos y dispositivos, considerando detalles del riesgo al que está expuesto el recurso afectado (matriz de riesgos), forma de explotación de cada vulnerabilidad y recomendaciones para mitigar y/o eliminar la vulnerabilidad. Este informe, de carácter confidencial y en idioma español, debe ser entregado dentro de los veinte (20) días calendario posteriores a la culminación de la actividad.
  - **Informe Ejecutivo del Ethical Hacking:** Se debe informar a alto nivel y de manera general el diagnóstico del análisis realizado, así como los puntos clave del plan para la mitigación de las vulnerabilidades encontradas en el MINJUSDH. Este informe, de carácter confidencial y en idioma español, debe ser entregado dentro de los veinte (20) días calendario posteriores a la culminación de la actividad.
  - **Plan de Acciones de Remediación:** Se debe consolidar las recomendaciones en Planes de Acción y/o Implementación de mejoras para favorecer su puesta en marcha y seguimiento, considerando los tiempos aproximados para la ejecución de las acciones de remediación. Este Plan debe ser entregado en idioma español y dentro de los treinta (30) días calendario posteriores a la culminación de la actividad del Ethical Hacking. En caso se identifique vulnerabilidades en los servicios publicados del MINJUSDH, el Contratista entregará todas las recomendaciones necesarias para gestionar las vulnerabilidades o hallazgos identificados.
- ✓ Al término de realizado el servicio de Ethical Hacking, el contratista deberá realizar talleres sobre concientización de manera presencial en la sede central del MINJUSDH a las áreas involucradas sobre los hallazgos y su impacto, previa coordinación con los especialistas de la Oficina de Infraestructura y Soporte Tecnológico (OIST) y el oficial de Seguridad de la Información del MINJUSDH. El taller deberá de considerar los siguientes elementos:
  - Informar sobre las Amenazas y/o Vulnerabilidades encontradas.
  - Impacto a la Organización
  - Solución a la Amenaza.

*Esta es una copia auténtica imprimible de un documento electrónico archivado por el Ministerio de Justicia y Derechos Humanos, aplicando lo dispuesto por el Art. 25 del D.S. 070-2013-PCM y la tercera Disposición Complementaria final del D.S. 026-2016-PCM. Su autenticidad e integridad pueden ser contrastadas a través de la siguiente dirección web: [https://sgd.minjus.gob.pe/gesdoc\\_web/login.jsp](https://sgd.minjus.gob.pe/gesdoc_web/login.jsp) e ingresando el Tipo de Documento, Número y Rango de Fechas de ser el caso o [https://sgd.minjus.gob.pe/gesdoc\\_web/verifica.jsp](https://sgd.minjus.gob.pe/gesdoc_web/verifica.jsp) e ingresando Tipo de Documento, Número, Remitente y Año, según corresponda."*







Ministerio  
de Justicia  
y Derechos Humanos

Secretaría  
General

Oficina General de  
Tecnologías de  
Información

Oficina de  
Infraestructura  
y Soporte Tecnológico

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

- Buenas prácticas.
- ✓ El Oficial de Seguridad de la Información gestionará las actividades, planes de acción y/o implementaciones de mejoras, propuestas en el Plan de Acciones de Remediación.
- ✓ El MINJUSDH cuenta con 1 chasis con 6 servidores, 3 storages con aproximadamente 18 clúster de servidores virtuales que alojan los sistemas de información que tienen como sistema operativos: Red Hat CentOS y Windows.

Cuadro N° 01

Ítem	Aplicaciones	Cantidad	Módulos por Aplicación	Tipo de Prueba	Sistema Operativo
Externos					
1	Web Publicados	82		Caja Negra	
2	Webs No publicados	2		Caja Blanca	

#### D. PROTECCIÓN ANTIDIDOS PERIMETRAL NO VOLUMETRICO

El servicio deberá brindarse a través de una solución on – premise. El contratista deberá ofrecer un (01) equipo de protección para mitigación contra ataques de denegación de servicio. El equipamiento deberá ser nuevo y de primer uso, con tecnología vigente, no deberá encontrarse en End Of Sale ni End of Life o End Support, considerando las siguientes características:

- La solución deberá brindar protección para un volumen total de tráfico de 9Gb como mínimo.
- Mínimo ocho (08) puertos 1Gb y/o 10Gb, con su respectivo Bypass interno o externo. Siendo 04 puertos para el ingreso de tráfico y 04 para la salida de tráfico.
- El equipo debe contar con 02 fuentes de poder o energía redundantes (1+1)
- Debe contar con un (01) puerto de administración RJ-45 fuera de banda.
- Soporte IPv4 e IPv6
- La ubicación de este equipo debe estar definida por el personal técnico del CONTRATISTA pudiendo ubicarse antes o después del equipamiento router.
- Compatibilidad con TLS 1.3.
- La protección contra ataques HTTPS deberá soportar la inspección y mitigación de tráfico cifrado utilizando versiones de protocolo TLS 1.2 y TLS 1.3, y de manera opcional, podrá incluir soporte para versiones

*Esta es una copia auténtica imprimible de un documento electrónico archivado por el Ministerio de Justicia y Derechos Humanos, aplicando lo dispuesto por el Art. 25 del D.S. 070-2013-PCM y la tercera Disposición Complementaria final del D.S. 026-2016-PCM. Su autenticidad e integridad pueden ser contrastadas a través de la siguiente dirección web: [https://sgd.minjus.gob.pe/gesdoc\\_web/login.jsp](https://sgd.minjus.gob.pe/gesdoc_web/login.jsp) e ingresando el Tipo de Documento, Número y Rango de Fechas de ser el caso o [https://sgd.minjus.gob.pe/gesdoc\\_web/verifica.jsp](https://sgd.minjus.gob.pe/gesdoc_web/verifica.jsp) e ingresando Tipo de Documento, Número, Remitente y Año, según corresponda."*





PERÚ

Ministerio  
de Justicia  
y Derechos Humanos

Secretaría  
General

Oficina General de  
Tecnologías de  
Información

Oficina de  
Infraestructura  
y Soporte Tecnológico

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

anteriores (SSL 3.0, TLS 1.0, TLS 1.1) si se requiere compatibilidad con sistemas legados.

- La solución propuesta deberá analizar el tráfico de bajada y los servicios y/o aplicaciones web publicadas por el MINJUSDH. Asimismo, deberá incluir la capacidad de detección de ataques de denegación de servicio a nivel de aplicación con o sin estados (stateless).
- La "capacidad de detección de ataques" también hace referencia a "capacidad de mitigación de ataques"
- La solución propuesta deberá ser instalado en la red e infraestructura del MINJUSDH, de tecnología específica para la mitigación de ataques de denegación de servicios. No se aceptarán soluciones en las que la protección DDoS sea una funcionalidad adicional de equipos Firewall, Next Generation Firewalls, Application Delivery Controllers, Routers u otros equipos de redes.
- La solución de Mitigación DDoS deberá basar su mitigación de ataques basándose principalmente en el comportamiento del tráfico entrante.
- La solución de Mitigación DDoS deberá tener un sistema de creación automática de firmas en tiempo real para la protección frente a ataques emergentes de día cero.
- La solución propuesta deberá ser de tipo Stateless.
- La solución propuesta deberá proteger frente a ataques de denegación de servicios en una arquitectura "always on" - también denominada en línea o siempre activa.
- La solución deberá ser capaz de reenviar eventos a la solución SIEM.
- Opcional: La solución deberá ser capaz de generar indicadores IOC's, los cuales deberán ser compartidos con las herramientas de seguridad perimetral como firewall, WAF.
- Además, deberá proteger de ataques volumétricos y no volumétricos de denegación de servicios principalmente de capa 3, 4 y 7:
  - Detección y mitigación de ataques HTTPS
  - Mitigación de ataques HTTPS Flood
  - Generación de baselines y aprendizaje de tráfico HTTPS.
  - La solución debe incluir un mecanismo preciso de detección de inundaciones UDP que tenga en cuenta parámetros que varíen con la tasa de tráfico y parámetros que no varíen con la tasa de tráfico, incluyendo:
    - Ancho de banda UDP.
    - Tasa de paquetes por segundo.
    - Tasa de conexiones por segundo.
- La solución de mitigación de ataques DDoS debe soportar la inspección de los encabezados internos o externos de túneles L2TP y/o GRE, GTP, IPinIP

*Esta es una copia auténtica imprimible de un documento electrónico archivado por el Ministerio de Justicia y Derechos Humanos, aplicando lo dispuesto por el Art. 25 del D.S. 070-2013-PCM y la tercera Disposición Complementaria final del D.S. 026-2016-PCM. Su autenticidad e integridad pueden ser contrastadas a través de la siguiente dirección web: [https://sgd.minjus.gob.pe/gesdoc\\_web/login.jsp](https://sgd.minjus.gob.pe/gesdoc_web/login.jsp) e ingresando el Tipo de Documento, Número y Rango de Fechas de ser el caso o [https://sgd.minjus.gob.pe/gesdoc\\_web/verifica.jsp](https://sgd.minjus.gob.pe/gesdoc_web/verifica.jsp) e ingresando Tipo de Documento, Número, Remitente y Año, según corresponda."*





PERÚ

Ministerio  
de Justicia  
y Derechos Humanos

Secretaría  
General

Oficina General de  
Tecnologías de  
Información

Oficina de  
Infraestructura  
y Soporte Tecnológico

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

- o La solución de mitigación de ataques DDoS debe tener una latencia menor a 60 microsegundos.
- o Se precisa que, para acreditar las características técnicas del equipamiento o solución de la Protección AntiDDOS perimetral no volumétrico, el Contratista deberá sustentarlo en el **ANEXO de Características Técnicas**. Asimismo, el contratista podrá adjuntar carta de fabricante para complementar las demás características técnicas requeridas en los TDR a excepción de las requeridas en el **ANEXO de Características Técnicas**.

#### E. SERVICIO DE PROTECCIÓN DE CORREO ELECTRONICO (ANTISPAM)

El servicio requerido debe proveer una protección de correo electrónico (Antispam) para proteger 5000 buzones cuenta de correos electrónicos, el cuál debe integrarse a plataformas de correo electrónico on premise Exchange, Zimbra o plataforma de correo en nube (Google WorkSpace o Office 365).

El soporte técnico que el Contratista contrate al fabricante de la solución Antispam debe ser un nivel de soporte que incluya la atención 24x7 durante el periodo de servicio.

El servicio debe proveerse como SaaS o en nube.

La solución debe tener la capacidad de analizar el correo entrante y saliente hacia los servicios de Google WorkSpace u Office 365 tanto de manera en línea como a través de API, de manera que pueda ser aplicado el control de antispam y/o antivirus y detectar dichas amenazas.

A fin de evitar complejidad en la arquitectura y garantizar una solución de administración óptima, la solución no debe requerir desplegar en la red del Ministerio de Justicia y Derechos Humanos ningún elemento adicional para la administración y monitoreo que requieran aprovisionamiento de software, ya sea, por ejemplo: bases de datos, software sobre servidores u otro parecido.

Debe detectar y bloquear el spam, phishing y APTs en los mensajes de correos electrónicos entrantes que introducen ransomware y otras amenazas avanzadas, actualizándose permanentemente.

Debe incluir el filtrado de contenido para el control de datos salientes y el cifrado de correo electrónico mediante cifrado de canal de comunicación tanto entrante como saliente.

Debe permitir colocar un disclaimer personalizada para los correos entrantes.  
Debe incluir la capacidad de cifrar el correo encapsulando el contenido, no solo a nivel de la transferencia (conexión).

Debe contar con la capacidad de realizar DLP del correo entrante y saliente para

*Esta es una copia auténtica imprimible de un documento electrónico archivado por el Ministerio de Justicia y Derechos Humanos, aplicando lo dispuesto por el Art. 25 del D.S. 070-2013-PCM y la tercera Disposición Complementaria final del D.S. 026-2016-PCM. Su autenticidad e integridad pueden ser contrastadas a través de la siguiente dirección web: [https://sgd.minjus.gob.pe/gesdoc\\_web/login.jsp](https://sgd.minjus.gob.pe/gesdoc_web/login.jsp) e ingresando el Tipo de Documento, Número y Rango de Fechas de ser el caso o [https://sgd.minjus.gob.pe/gesdoc\\_web/verifica.jsp](https://sgd.minjus.gob.pe/gesdoc_web/verifica.jsp) e ingresando Tipo de Documento, Número, Remitente y Año, según corresponda."*





PERÚ

Ministerio  
de Justicia  
y Derechos Humanos

Secretaría  
General

Oficina General de  
Tecnologías de  
Información

Oficina de  
Infraestructura  
y Soporte Tecnológico

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

evitar la fuga de información.

La solución debe proteger todo el correo electrónico entrante y saliente al dominio incluso antes de que sea entregado en la bandeja del usuario final, de manera que se pueda proteger al usuarios final que accede incluso desde dispositivos móviles.

Debe contar con una base de firmas actualizadas periódicamente con las nuevas amenazas para el bloqueo de correos maliciosos, esta base de firmas deberá ser del propio fabricante, no se permitirá firmas de terceros.

#### Distribución e Instalación

Bastará con configurar los registros de intercambio de correo (MX).

La solución debe ser capaz de integrarse con cualquier plataforma de Mensajería vía SMTP como, por ejemplo, Microsoft Exchange y/o Zimbra.

Deberá poder analizar el tráfico entrante y saliente SMTP a través de la misma plataforma.

Los componentes de Reportes y consola deben estar en la misma plataforma.

#### Características Generales

- Tener la capacidad de generar políticas al tráfico entrante y al tráfico saliente, de forma independiente. Todas las características solicitadas a continuación se deberán contemplar para el tráfico entrante como saliente.
- La herramienta debe contar con reportes a los usuarios finales que permitan tomar acciones como liberar o notificar spam, vía correo electrónico o bien a través de un portal de usuario. Deberá configurarse para un grupo de usuarios o para toda la entidad.
- Contar con múltiples opciones de respuesta:
  - Descartar o eliminar el mensaje
  - Reenviar Mensaje a un recipiente especificado
  - Guardar el Mensaje en una Cuarentena
  - Enviar Notificación
- Tener la flexibilidad de establecer distintas configuraciones de seguridad de correo electrónico, como políticas, a usuarios y grupos basados en sus direcciones de correo y dominios.
- Debe crear una cuarentena personal por usuario o buzón de correo.
- Debe crear una cuarentena a nivel global o por todo el sistema.
- Incluir un grupo de funciones mínimas que permitan:
  - Agregar funciones de análisis de Antivirus
  - Agregar funciones para prevenir los ataques de Spear-phishing and Whale Phishing.
  - Agregar funciones de análisis de URL embebidas en el correo
  - Agregar funciones de análisis de archivos maliciosos embebidas en el correo.
  - Agregar funciones de AntiSpam
  - Agregar funciones para prevenir suplantación de identidad.
  - Agregar funciones para prevenir ataques de Compromiso de correo electrónico comercial.
  - Agregar funciones de Disclaimer

*Esta es una copia auténtica imprimible de un documento electrónico archivado por el Ministerio de Justicia y Derechos Humanos, aplicando lo dispuesto por el Art. 25 del D.S. 070-2013-PCM y la tercera Disposición Complementaria final del D.S. 026-2016-PCM. Su autenticidad e integridad pueden ser contrastadas a través de la siguiente dirección web: [https://sgd.minjus.gob.pe/gesdoc\\_web/login.jsp](https://sgd.minjus.gob.pe/gesdoc_web/login.jsp) e ingresando el Tipo de Documento, Número y Rango de Fechas de ser el caso o [https://sgd.minjus.gob.pe/gesdoc\\_web/verifica.jsp](https://sgd.minjus.gob.pe/gesdoc_web/verifica.jsp) e ingresando Tipo de Documento, Número, Remitente y Año, según corresponda."*





PERÚ

Ministerio  
de Justicia  
y Derechos Humanos

Secretaría  
General

Oficina General de  
Tecnologías de  
Información

Oficina de  
Infraestructura  
y Soporte Tecnológico

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

- Poseer técnicas de filtrado de spam, basados en firmas de spam, filtrado de URL, combinación de patrones utilizados en el spam y heurístico.
- Debe identificar ataques de tipo BEC a través de un análisis automático y dinámico para identificar cuáles son las personas más atacadas de la organización.
- Debe soportar SPF, DMARC y DKIM tanto para la validación de la entrada de correos como para la salida a través de llaves de infraestructura pública o certificados digitales.
- Deberá soportar SPF (Sender Policy Framework)
- Contar con reglas de filtrado por:
  - Dirección IP del correo
  - Casilla de quién envía
  - Casilla de recipiente
  - Cantidad de Recipientes
  - Campo From:
  - Campo To:
  - Campo Subject:
  - Cabecera del Correo
  - Texto en el cuerpo
  - Tamaño del Mensaje
  - Resultado de la validación DKIM
  - Bloqueo de Archivos

#### Seguridad

- Debe proveer una solución antimalware
- Debe permitir el bloqueo de archivos por nombre, por extensión y por tipo, al usuario de destino.
- Debe tener la capacidad de integrarse con el directorio activo de la entidad on premise para validar la existencia de los correos destinatarios de la entidad antes de que ingresen a cada buzón.
- Debe mostrar en un dashboard si la entidad está bajo un ataque de masivo a través del envío de malware para distintos buzones de la entidad, con la finalidad de identificar rápidamente una campaña y priorizar la respuesta ante un posible incidente.
- Debe incluir la capacidad de bloquear comunicaciones en base al puntaje de host o usuario, obtenido de evaluar la reputación de los dispositivos finales o usuarios finales.
- Deberá tener la capacidad de analizar archivos adjuntos comprimidos infectados y tomar acciones correspondientes.
- Debe tener la capacidad de desarmar el correo electrónico o desinfección de archivos.
- El motor de seguridad de esta solución deberá descomprimir los archivos adjuntos sin necesidad de recurrir a programas externos, sin alterar el cuerpo del mensaje.
- Deberá revisar categorías como drogas, URL con problemas de seguridad, Hacking, entre otras.

*Esta es una copia auténtica imprimible de un documento electrónico archivado por el Ministerio de Justicia y Derechos Humanos, aplicando lo dispuesto por el Art. 25 del D.S. 070-2013-PCM y la tercera Disposición Complementaria final del D.S. 026-2016-PCM. Su autenticidad e integridad pueden ser contrastadas a través de la siguiente dirección web: [https://sgd.minjus.gob.pe/gesdoc\\_web/login.jsp](https://sgd.minjus.gob.pe/gesdoc_web/login.jsp) e ingresando el Tipo de Documento, Número y Rango de Fechas de ser el caso o [https://sgd.minjus.gob.pe/gesdoc\\_web/verifica.jsp](https://sgd.minjus.gob.pe/gesdoc_web/verifica.jsp) e ingresando Tipo de Documento, Número, Remitente y Año, según corresponda."*





PERÚ

Ministerio  
de Justicia  
y Derechos Humanos

Secretaría  
General

Oficina General de  
Tecnologías de  
Información

Oficina de  
Infraestructura  
y Soporte Tecnológico

“Decenio de la igualdad de oportunidades para mujeres y hombres”  
“Año de la recuperación y consolidación de la economía peruana”

- La base de datos deberá ser propietaria del fabricante de la solución. No se aceptarán soluciones de filtrado que no sean del propio fabricante. Debe presentar documentación oficial del fabricante en donde se listen las categorías ofertadas y deberá poder reemplazar las URL comprometidas con un texto en particular

#### Servicios de Sandboxing

- Permite la protección de las URL embebidas en los correos electrónicos al momento de que el usuario realice un click sobre la URL. Esto permitirá que el servicio analice las URL de los mensajes en caso de riesgos de seguridad y cada vez que el usuario haga click en la URL se ejecute un procedimiento de análisis en tiempo real de la URL ejecutada. El producto podrá dar un veredicto si es seguro ir a la URL o no mostrando un mensaje de bloqueo o advertencia al usuario final fuera o dentro de la organización sin necesidad de utilizar productos adicionales de análisis de URL. Se aceptarán elementos adicionales para cumplir el requerimiento.
- El producto debe contar con un servicio de sandboxing de archivos que permitirá analizar los siguientes archivos:
  - exe
  - pdf
  - dll
  - Microsoft Office: .docx, .xlsx, .pptx
  - .rar, .zip
  - Microsoft Office: Word, Excel, PowerPoint, entre otros
  - Adobe: PDF, SWF y Flash.
  - Archivos web como HTML.
- El servicio brindará un veredicto de la posible amenaza y retendrá el correo que contiene el archivo sospechoso a la espera del veredicto de la caja de arena (Sandbox).
- El servicio de caja de arena o sandbox deberá ser una solución cloud y no requerirá instalación adicional de servicios.

#### Uso de Mecanismos de TLS

- Deberá permitir la conexión de sesiones TLS
- Deberá permitir verificar la versión de TLS, mínimo 1.2 y/o 1.3.
- Deberá permitir forzar conexiones TLS tanto entrantes como salientes
- Los perfiles TLS le permiten deshabilitar o habilitar TLS de forma selectiva para patrones de destinatarios de correo electrónico específicos, subredes de IP, entre otros.
- Los perfiles TLS deberán hacer cumplir el transporte TLS a un dominio específico y verificar el certificado de los servidores receptores.
- Deberá establecer un orden de prioridad especificando un nivel de seguridad para determinada conexión en la cual debe verificar y validar que el certificado es de una certificación de confianza válida.

#### Gestión y Reporte

*Esta es una copia auténtica imprimible de un documento electrónico archivado por el Ministerio de Justicia y Derechos Humanos, aplicando lo dispuesto por el Art. 25 del D.S. 070-2013-PCM y la tercera Disposición Complementaria final del D.S. 026-2016-PCM. Su autenticidad e integridad pueden ser contrastadas a través de la siguiente dirección web: [https://sgd.minjus.gob.pe/gesdoc\\_web/login.jsp](https://sgd.minjus.gob.pe/gesdoc_web/login.jsp) e ingresando el Tipo de Documento, Número y Rango de Fechas de ser el caso o [https://sgd.minjus.gob.pe/gesdoc\\_web/verifica.jsp](https://sgd.minjus.gob.pe/gesdoc_web/verifica.jsp) e ingresando Tipo de Documento, Número, Remitente y Año, según corresponda.”*





PERÚ

Ministerio  
de Justicia  
y Derechos Humanos

Secretaría  
General

Oficina General de  
Tecnologías de  
Información

Oficina de  
Infraestructura  
y Soporte Tecnológico

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

- Los Especialista de la Oficina de Infraestructura y Soporte Tecnológico pueden administrar y revisar varios widgets que muestran resúmenes y el estado actual.
- Debe incluir reportes o selecciones predefinidas dentro de la solución, incluyendo mínimamente:
  - Resúmenes del tamaño de archivo de correo electrónico en la cual se detecta virus o spam.
  - Resúmenes de la cantidad de mensajes de correo electrónico en la cual se detecta virus o spam.
  - Resúmenes de la cantidad de tiempo que se retrasaron las notificaciones.
  - Resúmenes del número de notificaciones recibidas.
  - Resumen de correo no deseado y virus.
  - Principales destinatarios y remitentes de correo electrónico, principales virus y principales spams.
  - Número de mensajes de correo electrónico.
  - Tamaño de los mensajes de correo electrónico.
  - Velocidad de escaneo de los mensajes de correo electrónico.
  - Velocidad de transferencia de mensajes de correo electrónico.
  - Entre otros contenidos del análisis realizada por la unidad.
- Debe permitir modificar el período de tiempo variables incluidos minutos, horas, días, meses y años.
- Debe permitir la programación de informes o emisión de informes con determinada frecuencia en diversos formatos PDF o HTML y/o XML y/o CSV.

Debe tener la opción de enviar datos por syslog para que los use una solución de seguridad de información y eventos de terceros (SIEM).

#### F. SERVICIO DE UN CENTRO DE OPERACIONES DE CIBERSEGURIDAD (CYBERSOC).

##### Consideraciones Generales:

El Centro de Operaciones de Ciberseguridad (CyberSOC), deberá ser propio del contratista para brindar una atención al MINJUSDH de 24x7x365 durante el periodo de contrato. El Contratista debe proveer el enlace de comunicaciones adecuado en caso se requiera, entre la Sede Central del MINJUSDH y sus instalaciones para la provisión de este servicio (se aceptará el tipo de conexión a través de una VPN con los equipos de seguridad Firewalls perimetrales de acceso a Internet a implementar en el Componente A).

##### Gestión de las soluciones implementadas para brindar el servicio.

El contratista debe asegurar y garantizar que el CiberSoc atenderá los requerimientos operativos e incidentes, reportados por el MINJUSDH, con el personal requerido para la prestación del servicio, en el horario de 24x7x365, considerando los acuerdos de niveles de servicios establecidos para cada nivel de criticidad.

Esta es una copia auténtica imprimible de un documento electrónico archivado por el Ministerio de Justicia y Derechos Humanos, aplicando lo dispuesto por el Art. 25 del D.S. 070-2013-PCM y la tercera Disposición Complementaria final del D.S. 026-2016-PCM. Su autenticidad e integridad pueden ser contrastadas a través de la siguiente dirección web: [https://sgd.minjus.gob.pe/gesdoc\\_web/login.jsp](https://sgd.minjus.gob.pe/gesdoc_web/login.jsp) e ingresando el Tipo de Documento, Número y Rango de Fechas de ser el caso o [https://sgd.minjus.gob.pe/gesdoc\\_web/verifica.jsp](https://sgd.minjus.gob.pe/gesdoc_web/verifica.jsp) e ingresando Tipo de Documento, Número, Remitente y Año, según corresponda."







PERÚ

Ministerio  
de Justicia  
y Derechos Humanos

Secretaría  
General

Oficina General de  
Tecnologías de  
Información

Oficina de  
Infraestructura  
y Soporte Tecnológico

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

El contratista deberá contar con estándares internacionales como la certificación vigente de la ISO 27001 como mínimo, la misma que deberá ser entregada para la etapa de presentación de ofertas.

Todos los servicios de seguridad requeridos y descritos en los presentes términos de referencia, serán gestionados desde el CyberSOC, a través de personal exclusivo para el MINJUSDH: un (01) analista para las atenciones en horario laboral de 8:00am a 5:00pm para cubrir las atenciones de NIVEL 2 (Actividades operativas relacionadas a la gestión de las soluciones y la atención especializada de eventos/incidencias), y de NIVEL 3 (Resolución definitiva a un evento/incidencia y/o soporte técnico escalado por NIVEL 2) que el Contratista considere necesario para la provisión del servicio. Considerando que fuera del horario indicado, las atenciones serán efectuadas y/o realizadas por el personal de turno del CyberSOC.

El término "exclusivo para el MINJUSDH" hace referencia a un personal dedicado en las oficinas del MINJUS para atender todas las incidencias y/o requerimientos que tenga la entidad con un menor tiempo de respuesta., en caso el personal se encuentre con pendientes, el CyberSoc deberá entrar en apoyo de manera remota ante los requerimientos e incidencias de la entidad.

Es de indicar, que la gestión de las soluciones que se implementen en el MINJUSDH será compartida con el equipo de la Oficina de Infraestructura y Soporte Tecnológico (OIST) del MINJUSDH. El personal de NIVEL 2, en las instalaciones del CyberSOC, debe cumplir con los requisitos definidos en el numeral 5.6. Requerimientos del proveedor y de su personal. Es de indicar, que el personal del CyberSOC dedicado a las atenciones del MINJUSDH, en su conjunto, deben contar con las capacitaciones de todas las soluciones implementadas: AntiDDoS, Firewalls de siguiente generación o Acceso Remoto VPN o Sandboxing y Firewall de Aplicaciones Web. El Contratista debe acreditar mediante documentos y/o certificados oficiales lo requerido para la conformidad de la implementación e inicio del servicio.

Los servicios especializados del CyberSOC (NIVEL 2 y NIVEL 3) deben estar basados en al menos cuatro pilares fundamentales:

#### 1. Prevención

Disminuir la probabilidad de aparición de cualquier incidente. La prevención implica realizar vigilancia permanente de nuevos ataques que puedan comprometer la seguridad, así como la aplicación de medidas preventivas que reduzcan la probabilidad de materialización de amenazas.

#### 2. Detección.

*Esta es una copia auténtica imprimible de un documento electrónico archivado por el Ministerio de Justicia y Derechos Humanos, aplicando lo dispuesto por el Art. 25 del D.S. 070-2013-PCM y la tercera Disposición Complementaria final del D.S. 026-2016-PCM. Su autenticidad e integridad pueden ser contrastadas a través de la siguiente dirección web: [https://sgd.minjus.gob.pe/gesdoc\\_web/login.jsp](https://sgd.minjus.gob.pe/gesdoc_web/login.jsp) e ingresando el Tipo de Documento, Número y Rango de Fechas de ser el caso o [https://sgd.minjus.gob.pe/gesdoc\\_web/verifica.jsp](https://sgd.minjus.gob.pe/gesdoc_web/verifica.jsp) e ingresando Tipo de Documento, Número, Remitente y Año, según corresponda."*





PERÚ

Ministerio  
de Justicia  
y Derechos Humanos

Secretaría  
General

Oficina General de  
Tecnologías de  
Información

Oficina de  
Infraestructura  
y Soporte Tecnológico

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

Monitoreo constante con el único propósito de detectar amenazas, vulnerabilidades, intrusiones, ataques de seguridad, o cualquier indicio que refleje un posible incidente de seguridad.

### 3. Análisis

Estudio de los incidentes descubiertos por la detección. Con el análisis se pretende discernir entre amenazas reales o falsos positivos.

### 4. Respuesta

Reacción ante cualquier incidente real de seguridad. Sus funciones principales son:

- Monitorización continua de la seguridad.
- Detección y gestión de vulnerabilidades.
- Centralización, tratamiento y custodia de logs.
- Respuesta de resolución.
- Asesoría de seguridad.
- Programas de prevención

El CyberSOC debe contar con una Mesa de Ayuda o Mesa de Servicios para asignación de tickets de atención exclusiva al MINJUSDH. El ticket generado debe ser enviado automáticamente vía correo electrónico al personal del MINJUSDH para su seguimiento y control. Las asignaciones de tickets por las solicitudes o incidentes reportadas por el MINJUSDH, no deben exceder de los 15 minutos, las resoluciones de las solicitudes y/o incidentes críticos o altos no deben exceder de las 2 horas, las resoluciones de solicitudes y/o incidentes medios o moderados no deben exceder de las 4 horas y las resoluciones para las solicitudes y/o incidentes bajos no deben exceder de las 8 horas.

#### Niveles de criticidad.

- **Crítico:** Impacto grave, muy alto o catastrófico al servicio, ocasionando pérdida de imagen Institucional y/o ocasionando graves pérdidas económicas.
- **Moderado:** Impacto leve, medio o moderado al servicio, ocasionando incumplimiento de ANSs y/o pérdidas económicas importantes y moderadas.
- **Bajo:** Impacto bajo o muy bajo al servicio, ocasionando pérdidas económicas bajas.

Nivel de soporte	Tipo de Asistencia	Tiempo máximo de resolución
Crítico o alto	In site o Asistencia remota	2 horas
Medio o Moderado	In site o Asistencia remota	4 horas
Bajo	Asistencia Remota	8 horas

*Esta es una copia auténtica imprimible de un documento electrónico archivado por el Ministerio de Justicia y Derechos Humanos, aplicando lo dispuesto por el Art. 25 del D.S. 070-2013-PCM y la tercera Disposición Complementaria final del D.S. 026-2016-PCM. Su autenticidad e integridad pueden ser contrastadas a través de la siguiente dirección web: [https://sgd.minjus.gob.pe/gesdoc\\_web/login.jsp](https://sgd.minjus.gob.pe/gesdoc_web/login.jsp) e ingresando el Tipo de Documento, Número y Rango de Fechas de ser el caso o [https://sgd.minjus.gob.pe/gesdoc\\_web/verifica.jsp](https://sgd.minjus.gob.pe/gesdoc_web/verifica.jsp) e ingresando Tipo de Documento, Número, Remitente y Año, según corresponda."*





PERÚ

Ministerio  
de Justicia  
y Derechos Humanos

Secretaría  
General

Oficina General de  
Tecnologías de  
Información

Oficina de  
Infraestructura  
y Soporte Tecnológico

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

El Contratista debe brindar una plataforma de colaboración (herramienta licenciada para sesiones remotas, para diez (10) usuarios) para la comunicación exclusiva entre personal de la Oficina de Infraestructura y Soporte Tecnológico (OIST) y el personal del CyberSOC, con el objetivo de mantener una comunicación continua, fluida y eficiente. Además, debe proveer las herramientas necesarias para que personal de la Oficina de Infraestructura y Soporte Tecnológico (OIST) monitoreen la disponibilidad de todas las soluciones de seguridad a implementar para la provisión del servicio.

El contratista debe generar y mantener actualizada toda la documentación necesaria relacionada con los servicios implementados: Esquemas, topologías, layouts, control de cambios, procedimientos, guías operativas, manuales, reportes, informes, entre otros; la cual estará siempre disponible para el personal de la Oficina de Infraestructura y Soporte Tecnológico (OIST) del MINJUSDH, en formato PDF y en sus formatos originales.

Asimismo, de requerir algún licenciamiento para visualizar la documentación actualizada relacionada con los servicios implementados, será brindado por el contratista sin generar costo adicional para la entidad.

La Oficina de Infraestructura y Soporte Tecnológico (OIST) del MINJUSDH, se reserva el derecho de solicitar algún cambio en el personal del Contratista, cuando se evidencie la falta de experticia y/o conocimientos o cuando incumpla con las políticas de seguridad de la información del MINJUSDH. Para estos casos, se notificará al Contratista y se le dará un plazo máximo de treinta (30) días calendario para que ejecute el cambio correspondiente sin que ello signifique un costo adicional para la Entidad. El personal de cambio debe cumplir con los requisitos definidos en estos términos de referencia y debe iniciar sus labores al día siguiente de haber dejado de laborar su predecesor.

#### **Consideraciones Específicas:**

##### ***De las responsabilidades del personal de NIVEL 2 del CyberSOC.***

**Profesionales asignados al proyecto:** Gestión, tuning y operación de todas las soluciones a implementar en las instalaciones del MINJUSDH para brindar el servicio solicitado:

- ✓ Seguridad perimetral.
  - Seguridad perimetral con tecnologías de Firewalls de siguiente generación,
  - Acceso remoto por Virtual Private Network (VPN.),
  - Protección con tecnología sandboxing.
- ✓ Protección contra ataques a las aplicaciones y servicios web.

Esta es una copia auténtica imprimible de un documento electrónico archivado por el Ministerio de Justicia y Derechos Humanos, aplicando lo dispuesto por el Art. 25 del D.S. 070-2013-PCM y la tercera Disposición Complementaria final del D.S. 026-2016-PCM. Su autenticidad e integridad pueden ser contrastadas a través de la siguiente dirección web: [https://sgd.minjus.gob.pe/gesdoc\\_web/login.jsp](https://sgd.minjus.gob.pe/gesdoc_web/login.jsp) e ingresando el Tipo de Documento, Número y Rango de Fechas de ser el caso o [https://sgd.minjus.gob.pe/gesdoc\\_web/verifica.jsp](https://sgd.minjus.gob.pe/gesdoc_web/verifica.jsp) e ingresando Tipo de Documento, Número, Remitente y Año, según corresponda."



PERÚ

Ministerio  
de Justicia  
y Derechos Humanos

Secretaría  
General

Oficina General de  
Tecnologías de  
Información

Oficina de  
Infraestructura  
y Soporte Tecnológico

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

- ✓ Monitoreo Proactivo de Eventos de Seguridad
- ✓ Correlación Extendida para la Detección y Respuesta a Incidentes
- ✓ Detección y Desactivación de Amenazas Digitales Externas
- ✓ Protección de correo electrónico
- ✓ Ethical Hacking

#### **De los servicios especializados requeridos del CyberSOC.**

El CyberSOC debe brindar información de eventos e incidentes de seguridad, a través de consolas de visualización unificadas o consolas individuales de cada solución, que seguidos por los lineamientos especificados en el procedimiento de respuestas a incidentes faciliten la toma de decisiones a fin de mitigar los riesgos que pueden afectar notoriamente a los activos informáticos del MINJUSDH. Esas consolas deben estar disponibles a través de interfaces web, para visualización de indicadores de compromiso, indicadores de ataque, indicadores de gestión de incidentes, entre otros, por parte de la Oficina de Infraestructura y Soporte Tecnológico (OIST) del MINJUSDH.

El CyberSOC debe poder recopilar eventos relevantes para la gestión de seguridad del MINJUSDH, asimismo también debe realizar la recolección de logs de Active Directory.

La consola de eventos e incidentes deberá permitir exportar los resultados de la búsqueda en archivo CSV y .PDF como mínimo.

La consola de eventos e incidentes deberá soportar como mínimo el envío de alertas en formato Syslog.

La consola debe poder recopilar logs de fuentes terceras a través de SYSLOG como mínimo.

El CyberSOC debe realizar labores orientadas al monitoreo, aseguramiento y defensa de los activos informáticos del MINJUSDH durante las 24 horas del día y los 7 días de la semana (24x7x365).

El Contratista será responsable de elaborar, definir políticas y procedimientos de comunicación para todo el personal del CyberSOC exclusivo para el MINJUSDH, como son:

- Políticas específicas para informar al responsable del CyberSOC / CISO
- Políticas específicas para asignar el incidente
- Políticas específicas para solicitar acciones de contención
- Políticas específicas para atender el incidente
- Políticas específicas para recuperar los servicios
- Políticas específicas para coordinar seguimiento del incidente
- Políticas específicas para documentar el incidente
- Políticas específicas para evaluar la atención del incidente
- Políticas específicas para reasignar el incidente
- Políticas específicas para cerrar el incidente

Esta es una copia auténtica imprimible de un documento electrónico archivado por el Ministerio de Justicia y Derechos Humanos, aplicando lo dispuesto por el Art. 25 del D.S. 070-2013-PCM y la tercera Disposición Complementaria final del D.S. 026-2016-PCM. Su autenticidad e integridad pueden ser contrastadas a través de la siguiente dirección web: [https://sgd.minjus.gob.pe/gesdoc\\_web/login.jsp](https://sgd.minjus.gob.pe/gesdoc_web/login.jsp) e ingresando el Tipo de Documento, Número y Rango de Fechas de ser el caso o [https://sgd.minjus.gob.pe/gesdoc\\_web/verifica.jsp](https://sgd.minjus.gob.pe/gesdoc_web/verifica.jsp) e ingresando Tipo de Documento, Número, Remitente y Año, según corresponda."







PERÚ

Ministerio  
de Justicia  
y Derechos Humanos

Secretaría  
General

Oficina General de  
Tecnologías de  
Información

Oficina de  
Infraestructura  
y Soporte Tecnológico

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

Las políticas del CyberSOC pueden alinearse con los servicios del CSIRT bajo los estándares de FIRST.

Estas políticas serán entregadas al MINJUSDH con el Plan de Trabajo del servicio y para su desarrollo deben tener en cuenta marcos de referencia como NIST y/o COBIT y/o NTP ISO 27001, ITIL, NTP ISO 31001 y las Directivas internas en TI del MINJUSDH.

Con el objetivo de establecer una adecuada gestión de incidentes desde el CyberSOC, se deben tener indicadores de rendimiento, basados en métricas y metas. Dichos indicadores deben considerar,

En el caso de métricas:

- Cantidad de Incidentes repetidos x Herramienta y/o servicio
- Cantidad de incidentes registrados
- Cantidad de incidentes escalados
- Tiempo de atención de incidentes
- Tiempo medio para cerrar un incidente

En el caso de metas:

- Porcentaje de incidentes registrados en el mes.
- Cantidad de incidentes registrados versus los solucionados durante el mes.
- Tiempo de duración para resolver un incidente
- Tiempo de duración para cerrar un incidente.

Se deben registrar estadísticas asociadas a:

- Intentos de escaneo y ataques repelidos
- Malware identificado y controlado
- Comportamiento de las soluciones especializadas (soluciones implementadas por el CyberSoc).
- Tiempo de inactividad atribuible a incidentes de seguridad
- Tiempo para detectar, analizar y escalar incidentes.

El término "Comportamiento de soluciones especializadas" hace referencia a la capacidad del servicio de CyberSOC a implementar e integrar de manera eficiente las nuevas tecnologías adquiridas, tales como: firewall, XDR, WAF, anti-DDoS, antispam.

*Esta es una copia auténtica imprimible de un documento electrónico archivado por el Ministerio de Justicia y Derechos Humanos, aplicando lo dispuesto por el Art. 25 del D.S. 070-2013-PCM y la tercera Disposición Complementaria final del D.S. 026-2016-PCM. Su autenticidad e integridad pueden ser contrastadas a través de la siguiente dirección web: [https://sgd.minjus.gob.pe/gesdoc\\_web/login.jsp](https://sgd.minjus.gob.pe/gesdoc_web/login.jsp) e ingresando el Tipo de Documento, Número y Rango de Fechas de ser el caso o [https://sgd.minjus.gob.pe/gesdoc\\_web/verifica.jsp](https://sgd.minjus.gob.pe/gesdoc_web/verifica.jsp) e ingresando Tipo de Documento, Número, Remitente y Año, según corresponda."*





PERÚ

Ministerio  
de Justicia  
y Derechos Humanos

Secretaría  
General

Oficina General de  
Tecnologías de  
Información

Oficina de  
Infraestructura  
y Soporte Tecnológico

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

El comportamiento se evaluará en función del desempeño operativo de dichas soluciones, su interoperabilidad, y la efectividad en la detección de amenazas, gestión y respuesta frente a incidentes de seguridad.

El contratista informará los registros estadísticos mencionados en el informe mensual de la prestación del servicio.

El CyberSOC debe proveer también para el MINJUSDH los siguientes servicios especializados y personalizados:

- **Respuesta a Incidentes de ciberseguridad:** Manejo de ciber crisis, respuesta a incidentes cibernéticos, resiliencia y recuperación de TI, notificación de incumplimiento y respuesta. Implementación de respuestas automatizadas vía solución

La Oficina de Infraestructura y Soporte Tecnológico (OIST) del MINJUSDH, se reserva el derecho de realizar visitas inopinadas a las instalaciones del CyberSOC del contratista para verificar la ejecución de los servicios implementados.

La solución debe incorporar equipamiento para visualización de Dashboards que incluya tres (03) monitores de 55 " (Matriz 3x1), accesorios de sujeción y el software, de ser necesario, para la distribución de paneles de monitoreo para las diferentes consolas de la solución ofertada. Asimismo, debe permitir definir dashboards de monitoreo personalizados. Dicho conjunto de visualización de Dashboards debe ser implementados en las Oficinas de la Sede Central del Ministerio de Justicia y Derechos Humanos, en un ambiente determinado por la Oficina de Infraestructura y Soporte Tecnológico y dentro de lo estipulado en el numeral 5.7 LUGAR Y PLAZO DE PRESTACIÓN DEL SERVICIO del presente documento, sección Plazo de Implementación.

#### 5.1 ACTIVIDADES.

1. Reunión de KickOff, a los dos (2) días calendario de firmado el contrato. El contratista presentará a su personal responsable por cada uno de los proyectos a implementar.
2. Visitas técnicas del contratista a las instalaciones del MINJUSDH, Centro de Datos del MINJUSDH. El cronograma de visitas será definido en la reunión de KickOff.
3. Reuniones con el Contratista para tratar los temas de diseño de las topologías de las soluciones a implementar para la provisión del servicio. El cronograma de reuniones será definido en la reunión de KickOff.
4. El plazo de entrega del Plan de Trabajo del servicio, es de hasta veinte (20) días calendario contados a partir del día siguiente de firmado el contrato.

*Esta es una copia auténtica imprimible de un documento electrónico archivado por el Ministerio de Justicia y Derechos Humanos, aplicando lo dispuesto por el Art. 25 del D.S. 070-2013-PCM y la tercera Disposición Complementaria final del D.S. 026-2016-PCM. Su autenticidad e integridad pueden ser contrastadas a través de la siguiente dirección web: [https://sgd.minjus.gob.pe/gesdoc\\_web/login.jsp](https://sgd.minjus.gob.pe/gesdoc_web/login.jsp) e ingresando el Tipo de Documento, Número y Rango de Fechas de ser el caso o [https://sgd.minjus.gob.pe/gesdoc\\_web/verifica.jsp](https://sgd.minjus.gob.pe/gesdoc_web/verifica.jsp) e ingresando Tipo de Documento, Número, Remitente y Año, según corresponda."*



PERÚ

Ministerio  
de Justicia  
y Derechos Humanos

Secretaría  
General

Oficina General de  
Tecnologías de  
Información

Oficina de  
Infraestructura  
y Soporte Tecnológico

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

5. Aprobación del Plan de Trabajo del Servicio por parte de la Oficina de Infraestructura y Soporte Tecnológico (OIST) del MINJUSDH, dentro de los siete (7) días de recibido el plan de trabajo.
6. Reuniones con el Contratista para tratar temas de la implementación de cada una de las soluciones ofertadas para brindar el servicio.
7. Reuniones periódicas con el Jefe de proyecto para el seguimiento de la implementación de cada uno de los componentes del servicio. El cronograma será definido en la reunión de KickOff.
8. Protocolo de pruebas para cada uno de los componentes del servicio.
9. Presentación del personal del CyberSOC de atención exclusiva para el MINJUSDH.
10. Visita del personal de la Oficina de Infraestructura y Soporte Tecnológico (OIST) a las instalaciones del CyberSOC.
11. Conformidad de la Implementación del servicio.
12. Inicio del servicio.

## 5.2 PLAN DE TRABAJO DEL SERVICIO

### 5.2.1 Planteamiento del Proyecto

Dentro de los veinte (20) días calendarios contados a partir del día siguiente de firmado el contrato de no cumplir con dicho plazo se aplicará al contratista la penalidad mencionada en el numeral 5.13. de los Términos de Referencia, el Contratista debe entregar un Plan de Trabajo del Servicio, el cual debe contener el detalle de las actividades de implementación, instalación, configuración y puesta en operación de cada una de las soluciones que componen la prestación del servicio; además, debe incluir como mínimo los siguientes rubros:

- a. Planeamiento de Red y Seguridad: Descripción de la arquitectura/topología, descripción de actividades, análisis y diseño, detallando las soluciones que implementará el Contratista.
- b. Aprovisionamiento de Equipos: Descripción del listado general de equipos que se instalarán para el servicio.
- c. Trabajos de Montaje e Instalación: Descripción del montaje y configuración de los equipos.
- d. Pruebas de Aceptación y puesta en Servicio: Descripción del Protocolo de Pruebas para la aceptación y monitoreo de los Niveles de Servicio, pruebas de parámetros de Niveles de Servicio. El protocolo de pruebas propuesto será validado por el MINJUSDH conjuntamente con el Contratista.
- e. Cronograma: Diagrama de Gantt y Desarrollo de PERT. El diagrama Gantt explicará en días el plan de trabajo, indicando las

Esta es una copia auténtica imprimible de un documento electrónico archivado por el Ministerio de Justicia y Derechos Humanos, aplicando lo dispuesto por el Art. 25 del D.S. 070-2013-PCM y la tercera Disposición Complementaria final del D.S. 026-2016-PCM. Su autenticidad e integridad pueden ser contrastadas a través de la siguiente dirección web: [https://sgd.minjus.gob.pe/gesdoc\\_web/login.jsp](https://sgd.minjus.gob.pe/gesdoc_web/login.jsp) e ingresando el Tipo de Documento, Número y Rango de Fechas de ser el caso o [https://sgd.minjus.gob.pe/gesdoc\\_web/verifica.jsp](https://sgd.minjus.gob.pe/gesdoc_web/verifica.jsp) e ingresando Tipo de Documento, Número, Remitente y Año, según corresponda."





PERÚ

Ministerio  
de Justicia  
y Derechos Humanos

Secretaría  
General

Oficina General de  
Tecnologías de  
Información

Oficina de  
Infraestructura  
y Soporte Tecnológico

“Decenio de la igualdad de oportunidades para mujeres y hombres”  
“Año de la recuperación y consolidación de la economía peruana”

actividades/tareas y el desarrollo PERT permitirá conocer la ruta crítica correspondiente.

- f. Plan de Capacitación: El contenido (syllabus) de los cursos oficiales, fechas tentativas para su ejecución y la información relacionada al centro de instrucción encargada de la capacitación y el certificado del instructor.

### 5.2.2 Inicio del Servicio

El inicio del servicio se contará a partir del día siguiente de culminada la etapa de implementación, con la suscripción del Acta de culminación de la implementación, instalación y configuración total del servicio.

Para dar inicio al servicio, se debe emitir previamente el Acta de culminación de la implementación, instalación y configuración total del servicio, que será suscrita por el Contratista y la Oficina de Infraestructura y Soporte Tecnológico (OIST) del MINJUSDH. Para la emisión de la conformidad, el Contratista debe cumplir con todo lo requerido en los presentes términos de referencia, cuyo criterio de validación se basará en el informe final de la Implementación emitido por el Contratista.

Dentro de los siete (7) días calendario posteriores a la implementación total del servicio, el Contratista debe entregar por Mesa de Partes Virtual un Informe Final de la Implementación en formato digital (PDF), que detalle por cada solución implementada, lo siguiente:

- Descripción de la arquitectura implementada y diagrama de la Topología de la red.
- Equipos instalados.
- Configuración de equipos instalados.
- Protocolos de pruebas
- Información de contactos para el reporte, atención de averías y escalamiento de solicitudes para el cumplimiento de los Acuerdos de Nivel de Servicio (ANS), el cual debe incluir como mínimo: Teléfonos, correo electrónico y página web.
- Procedimiento e información de contacto para solicitudes al área comercial, el cual debe incluir como mínimo: Teléfonos y correo electrónico.

El MINJUSDH se reserva el derecho de realizar otras pruebas de monitoreo que validen el cumplimiento de los ANS's solicitados. En caso los resultados de las mismas no cumplan con los niveles de servicio esperados, dichos resultados se entregarán al Contratista y obligarán al mismo a la revisión y nueva ejecución de las pruebas de aceptación, hasta demostrar el cumplimiento de los ANS's.

*Esta es una copia auténtica imprimible de un documento electrónico archivado por el Ministerio de Justicia y Derechos Humanos, aplicando lo dispuesto por el Art. 25 del D.S. 070-2013-PCM y la tercera Disposición Complementaria final del D.S. 026-2016-PCM. Su autenticidad e integridad pueden ser contrastadas a través de la siguiente dirección web: [https://sgd.minjus.gob.pe/gesdoc\\_web/login.jsp](https://sgd.minjus.gob.pe/gesdoc_web/login.jsp) e ingresando el Tipo de Documento, Número y Rango de Fechas de ser el caso o [https://sgd.minjus.gob.pe/gesdoc\\_web/verifica.jsp](https://sgd.minjus.gob.pe/gesdoc_web/verifica.jsp) e ingresando Tipo de Documento, Número, Remitente y Año, según corresponda.”*







PERÚ

Ministerio  
de Justicia  
y Derechos Humanos

Secretaría  
General

Oficina General de  
Tecnologías de  
Información

Oficina de  
Infraestructura  
y Soporte Tecnológico

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

### 5.3 RECURSOS A SER PROVISTOS POR EL CONTRATISTA.

Todos los equipos, materiales y accesorios necesarios, así como las obras civiles necesarias para el servicio serán provistos por el Contratista. El Contratista debe proporcionar todo el equipamiento que sea necesario para el cumplimiento del servicio (a excepción de lo declarado explícitamente como recurso a ser provisto por el MINJUSDH, en el numeral 5.4).

Será de total y exclusiva responsabilidad del Contratista contemplar todas las actividades, dispositivos, componentes y accesorios para la correcta instalación de los componentes para brindar el servicio requerido en los plazos mencionados.

El Contratista será responsable de las siguientes actividades requeridas para el suministro del servicio:

- ✓ Estudio de campo (en caso sea necesario).
- ✓ Obras civiles (en caso necesario).
- ✓ Gestión de los permisos municipales necesarios para la ejecución de obras civiles en caso sean necesarios. Todos estos gastos serán asumidos por el Contratista.
- ✓ Transporte de los equipos.
- ✓ Montaje de los equipos.
- ✓ Instalación, configuración de equipos y las conexiones necesarias para dejar operativos los equipos a suministrar. Asimismo, toda instalación de equipamiento será dentro del Centro de Datos del MINJUSDH dentro de los gabinetes asignados por la OIST, cabe precisar que el cableado eléctrico y/o datos adicional debe ser cubierto por el postor.
- ✓ Pruebas de funcionamiento y aceptación según protocolo.
- ✓ Puesta en servicio.
- ✓ Transferencia de conocimientos sobre la infraestructura implementada en un workshop que incluya aspectos teóricos y prácticos de al menos ocho (8) horas de duración, los cuales podrán darse hasta en 3 días calendarios. Debe realizarse previa coordinación con el personal de la Oficina de Infraestructura y Soporte Tecnológico (OIST).
- ✓ Mantenimiento del sistema: El Contratista debe ejecutar medidas preventivas a todas las soluciones implementadas, a fin de asegurar la operatividad de todos los componentes del servicio. Se debe anexar al informe mensual con el detalle de estas medidas ejecutadas.
- ✓ Supervisión permanente de los acuerdos de niveles de servicio (ANS).
- ✓ Otras actividades inherentes a la provisión del servicio, es decir cualquier otra actividad no específicamente detallada en los términos de referencia y que sea necesaria para dejar operativo el servicio a suministrar.

*Esta es una copia auténtica imprimible de un documento electrónico archivado por el Ministerio de Justicia y Derechos Humanos, aplicando lo dispuesto por el Art. 25 del D.S. 070-2013-PCM y la tercera Disposición Complementaria final del D.S. 026-2016-PCM. Su autenticidad e integridad pueden ser contrastadas a través de la siguiente dirección web: [https://sgd.minjus.gob.pe/gesdoc\\_web/login.jsp](https://sgd.minjus.gob.pe/gesdoc_web/login.jsp) e ingresando el Tipo de Documento, Número y Rango de Fechas de ser el caso o [https://sgd.minjus.gob.pe/gesdoc\\_web/verifica.jsp](https://sgd.minjus.gob.pe/gesdoc_web/verifica.jsp) e ingresando Tipo de Documento, Número, Remitente y Año, según corresponda."*







PERÚ

Ministerio  
de Justicia  
y Derechos Humanos

Secretaría  
General

Oficina General de  
Tecnologías de  
Información

Oficina de  
Infraestructura  
y Soporte Tecnológico

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

#### 5.4 RECURSOS A SER PROVISTOS POR LA ENTIDAD

- ✓ El MINJUSDH brindará todas las facilidades de acceso a sus oficinas al personal del Contratista del servicio y realizará las gestiones correspondientes en el Centro de Datos de la sede central del MINJUSDH. Es responsabilidad del Contratista la gestión de permisos, autorizaciones y licencias para los trabajos que tengan que realizar en espacios que no son propiedad del MINJUSDH o que estén fuera del Centro de Datos de la sede central del MINJUSDH y de existir gastos relacionados al mismo, estos deben ser asumidos por el Contratista.
- ✓ También se brindará el espacio físico para la instalación de los equipos.
- ✓ Suministro eléctrico (220 Vac), para los equipos a ser instalados. Los PDU instalados en los gabinetes son del tipo C-13. Sólo se aceptarán cables de poder de fábrica y no adaptaciones.
- ✓ Disponibilidad de puertos en los switch core para la interconexión del HA de los Firewall de nueva generación, consola de administración.

#### 5.5 PRESTACIONES ACCESORIAS A LA PRESTACIÓN PRINCIPAL

##### 5.5.1 Capacitación.

El Contratista debe brindar cursos oficiales de capacitación en la administración de las soluciones implementadas, considerando un curso por cada solución. Adicionalmente debe otorgarse capacitación en temas de seguridad informática, de la información y/o ciberseguridad, por ser necesarios para una mejor comprensión de las amenazas actuales, analizar los riesgos, gestionar los riesgos, implementar controles, y gestionar la continuidad de las operaciones por parte del personal de la Oficina de Infraestructura y Soporte Tecnológico (OIST) del MINJUSDH. Los cursos oficiales de capacitación en la administración de las soluciones implementadas deben cumplir con los siguientes requerimientos a fin de asegurar su idoneidad técnica para el desarrollo de los temas requeridos:

- Dictado por instructor certificado por la marca de la solución implementada y/o centro autorizado, que deberá ser acreditada al momento de la presentación del plan de capacitación.
- El centro de instrucción debe contar con los recursos necesarios para el correcto dictado del curso, como son: equipos virtuales para el desarrollo de prácticas y/o laboratorios si las hubiera en cada uno de los temas incluidos. Se aceptará que los cursos sean en modalidad presencial o virtual.

Esta es una copia auténtica imprimible de un documento electrónico archivado por el Ministerio de Justicia y Derechos Humanos, aplicando lo dispuesto por el Art. 25 del D.S. 070-2013-PCM y la tercera Disposición Complementaria final del D.S. 026-2016-PCM. Su autenticidad e integridad pueden ser contrastadas a través de la siguiente dirección web: [https://sgd.minjus.gob.pe/gesdoc\\_web/login.jsp](https://sgd.minjus.gob.pe/gesdoc_web/login.jsp) e ingresando el Tipo de Documento, Número y Rango de Fechas de ser el caso o [https://sgd.minjus.gob.pe/gesdoc\\_web/verifica.jsp](https://sgd.minjus.gob.pe/gesdoc_web/verifica.jsp) e ingresando Tipo de Documento, Número, Remitente y Año, según corresponda."





PERÚ

Ministerio  
de Justicia  
y Derechos Humanos

Secretaría  
General

Oficina General de  
Tecnologías de  
Información

Oficina de  
Infraestructura  
y Soporte Tecnológico

"Decenio de la igualdad de oportunidades para mujeres y hombres"

"Año de la recuperación y consolidación de la economía peruana"

- Los horarios para el dictado de los cursos serán definidos en coordinación con el personal de la Oficina de Infraestructura y Soporte Tecnológico (OIST) del MINJUSDH.
- Capacitación con cursos oficiales a seis (6) integrantes de la Oficina de Infraestructura y Soporte Tecnológico (OIST) en la administración de todos los servicios y/o soluciones implementadas como son: Seguridad Perimetral, Protección Contra Ataques a las aplicaciones y servicios web, Ethical Hacking, Protección AntiDDos Perimetral no volumétrico, Protección de Correo electrónico (Antispam), considerando un curso por cada servicio y/o solución implementada, debiendo entregar los certificados oficiales de participación del curso emitido por la marca (Con excepción de CyberSOC), en un plazo de quince (15) días calendarios contados a partir del día siguiente de culminado el dictado del curso correspondiente, de no presentar el certificado en los tiempos requeridos se aplicará la penalidad mencionada en el numeral 5.13 de los Términos de Referencia
- El plan de capacitación con mención de fechas tentativas será entregado con el Plan de Trabajo del Servicio. La duración de cada curso oficial será como mínimo dieciséis (16) horas, debiendo impartirse hasta en un plazo de sesenta (60) días calendario contados a partir del día siguiente de la suscripción del acta de Conformidad por la implementación del servicio, otorgándose un certificado oficial de participación al curso emitido por la marca por cada participante.
- El contratista debe anexar con el plan de capacitación la información relacionada al centro de instrucción encargada de la capacitación, las referencias de la misma y la(s) certificación(es) del(los) instructor(es).
- **El contratista** debe anexar en su plan de capacitación el contenido (syllabus) de los cursos oficiales en inglés o español, donde se mencione detalladamente los temas a tratar y el nivel que se obtendrá luego de completar estos cursos.
- Se precisa que solo en el caso que alguna de las marcas de las soluciones implementadas no cuente con un curso oficial, el Contratista debe acreditar dicha condición y por consiguiente se aceptará un curso con contenido oficial y certificado local emitido por el Contratista.

*(\*) Previa al inicio de la capacitación el Contratista debe acreditar la(s) certificación(es) del(los) instructor(es).*

Esta es una copia auténtica imprimible de un documento electrónico archivado por el Ministerio de Justicia y Derechos Humanos, aplicando lo dispuesto por el Art. 25 del D.S. 070-2013-PCM y la tercera Disposición Complementaria final del D.S. 026-2016-PCM. Su autenticidad e integridad pueden ser contrastadas a través de la siguiente dirección web: [https://sgd.minjus.gob.pe/gesdoc\\_web/login.jsp](https://sgd.minjus.gob.pe/gesdoc_web/login.jsp) e ingresando el Tipo de Documento, Número y Rango de Fechas de ser el caso o [https://sgd.minjus.gob.pe/gesdoc\\_web/verifica.jsp](https://sgd.minjus.gob.pe/gesdoc_web/verifica.jsp) e ingresando Tipo de Documento, Número, Remitente y Año, según corresponda."





PERÚ

Ministerio  
de Justicia  
y Derechos Humanos

Secretaría  
General

Oficina General de  
Tecnologías de  
Información

Oficina de  
Infraestructura  
y Soporte Tecnológico

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

## 5.6 REQUERIMIENTOS DEL PROVEEDOR Y DE SU PERSONAL

El proveedor debe cumplir con los siguientes profesionales:

### ○ PARA EL PERIODO DE IMPLEMENTACIÓN.

#### a) Jefe de Proyecto (01):

Debe asignarse un responsable de la gestión del proyecto, el cual debe contar con certificación PMP o capacitación en gestión de proyectos (100 horas lectivas como mínimo).

#### Perfil:

Titulado en Ingeniería de Sistemas o Ingeniería electrónica o Ingeniería de telecomunicaciones o Ingeniería informática o Ingeniería de computación o Ingeniería Empresarial y de Sistemas o Ingeniería Computación y Sistemas.

El jefe de proyecto deberá estar habilitado para el ejercicio de la profesión, siendo que la habilitación se presentará para el inicio de su participación efectiva en el contrato.

#### Experiencia

Mínima de tres (03) años en proyectos que comprendan alguna de las siguientes actividades:

- Instalación y/o implementación de soluciones de seguridad.
- Instalación y/o supervisión de soluciones de seguridad.
- Instalación y/o gestión de soluciones de seguridad.
- Instalación y/o implementación de soluciones de seguridad perimetral.

Asimismo, el personal deberá realizar reuniones de control y seguimiento en la etapa de implementación del presente servicio, debiendo presentar y sustentar de acuerdo a las buenas prácticas, el avance periódico de las actividades. El MINJUSDH podrá solicitar el reemplazo de dicho personal, en caso de incumplimiento u omisión a sus actividades profesionales.

#### Acreditación:

- La forma de acreditación de la formación académica, experiencia y certificación o capacitación del jefe de Proyectos será conforme a lo establecido en los requisitos de calificación.

#### b) Ingenieros de implementación (02):

Debe asignarse personal para la instalación, implementación y puesta en operación del servicio requerido, el cual debe contar con al menos

Esta es una copia auténtica imprimible de un documento electrónico archivado por el Ministerio de Justicia y Derechos Humanos, aplicando lo dispuesto por el Art. 25 del D.S. 070-2013-PCM y la tercera Disposición Complementaria final del D.S. 026-2016-PCM. Su autenticidad e integridad pueden ser contrastadas a través de la siguiente dirección web: [https://sgd.minjus.gob.pe/gesdoc\\_web/login.jsp](https://sgd.minjus.gob.pe/gesdoc_web/login.jsp) e ingresando el Tipo de Documento, Número y Rango de Fechas de ser el caso o [https://sgd.minjus.gob.pe/gesdoc\\_web/verifica.jsp](https://sgd.minjus.gob.pe/gesdoc_web/verifica.jsp) e ingresando Tipo de Documento, Número, Remitente y Año, según corresponda."







PERÚ

Ministerio  
de Justicia  
y Derechos Humanos

Secretaría  
General

Oficina General de  
Tecnologías de  
Información

Oficina de  
Infraestructura  
y Soporte Tecnológico

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

una certificación oficial o capacitación en las soluciones requeridas tales como Seguridad perimetral, Protección contra ataques a las aplicaciones y servicios web, Ethical Hacking, Protección AntiDDoS perimetral no volumétrico, Antispam y Centro de Operaciones de Ciberseguridad (CyberSOC) (20 horas lectivas como mínimo para cursos/capacitaciones/diplomados, para certificaciones no corresponde horas lectivas).

**Perfil:**

Ingenieros Titulados y/o bachilleres en las carreras de Ingeniería de Sistemas o Ingeniería de Computación e informática o Ingeniería de Telecomunicaciones o Ingeniería de Seguridad Informática o Ingeniería Electrónica o Ingeniería de Redes y Comunicaciones o Ingeniería en Seguridad y Auditoría Informática o Ingeniería de Telecomunicaciones y Redes o Ingeniería de software o Ingeniero de seguridad de la información o Ingeniería de Redes y Seguridad Informática o Ingeniería de Sistemas y computación.

**Experiencia:**

Mínima de dos (02) años en proyectos que comprendan alguna de las siguientes actividades:

- Instalación y/o implementación en soluciones de Firewall.
- Instalación y/o implementación y/o supervisión en soluciones WAF, Sandboxing, VPN y/o herramientas de seguridad perimetral.
- Ejecución y/o supervisión de servicios de Ethical Hacking.
- Implementación en soluciones de ciberseguridad y/o seguridad perimetral y/o proyectos de seguridad informática siempre que esta refieran a herramientas de seguridad perimetral.

**Acreditación:**

- La forma de acreditación de la formación académica, experiencia y certificación o capacitación del Ingeniero de Implementación será conforme a lo establecido en los requisitos de calificación.

○ **PARA PERIODO DE EJECUCIÓN DEL SERVICIO:**

a) **Profesional asignado al proyecto (01) - Dedicado**

**Perfil:**

Ingeniero Titulado o Bachiller en las carreras de Ingeniería de Sistemas o Ingeniería de Computación e informática o Ingeniería de Telecomunicaciones o Ingeniería de Seguridad Informática o

Esta es una copia auténtica imprimible de un documento electrónico archivado por el Ministerio de Justicia y Derechos Humanos, aplicando lo dispuesto por el Art. 25 del D.S. 070-2013-PCM y la tercera Disposición Complementaria final del D.S. 026-2016-PCM. Su autenticidad e integridad pueden ser contrastadas a través de la siguiente dirección web: [https://sgd.minjus.gob.pe/gesdoc\\_web/login.jsp](https://sgd.minjus.gob.pe/gesdoc_web/login.jsp) e ingresando el Tipo de Documento, Número y Rango de Fechas de ser el caso o [https://sgd.minjus.gob.pe/gesdoc\\_web/verifica.jsp](https://sgd.minjus.gob.pe/gesdoc_web/verifica.jsp) e ingresando Tipo de Documento, Número, Remitente y Año, según corresponda."



PERÚ

Ministerio  
de Justicia  
y Derechos Humanos

Secretaría  
General

Oficina General de  
Tecnologías de  
Información

Oficina de  
Infraestructura  
y Soporte Tecnológico

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

Ingeniería Electrónica o Ingeniería de Redes y Comunicaciones o Ingeniería de Software o Ingeniería Informática o Ingeniería de Seguridad de la Información o Ingeniería de Redes o Ingeniería Electrónica y Comunicaciones o Ingeniería de Seguridad y Auditoría Informática.

Debe tener al menos una (1) certificación oficial en las herramientas y/o soluciones requeridas tales como Seguridad perimetral, Protección contra ataques a las aplicaciones y servicios web, Ethical Hacking, Protección AntiDDoS perimetral no volumétrico, Antispam y Centro de Operaciones de Ciberseguridad (CyberSOC) y en su conjunto debe contar con las capacitaciones de cada una de las soluciones implementadas (20 horas lectivas como mínimo): Seguridad perimetral, Protección contra ataques a las aplicaciones y servicios web, Ethical Hacking, Protección AntiDDoS perimetral no volumétrico, Antispam y Centro de Operaciones de Ciberseguridad (CyberSOC)

El profesional tendrá un horario laboral de lunes a viernes en horario de oficina. Asimismo, brindará el soporte y monitoreo del servicio implementado, tales como son Seguridad perimetral, Protección contra ataques a las aplicaciones y servicios web, Protección AntiDDoS perimetral no volumétrico y Antispam.

**Experiencia:**

Mínima de dos (02) años administrando y/o implementando soluciones de ciberseguridad y/o seguridad perimetral y/o protección contra ataques a aplicaciones y servicios web.

**Acreditación:**

- La forma de acreditación de la formación académica, experiencia y certificación o capacitación del Profesional asignado al proyecto será conforme a lo establecido en los requisitos de calificación.

Se podrá asignar a los ingenieros de implementación para la ejecución del servicio (personal dedicado) brindando la documentación y experiencia solicitada según el perfil o para periodo de ejecución del servicio.

## 5.7 LUGAR Y PLAZO DE PRESTACIÓN DEL SERVICIO

### Lugar Prestación Principal:

*Esta es una copia auténtica imprimible de un documento electrónico archivado por el Ministerio de Justicia y Derechos Humanos, aplicando lo dispuesto por el Art. 25 del D.S. 070-2013-PCM y la tercera Disposición Complementaria final del D.S. 026-2016-PCM. Su autenticidad e integridad pueden ser contrastadas a través de la siguiente dirección web: [https://sgd.minjus.gob.pe/gesdoc\\_web/login.jsp](https://sgd.minjus.gob.pe/gesdoc_web/login.jsp) e ingresando el Tipo de Documento, Número y Rango de Fechas de ser el caso o [https://sgd.minjus.gob.pe/gesdoc\\_web/verifica.jsp](https://sgd.minjus.gob.pe/gesdoc_web/verifica.jsp) e ingresando Tipo de Documento, Número, Remitente y Año, según corresponda."*

56





Ministerio  
de Justicia  
y Derechos Humanos

Secretaría  
General

Oficina General de  
Tecnologías de  
Información

Oficina de  
Infraestructura  
y Soporte Tecnológico

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

La prestación del servicio se debe realizar en la locación del Centro de Datos de la Sede central del MINJUSDH, sito en Scipion Llona 350 - Miraflores, en el horario 24 x 7.

#### **Plazo Prestación Principal:**

##### **Anterior al inicio del servicio (implementación).**

###### **Plan de Trabajo**

- El plazo de entrega del Plan de Trabajo del servicio, es de hasta veinte (20) días calendario contados a partir del día siguiente de la suscripción del contrato. Por el incumplimiento en los plazos, se aplicará la penalidad establecida en el numeral 5.13 de los Términos de Referencia.
- El plan de trabajo será evaluado y aprobado mediante correo electrónico por los especialistas de la OIST, en un plazo máximo de 02 días calendario.
- En caso de ser observado el plan de trabajo, el contratista tendrá un plazo no mayor de 02 días calendario para subsanar las observaciones, este plazo no será computable respecto al plazo total.
- Las observaciones y las aprobaciones del plan serán remitidas vía correo electrónico.

###### **Plazo de Implementación**

- El plazo de implementación del servicio será de hasta noventa (90) días calendario contados a partir del día siguiente de aprobado el plan de trabajo.

##### **Plazo de ejecución del servicio.**

- La prestación del servicio es por treinta y seis (36) meses, contados a partir del día siguiente de la fecha de suscripción del acta de Conformidad por la implementación del servicio.

##### **Posterior al inicio del servicio.**

- El plazo para ejecutar el "plan de actividades" deducidas de la documentación entregada por el fabricante (correspondiente a la revisión solicitada) de los Firewalls perimetrales y Sandboxing, previamente aprobadas por el MINJUSDH, es de veinte (20) días calendario, contados a partir del día siguiente de su aprobación.
- El plazo para ejecutar el cambio de algún personal del CyberSOC (de atención exclusiva al MINJUSDH) es de treinta (30) días calendario contados a partir del día siguiente de la recepción de la notificación.

*Esta es una copia auténtica imprimible de un documento electrónico archivado por el Ministerio de Justicia y Derechos Humanos, aplicando lo dispuesto por el Art. 25 del D.S. 070-2013-PCM y la tercera Disposición Complementaria final del D.S. 026-2016-PCM. Su autenticidad e integridad pueden ser contrastadas a través de la siguiente dirección web: [https://sgd.minjus.gob.pe/gesdoc\\_web/login.jsp](https://sgd.minjus.gob.pe/gesdoc_web/login.jsp) e ingresando el Tipo de Documento, Número y Rango de Fechas de ser el caso o [https://sgd.minjus.gob.pe/gesdoc\\_web/verifica.jsp](https://sgd.minjus.gob.pe/gesdoc_web/verifica.jsp) e ingresando Tipo de Documento, Número, Remitente y Año, según corresponda."*







PERÚ

Ministerio  
de Justicia  
y Derechos Humanos

Secretaría  
General

Oficina General de  
Tecnologías de  
Información

Oficina de  
Infraestructura  
y Soporte Tecnológico

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

**Para el cambio de soluciones, en caso amerite, posterior al inicio del servicio.**

- El plazo para el reemplazo de una solución en nube, es de tres (03) días calendarios, contados a partir del día siguiente de recibida la notificación por parte del MINJUSDH.
- El plazo para el reemplazo de una solución on-premise, es de diez (10) días calendario, contados a partir del día siguiente de recibida la notificación por parte del MINJUSDH.

**Lugar de la Prestación Accesorio: Capacitación**

El servicio se desarrollará en modo presencial o virtual. De realizarse en modo presencial se llevará a cabo en la sede del Centro de Instrucción elegido por el proveedor. El horario del dictado de los cursos será coordinado con el personal de la Oficina de Infraestructura y Soporte Tecnológico (OIST) y el Contratista, siendo preferentemente en horarios fuera de oficina, considerando lo expuesto en el numeral 5.5.1.

**Plazo Prestación Accesorio: Capacitación**

La prestación de este servicio es de sesenta días (60) calendarios, contados a partir del día siguiente de la suscripción del acta de Conformidad por la implementación del servicio.

**5.8 ENTREGABLES DEL SERVICIO**

**Entregable "Plan de Trabajo del Servicio", durante el plazo de implementación.**

De acuerdo a lo definido en el numeral 5.2.1 Planteamiento del Proyecto. El Contratista debe entregar el "Plan de Trabajo del Servicio" por mesa de partes del MINJUSDH.

**Entregable "Informe Final de implementación", culminada la implementación.**

De acuerdo a lo definido en el numeral 5.2.2. Inicio del Servicio. El Contratista debe entregar el "Informe Final" por mesa de partes del MINJUSDH.

**Entregable mensual, posterior al inicio del servicio.**

El contratista debe presentar un "Informe de Servicio" correspondiente al período de facturación (mensual), en el que debe incluir: los niveles de disponibilidad, el detalle de averías presentadas en el período, la cantidad de averías, tiempo total y medio de reparación. El mismo detalle de información debe presentarse por cada uno de los componentes del servicio, consolidando toda la información en un solo informe, incluyendo siempre las "conclusiones" y las "recomendaciones" del caso.

Esta es una copia auténtica imprimible de un documento electrónico archivado por el Ministerio de Justicia y Derechos Humanos, aplicando lo dispuesto por el Art. 25 del D.S. 070-2013-PCM y la tercera Disposición Complementaria final del D.S. 026-2016-PCM. Su autenticidad e integridad pueden ser contrastadas a través de la siguiente dirección web: [https://sgd.minjus.gob.pe/gesdoc\\_web/login.jsp](https://sgd.minjus.gob.pe/gesdoc_web/login.jsp) e ingresando el Tipo de Documento, Número y Rango de Fechas de ser el caso o [https://sgd.minjus.gob.pe/gesdoc\\_web/verifica.jsp](https://sgd.minjus.gob.pe/gesdoc_web/verifica.jsp) e ingresando Tipo de Documento, Número, Remitente y Año, según corresponda."





Ministerio  
de Justicia  
y Derechos Humanos

Secretaría  
General

Oficina General de  
Tecnologías de  
Información

Oficina de  
Infraestructura  
y Soporte Tecnológico

“Decenio de la igualdad de oportunidades para mujeres y hombres”  
“Año de la recuperación y consolidación de la economía peruana”

El contratista debe presentar un “Informe técnico de Ciberseguridad” correspondiente al período de facturación (mensual), en el que debe incluir: Un resumen de ciberseguridad de cada componente del servicio, así como por cada solución de ciberseguridad implementado, indicando los top de ataques (ataques desde la capa 3 hasta la capa 7), top de origen de ataques, top de servicios más atacados, top de malware, indicadores de compromiso, entre otros indicadores de mayor relevancia, incidentes y sus respuestas, incluyendo siempre las “conclusiones” y las “recomendaciones” del caso.

El contratista debe presentar un “Informe ejecutivo de Ciberseguridad” correspondiente al período de facturación (mensual), en el que debe incluir: Un resumen de ciberseguridad a nivel ejecutivo de cada componente del servicio, con la explicación y análisis de los indicadores más relevantes que se mencionaron en el “Informe técnico de Ciberseguridad”.

El contratista debe entregar por mesa de partes del MINJUSDH, los informes descritos líneas arriba, dentro de los siete (7) días calendario posteriores a la culminación de cada período mensual, para ser revisado y aprobado por la Oficina de Infraestructura y Soporte Tecnológico (OIST) dentro de los cinco (5) días calendario posteriores a la recepción del mismo. La OIST está facultada a rechazar un informe en caso no se consigne la información con el detalle solicitado.

## 5.9 OTRAS OBLIGACIONES DEL CONTRATISTA

El Contratista es responsable directo y absoluto de las actividades que realizará directamente y aquellas que desarrollará su personal, debiendo responder por el servicio brindado, en lo que corresponda.

Los equipos y materiales que serán entregados como parte del servicio deberán:

- ✓ Tener una garantía técnica contra fallas y defectos de fabricación de tres (3) años contados a partir del inicio del servicio.
- ✓ El Contratista debe reemplazar sin costo todos aquellos equipos y materiales que presenten averías que requieran reparación, se determinen con defectos de fabricación o no cumplan con las características técnicas requeridas contratadas, a la vez que asistirán en la solución de los problemas que se presenten como consecuencia de esta.

Todo personal que efectúe actividades dentro de las instalaciones de la sede central del MINJUSDH, debe utilizar los equipos necesarios y cumplir con las medidas de seguridad y todas las referidas a la Ley 29783 Ley de Seguridad y Salud en el Trabajo y su Reglamento o norma que la sustituya, durante toda la vigencia del contrato:

*Esta es una copia auténtica imprimible de un documento electrónico archivado por el Ministerio de Justicia y Derechos Humanos, aplicando lo dispuesto por el Art. 25 del D.S. 070-2013-PCM y la tercera Disposición Complementaria final del D.S. 026-2016-PCM. Su autenticidad e integridad pueden ser contrastadas a través de la siguiente dirección web: [https://sgd.minjus.gob.pe/gesdoc\\_web/login.jsp](https://sgd.minjus.gob.pe/gesdoc_web/login.jsp) e ingresando el Tipo de Documento, Número y Rango de Fechas de ser el caso o [https://sgd.minjus.gob.pe/gesdoc\\_web/verifica.jsp](https://sgd.minjus.gob.pe/gesdoc_web/verifica.jsp) e ingresando Tipo de Documento, Número, Remitente y Año, según corresponda.”*





PERÚ

Ministerio  
de Justicia  
y Derechos Humanos

Secretaría  
General

Oficina General de  
Tecnologías de  
Información

Oficina de  
Infraestructura  
y Soporte Tecnológico

“Decenio de la igualdad de oportunidades para mujeres y hombres”  
“Año de la recuperación y consolidación de la economía peruana”

## 5.10 CONFIDENCIALIDAD

El Contratista y su personal no divulgará a terceras partes, la información que reciba del MINJUSDH, sea en forma oral, visual, escrita, grabada en medios magnéticos, correo o en cualquier otra forma tangible.

Toda información del MINJUSDH a que tenga acceso el Contratista, así como su personal, es estrictamente confidencial. El Contratista y su personal se comprometerán vía Declaración Jurada a mantener las reservas del caso y no transmitirla a ninguna persona (natural o jurídica) sin la autorización expresa y por escrito del MINJUSDH, previa coordinación con la Oficina de Infraestructura y Soporte Tecnológico (OIST), en la reunión de kickoff el contratista y su personal deberán firmar un acta de confidencialidad en cumplimiento de lo expuesto en los términos de referencia.

Ante la inobservancia del párrafo anterior, esta se entenderá como un incumplimiento que no puede ser revertido, en ese sentido la parte perjudicada (la entidad) podrá solicitar la resolución del contrato y/o la indemnización por daños y perjuicios, por lo que se le requerirá mediante carta por vía notarial bajo apercibimiento conforme lo establece el artículo 165° del Reglamento de la Ley de Contrataciones del Estado y artículo 36° de la Ley de Contrataciones del Estado.

## 5.11 FORMA DE PAGO

### PRESTACIÓN PRINCIPAL

El pago de servicio se efectuará en treinta y seis (36) cuotas mensuales iguales, para ello el contratista deberá cumplir con presentar de forma mensual el informe que corresponda al periodo a facturarse, el mismo que deberá ser verificado por la Oficina de Infraestructura y Soporte Tecnológico (OIST) del MINJUSDH para la emisión y suscripción de las actas de conformidad.

Los pagos del servicio se realizarán en un plazo máximo de diez (10) días calendario de emitida la conformidad por parte de la Oficina de Infraestructura y Soporte Tecnológico (OIST) del MINJUSDH, en aplicación al artículo 171° del Reglamento de la Ley de Contrataciones del Estado y la modificación del numeral 171.1 por la Primera Disposición Complementaria Modificatoria del D.S. N° 168-2020-EF.

### PRESTACIÓN ACCESORIA – ENTRENAMIENTO O CAPACITACIÓN

El pago se realizará concluido el adiestramiento o entrenamiento y entrega de certificados dentro de los diez (10) días calendarios, siguientes al otorgamiento de la conformidad respectiva en aplicación al artículo 171° del Reglamento de la Ley de Contrataciones del Estado y la modificación del numeral 171.1 por la Primera Disposición Complementaria Modificatoria del D.S. N° 168-2020-EF.

## 5.12. PENALIDAD POR MORA

*Esta es una copia auténtica imprimible de un documento electrónico archivado por el Ministerio de Justicia y Derechos Humanos, aplicando lo dispuesto por el Art. 25 del D.S. 070-2013-PCM y la tercera Disposición Complementaria final del D.S. 026-2016-PCM. Su autenticidad e integridad pueden ser contrastadas a través de la siguiente dirección web: [https://sgd.minjus.gob.pe/gesdoc\\_web/login.jsp](https://sgd.minjus.gob.pe/gesdoc_web/login.jsp) e ingresando el Tipo de Documento, Número y Rango de Fechas de ser el caso o [https://sgd.minjus.gob.pe/gesdoc\\_web/verifica.jsp](https://sgd.minjus.gob.pe/gesdoc_web/verifica.jsp) e ingresando Tipo de Documento, Número, Remitente y Año, según corresponda.”*







PERÚ

Ministerio  
de Justicia  
y Derechos Humanos

Secretaría  
General

Oficina General de  
Tecnologías de  
Información

Oficina de  
Infraestructura  
y Soporte Tecnológico

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

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. La penalidad se aplica automáticamente y se calcula de acuerdo a la siguiente formula:

Penalidad diaria =  $0.10 \times \text{Monto}$

FxPlazo en días

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

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

### 5.13 OTRAS PENALIDADES APLICABLES

Conforme establece el artículo 163 del Reglamento de la ley de Contrataciones del Estado, la entidad tiene la potestad de establecer penalidades, las mismas que son calculadas de forma independiente dentro de los parámetros establecidos.

**Penalidad por incumplimiento de los acuerdos de nivel de servicio, incumplimiento de los objetivos del servicio e incumplimiento de los plazos de ejecución.**

Se aplicarán penalidades al contratista los mismos que se deducirán de las facturaciones mensuales del servicio, de los pagos a cuenta, de las valorizaciones, del pago final o en la liquidación final según corresponda, y de ser necesario se cobrará del monto resultante de la ejecución de la garantía de fiel cumplimiento, basados en el cumplimiento de los Acuerdos de Nivel de Servicio (ANS), cumplimiento de los objetivos del servicio y cumplimiento de los plazos de ejecución para cada componente del servicio requerido, obtenidos por los reportes e informes que emitirá el contratista mensualmente y corroborado por los especialistas de la Oficina de Infraestructura y Soporte Tecnológico (OIST) del MINJUSDH a cargo del control mensual de cada uno de los componentes del servicio.

Dichas penalidades serán aplicadas al contratista por incumplimiento de los ANS, incumplimiento de los objetivos del servicio e incumplimiento de los plazos de ejecución, en forma mensual y determinado por el % de disponibilidad de cada componente del servicio. Si alguna de las interrupciones reportadas es imputable al MINJUSDH, estas no serán consideradas.

- **Penalidad del componente A (Servicio de seguridad perimetral): Incumplimiento del ANS.**

*Esta es una copia auténtica imprimible de un documento electrónico archivado por el Ministerio de Justicia y Derechos Humanos, aplicando lo dispuesto por el Art. 25 del D.S. 070-2013-PCM y la tercera Disposición Complementaria final del D.S. 026-2016-PCM. Su autenticidad e integridad pueden ser contrastadas a través de la siguiente dirección web: [https://sgd.minjus.gob.pe/gesdoc\\_web/login.jsp](https://sgd.minjus.gob.pe/gesdoc_web/login.jsp) e ingresando el Tipo de Documento, Número y Rango de Fechas de ser el caso o [https://sgd.minjus.gob.pe/gesdoc\\_web/verifica.jsp](https://sgd.minjus.gob.pe/gesdoc_web/verifica.jsp) e ingresando Tipo de Documento, Número, Remitente y Año, según corresponda."*





PERÚ

Ministerio  
de Justicia  
y Derechos Humanos

Secretaría  
General

Oficina General de  
Tecnologías de  
Información

Oficina de  
Infraestructura  
y Soporte Tecnológico

“Decenio de la igualdad de oportunidades para mujeres y hombres”  
“Año de la recuperación y consolidación de la economía peruana”

Ítem	Incumplimiento	Penalidad	Procedimiento de Verificación
A	Disponibilidad del servicio de seguridad perimetral < 99.9%	2 UIT, si la disponibilidad es $\geq$ a 99.5 pero < a 99.9%. 4 UIT, si la disponibilidad es $\geq$ a 99 pero < a 99.5%. 6 UIT, si la disponibilidad es $\geq$ a 97 pero < a 99%. 8 UIT, si la disponibilidad es < a 97%.	La Oficina de Infraestructura y Soporte Tecnológico (OIST) del MINJUSDH debe contrastar el cumplimiento de los ANS, con el entregable mensual del Contratista.
B	Disponibilidad del servicio de protección con tecnología sandboxing perimetral < 99.9%	2 UIT, si la disponibilidad es $\geq$ a 99.5 pero < a 99.9%. 4 UIT, si la disponibilidad es $\geq$ a 99 pero < a 99.5%. 6 UIT, si la disponibilidad es $\geq$ a 97 pero < a 99%. 8 UIT, si la disponibilidad es < a 97%.	La Oficina de Infraestructura y Soporte Tecnológico (OIST) del MINJUSDH debe contrastar el cumplimiento de los ANS, con el entregable mensual del contratista.
C	Disponibilidad del servicio de acceso remoto VPN < 99.9%	2 UIT, si la disponibilidad es $\geq$ a 99.5 pero < a 99.9%. 4 UIT, si la disponibilidad es $\geq$ a 99 pero < a 99.5%. 6UIT, si la disponibilidad es $\geq$ a 97 pero < a 99%. 8 UIT, si la disponibilidad es < a 97%.	La Oficina de Infraestructura y Soporte Tecnológico (OIST) del MINJUSDH debe contrastar el cumplimiento de los ANS, con el entregable mensual del contratista.
D	Indisponibilidad del equipamiento (02 appliances) del servicio de seguridad perimetral	1 UIT, por tiempo transcurrido 1 a 60 minutos 2 UIT, por tiempo transcurrido 61 a 120 minutos 3 UIT, por tiempo transcurrido 121 a 180 minutos 4 UIT, por cada hora transcurrido por encima de los 181 minutos.	La Oficina de Infraestructura y Soporte Tecnológico (OIST) del MINJUSDH debe contrastar el cumplimiento del tiempo de reemplazo por fallas en el entregable mensual del contratista.

- **Penalidad del componente B (Servicio de protección contra ataques a las aplicaciones y servicios web): Incumplimiento del ANS.**

Esta es una copia auténtica imprimible de un documento electrónico archivado por el Ministerio de Justicia y Derechos Humanos, aplicando lo dispuesto por el Art. 25 del D.S. 070-2013-PCM y la tercera Disposición Complementaria final del D.S. 026-2016-PCM. Su autenticidad e integridad pueden ser contrastadas a través de la siguiente dirección web: [https://sgd.minjus.gob.pe/gesdoc\\_web/login.jsp](https://sgd.minjus.gob.pe/gesdoc_web/login.jsp) e ingresando el Tipo de Documento, Número y Rango de Fechas de ser el caso o [https://sgd.minjus.gob.pe/gesdoc\\_web/verifica.jsp](https://sgd.minjus.gob.pe/gesdoc_web/verifica.jsp) e ingresando Tipo de Documento, Número, Remitente y Año, según corresponda.”





Ministerio  
de Justicia  
y Derechos Humanos

Secretaría  
General

Oficina General de  
Tecnologías de  
Información

Oficina de  
Infraestructura  
y Soporte Tecnológico

“Decenio de la igualdad de oportunidades para mujeres y hombres”  
“Año de la recuperación y consolidación de la economía peruana”

Ítem	Incumplimiento	Penalidad	Procedimiento de Verificación
A	Disponibilidad del servicio de protección contra ataques a las aplicaciones y servicios web < 99.9%	2 UIT, si la disponibilidad es $\geq$ a 99.5 pero < a 99.9%. 4 UIT, si la disponibilidad es $\geq$ a 99 pero < a 99.5%. 6 UIT, si la disponibilidad es $\geq$ a 97 pero < a 99%. 8 UIT, si la disponibilidad es < a 97%.	La Oficina de Infraestructura y Soporte Tecnológico (OIST) del MINJUSDH debe contrastar el cumplimiento de los ANS, con el entregable mensual del contratista.

• **Penalidad del componente C (por Incumplimiento en servicio de análisis de vulnerabilidades “Ethical Hacking”)**

Ítem	Incumplimiento	Penalidad	Procedimiento de Verificación
A	En la realización, periódica, de actividad de Ethical Hacking externo	1 UIT por cada actividad de Ethical Hacking externo, no ejecutada.	Se verificará con la entrega de los Informe de Diagnostico entregados
B	En el plazo de entrega del Informe de Diagnostico, mayor a los veinte (20) días calendario posterior de culminado la actividad de Ethical Hacking externo.	25% UIT, por cada día de demora, posterior a los veinte (20) días calendario del plazo establecido	Se verificará con la entrega del Informe de Diagnostico
C	En el plazo de entrega del Informe Ejecutivo, mayor a los veinte (20) días calendario posterior de culminado la actividad de Ethical Hacking externo.	25% UIT, por cada día de demora, posterior a los veinte (20) días calendario del plazo establecido	Se verificará con la entrega del Informe de Ejecutivo
D	En el plazo de entrega del Plan de Acciones de Remediación, mayor a los treinta (30) días calendario, posteriores a la culminación de la actividad de Ethical Hacking externo.	25% UIT, por cada día de demora, posterior a los treinta (30) días calendario del plazo establecido	Se verificará con la entrega del Plan de Remediación

• **Penalidad del componente F (Centro de Operaciones de Ciberseguridad (CyberSOC)):**  
**Incumplimiento en los tiempos de atención de incidentes**  
**Incumplimiento del ANS.**

Esta es una copia auténtica imprimible de un documento electrónico archivado por el Ministerio de Justicia y Derechos Humanos, aplicando lo dispuesto por el Art. 25 del D.S. 070-2013-PCM y la tercera Disposición Complementaria final del D.S. 026-2016-PCM. Su autenticidad e integridad pueden ser contrastadas a través de la siguiente dirección web: [https://sgd.minjus.gob.pe/gesdoc\\_web/login.jsp](https://sgd.minjus.gob.pe/gesdoc_web/login.jsp) e ingresando el Tipo de Documento, Número y Rango de Fechas de ser el caso o [https://sgd.minjus.gob.pe/gesdoc\\_web/verifica.jsp](https://sgd.minjus.gob.pe/gesdoc_web/verifica.jsp) e ingresando Tipo de Documento, Número, Remitente y Año, según corresponda.”







PERÚ

Ministerio  
de Justicia  
y Derechos Humanos

Secretaría  
General

Oficina General de  
Tecnologías de  
Información

Oficina de  
Infraestructura  
y Soporte Tecnológico

"Decenio de la igualdad de oportunidades para mujeres y hombres"

"Año de la recuperación y consolidación de la economía peruana"

Ítem	Incumplimiento	Penalidad	Procedimiento de Verificación
A	Demora en la asignación de tickets de las solicitudes o incidentes reportadas por el MINJUSDH >a 15 minutos.	10% de una UIT, por cada 5 minutos adicionales de demora en generar los tickets. (El tiempo adicional se cuenta una vez se supere el tiempo máximo definido en el Literal F.	La Oficina de Infraestructura y Soporte Tecnológico (OIST) del MINJUSDH verificará el cumplimiento en el informe mensual que entregará el contratista y que debe contener el reporte de solicitudes o incidentes reportados durante el mes.
B	Demora en la resolución de las solicitudes y/o incidentes Críticos o Altos >2 horas	1 UIT, por cada hora adicional y en caso de fracción de hora de retraso será 1/60 UIT por cada minuto adicional. (El tiempo adicional se cuenta una vez se supere el tiempo máximo definido en el literal F. (Nivel de criticidad).	La Oficina de Infraestructura y Soporte Tecnológico (OIST) del MINJUSDH verificará el cumplimiento en el informe mensual que entregará el contratista y que debe contener el reporte de solicitudes o incidentes reportados durante el mes.
C	Demora en la resolución de las solicitudes y/o incidentes Medios o Moderados >4 horas	50% de la UIT, por cada hora adicional y en caso de fracción de hora de retraso será 1/120 UIT por cada minuto adicional. (El tiempo adicional se cuenta una vez se supere el tiempo máximo definido en el literal F. (Nivel de criticidad).	La Oficina de Infraestructura y Soporte Tecnológico (OIST) del MINJUSDH verificará el cumplimiento en el informe mensual que entregará el contratista y que debe contener el reporte de solicitudes o incidentes reportados durante el mes.
D	Demora en la resolución de las solicitudes y/o incidentes Bajos >8 horas	25% de la UIT, por cada hora adicional y en caso de fracción de hora de retraso será 1/240 UIT por cada minuto adicional. (El tiempo adicional se cuenta una vez se supere el tiempo máximo definido en el literal F. (Nivel de criticidad).	La Oficina de Infraestructura y Soporte Tecnológico (OIST) del MINJUSDH verificará el cumplimiento en el informe mensual que entregará el contratista y que debe contener el reporte de solicitudes o incidentes reportados durante el mes.

• Penalidad por el Incumplimiento de los objetivos del servicio.

Ítem	Incumplimiento	Penalidad	Procedimiento de Verificación
A	Ataque consolidado a los subdominios/aplicaciones/servicios web publicados a internet.	2 UIT, por cada subdominio/aplicación/ servicio comprometido.	La Oficina de Infraestructura y Soporte Tecnológico (OIST) del MINJUSDH verificará el cumplimiento en el informe mensual que entregará el contratista.

Esta es una copia auténtica imprimible de un documento electrónico archivado por el Ministerio de Justicia y Derechos Humanos, aplicando lo dispuesto por el Art. 25 del D.S. 070-2013-PCM y la tercera Disposición Complementaria final del D.S. 026-2016-PCM. Su autenticidad e integridad pueden ser contrastadas a través de la siguiente dirección web: [https://sgd.minjus.gob.pe/gesdoc\\_web/login.jsp](https://sgd.minjus.gob.pe/gesdoc_web/login.jsp) e ingresando el Tipo de Documento, Número y Rango de Fechas de ser el caso o [https://sgd.minjus.gob.pe/gesdoc\\_web/verifica.jsp](https://sgd.minjus.gob.pe/gesdoc_web/verifica.jsp) e ingresando Tipo de Documento, Número, Remitente y Año, según corresponda."





PERÚ

Ministerio  
de Justicia  
y Derechos Humanos

Secretaría  
General

Oficina General de  
Tecnologías de  
Información

Oficina de  
Infraestructura  
y Soporte Tecnológico

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

Ítem	Incumplimiento	Penalidad	Procedimiento de Verificación
<b>B</b>	Ataque consolidado de Ransomware que no fue detectado por la solución Sandboxing.	1 UIT, por cada host de usuario final afectado e identificado. 5 UIT, por cada servidor afectado e identificado.	La Oficina de Infraestructura y Soporte Tecnológico (OIST) del MINJUSDH verificará el cumplimiento en el informe mensual que entregará el contratista.
<b>C</b>	Spam, Malware, Phishing que no fue detectado por la Solución de Protección de Correo electrónico (Antispam)	1 UIT, por cada host de usuario final afectado e identificado.	La Oficina de Infraestructura y Soporte Tecnológico (OIST) del MINJUSDH verificará el cumplimiento en el informe mensual que entregará el contratista.
<b>D</b>	Ataque de Denegación de Servicio que no fue detectado por la Protección AntiDDos Perimetral no Volumétrico	1 UIT, por cada hora que se tenga la indisponibilidad de los servicios del MINJUSDH	La Oficina de Infraestructura y Soporte Tecnológico (OIST) del MINJUSDH verificará el cumplimiento en el informe mensual que entregará el contratista.

• **Penalidad por Incumplimiento del plazo de presentación del Plan de Trabajo**

Ítem	Incumplimiento	Penalidad	Procedimiento de Verificación
<b>A</b>	Por no presentar el Plan de Trabajo dentro del plazo requerido en los TDR.	2 UIT, por cada día de retraso.	La Oficina de Infraestructura y Soporte Tecnológico (OIST) del MINJUSDH debe verificar y controlar los días de exceso del plazo para la presentación del plan de trabajo.

• **Penalidad por el Incumplimiento de los plazos de ejecución de despliegue o de integración o de cambio de personal o de automatización o de cambio/reemplazo de soluciones, según sea el caso, posterior al inicio de servicio.**

Ítem	Incumplimiento	Penalidad	Procedimiento de Verificación
<b>A</b>	Plazo para ejecutar el cambio de algún personal del CyberSOC > a 30 días.	50% de una UIT por cada día de exceso.	La Oficina de Infraestructura y Soporte Tecnológico (OIST) del MINJUSDH debe verificar y controlar los días de exceso del plazo para el cambio correspondiente.
<b>B</b>	Plazo para reemplazo de una solución on-premise > a 10 días.	50% de una UIT por cada día de exceso.	La Oficina de Infraestructura y Soporte Tecnológico (OIST) del MINJUSDH debe verificar y controlar los días de exceso del plazo para el reemplazo de la solución correspondiente.

Esta es una copia auténtica imprimible de un documento electrónico archivado por el Ministerio de Justicia y Derechos Humanos, aplicando lo dispuesto por el Art. 25 del D.S. 070-2013-PCM y la tercera Disposición Complementaria final del D.S. 026-2016-PCM. Su autenticidad e integridad pueden ser contrastadas a través de la siguiente dirección web: [https://sgd.minjus.gob.pe/gesdoc\\_web/login.jsp](https://sgd.minjus.gob.pe/gesdoc_web/login.jsp) e ingresando el Tipo de Documento, Número y Rango de Fechas de ser el caso o [https://sgd.minjus.gob.pe/gesdoc\\_web/verifica.jsp](https://sgd.minjus.gob.pe/gesdoc_web/verifica.jsp) e ingresando Tipo de Documento, Número, Remitente y Año, según corresponda."





PERÚ

Ministerio de Justicia y Derechos Humanos

Secretaría General

Oficina General de Tecnologías de Información

Oficina de Infraestructura y Soporte Tecnológico

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

Ítem	Incumplimiento	Penalidad	Procedimiento de Verificación
C	Plazo para reemplazo de una solución en nube > a 3 días.	50% de una UIT por cada día de exceso.	La Oficina de Infraestructura y Soporte Tecnológico (OIST) del MINJUSDH debe verificar y controlar los días de exceso del plazo para el reemplazo de la solución correspondiente.

• **Penalidad por la prestación accesoria: Incumplimiento por la capacitación.**

Ítem	Incumplimiento	Penalidad	Procedimiento de Verificación
A	Inicio o término del(os) curso(s) oficial(es) después del plazo estipulado.	2 UIT por cada día de retraso.	La Oficina de Infraestructura y Soporte Tecnológico (OIST) del MINJUSDH debe verificar y controlar los días de exceso del plazo para impartir y/o culminar la capacitación.
B	Por no presentar los certificados de la capacitación dentro del plazo requerido en los TDR.	1 UIT por cada día de retraso.	La Oficina de Infraestructura y Soporte Tecnológico (OIST) del MINJUSDH debe verificar y controlar los días de exceso del plazo para la entrega de los certificados de la capacitación.

• **Penalidad por el Incumplimiento en la entrega de los Informes mensuales.**

Ítem	Incumplimiento	Penalidad	Procedimiento de Verificación
A	Si el contratista demora más de siete (07) días en la entrega de los informes mensuales.	10% de una UIT por cada día de retraso.	La Oficina de Infraestructura y Soporte Tecnológico (OIST) del MINJUSDH debe verificar y controlar el cumplimiento del plazo de entrega del informe mensual.

#### 5.14 RESPONSABILIDAD POR VICIOS OCULTOS

Conforme establece el artículo 173° del Reglamento de la Ley de Contrataciones del Estado, la recepción conforme de la entidad no enerva su derecho a reclamar posteriormente por defectos o vicios ocultos, así mismo el artículo 40° de la Ley de Contrataciones del Estado el contratista es responsable por la calidad ofrecida y por los vicios ocultos **por tres (3) años, contados a partir de otorgada la conformidad.**

#### 5.15 CONFORMIDAD

##### PRESTACIÓN PRINCIPAL

El acta de conformidad será emitida por la Oficina de Infraestructura y Soporte Tecnológico, previo informe técnico de la misma oficina quien verificará el

*Esta es una copia auténtica imprimible de un documento electrónico archivado por el Ministerio de Justicia y Derechos Humanos, aplicando lo dispuesto por el Art. 25 del D.S. 070-2013-PCM y la tercera Disposición Complementaria final del D.S. 026-2016-PCM. Su autenticidad e integridad pueden ser contrastadas a través de la siguiente dirección web: [https://sgd.minjus.gob.pe/gesdoc\\_web/login.jsp](https://sgd.minjus.gob.pe/gesdoc_web/login.jsp) e ingresando el Tipo de Documento, Número y Rango de Fechas de ser el caso o [https://sgd.minjus.gob.pe/gesdoc\\_web/verifica.jsp](https://sgd.minjus.gob.pe/gesdoc_web/verifica.jsp) e ingresando Tipo de Documento, Número, Remitente y Año, según corresponda."*







PERÚ

Ministerio  
de Justicia  
y Derechos Humanos

Secretaría  
General

Oficina General de  
Tecnologías de  
Información

Oficina de  
Infraestructura  
y Soporte Tecnológico

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

cumplimiento de los entregables establecidos en el numeral 5.8. ENTREGABLES DEL SERVICIO, en concordancia con el artículo 168° del Reglamento de la Ley de Contrataciones.

#### PRESTACIÓN ACCESORIA – ENTRENAMIENTO O CAPACITACIÓN

El acta de conformidad será emitida por la Oficina de Infraestructura y Soporte Tecnológico, previo informe técnico de la misma oficina quien verificará el cumplimiento del entrenamiento o capacitación establecido en el numeral 5.5. PRESTACIONES ACCESORIAS A LA PRESTACIÓN PRINCIPAL, en concordancia con el artículo 168° del Reglamento de la Ley de Contrataciones.

#### 5.16 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.

#### 5.17 CLAUSULA DE INTEGRIDAD

En caso de falsedad de cualquiera de las declaraciones efectuadas por el contratista, el MINJUSDH declarará la nulidad del presente contrato por infracción del principio de presunción de veracidad, de conformidad con el literal b) del artículo 44° de la Ley N° 30225

*Esta es una copia auténtica imprimible de un documento electrónico archivado por el Ministerio de Justicia y Derechos Humanos, aplicando lo dispuesto por el Art. 25 del D.S. 070-2013-PCM y la tercera Disposición Complementaria final del D.S. 026-2016-PCM. Su autenticidad e integridad pueden ser contrastadas a través de la siguiente dirección web: [https://sgd.minjus.gob.pe/gesdoc\\_web/login.jsp](https://sgd.minjus.gob.pe/gesdoc_web/login.jsp) e ingresando el Tipo de Documento, Número y Rango de Fechas de ser el caso o [https://sgd.minjus.gob.pe/gesdoc\\_web/verifica.jsp](https://sgd.minjus.gob.pe/gesdoc_web/verifica.jsp) e ingresando Tipo de Documento, Número, Remitente y Año, según corresponda."*



MINISTERIO DE JUSTICIA Y DERECHOS HUMANOS  
CONCURSO PUBLICO N°003-2025-JUS "SERVICIO DE GESTIÓN DE CIBERSEGURIDAD PERIMETRAL  
PARA EL MINISTERIO DE JUSTICIA Y DERECHOS HUMANOS"



PERÚ

Ministerio  
de Justicia  
y Derechos Humanos

Secretaría  
General

Oficina General de  
Tecnologías de  
Información

Oficina de  
Infraestructura  
y Soporte Tecnológico

"Decenio de la igualdad de oportunidades para mujeres y hombres"

"Año de la recuperación y consolidación de la economía peruana"

ANEXO de Características Técnicas					
Servicios de Ciberseguridad para el MINJUSDH					
Ítem	Componentes	Soluciones y/o Servicios	Funcionalidad	Folio	Sustento en caso de no contar con documentación técnica que acredite el cumplimiento
A	SERVICIO DE SEGURIDAD PERIMETRAL	Seguridad perimetral con tecnologías de Firewalls de siguiente generación	Debe tener mínimo la siguiente cantidad de interfaces para el tráfico de datos: <ul style="list-style-type: none"> <li>4 Interfaces de 25GE SFP28</li> <li>8 Interfaces de 10GE SFP+</li> <li>8 Interfaces de 1GE de Cobre</li> <li>2 Interfaces de 40Gb/100 Gb</li> </ul>		
			la solución de seguridad perimetral debe estar certificada por USGv6 para operar con el protocolo IPv6 en las suites de Firewall y/o IPS. Se aceptará versiones de sistema operativo iguales o superiores a las certificadas por USG.		
			La solución de Firewall de siguiente generación debe ser capaz de enviar de manera automática a la solución sandboxing los archivos sospechosos que se propaguen por los protocolos HTTP, HTTPS, FTP, SMTP, POP3 e IMAP; tanto en IPv4 y/o IPv6.		
		Protección con tecnología sandboxing	Debe soportar el análisis de archivos ejecutables (EXE), DLLs, archivos comprimidos (ZIP y RAR), archivos office (.doc, .docx, .xls, .xlsx, .ppt, .pptx), archivos java (.jar), archivos de tipos script (.vbs, .ps1, .js).		
			se requiere que la plataforma cuente con las certificaciones SOC 2 de tipo 2 de AICPA y/o FedRAMP		
		Acceso remoto por Virtual Private Network (VPN)	La Solución e incorporar los mecanismos y soportes necesarios para que el servicio VPN brinde autenticación de doble factor, con certificado digital e integración con el Directorio Activo.		
			La solución 2FA debe ser del tipo "push notification" y/o DynamicID (es decir SMS y/o Email) para dispositivos Smartphone (soporte para Android y Apple)		
		Para las consolas de administración de las soluciones perimetrales	Seguridad perimetral con tecnologías de Firewalls de siguiente generación, Acceso remoto por Virtual Private Network (VPN.) y Protección con tecnología sandboxing, se gestionen		

Esta es una copia auténtica imprimible de un documento electrónico archivado por el Ministerio de Justicia y Derechos Humanos, aplicando lo dispuesto por el Art. 25 del D.S. 070-2013-PCM y la tercera Disposición Complementaria final del D.S. 026-2016-PCM. Su autenticidad e integridad pueden ser contrastadas a través de la siguiente dirección web: [https://sgd.minjus.gob.pe/gesdoc\\_web/login.jsp](https://sgd.minjus.gob.pe/gesdoc_web/login.jsp) e ingresando el Tipo de Documento, Número y Rango de Fechas de ser el caso o [https://sgd.minjus.gob.pe/gesdoc\\_web/verifica.jsp](https://sgd.minjus.gob.pe/gesdoc_web/verifica.jsp) e ingresando Tipo de Documento, Número, Remitente y Año, según corresponda."

68





PERÚ

Ministerio  
de Justicia  
y Derechos Humanos

Secretaría  
General

Oficina General de  
Tecnologías de  
Información

Oficina de  
Infraestructura  
y Soporte Tecnológico

"Decenio de la igualdad de oportunidades para mujeres y hombres"

"Año de la recuperación y consolidación de la economía peruana"

ANEXO de Características Técnicas					
Servicios de Ciberseguridad para el MINJUSDH					
			mediante una consola centralizada on-premise		
B	PROTECCIÓN CONTRA ATAQUES A LAS APLICACIONES Y SERVICIOS WEB	WAF	Auto-Aprendizaje de las aplicaciones y servicios web		
			Debe contar con generación y análisis automático de políticas de seguridad		
			Debe garantizar la persistencia de sesiones, se requieren métodos como cookie insert, cookie rewrite y cookie passive		
			El menú de la solución debe contar con la posibilidad de poder re escribir u ocultar la localización de paths en la URL, sin necesidad de realizar scripts o tener que modificar el código de la aplicación.		
			El Contratista debe implementar una consola en la nube u on-premise		
C	ETHICAL HACKING	Ethical Hacking	Debe proporcionar al menos dos (2) herramientas propietarias específicas para el escaneo de aplicaciones y servicios web.		
D	SERVICIO DE PROTECCIÓN ANTIDDS PERIMETRALES NO VOLUMETRICO	PROTECCIÓN ANTIDDS PERIMETRALES NO VOLUMETRICO	On-premise o en nube		
			Motor Stateless		
			Mecanismo de reto y respuesta o AntiSpoofing para la disminución de falsos positivos		
			Creación automática de firmas en tiempo real frente a ataques DDOS.		
			Tecnología especializada en mitigación de ataques DDOS		
E	SERVICIO DE PROTECCIÓN DE CORREO	SEGURIDAD	Poseer técnicas de filtrado de spam, basados en firmas de spam, filtrado de URL, combinación de patrones utilizados en el spam y heurístico.		

Esta es una copia auténtica imprimible de un documento electrónico archivado por el Ministerio de Justicia y Derechos Humanos, aplicando lo dispuesto por el Art. 25 del D.S. 070-2013-PCM y la tercera Disposición Complementaria final del D.S. 026-2016-PCM. Su autenticidad e integridad pueden ser contrastadas a través de la siguiente dirección web: [https://sgd.minjus.gob.pe/gesdoc\\_web/login.jsp](https://sgd.minjus.gob.pe/gesdoc_web/login.jsp) e ingresando el Tipo de Documento, Número y Rango de Fechas de ser el caso o [https://sgd.minjus.gob.pe/gesdoc\\_web/verifica.jsp](https://sgd.minjus.gob.pe/gesdoc_web/verifica.jsp) e ingresando Tipo de Documento, Número, Remitente y Año, según corresponda."







Ministerio  
de Justicia  
y Derechos Humanos

Secretaría  
General

Oficina General de  
Tecnologías de  
Información

Oficina de  
Infraestructura  
y Soporte Tecnológico

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

ANEXO de Características Técnicas					
Servicios de Ciberseguridad para el MINJUSDH					
	<b>ELECTRONICO (ANTISPAM)</b>		Debe soportar DMARC y DKIM tanto para la validación de la entrada de correos como para la salida a través de llaves de infraestructura pública o certificados digitales.		
			Debe proveer una solución antimalware.		
		<b>SERVICIOS DE SANBOXING</b>	Permite la protección de las URL embebidas en los correos electrónicos al momento de que el usuario realice un click sobre la URL		
		<b>GESTION Y REPORTE</b>	Resúmenes del tamaño de archivo de correo electrónico en la cual se detecta virus o spam.		
			Debe permitir programar informes para la entrega en una determinada frecuencia (diaria, semanal, mensual). Los informes pueden exportarse en formato PDF o HTML.		
<b>F</b>	<b>SERVICIO DE UN CENTRO DE OPERACIONES DE CIBERSEGURIDAD (CYBERSOC)</b>	<b>SERVICIO DE UN CENTRO DE OPERACIONES DE CIBERSEGURIDAD (CYBERSOC)</b>	Certificación 27001 vigente		

## 6. 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><b>Profesionales asignados al proyecto – Cuatro (04)</b></p> <p><b>Requisitos:</b>  <b>Jefe de Proyecto: Cantidad: Uno (01)</b>  Titulado en Ingeniería de Sistemas o Ingeniería electrónica o Ingeniería de telecomunicaciones o Ingeniería informática o Ingeniería de computación o Ingeniería Empresarial y de Sistemas o Ingeniería Computación y Sistemas</p> <p><b>Ingenieros de implementación: Dos (02)</b>  Ingenieros Titulados y/o bachilleres en las carreras de Ingeniería de Sistemas o Ingeniería de Computación e informática o Ingeniería de Telecomunicaciones o Ingeniería de Seguridad Informática o Ingeniería Electrónica o Ingeniería de Redes y Comunicaciones o Ingeniería en Seguridad y Auditoría Informática o Ingeniería de Telecomunicaciones y Redes o Ingeniería de software o Ingeniero de seguridad de la información o Ingeniería de Redes y Seguridad</p>

Esta es una copia auténtica imprimible de un documento electrónico archivado por el Ministerio de Justicia y Derechos Humanos, aplicando lo dispuesto por el Art. 25 del D.S. 070-2013-PCM y la tercera Disposición Complementaria final del D.S. 026-2016-PCM. Su autenticidad e integridad pueden ser contrastadas a través de la siguiente dirección web: [https://sgd.minjus.gob.pe/gesdoc\\_web/login.jsp](https://sgd.minjus.gob.pe/gesdoc_web/login.jsp) e ingresando el Tipo de Documento, Número y Rango de Fechas de ser el caso o [https://sgd.minjus.gob.pe/gesdoc\\_web/verifica.jsp](https://sgd.minjus.gob.pe/gesdoc_web/verifica.jsp) e ingresando Tipo de Documento, Número, Remitente y Año, según corresponda."

70





Ministerio  
de Justicia  
y Derechos Humanos

Secretaría  
General

Oficina General de  
Tecnologías de  
Información

Oficina de  
Infraestructura  
y Soporte Tecnológico

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

	<p>Informática o Ingeniería de Sistemas y computación.</p> <p><b>Profesional asignado al proyecto (01) – Dedicado</b> Ingeniero Titulado o Bachiller en las carreras de Ingeniería de Sistemas o Ingeniería de Computación e informática o Ingeniería de Telecomunicaciones o Ingeniería de Seguridad Informática o Ingeniería Electrónica o Ingeniería de Redes y Comunicaciones o Ingeniería de Software o Ingeniería Informática o Ingeniería de Seguridad de la Información o Ingeniería de Redes o Ingeniería Electrónica y Comunicaciones o Ingeniería de Seguridad y Auditoría Informática.</p> <p><u>Acreditación:</u></p> <p>El Título profesional y/o bachiller solicitado para el personal clave 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> <div style="border: 1px solid black; padding: 5px;"> <p><b>Importante para la Entidad</b></p> <p><i>El postor debe señalar los nombres y apellidos, DNI y profesión del personal clave, así como el nombre de la universidad o institución educativa que expidió el grado o título profesional requerido.</i></p> </div> <p>En caso que El Título profesional y/o bachiller solicitado para el personal clave 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.3.2</b>	<p><b>CAPACITACIÓN</b></p> <p><b>Requisitos:</b> <b>Jefe de Proyecto: Cantidad: Uno (01)</b> Mínimo de 100 horas lectivas en Gestión de Proyectos. De no contar con la capacitación en Gestión de Proyectos deberá presentar la Certificación PMP vigente.</p> <p><b>Ingeniero de Implementación: Dos (02)</b> Mínimo de 20 horas lectivas de una (01) de las soluciones requeridas tales como Seguridad perimetral, Protección contra ataques a las aplicaciones y servicios web, Ethical Hacking, Protección AntiDDoS perimetral no volumétrico, Antispam y Centro de Operaciones de Ciberseguridad (CyberSOC). De no contar con la Capacitación en las soluciones requeridas deberá presentar la Certificación oficial vigente en algunas soluciones requeridas.</p> <p><b>Profesional asignado al proyecto (01) – Dedicado</b> Mínimo de 20 horas lectivas de cada una de las herramientas y/o soluciones requeridas tales como Seguridad perimetral, Protección contra ataques a las aplicaciones y servicios web, Ethical Hacking, Protección AntiDDoS perimetral no volumétrico, Antispam y Centro de Operaciones de Ciberseguridad (CyberSOC). De no contar con la Capacitación en las soluciones requeridas deberá presentar al menos una certificación Oficial vigente de las herramientas y/o soluciones requeridas.</p>

Esta es una copia auténtica imprimible de un documento electrónico archivado por el Ministerio de Justicia y Derechos Humanos, aplicando lo dispuesto por el Art. 25 del D.S. 070-2013-PCM y la tercera Disposición Complementaria final del D.S. 026-2016-PCM. Su autenticidad e integridad pueden ser contrastadas a través de la siguiente dirección web: [https://sgd.minjus.gob.pe/gesdoc\\_web/login.jsp](https://sgd.minjus.gob.pe/gesdoc_web/login.jsp) e ingresando el Tipo de Documento, Número y Rango de Fechas de ser el caso o [https://sgd.minjus.gob.pe/gesdoc\\_web/verifica.jsp](https://sgd.minjus.gob.pe/gesdoc_web/verifica.jsp) e ingresando Tipo de Documento, Número, Remitente y Año, según corresponda."





PERÚ

Ministerio  
de Justicia  
y Derechos Humanos

Secretaría  
General

Oficina General de  
Tecnologías de  
Información

Oficina de  
Infraestructura  
y Soporte Tecnológico

“Decenio de la igualdad de oportunidades para mujeres y hombres”  
“Año de la recuperación y consolidación de la economía peruana”

	<p><b>Acreditación:</b> Se acreditará con copia simple de constancias, certificados, u otros documentos, según corresponda.</p> <div style="border: 1px solid black; padding: 5px; margin-top: 10px;"> <p><b>Importante</b></p> <p><i>Se podrá acreditar la capacitación mediante certificados de estudios de postgrado, considerando que cada crédito del curso que acredita la capacitación equivale a dieciséis horas lectivas, según la normativa de la materia.</i></p> </div>
<p><b>B.4</b></p>	<p><b>EXPERIENCIA DEL PERSONAL CLAVE</b></p> <p><b>Requisitos:</b> <b>Jefe de Proyecto: Cantidad: Uno (01)</b> Mínima de tres (03) años en proyectos que comprendan alguna de las siguientes actividades:</p> <ul style="list-style-type: none"> <li>• Instalación y/o implementación de soluciones de seguridad.</li> <li>• Instalación y/o supervisión de soluciones de seguridad.</li> <li>• Instalación y/o gestión de soluciones de seguridad.</li> <li>• Instalación y/o implementación de soluciones de seguridad perimetral.</li> </ul> <p><b>Ingenieros de implementación: Dos (02)</b> Mínima de dos (02) años en proyectos que comprendan alguna de las siguientes actividades:</p> <ul style="list-style-type: none"> <li>• Instalación y/o implementación en soluciones Firewall.</li> <li>• Instalación y/o implementación y/o supervisión en soluciones WAF, Sandboxing, VPN y/o herramientas de seguridad perimetral.</li> <li>• Ejecución y/o supervisión de servicios de Ethical Hacking.</li> <li>• Implementación en soluciones de ciberseguridad y/o seguridad perimetral y/o proyectos de seguridad informática siempre que esta refieran a herramientas de seguridad perimetral.</li> </ul> <p><b>Profesional asignado al proyecto (01) – Dedicado</b> Mínima de dos (02) años administrando y/o implementando soluciones de ciberseguridad y/o seguridad perimetral y/o protección contra ataques a aplicaciones y servicios web.</p> <p><u>De presentarse experiencia ejecutada paralelamente (trasape), para el cómputo del tiempo de dicha experiencia sólo se considerará una vez el periodo traslapado.</u></p> <p><b>Acreditación:</b> La experiencia del personal clave se acreditará con cualquiera de los siguientes documentos: (i) copia simple de contratos y su respectiva conformidad o (ii) constancias o (iii) certificados o (iv) cualquier otra documentación que, de manera fehaciente demuestre la experiencia del personal propuesto.</p> <div style="border: 1px solid black; padding: 5px; margin-top: 10px;"> <p><b>Importante</b></p> <ul style="list-style-type: none"> <li>• <i>Los documentos que acreditan la experiencia deben incluir los nombres y apellidos del personal clave, el cargo desempeñado, el plazo de la prestación indicando el día, mes y año de inicio y culminación, el nombre de la Entidad u organización que emite el documento, la fecha de emisión y nombres y apellidos</i></li> </ul> </div>

Esta es una copia auténtica imprimible de un documento electrónico archivado por el Ministerio de Justicia y Derechos Humanos, aplicando lo dispuesto por el Art. 25 del D.S. 070-2013-PCM y la tercera Disposición Complementaria final del D.S. 026-2016-PCM. Su autenticidad e integridad pueden ser contrastadas a través de la siguiente dirección web: [https://sgd.minjus.gob.pe/gesdoc\\_web/login.jsp](https://sgd.minjus.gob.pe/gesdoc_web/login.jsp) e ingresando el Tipo de Documento, Número y Rango de Fechas de ser el caso o [https://sgd.minjus.gob.pe/gesdoc\\_web/verifica.jsp](https://sgd.minjus.gob.pe/gesdoc_web/verifica.jsp) e ingresando Tipo de Documento, Número, Remitente y Año, según corresponda.”







Ministerio  
de Justicia  
y Derechos Humanos

Secretaría  
General

Oficina General de  
Tecnologías de  
Información

Oficina de  
Infraestructura  
y Soporte Tecnológico

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

	<p>de quien suscribe el documento.</p> <ul style="list-style-type: none"> <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>
<b>C</b>	<p><b>EXPERIENCIA DEL POSTOR EN LA ESPECIALIDAD</b></p> <p><b>Requisitos:</b> El postor debe acreditar un monto facturado acumulado equivalente a S/ 6,000,000.00 (seis 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:</p> <p>Servicio de seguridad gestionada. Servicio de Ciberseguridad Gestionada. Servicio de Centro de Operaciones de Seguridad (SOC). Servicio de Centro de Operaciones de Ciberseguridad (Cyber SOC). Servicio de integración de soluciones de seguridad. Servicio de implementación de soluciones de seguridad. Servicio de seguridad perimetral. Servicio de seguridad informática. Servicio de protección contra ataques DDoS. Servicio de acceso remoto VPN. Servicio de inteligencia de amenazas. Servicio de Threat Hunting o caza de amenazas. Servicio de protección de aplicaciones web. Servicio de correlación de eventos de seguridad. Servicio de Security Information and Event Management (SIEM). Servicio de monitoreo de eventos de seguridad (SOC) Servicios de Administración y monitoreo de las plataformas de seguridad Servicio de soporte, administración y monitoreo 24x7 de plataformas y eventos de Ciberseguridad. Servicio de Ciberinteligencia y Gestión de eventos e incidentes de seguridad informática Servicios de Cybersoc Gestionado. Servicio de SIEM y SOC Solución integral Tecnológica de Ciberseguridad Servicio Gestionado de Administración de plataformas de seguridad informática y CYBERSOC Servicio Gestionado de equipos de seguridad informática Servicio de soporte de mantenimiento, monitoreo y administración de plataformas de seguridad Servicio de soporte y mantenimiento al equipamiento de seguridad firewall.</p>

Esta es una copia auténtica imprimible de un documento electrónico archivado por el Ministerio de Justicia y Derechos Humanos, aplicando lo dispuesto por el Art. 25 del D.S. 070-2013-PCM y la tercera Disposición Complementaria final del D.S. 026-2016-PCM. Su autenticidad e integridad pueden ser contrastadas a través de la siguiente dirección web: [https://sgd.minjus.gob.pe/gesdoc\\_web/login.jsp](https://sgd.minjus.gob.pe/gesdoc_web/login.jsp) e ingresando el Tipo de Documento, Número y Rango de Fechas de ser el caso o [https://sgd.minjus.gob.pe/gesdoc\\_web/verifica.jsp](https://sgd.minjus.gob.pe/gesdoc_web/verifica.jsp) e ingresando Tipo de Documento, Número, Remitente y Año, según corresponda."





PERÚ

Ministerio  
de Justicia  
y Derechos Humanos

Secretaría  
General

Oficina General de  
Tecnologías de  
Información

Oficina de  
Infraestructura  
y Soporte Tecnológico

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

Servicio de soporte y mantenimiento de operaciones de seguridad en los equipos especializados de seguridad informática.  
Servicio de prevención y control de amenazas y soporte técnico NGFW  
Servicios de Sistemas de Seguridad en la red WAN y LAN.  
Servicio de Arrendamiento de Sistema de Seguridad contra ataques DDoS.  
Servicio de soporte a los equipos de seguridad perimetral.  
Servicio de soporte a los equipos de prevención y detección de software malicioso.  
Servicio de soporte en seguridad.  
Servicio de Mantenimiento de sistema de prevención de intrusos.  
Servicio y/o Venta e Instalación de equipos de seguridad informática: Firewall de Aplicación Web (WAF)  
Servicio y/o Venta e Instalación de equipos de seguridad informática: AntiDDoS.  
Servicio y/o Venta e Instalación de equipos de seguridad informática: Firewall de Siguiente Generación (NGFW)  
Servicio y/o Venta e Instalación de equipos de seguridad informática: Sandboxing  
Servicio y/o Venta e Instalación de equipos de seguridad informática: Solución de Acceso por VPN  
Servicio y/o Venta e Instalación de equipos de seguridad informática: Herramientas de Análisis de Vulnerabilidades.

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>1</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** referido a la Experiencia del Postor en la Especialidad.

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

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

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

1

Esta es una copia auténtica imprimible de un documento electrónico archivado por el Ministerio de Justicia y Derechos Humanos, aplicando lo dispuesto por el Art. 25 del D.S. 070-2013-PCM y la tercera Disposición Complementaria final del D.S. 026-2016-PCM. Su autenticidad e integridad pueden ser contrastadas a través de la siguiente dirección web: [https://sgd.minjus.gob.pe/gesdoc\\_web/login.jsp](https://sgd.minjus.gob.pe/gesdoc_web/login.jsp) e ingresando el Tipo de Documento, Número y Rango de Fechas de ser el caso o [https://sgd.minjus.gob.pe/gesdoc\\_web/verifica.jsp](https://sgd.minjus.gob.pe/gesdoc_web/verifica.jsp) e ingresando Tipo de Documento, Número, Remitente y Año, según corresponda."

74







PERÚ

Ministerio  
de Justicia  
y Derechos Humanos

Secretaría  
General

Oficina General de  
Tecnologías de  
Información

Oficina de  
Infraestructura  
y Soporte Tecnológico

"Decenio de la igualdad de oportunidades para mujeres y hombres"

"Año de la recuperación y consolidación de la economía peruana"

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 correspondiente**.

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** referido a la Experiencia del Postor en la Especialidad.

#### Importante

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

#### Importante

- *Si como resultado de una consulta u observación corresponde precisarse o ajustarse el requerimiento, se solicita la autorización del área usuaria y se pone de conocimiento de tal hecho a la dependencia que aprobó el expediente de contratación, de conformidad con el numeral 72.3 del Reglamento.*
- *El cumplimiento de los Términos de Referencia se realiza mediante la presentación de una declaración jurada. De ser el caso, adicionalmente la Entidad puede solicitar documentación que acredite el cumplimiento del algún componente de estos. Para dicho efecto, consignará de manera detallada los documentos que deben presentar los postores en el literal e) del numeral 2.2.1.1 de esta sección de las bases.*
- *Los requisitos de calificación determinan si los postores cuentan con las capacidades necesarias para ejecutar el contrato, lo que debe ser acreditado documentalmente, y no mediante declaración jurada.*

Esta es una copia auténtica imprimible de un documento electrónico archivado por el Ministerio de Justicia y Derechos Humanos, aplicando lo dispuesto por el Art. 25 del D.S. 070-2013-PCM y la tercera Disposición Complementaria final del D.S. 026-2016-PCM. Su autenticidad e integridad pueden ser contrastadas a través de la siguiente dirección web: [https://sgd.minjus.gob.pe/gesdoc\\_web/login.jsp](https://sgd.minjus.gob.pe/gesdoc_web/login.jsp) e ingresando el Tipo de Documento, Número y Rango de Fechas de ser el caso o [https://sgd.minjus.gob.pe/gesdoc\\_web/verifica.jsp](https://sgd.minjus.gob.pe/gesdoc_web/verifica.jsp) e ingresando Tipo de Documento, Número, Remitente y Año, según corresponda."





**MINISTERIO DE JUSTICIA Y DERECHOS HUMANOS**  
**CONCURSO PUBLICO N°003-2025-JUS “SERVICIO DE GESTIÓN DE CIBERSEGURIDAD PERIMETRAL**  
**PARA EL MINISTERIO DE JUSTICIA Y DERECHOS HUMANOS”**



**PERÚ**

**Ministerio  
de Justicia  
y Derechos Humanos**

**Secretaría  
General**

**Oficina General de  
Tecnologías de  
Información**

**Oficina de  
Infraestructura  
y Soporte Tecnológico**

“Decenio de la igualdad de oportunidades para mujeres y hombres”  
 “Año de la recuperación y consolidación de la economía peruana”

**Visado por:**



Firmado  
digitalmente por  
QUISPE PUCHOC  
Dennis Franco FAU  
20131371617 soft  
Fecha: 2025/04/11  
13:55:08 -05'00'



Firmado digitalmente por  
MANTILLA LEON, Ricardo  
Jhon Paul FAU 20131371617  
soft  
Fecha: 2025/04/11  
14:18:43 -05'00'



Firmado digitalmente por  
PEREZ O'RYAN, Jhonatan  
Jhonatan FAU 20131371617  
soft  
Fecha: 2025/04/11  
14:28:33 -05'00'

**Aprobado por:**



Firmado  
digitalmente  
por VIDAL KONG  
Luisa Maura FAU  
20131371617 soft  
Fecha:  
2025/04/11  
16:05:30 -05'00'

**Fecha de elaboración: 11/04/2025**

**Ver. 4.0**

Esta es una copia auténtica imprimible de un documento electrónico archivado por el Ministerio de Justicia y Derechos Humanos, aplicando lo dispuesto por el Art. 25 del D.S. 070-2013-PCM y la tercera Disposición Complementaria final del D.S. 026-2016-PCM. Su autenticidad e integridad pueden ser contrastadas a través de la siguiente dirección web: [https://sgd.minjus.gob.pe/gesdoc\\_web/login.jsp](https://sgd.minjus.gob.pe/gesdoc_web/login.jsp) e ingresando el Tipo de Documento, Número y Rango de Fechas de ser el caso o [https://sgd.minjus.gob.pe/gesdoc\\_web/verifica.jsp](https://sgd.minjus.gob.pe/gesdoc_web/verifica.jsp) e ingresando Tipo de Documento, Número, Remitente y Año, según corresponda.”

76



**Importante**

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

### 3.2. REQUISITOS DE CALIFICACIÓN

<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>Jefe de Proyecto: Cantidad: Uno (01)</b> Titulado en Ingeniería de Sistemas o Ingeniería electrónica o Ingeniería de telecomunicaciones o Ingeniería informática o Ingeniería de computación o Ingeniería Empresarial y de Sistemas o Ingeniería Computación y Sistemas.</p> <p><b>Ingenieros de implementación: Dos (02)</b> Ingenieros Titulados y/o bachilleres en las carreras de Ingeniería de Sistemas o Ingeniería de Computación e informática o Ingeniería de Telecomunicaciones o Ingeniería de Seguridad Informática o Ingeniería Electrónica o Ingeniería de Redes y Comunicaciones o Ingeniería en Seguridad y Auditoría Informática o Ingeniería de Telecomunicaciones y Redes o Ingeniería de software o Ingeniero de seguridad de la información o Ingeniería de Redes y Seguridad Informática o Ingeniería de Sistemas y computación.</p> <p><b>Profesional asignado al proyecto (01) – Dedicado</b> Ingeniero Titulado o Bachiller en las carreras de Ingeniería de Sistemas o Ingeniería de Computación e informática o Ingeniería de Telecomunicaciones o Ingeniería de Seguridad Informática o Ingeniería Electrónica o Ingeniería de Redes y Comunicaciones o Ingeniería de Software o Ingeniería Informática o Ingeniería de Seguridad de la Información o Ingeniería de Redes o Ingeniería Electrónica y Comunicaciones o Ingeniería de Seguridad y Auditoría Informática.</p> <p><u>Acreditación:</u></p> <p>El Título y/o 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> <div style="border: 1px solid black; padding: 5px; margin-top: 10px;"> <p><b>Importante para la Entidad</b></p> <p><i>El postor debe señalar los nombres y apellidos, DNI y profesión del personal clave, así como el nombre de la universidad o institución educativa que expidió el grado o título profesional requerido.</i></p> </div> <p>En caso que el Título y/o bachiller solicitado para el personal clave 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.3.2</b>	<b>CAPACITACIÓN</b>
	<p><u>Requisitos:</u></p> <p><b>Jefe de Proyecto: Cantidad: Uno (01)</b> Mínimo de 100 horas lectivas en Gestión de Proyectos. De no contar con la capacitación en Gestión de Proyectos deberá presentar la Certificación PMP vigente.</p>

	<p><b>Ingeniero de Implementación: Dos (02)</b> Mínimo de 20 horas lectivas de una (01) de las soluciones requeridas tales como Seguridad perimetral, Protección contra ataques a las aplicaciones y servicios web, Ethical Hacking, Protección AntiDDoS perimetral no volumétrico, Antispam y Centro de Operaciones de Ciberseguridad (CyberSOC). De no contar con la Capacitación en las soluciones requeridas deberá presentar la Certificación oficial vigente en algunas soluciones requeridas.</p> <p><b>Profesional asignado al proyecto (01) – Dedicado</b> Mínimo de 20 horas lectivas de cada una de las herramientas y/o soluciones requeridas tales como Seguridad perimetral, Protección contra ataques a las aplicaciones y servicios web, Ethical Hacking, Protección AntiDDoS perimetral no volumétrico, Antispam y Centro de Operaciones de Ciberseguridad (CyberSOC). De no contar con la Capacitación en las soluciones requeridas deberá presentar al menos una certificación Oficial vigente de las herramientas y/o soluciones requeridas.</p> <p><u>Acreditación:</u></p> <p>Se acreditará con copia simple de constancias, certificados, u otros documentos, según corresponda.</p> <div style="border: 1px solid black; padding: 5px; margin-top: 10px;"> <p><b>Importante</b></p> <p><i>Se podrá acreditar la capacitación mediante certificados de estudios de postgrado, considerando que cada crédito del curso que acredita la capacitación equivale a dieciséis horas lectivas, según la normativa de la materia.</i></p> </div>
<b>B.4</b>	<p><b>EXPERIENCIA DEL PERSONAL CLAVE</b></p> <p><u>Requisitos:</u></p> <p><b>Jefe de Proyecto: Cantidad: Uno (01)</b> Mínima de tres (03) años en proyectos que comprendan alguna de las siguientes actividades:</p> <ul style="list-style-type: none"> <li>• Instalación y/o implementación de soluciones de seguridad.</li> <li>• Instalación y/o supervisión de soluciones de seguridad.</li> <li>• Instalación y/o gestión de soluciones de seguridad.</li> <li>• Instalación y/o implementación de soluciones de seguridad perimetral.</li> </ul> <p><b>Ingenieros de implementación: Dos (02)</b> Mínima de dos (02) años en proyectos que comprendan alguna de las siguientes actividades:</p> <ul style="list-style-type: none"> <li>• Instalación y/o implementación en soluciones Firewall.</li> <li>▪ Instalación y/o implementación y/o supervisión en soluciones WAF, Sandboxing, VPN y/o herramientas de seguridad perimetral.</li> <li>• Ejecución y/o supervisión de servicios de Ethical Hacking.</li> <li>• Implementación en soluciones de ciberseguridad y/o seguridad perimetral y/o proyectos de seguridad informática siempre que esta refieran a herramientas de seguridad perimetral.</li> </ul> <p><b>Profesional asignado al proyecto (01) – Dedicado</b> Mínima de dos (02) años administrando y/o implementando soluciones de ciberseguridad y/o seguridad perimetral y/o protección contra ataques a aplicaciones y servicios web.</p> <p><u>De presentarse experiencia ejecutada paralelamente (traslape), para el cómputo del tiempo de dicha experiencia sólo se considerará una vez el periodo traslapado.</u></p> <p><u>Acreditación:</u></p> <p>La experiencia del personal clave se acreditará con cualquiera de los siguientes documentos: (i) copia simple de contratos y su respectiva conformidad o (ii) constancias o (iii) certificados o (iv) cualquier otra documentación que, de manera fehaciente demuestre la experiencia del personal propuesto.</p> <div style="border: 1px solid black; padding: 5px; margin-top: 10px;"> <p><b>Importante</b></p> </div>



	<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>
<b>C</b>	<b>EXPERIENCIA DEL POSTOR EN LA ESPECIALIDAD</b>
	<p><u>Requisitos:</u></p> <p>El postor debe acreditar un monto facturado acumulado equivalente a S/ 6,000,000.00 (Seis 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> <p>Servicio de seguridad gestionada.  Servicio de Ciberseguridad Gestionada.  Servicio de Centro de Operaciones de Seguridad (SOC).  Servicio de Centro de Operaciones de Ciberseguridad (Cyber SOC).  Servicio de integración de soluciones de seguridad.  Servicio de implementación de soluciones de seguridad.  Servicio de seguridad perimetral.  Servicio de seguridad informática.  Servicio de protección contra ataques DDoS.  Servicio de acceso remoto VPN.  Servicio de inteligencia de amenazas.  Servicio de Threat Hunting o caza de amenazas.  Servicio de protección de aplicaciones web.  Servicio de correlación de eventos de seguridad.  Servicio de Security Information and Event Management (SIEM).  Servicio de monitoreo de eventos de seguridad (SOC)  Servicios de Administración y monitoreo de las plataformas de seguridad.  Servicio de soporte, administración y monitoreo 24x7 de plataformas y eventos de Ciberseguridad.  Servicio de Ciberinteligencia y Gestión de eventos e incidentes de seguridad informática.  Servicios de Cybersoc Gestionado.  Servicio de SIEM y SOC.  Solución integral Tecnológica de Ciberseguridad.  Servicio Gestionado de Administración de plataformas de seguridad informática y CYBERSOC.  Servicio Gestionado de equipos de seguridad informática  Servicio de soporte de mantenimiento, monitoreo y administración de plataformas de seguridad.  Servicio de soporte y mantenimiento al equipamiento de seguridad firewall.  Servicio de soporte y mantenimiento de operaciones de seguridad en los equipos especializados de seguridad informática.  Servicio de prevención y control de amenazas y soporte técnico NGFW  Servicios de Sistemas de Seguridad en la red WAN y LAN.  Servicio de Arrendamiento de Sistema de Seguridad contra ataques DDoS.  Servicio de soporte a los equipos de seguridad perimetral.  Servicio de soporte a los equipos de prevención y detección de software malicioso.  Servicio de soporte en seguridad.  Servicio de Mantenimiento de sistema de prevención de intrusos.  Servicio y/o Venta e Instalación de equipos de seguridad informática: Firewall de Aplicación Web (WAF)  Servicio y/o Venta e Instalación de equipos de seguridad informática: AntiDDoS,</p>

	<p>Servicio y/o Venta e Instalación de equipos de seguridad informática: Firewall de Siguierte Generación (NGFW)</p> <p>Servicio y/o Venta e Instalación de equipos de seguridad informática: Sandboxing</p> <p>Servicio y/o Venta e Instalación de equipos de seguridad informática: Solución de Acceso por VPN</p> <p>Servicio y/o Venta e Instalación de equipos de seguridad informática: Herramientas de Análisis de Vulnerabilidades.</p> <p><u>Acreditación:</u></p> <p>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>10</sup>, correspondientes a un máximo de veinte (20) contrataciones.</p> <p>En caso los postores presenten varios comprobantes de pago para acreditar una sola contratación, se debe acreditar que corresponden a dicha contratación; de lo contrario, se asumirá que los comprobantes acreditan contrataciones independientes, en cuyo caso solo se considerará, para la evaluación, las veinte (20) primeras contrataciones indicadas en el <b>Anexo N° 8</b> referido a la Experiencia del Postor en la Especialidad.</p> <p>En el caso de servicios de ejecución periódica o continuada, solo se considera como experiencia la parte del contrato que haya sido ejecutada durante los ocho (8) años anteriores a la fecha de presentación de ofertas, debiendo adjuntarse copia de las conformidades correspondientes a tal parte o los respectivos comprobantes de pago cancelados.</p> <p>En los casos que se acredite experiencia adquirida en consorcio, debe presentarse la promesa de consorcio o el contrato de consorcio del cual se desprenda fehacientemente el porcentaje de las obligaciones que se asumió en el contrato presentado; de lo contrario, no se computará la experiencia proveniente de dicho contrato.</p> <p>Asimismo, cuando se presenten contratos derivados de procesos de selección convocados antes del 20.09.2012, la calificación se ceñirá al método descrito en la Directiva “Participación de Proveedores en Consorcio en las 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.</p> <p>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.</p> <p>Si el postor acredita experiencia de otra persona jurídica como consecuencia de una reorganización societaria, debe presentar adicionalmente el <b>Anexo N° 9</b>.</p> <p>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.</p> <p>Sin perjuicio de lo anterior, los postores deben llenar y presentar el <b>Anexo N° 8</b> referido a la Experiencia del Postor en la Especialidad.</p>
--	--

<sup>10</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”.

**Importante**

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

**Importante**

- *Si como resultado de una consulta u observación corresponde precisarse o ajustarse el requerimiento, se solicita la autorización del área usuaria y se pone de conocimiento de tal hecho a la dependencia que aprobó el expediente de contratación, de conformidad con el numeral 72.3 del artículo 72 del Reglamento.*
- *El cumplimiento de los Términos de Referencia se realiza mediante la presentación de una declaración jurada. De ser el caso, adicionalmente la Entidad puede solicitar documentación que acredite el cumplimiento del algún componente de estos. Para dicho efecto, consignará de manera detallada los documentos que deben presentar los postores en el literal e) del numeral 2.2.1.1 de esta sección de las bases.*
- *Los requisitos de calificación determinan si los postores cuentan con las capacidades necesarias para ejecutar el contrato, lo que debe ser acreditado documentalmente, y no mediante declaración jurada.*



#### CAPÍTULO IV FACTORES DE EVALUACIÓN

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

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

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

#### Importante

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

## CAPÍTULO V PROFORMA DEL CONTRATO

### Importante

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

Conste por el presente documento, la contratación del Servicio de Gestión de Ciberseguridad Perimetral para el Ministerio de Justicia y Derechos Humanos, que celebra de una parte el Ministerio de Justicia y Derechos Humanos en adelante LA ENTIDAD, con RUC N°20131371617, con domicilio legal en [...], representada por [...], identificado con DNI N° [...], y de otra parte [...], con RUC N° [...], con domicilio legal en [...], inscrita en la Ficha N° [...] Asiento N° [...] del Registro de Personas Jurídicas de la ciudad de [...], debidamente representado por su Representante Legal, [...], con DNI N° [...], según poder inscrito en la Ficha N° [...], Asiento N° [...] del Registro de Personas Jurídicas de la ciudad de [...], a quien en adelante se le denominará EL CONTRATISTA en los términos y condiciones siguientes:

### **CLÁUSULA PRIMERA: ANTECEDENTES**

Con fecha [...], el comité de selección adjudicó la buena pro del **CONCURSO PÚBLICO Nº 003-2025-JUS** para la contratación del **Servicio de Gestión de Ciberseguridad Perimetral para el Ministerio de Justicia y Derechos Humanos**, 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 el **Servicio de Gestión de Ciberseguridad Perimetral para el Ministerio de Justicia y Derechos Humanos**.

### **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>11</sup>**

LA ENTIDAD se obliga a pagar la contraprestación a EL CONTRATISTA en Soles:

#### **PRESTACIÓN PRINCIPAL:**

El pago de servicio se efectuará en treinta y seis (36) cuotas mensuales iguales, para ello el contratista deberá cumplir con presentar de forma mensual el informe que corresponda al periodo a facturarse, el mismo que deberá ser verificado por la Oficina de Infraestructura y Soporte Tecnológico (OIST) del MINJUSDH para la emisión y suscripción de las actas de conformidad.

#### **PRESTACIÓN ACCESORIA – ENTRENAMIENTO O CAPACITACIÓN:**

El pago se realizará concluido el adiestramiento o entrenamiento y entrega de certificados dentro de los diez (10) días calendarios, siguientes al otorgamiento de la conformidad respectiva.

<sup>11</sup> En cada caso concreto, dependiendo de la naturaleza del contrato, podrá adicionarse la información que resulte pertinente a efectos de generar el pago.

Luego de la recepción formal y completa de la documentación correspondiente, según lo establecido en el artículo 171 del Reglamento de la Ley de Contrataciones del Estado.

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

LA ENTIDAD debe efectuar el pago de las contraprestaciones pactadas a favor del CONTRATISTA dentro de los diez (10) días calendario siguientes de otorgada la conformidad de los servicios, siempre que se verifiquen las condiciones establecidas en el contrato para ello, bajo responsabilidad del funcionario competente.

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

#### **CLÁUSULA QUINTA: DEL PLAZO DE LA EJECUCIÓN DE LA PRESTACIÓN**

El plazo de ejecución del presente contrato es de:

##### **Plazo de Prestación Principal:**

- El plazo de entrega del Plan de Trabajo del servicio, es de hasta veinte (20) días calendario contados a partir del día siguiente de la suscripción del contrato.
- El plazo de implementación del servicio será de hasta noventa (90) días calendario contados a partir del día siguiente de aprobado el plan de trabajo.
- El plazo de la prestación del servicio es por treinta y seis (36) meses, contados a partir del día siguiente de la fecha de suscripción del acta de Conformidad por la implementación del servicio.

##### **Plazo de Prestación Accesorio:**

- Capacitación: la prestación de este servicio es de sesenta días (60) calendarios, contados a partir del día siguiente de la suscripción del acta de Conformidad por la implementación del servicio.

#### **CLÁUSULA SEXTA: PARTES INTEGRANTES DEL CONTRATO**

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

#### **CLÁUSULA SÉTIMA: GARANTÍAS**

EL CONTRATISTA entregó al perfeccionamiento del contrato la respectiva garantía incondicional, solidaria, irrevocable, y de realización automática en el país al solo requerimiento, a favor de LA ENTIDAD, por los conceptos, montos y vigencias siguientes:

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

##### **Importante**

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



siguiente:

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

En el caso que corresponda, consignar lo siguiente:

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

#### Importante

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

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

#### Importante

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

#### **CLÁUSULA OCTAVA: EJECUCIÓN DE GARANTÍAS POR FALTA DE RENOVACIÓN**

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

#### **CLÁUSULA DÉCIMA: CONFORMIDAD DE LA PRESTACIÓN DEL SERVICIO**

La conformidad de la prestación del servicio se regula por lo dispuesto en el artículo 168 del Reglamento de la Ley de Contrataciones del Estado. La conformidad será otorgada por **la Oficina de Infraestructura y soporte Tecnológico** 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 UNDÉCIMA: DECLARACIÓN JURADA DEL CONTRATISTA**

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

#### **CLÁUSULA DUODÉCIMA: RESPONSABILIDAD POR VICIOS OCULTOS**

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

El plazo máximo de responsabilidad del contratista es de **tres (3) año(s)** contado a partir de la conformidad otorgada por LA ENTIDAD.

#### **CLÁUSULA DÉCIMA TERCERA: PENALIDADES**

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

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

Donde:

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

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

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

#### **Importante**

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

#### **OTRAS PENALIDADES:**

**Penalidad por incumplimiento de los acuerdos de nivel de servicio, incumplimiento de los objetivos del servicio e incumplimiento de los plazos de ejecución.**

Se aplicarán penalidades al contratista los mismos que se deducirán de las facturaciones mensuales del servicio, de los pagos a cuenta, de las valorizaciones, del pago final o en la liquidación final según corresponda, y de ser necesario se cobrará del monto resultante de la ejecución de la garantía de fiel cumplimiento, basados en el cumplimiento de los Acuerdos de Nivel de Servicio (ANS), cumplimiento de los objetivos del servicio y cumplimiento de los plazos de ejecución para cada componente del servicio requerido, obtenidos por los reportes e informes que emitirá el contratista mensualmente y corroborado por los especialistas de la Oficina de Infraestructura y Soporte Tecnológico (OIST) del MINJUSDH a cargo del control mensual de cada uno de los componentes del servicio.

Dichas penalidades serán aplicadas al contratista por incumplimiento de los ANS, incumplimiento de los objetivos del servicio e incumplimiento de los plazos de ejecución, en forma mensual y determinado por el % de disponibilidad de cada componente del servicio. Si alguna de las interrupciones reportadas es imputable al MINJUSDH, estas no serán consideradas.

- **Penalidad del componente A (Servicio de seguridad perimetral): Incumplimiento del ANS.**

Ítem	Incumplimiento	Penalidad	Procedimiento de Verificación
<b>A</b>	Disponibilidad del servicio de seguridad perimetral < 99.9%	2 UIT, si la disponibilidad es $\geq$ a 99.5 pero < a 99.9%. 4 UIT, si la disponibilidad es $\geq$ a 99 pero < a 99.5%. 6 UIT, si la disponibilidad es $\geq$ a 97 pero < a 99%. 8 UIT, si la disponibilidad es < a 97%.	La Oficina de Infraestructura y Soporte Tecnológico (OIST) del MINJUSDH debe contrastar el cumplimiento de los ANS, con el entregable mensual del Contratista.
<b>B</b>	Disponibilidad del servicio de protección con tecnología sandboxing perimetral < 99.9%	2 UIT, si la disponibilidad es $\geq$ a 99.5 pero < a 99.9%. 4 UIT, si la disponibilidad es $\geq$ a 99 pero < a 99.5%. 6 UIT, si la disponibilidad es $\geq$ a 97 pero < a 99%. 8 UIT, si la disponibilidad es < a 97%.	La Oficina de Infraestructura y Soporte Tecnológico (OIST) del MINJUSDH debe contrastar el cumplimiento de los ANS, con el entregable mensual del contratista.
<b>C</b>	Disponibilidad del servicio de acceso remoto VPN < 99.9%	2 UIT, si la disponibilidad es $\geq$ a 99.5 pero < a 99.9%. 4 UIT, si la disponibilidad es $\geq$ a 99 pero < a 99.5%. 6UIT, si la disponibilidad es $\geq$ a 97 pero < a 99%. 8 UIT, si la disponibilidad es < a 97%.	La Oficina de Infraestructura y Soporte Tecnológico (OIST) del MINJUSDH debe contrastar el cumplimiento de los ANS, con el entregable mensual del contratista.
<b>D</b>	Indisponibilidad del equipamiento (02 appliances) del servicio de seguridad perimetral	1 UIT, por tiempo transcurrido 1 a 60 minutos 2 UIT, por tiempo transcurrido 61 a 120 minutos 3 UIT, por tiempo transcurrido 121 a 180 minutos 4 UIT, por cada hora transcurrido por encima de los 181 minutos.	La Oficina de Infraestructura y Soporte Tecnológico (OIST) del MINJUSDH debe contrastar el cumplimiento del tiempo de reemplazo por fallas en el entregable mensual del contratista.

- **Penalidad del componente B (Servicio de protección contra ataques a las aplicaciones y servicios web): Incumplimiento del ANS.**

Ítem	Incumplimiento	Penalidad	Procedimiento de Verificación
<b>A</b>	Disponibilidad del servicio de protección contra ataques a las aplicaciones y servicios web < 99.9%	2 UIT, si la disponibilidad es $\geq$ a 99.5 pero < a 99.9%. 4 UIT, si la disponibilidad es $\geq$ a 99 pero < a 99.5%. 6 UIT, si la disponibilidad es $\geq$ a 97 pero < a 99%. 8 UIT, si la disponibilidad es < a 97%.	La Oficina de Infraestructura y Soporte Tecnológico (OIST) del MINJUSDH debe contrastar el cumplimiento de los ANS, con el entregable mensual del contratista.

- **Penalidad del componente C (por Incumplimiento en servicio de análisis de vulnerabilidades “Ethical Hacking”).**



Ítem	Incumplimiento	Penalidad	Procedimiento de Verificación
<b>A</b>	En la realización, periódica, de actividad de Ethical Hacking externo	1 UIT por cada actividad de Ethical Hacking externo, no ejecutada.	Se verificará con la entrega de los Informe de Diagnostico entregados
<b>B</b>	En el plazo de entrega del Informe de Diagnostico, mayor a los veinte (20) días calendario posterior de culminado la actividad de Ethical Hacking externo.	25% UIT, por cada día de demora, posterior a los veinte (20) días calendario del plazo establecido	Se verificará con la entrega del Informe de Diagnostico
<b>C</b>	En el plazo de entrega del Informe Ejecutivo, mayor a los veinte (20) días calendario posterior de culminado la actividad de Ethical Hacking externo.	25% UIT, por cada día de demora, posterior a los veinte (20) días calendario del plazo establecido	Se verificará con la entrega del Informe de Ejecutivo
<b>D</b>	En el plazo de entrega del Plan de Acciones de Remediación, mayor a los treinta (30) días calendario, posteriores a la culminación de la actividad de Ethical Hacking externo.	25% UIT, por cada día de demora, posterior a los treinta (30) días calendario del plazo establecido	Se verificará con la entrega del Plan de Remediación

- **Penalidad del componente F (Centro de Operaciones de Ciberseguridad (CyberSOC)):**  
**Incumplimiento en los tiempos de atención de incidentes**  
**Incumplimiento del ANS.**

Ítem	Incumplimiento	Penalidad	Procedimiento de Verificación
<b>A</b>	Demora en la asignación de tickets de las solicitudes o incidentes reportadas por el MINJUSDH >a 15minutos.	10% de una UIT, por cada 5 minutos adicionales de demora en generar los tickets. (El tiempo adicional se cuenta una vez se supere el tiempo máximo definido en el Literal F.	La Oficina de Infraestructura y Soporte Tecnológico (OIST) del MINJUSDH verificará el cumplimiento en el informe mensual que entregará el contratista y que debe contener el reporte de solicitudes o incidentes reportados durante el mes.
<b>B</b>	Demora en la resolución de las solicitudes y/o incidentes Críticos o Altos >2 horas	1 UIT, por cada hora adicional y en caso de fracción de hora de retraso será 1/60 UIT por cada minuto adicional. (El tiempo adicional se cuenta una vez se supere el tiempo máximo definido en el literal F. <b>(Nivel de criticidad)</b> ).	La Oficina de Infraestructura y Soporte Tecnológico (OIST) del MINJUSDH verificará el cumplimiento en el informe mensual que entregará el contratista y que debe contener el reporte de solicitudes o incidentes reportados durante el mes.
<b>C</b>	Demora en la resolución de las solicitudes y/o incidentes Medios o Moderados >4 horas	50% de la UIT, por cada hora adicional y en caso de fracción de hora de retraso será 1/120 UIT por cada minuto adicional. (El tiempo adicional se cuenta una vez se supere el tiempo máximo definido en el literal F. <b>(Nivel de criticidad)</b> ).	La Oficina de Infraestructura y Soporte Tecnológico (OIST) del MINJUSDH verificará el cumplimiento en el informe mensual que entregará el contratista y que debe contener el reporte de solicitudes o incidentes reportados durante el mes.
<b>D</b>	Demora en la resolución de las solicitudes y/o incidentes Bajos >8 horas	25% de la UIT, por cada hora adicional y en caso de fracción de hora de retraso será 1/240 UIT por cada minuto adicional. (El tiempo adicional se cuenta una vez se supere el tiempo máximo definido en el literal F. <b>(Nivel de criticidad)</b> ).	La Oficina de Infraestructura y Soporte Tecnológico (OIST) del MINJUSDH verificará el cumplimiento en el informe mensual que entregará el contratista y que debe contener el reporte de solicitudes o incidentes reportados durante el mes.

- **Penalidad por el Incumplimiento de los objetivos del servicio.**

Ítem	Incumplimiento	Penalidad	Procedimiento de Verificación
<b>A</b>	Ataque consolidado a los subdominios/aplicaciones/servicios web publicados a internet.	2 UIT, por cada subdominio/aplicación/ servicio comprometido.	La Oficina de Infraestructura y Soporte Tecnológico (OIST) del MINJUSDH verificará el cumplimiento en el informe mensual que entregará el contratista.
Ítem	Incumplimiento	Penalidad	Procedimiento de Verificación
<b>B</b>	Ataque consolidado de Ransomware que no fue detectado por la solución Sandboxing.	1 UIT, por cada host de usuario final afectado e identificado. 5 UIT, por cada servidor afectado e identificado.	La Oficina de Infraestructura y Soporte Tecnológico (OIST) del MINJUSDH verificará el cumplimiento en el informe mensual que entregará el contratista.
<b>C</b>	Spam, Malware, Phishing que no fue detectado por la Solución de Protección de Correo electrónico (Antispam)	1 UIT, por cada host de usuario final afectado e identificado.	La Oficina de Infraestructura y Soporte Tecnológico (OIST) del MINJUSDH verificará el cumplimiento en el informe mensual que entregará el contratista.
<b>D</b>	Ataque de Denegación de Servicio que no fue detectado por la Protección AntiDDos Perimetral no Volumétrico	1 UIT, por cada hora que se tenga la indisponibilidad de los servicios del MINJUSDH	La Oficina de Infraestructura y Soporte Tecnológico (OIST) del MINJUSDH verificará el cumplimiento en el informe mensual que entregará el contratista.

- **Penalidad por Incumplimiento del plazo de presentación del Plan de Trabajo.**

Ítem	Incumplimiento	Penalidad	Procedimiento de Verificación
<b>A</b>	Por no presentar el Plan de Trabajo dentro del plazo requerido en los TDR.	2 UIT, por cada día de retraso.	La Oficina de Infraestructura y Soporte Tecnológico (OIST) del MINJUSDH debe verificar y controlar los días de exceso del plazo para la presentación del plan de trabajo.

- **Penalidad por el Incumplimiento de los plazos de ejecución de despliegue o de integración o de cambio de personal o de automatización o de cambio/reemplazo de soluciones, según sea el caso, posterior al inicio de servicio.**

Ítem	Incumplimiento	Penalidad	Procedimiento de Verificación
<b>A</b>	Plazo para ejecutar el cambio de algún personal del CyberSOC > a 30 días.	50% de una UIT por cada día de exceso.	La Oficina de Infraestructura y Soporte Tecnológico (OIST) del MINJUSDH debe verificar y controlar los días de exceso del plazo para el cambio correspondiente.
<b>B</b>	Plazo para reemplazo de una solución on-premise > a 10 días.	50% de una UIT por cada día de exceso.	La Oficina de Infraestructura y Soporte Tecnológico (OIST) del MINJUSDH debe verificar y controlar los días de exceso del plazo para el reemplazo de la solución correspondiente.

Ítem	Incumplimiento	Penalidad	Procedimiento de Verificación
C	Plazo para reemplazo de una solución en nube > a 3 días.	50% de una UIT por cada día de exceso.	La Oficina de Infraestructura y Soporte Tecnológico (OIST) del MINJUSDH debe verificar y controlar los días de exceso del plazo para el reemplazo de la solución correspondiente.

• **Penalidad por la prestación accesoria: Incumplimiento por la capacitación.**

Ítem	Incumplimiento	Penalidad	Procedimiento de Verificación
A	Inicio o término del(os) curso(s) oficial(es) después del plazo estipulado.	2 UIT por cada día de retraso.	La Oficina de Infraestructura y Soporte Tecnológico (OIST) del MINJUSDH debe verificar y controlar los días de exceso del plazo para impartir y/o culminar la capacitación.
B	Por no presentar los certificados de la capacitación dentro del plazo requerido en los TDR.	1 UIT por cada día de retraso.	La Oficina de Infraestructura y Soporte Tecnológico (OIST) del MINJUSDH debe verificar y controlar los días de exceso del plazo para la entrega de los certificados de la capacitación.

• **Penalidad por el Incumplimiento en la entrega de los Informes mensuales.**

Ítem	Incumplimiento	Penalidad	Procedimiento de Verificación
A	Si el contratista demora más de siete (07) días en la entrega de los informes mensuales.	10% de una UIT por cada día de retraso.	La Oficina de Infraestructura y Soporte Tecnológico (OIST) del MINJUSDH debe verificar y controlar el cumplimiento del plazo de entrega del informe mensual.

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

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

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

**CLÁUSULA DÉCIMA CUARTA: RESOLUCIÓN DEL CONTRATO**

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

**CLÁUSULA DÉCIMA QUINTA: RESPONSABILIDAD DE LAS PARTES**

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

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

**CLÁUSULA DÉCIMA SEXTA: ANTICORRUPCIÓN**

EL CONTRATISTA declara y garantiza no haber, directa o indirectamente, o tratándose de una persona jurídica a través de sus socios, integrantes de los órganos de administración, apoderados,



representantes legales, funcionarios, asesores o personas vinculadas a las que se refiere el artículo 7 del Reglamento de la Ley de Contrataciones del Estado, ofrecido, negociado o efectuado, cualquier pago o, en general, cualquier beneficio o incentivo ilegal en relación al contrato.

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

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

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

#### **CLÁUSULA DÉCIMA SÉTIMA: MARCO LEGAL DEL CONTRATO**

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

#### **CLÁUSULA DÉCIMA OCTAVA: SOLUCIÓN DE CONTROVERSIAS<sup>12</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.

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 arbitraje será resuelto a través de un Tribunal Arbitral, conformado por tres (3) árbitros, proponiéndose a los efectos administrativos las siguientes instituciones arbitrales y respetándose el orden de prelación que se establece a continuación:

1. Centro de Análisis y Resolución de Conflictos de la Pontificia Universidad Católica del Perú.
2. Centro de Arbitraje en la Cámara de Comercio de Lima.
3. Centro de Análisis y Resolución de Disputas del Colegio de Ingenieros del Perú.

Se precisa que, una vez cualquiera de las partes elija iniciar el acto arbitral, ante los centros de arbitrajes señalados, se deberá de continuar con las posteriores controversias en el mismo centro.

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

#### **CLÁUSULA DÉCIMA NOVENA: FACULTAD DE ELEVAR A ESCRITURA PÚBLICA**

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

#### **CLÁUSULA VIGÉSIMA: DOMICILIO PARA EFECTOS DE LA EJECUCIÓN CONTRACTUAL**

---

<sup>12</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).

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

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

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

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

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

---

"LA ENTIDAD"

---

"EL CONTRATISTA"

#### **Importante**

*Este documento puede firmarse digitalmente si ambas partes cuentan con firma digital, según la Ley N° 27269, Ley de Firmas y Certificados Digitales<sup>13</sup>.*

---

<sup>13</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



**ANEXO N° 1**

**DECLARACIÓN JURADA DE DATOS DEL POSTOR**

Señores  
**COMITÉ DE SELECCIÓN**  
**CONCURSO PÚBLICO N° 003-2025-JUS**  
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>14</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>15</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>14</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.

<sup>15</sup> Consignar en el caso de procedimientos de selección por relación de ítems, cuando el monto del valor estimado del ítem no supere los doscientos mil Soles (S/ 200 000.00), cuando se haya optado por perfeccionar el contrato con una orden de servicios.

**Importante**

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

**ANEXO N° 1**

**DECLARACIÓN JURADA DE DATOS DEL POSTOR**

Señores

**COMITÉ DE SELECCIÓN**

**CONCURSO PÚBLICO N°003-2025-JUS**

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>16</sup>		Sí	No	
Correo electrónico :				

Datos del consorciado 2				
Nombre, Denominación o Razón Social :				
Domicilio Legal :				
RUC :	Teléfono(s) :			
MYPE <sup>17</sup>		Sí	No	
Correo electrónico :				

Datos del consorciado ...				
Nombre, Denominación o Razón Social :				
Domicilio Legal :				
RUC :	Teléfono(s) :			
MYPE <sup>18</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:

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.

<sup>16</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. Para dicho efecto, todos los integrantes del consorcio deben acreditar la condición de micro o pequeña empresa.

<sup>17</sup> Ibídem.

<sup>18</sup> Ibídem.

4. Solicitud para presentar los documentos para perfeccionar el contrato, según orden de prelación, de conformidad con lo previsto en el artículo 141 del Reglamento.
5. Respuesta a la solicitud de acceso al expediente de contratación.
6. Notificación de la orden de servicios<sup>19</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>19</sup> Consignar en el caso de procedimientos de selección por relación de ítems, cuando el monto del valor estimado del ítem no supere los doscientos mil Soles (S/ 200 000.00), cuando se haya optado por perfeccionar el contrato con una orden de servicios.

## ANEXO N° 2

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

Señores  
**COMITÉ DE SELECCIÓN**  
**CONCURSO PÚBLICO N°003-2025-JUS**  
Presente.-

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

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

[CONSIGNAR CIUDAD Y FECHA]

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

#### **Importante**

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



### ANEXO N° 3

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

Señores

**COMITÉ DE SELECCIÓN**

**CONCURSO PÚBLICO N°003-2025-JUS**

Presente.-

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

[CONSIGNAR CIUDAD Y FECHA]

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

#### **Importante**

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

## ANEXO N° 4

### DECLARACIÓN JURADA DE PLAZO DE PRESTACIÓN DEL SERVICIO

Señores  
**COMITÉ DE SELECCIÓN**  
**CONCURSO PÚBLICO N°003-2025-JUS**  
Presente.-

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

#### **Plazo de Prestación Principal:**

- El plazo de entrega del Plan de Trabajo del servicio, es de hasta veinte (20) días calendario contados a partir del día siguiente de la suscripción del contrato.
- El plazo de implementación del servicio será de hasta noventa (90) días calendario contados a partir del día siguiente de aprobado el plan de trabajo.
- El plazo de la prestación del servicio es por treinta y seis (36) meses, contados a partir del día siguiente de la fecha de suscripción del acta de Conformidad por la implementación del servicio.

#### **Plazo de Prestación Accesorio:**

- Capacitación: la prestación de este servicio es de sesenta días (60) calendarios, contados a partir del día siguiente de la suscripción del acta de Conformidad por la implementación del servicio.

[CONSIGNAR CIUDAD Y FECHA]

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

## ANEXO N° 5

### PROMESA DE CONSORCIO

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

Señores

**COMITÉ DE SELECCIÓN**

**CONCURSO PÚBLICO N°003-2025-JUS**

Presente.-

Los suscritos declaramos expresamente que hemos convenido en forma irrevocable, durante el lapso que dure el procedimiento de selección, para presentar una oferta conjunta al **CONCURSO PÚBLICO N° [CONSIGNAR NOMENCLATURA DEL PROCEDIMIENTO]**.

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>20</sup>

[DESCRIBIR LAS OBLIGACIONES DEL CONSORCIADO 1]

2. OBLIGACIONES DE [NOMBRE, DENOMINACIÓN O RAZÓN SOCIAL DEL CONSORCIADO 2] [ % ]<sup>21</sup>

[DESCRIBIR LAS OBLIGACIONES DEL CONSORCIADO 2]

TOTAL OBLIGACIONES

100%<sup>22</sup>

[CONSIGNAR CIUDAD Y FECHA]

<sup>20</sup> Consignar únicamente el porcentaje total de las obligaciones, el cual debe ser expresado en número entero, sin decimales.

<sup>21</sup> Consignar únicamente el porcentaje total de las obligaciones, el cual debe ser expresado en número entero, sin decimales.

<sup>22</sup> Este porcentaje corresponde a la sumatoria de los porcentajes de las obligaciones de cada uno de los integrantes del consorcio.

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

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

**Importante**

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



## ANEXO N° 6

### PRECIO DE LA OFERTA

Señores  
**COMITÉ DE SELECCIÓN**  
**CONCURSO PÚBLICO N°003-2025-JUS**  
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
<b>PRESTACIÓN PRINCIPAL</b> (Servicio de Gestión de Ciberseguridad Perimetral)	
<b>PRESTACIÓN ACCESORIA</b> (Capacitación)	
<b>TOTAL</b>	

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

[CONSIGNAR CIUDAD Y FECHA]

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

#### Importante

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

- “El postor debe detallar en el precio de su oferta, el monto correspondiente a la prestación principal y las prestaciones accesorias”.**

## ANEXO N° 8

### EXPERIENCIA DEL POSTOR EN LA ESPECIALIDAD

Señores  
**COMITÉ DE SELECCIÓN**  
**CONCURSO PÚBLICO N°003-2025-JUS**  
Presente.-

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

Nº	CLIENTE	OBJETO DEL CONTRATO	N° CONTRATO / O/S / COMPROBANTE DE PAGO	FECHA DEL CONTRATO O CP <sup>23</sup>	FECHA DE LA CONFORMIDAD DE SER EL CASO <sup>24</sup>	EXPERIENCIA PROVENIENTE <sup>25</sup> DE:	MONEDA	IMPORTE <sup>26</sup>	TIPO DE CAMBIO VENTA <sup>27</sup>	MONTO FACTURADO ACUMULADO <sup>28</sup>
1										
2										
3										
4										

<sup>23</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>24</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 periodo.

<sup>25</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>26</sup> Se refiere al monto del contrato ejecutado incluido adicionales y reducciones, de ser el caso.

<sup>27</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>28</sup> Consignar en la moneda establecida en las bases.

Nº	CLIENTE	OBJETO DEL CONTRATO	N° CONTRATO / O/S / COMPROBANTE DE PAGO	FECHA DEL CONTRATO O CP <sup>23</sup>	FECHA DE LA CONFORMIDAD DE SER EL CASO <sup>24</sup>	EXPERIENCIA PROVENIENTE <sup>25</sup> DE:	MONEDA	IMPORTE <sup>26</sup>	TIPO DE CAMBIO VENTA <sup>27</sup>	MONTO FACTURADO ACUMULADO <sup>28</sup>
5										
6										
7										
8										
9										
10										
	...									
20										
TOTAL										

[CONSIGNAR CIUDAD Y FECHA]

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

## ANEXO N° 9

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

Señores  
**COMITÉ DE SELECCIÓN**  
**CONCURSO PÚBLICO N°003-2025-JUS**  
Presente.-

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

[CONSIGNAR CIUDAD Y FECHA]

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

#### **Importante**

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

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



**ANEXO N° 12**

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

**(DOCUMENTO A PRESENTAR EN EL PERFECCIONAMIENTO DEL CONTRATO)**

Señores  
**COMITÉ DE SELECCIÓN**  
**CONCURSO PÚBLICO N°003-2025-JUS**  
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.*