

# 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 Izquierda: 2.5 cm Inferior: 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°  
002-2025-CR**

**CONTRATACIÓN DE SERVICIO DE SUSCRIPCIÓN PARA  
UNA PLATAFORMA DE CORRELACIONADOR DE  
EVENTOS (SIEM) Y CYBER SOC DELEGADA TIPO SOAR  
PARA EL MONITOREO, PREVENCIÓN, DETECCIÓN Y  
RESPUESTA ANTE INCIDENTES CIBERNÉTICOS CON  
SEGURIDAD GESTIONADA PARA EL CONGRESO DE LA  
REPUBLICA**

## 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*

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

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

### 1.8. PRESENTACIÓN Y APERTURA DE OFERTAS

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

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

#### Importante

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

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

### 1.9. EVALUACIÓN DE LAS OFERTAS

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

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

### 1.10. CALIFICACIÓN DE OFERTAS

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

### 1.11. SUBSANACIÓN DE LAS OFERTAS

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

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

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

### 1.12. RECHAZO DE LAS OFERTAS

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



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

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

#### 1.13. OTORGAMIENTO DE LA BUENA PRO

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

#### 1.14. CONSENTIMIENTO DE LA BUENA PRO

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

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

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

##### Importante

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

## CAPÍTULO II SOLUCIÓN DE CONTROVERSIAS DURANTE EL PROCEDIMIENTO DE SELECCIÓN

### 2.1. RECURSO DE APELACIÓN

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

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

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

#### Importante

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

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

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

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

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

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

### CAPÍTULO III DEL CONTRATO

#### 3.1. PERFECCIONAMIENTO DEL CONTRATO

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

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

#### 3.2. GARANTÍAS

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

##### 3.2.1. GARANTÍA DE FIEL CUMPLIMIENTO

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

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

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

##### Importante

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

##### 3.2.3. GARANTÍA POR ADELANTO

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

### 3.3. REQUISITOS DE LAS GARANTÍAS

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

#### Importante

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

#### Advertencia

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

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

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

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

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

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

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

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

### 3.4. EJECUCIÓN DE GARANTÍAS

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

### 3.5. ADELANTOS

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

### 3.6. PENALIDADES

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

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

#### 3.6.2. OTRAS PENALIDADES

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

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

### 3.7. INCUMPLIMIENTO DEL CONTRATO

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

### 3.8. PAGOS

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

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

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

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

#### **Advertencia**

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

### 3.9. DISPOSICIONES FINALES

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

## **SECCIÓN ESPECÍFICA**

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

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

## CAPÍTULO I GENERALIDADES

### 1.1. ENTIDAD CONVOCANTE

Nombre : CONGRESO DE LA REPUBLICA  
RUC N° : 20161749126  
Domicilio legal : Jr. Huallaga N°358 – Lima  
Teléfono: : 01 317 7777 – Anexo 6680  
Correo electrónico: : jcisneros@congreso.gob.pe; atroncos@congreso.gob.pe;  
llopez@congreso.gob.pe

### 1.2. OBJETO DE LA CONVOCATORIA

El presente procedimiento de selección tiene por objeto la contratación del servicio de **SERVICIO DE SUSCRIPCIÓN PARA UNA PLATAFORMA DE CORRELACIONADOR DE EVENTOS (SIEM) Y CYBER SOC DELEGADA TIPO SOAR PARA EL MONITOREO, PREVENCIÓN, DETECCIÓN Y RESPUESTA ANTE INCIDENTES CIBERNÉTICOS CON SEGURIDAD GESTIONADA PARA EL CONGRESO DE LA REPUBLICA**, en base a los siguientes destinos y cantidades referenciales:

### 1.3. EXPEDIENTE DE CONTRATACIÓN

El expediente de contratación fue aprobado mediante **Formato 02 N°003-2025-DGA-CR** el 31 de enero 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:

**El plazo para la ejecución del servicio es de setecientos treinta (730) días calendarios, contados a partir del día siguiente de la implementación del servicio.**

**El plazo máximo para la implementación del servicio será de treinta (30) días calendario, contados desde el día siguiente de la firma del contrato. Este proceso deberá concluir con la suscripción de un acta de culminación de implementación, documento que marcará el inicio oficial del período de ejecución del servicio, conforme a los plazos establecidos.**

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, en forma gratuita, en Jr. Ancash N°569- Edificio Hospicio Ruiz Dávila – Cercado de Lima.

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

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

### 1.10. BASE LEGAL

- Ley de Presupuesto del Sector Público para el Año Fiscal 2025.
- Ley de Equilibrio Financiero del Presupuesto del Sector Público del año fiscal 2025.
- Ley del Endeudamiento del Sector Público del año fiscal 2025.
- Ley N°27806.- Ley de Transparencia y Acceso a la Información Pública.
- Texto Único Ordenado de la Ley N°30225, Ley de Contrataciones del Estado. Aprobado mediante Decreto Supremo N°082-2019-EF.
- Decreto Supremo N°344-2018-EF, que aprueba el Reglamento de la Ley N° 30225 - Ley de Contrataciones del Estado; y, sus modificatorias.
- Directivas, Pronunciamientos, Opiniones, y Comunicados del Organismo Supervisor de Contrataciones del Estado.

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



## CAPÍTULO II DEL PROCEDIMIENTO DE SELECCIÓN

### 2.1. CALENDARIO DEL PROCEDIMIENTO DE SELECCIÓN

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

#### Importante

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

### 2.2. CONTENIDO DE LAS OFERTAS

La oferta contendrá, además de un índice de documentos<sup>2</sup>, la siguiente documentación:

#### 2.2.1. Documentación de presentación obligatoria

##### 2.2.1.1. Documentos para la admisión de la oferta

- Declaración jurada de datos del postor. (Anexo N° 1)
- 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.*

- Declaración jurada de acuerdo con el literal b) del artículo 52 del Reglamento. (Anexo N° 2)
- 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) Catálogos y/o brochure y/o folletería y/o instructivos y/o ficha técnica y/o manuales y/o capturas de pantalla de las plataformas en funcionamiento.

Las características principales a verificar serán las siguientes:

Compatibilidad con sistemas operativos especificados, integración con fuentes de datos de seguridad (firewalls, antivirus, correo, directorio activo, componentes de red), autenticación de dos factores (2FA), protocolos de comunicación segura, aislamiento del agente (sin conexiones entrantes ni control remoto), coadministración basada en roles (propietario, visualizador, resolutor de incidentes), capacidades avanzadas de detección y respuesta (SOAR) integradas con MITRE ATT&CK, reducción de la superficie de ataque mediante pruebas de penetración y priorización de vulnerabilidades, monitoreo 24x7 de eventos de seguridad con alertas en tiempo real, respuesta automatizada a incidentes (aislamiento de hosts comprometidos, remediación de amenazas), certificaciones internacionales (ISO/IEC 27001, 27017, 27018, CSA STAR, SOC 3), generación de reportes (inventario, vulnerabilidades, eventos detectados), modalidad SaaS desde un SOC Data Center certificado, capacidad de análisis predictivo mediante Cyber Threat Intelligence (dark web, día 0/1 día), cumplimiento de normativas internacionales (ISO, NIST, STIG).

- f) Declaración jurada de plazo de prestación del servicio. **(Anexo N° 4)**<sup>4</sup>
- g) Promesa de consorcio con firmas legalizadas, de ser el caso, en la que se consigne los integrantes, el representante común, el domicilio común y las obligaciones a las que se compromete cada uno de los integrantes del consorcio, así como el porcentaje equivalente a dichas obligaciones. **(Anexo N° 5)**
- h) El precio de la oferta en **SOLES**. Adjuntar obligatoriamente el **Anexo N° 6**.

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

#### Importante

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

#### 2.2.1.2. Documentos para acreditar los requisitos de calificación

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

#### Advertencia

El comité de selección no podrá exigir al postor la presentación de documentos que no hayan sido indicados en los acápites "**Documentos para la admisión de la oferta**", "**Requisitos de calificación**" y "**Factores de evaluación**".

#### 2.3. REQUISITOS PARA PERFECCIONAR EL CONTRATO

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

<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.

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

#### Advertencia

*De acuerdo con el artículo 4 del Decreto Legislativo N° 1246, las Entidades están prohibidas de exigir a los administrados o usuarios la información que puedan obtener directamente mediante la interoperabilidad a que se refieren los artículos 2 y 3 de dicho Decreto Legislativo. En esa medida, si la Entidad es usuaria de la Plataforma de Interoperabilidad del Estado – 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).*

- f) Domicilio para efectos de la notificación durante la ejecución del contrato.
- g) Autorización de notificación de la decisión de la Entidad sobre la solicitud de ampliación de plazo mediante medios electrónicos de comunicación<sup>6</sup> (Anexo N° 12).
- h) Detalle de los precios unitarios del precio ofertado<sup>7</sup>.
- i) Copias simples de los certificados oficiales emitidos por la entidad autorizada o documentos de designación formal para acreditar contar con al menos 2 certificaciones de soluciones de Ciberseguridad.
- j) Declaración jurada que certifique la disponibilidad de un centro de atención al cliente con servicio continuo (24x7) para acreditar tener un centro de Atención al Cliente 24x7 de tipo call center.
- k) Documento que acredite ser distribuidor autorizado de la solución ofertada.
- l) Documentos solicitados al personal propuesto en el cargo de **Jefe de Proyectos**:
  - Certificación vigente en gestión de proyectos PMP o Scrum Master Certified
  - Certificación en Ciberseguridad Lead Cybersecurity Professional Certificate (LCSPC).
- m) Documentos solicitados al personal propuesto en el cargo de **Operador de Servicio**:
  - Certificación técnica vigente en CEH V12 - Certified Ethical Hacker

#### Importante

- *En caso que el postor ganador de la buena pro sea un consorcio, las garantías que presente este para el perfeccionamiento del contrato, así como durante la ejecución contractual, de ser el caso, además de cumplir con las condiciones establecidas en el artículo 33 de la Ley y el artículo 148 del Reglamento, deben consignar expresamente el nombre completo o la denominación o razón social de los integrantes del consorcio, en calidad de garantizados, de lo contrario no podrán ser aceptadas por las Entidades. No se cumple el requisito antes indicado si se consigna únicamente la denominación del consorcio, conforme lo dispuesto en la Directiva "Participación de Proveedores en Consorcio en las Contrataciones del Estado".*
- *En los contratos periódicos de prestación de servicios en general que celebren las Entidades con las micro y pequeñas empresas, estas últimas pueden otorgar como garantía de fiel cumplimiento el diez por ciento (10%) del monto del contrato, porcentaje que es retenido por la Entidad durante la primera mitad del número total de pagos a realizarse, de forma prorrateada en cada pago, con cargo a ser devuelto a la finalización del mismo, conforme lo establece el numeral 149.4 del artículo 149 del Reglamento y numeral 151.2 del artículo 151 del Reglamento. Para dicho efecto los postores deben encontrarse registrados en el REMYPE, consignando en la Declaración Jurada de Datos del Postor (Anexo N° 1) o en la*

<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.

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>8</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 la Mesa de Partes Virtual de la Entidad (<https://wb2server.congreso.gob.pe/mpvirtual/>) o en la Mesa de Partes Presencial, ubicada en Av. Andahuaylas cuadra 4, Cercado de Lima. En caso requiera presentar documentos originales (carta fianza u otros), deberá necesariamente presentar a través de mesa de partes física y dentro de los plazos legales.

#### Importante

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

## 2.5. FORMA DE PAGO

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

El pago se efectuará en tres (03) armadas después de emitida la conformidad por parte del Área de Infraestructura Tecnológica y refrendado por el Departamento de Tecnologías de la Información, efectuándose según siguiente detalle:

<sup>8</sup> Según lo previsto en la Opinión N° 009-2016/DTN.

Pago	Porcentaje de pago	Condición de pago
1	40% del monto total de la prestación	A la conformidad del Primer Entregable.
2	30% del monto total de la prestación	A la conformidad del Segundo Entregable.
3	30% del monto total de la prestación	A la conformidad del Tercer Entregable.

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

- Documento suscrito por el funcionario responsable del Área de Infraestructura Tecnológica del Departamento de Tecnológicas de Información emitiendo la conformidad de la prestación efectuada.
- Comprobante de pago.

Dicha documentación se debe presentar en en la Mesa de Partes Virtual de la Entidad (<https://wb2server.congreso.gob.pe/mpvirtual/>) o en la Mesa de Partes Presencial, ubicada en Av. Andahuaylas cuadra 4, Cercado de Lima.

### CAPÍTULO III REQUERIMIENTO

#### Importante

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

### 3.1. TERMINOS DE REFERENCIA

#### TÉRMINOS DE REFERENCIA

#### SERVICIO DE SUSCRIPCIÓN PARA UNA PLATAFORMA DE CORRELACIONADOR DE EVENTOS (SIEM) Y CYBER SOC DELEGADA TIPO SOAR PARA EL MONITOREO, PREVENCIÓN, DETECCIÓN Y RESPUESTA ANTE INCIDENTES CIBERNÉTICOS CON SEGURIDAD GESTIONADA PARA EL CONGRESO DE LA REPUBLICA

##### 1. DEPENDENCIA QUE REQUIERE EL SERVICIO

Área de Infraestructura Tecnológica del Departamento de Tecnologías de la Información del Congreso de la República.

##### 2. OBJETO DEL SERVICIO

El objeto del servicio es la contratación de una solución de ciberseguridad delegada tipo SOAR para proveer, implementar, administrar y mantener de manera continua capacidades de monitoreo 24x7, prevención, detección, investigación y respuesta a amenazas cibernéticas a través de una plataforma de CYBER SOC delegada, que permita la coadministración de la gestión por parte del equipo del Congreso de la República a fin de asegurar la contención oportuna ante cualquier ataque dirigido y no dirigido sobre servidores y/o activos de misión crítica.

##### 3. FINALIDAD PÚBLICA

La presente contratación de una solución de suscripción de plataforma de CYBER SOC delegada tipo SOAR para el monitoreo, prevención, detección y respuesta ante incidentes cibernéticos con seguridad gestionada para el Congreso de la República permitirá fortalecer las capacidades de vigilancia, detección y respuesta frente a amenazas de seguridad informática, asegurando la integridad y confidencialidad de la información institucional.

##### 4. VINCULACIÓN CON EL PLAN OPERATIVO INSTITUCIONAL

CÓDIGO	ACTIVIDAD OPERATIVA
202504025160307	Implementación del plan de adquisición de equipamiento para la renovación de la infraestructura tecnológica, en el marco del Plan de Gobierno Digital.

##### 5. NORMATIVA

La implementación de la solución de suscripción de plataforma de CYBER SOC delegada tipo SOAR para el monitoreo, prevención, detección y respuesta ante incidentes cibernéticos con seguridad gestionada para el Congreso de la República deberá realizarse en estricto cumplimiento de las disposiciones legales y normas técnicas vigentes aplicables. Estas normativas incluyen, pero no se limitan a, las siguientes: ISO/IEC 27001:2022, 27017:2015, 27018:2019, 27701:2019, 22301:2019, 20000-1:2018, 9001:2015 y CSA STAR CCM V4.0.

##### 6. ANTECEDENTES

El Departamento de Tecnologías de la Información tiene a su cargo la gestión de los Centros de Datos del Congreso de la República ubicado en el Edificio Luis Alberto Sánchez y en Palacio Legislativo.

- Así mismo, existen diversas observaciones al estado actual de los Centros de Datos mencionados, lo cual fue evidenciado en la Carta de Control Interno de la Auditoría a los Estados Financieros y Presupuestales al 31 de diciembre de 2022.



CONGRESO  
REPUBLICA

**AREA DE INFRAESTRUCTURA TECNOLÓGICA**

Decenio de la Igualdad de Oportunidades para Mujeres y Hombres  
Año de la recuperación y consolidación de la economía peruana

- Esta situación ha evidenciado falencias en la planificación y gestión de la vigilancia, detección y respuestas ante incidentes o amenazas de seguridad informática, asegurando la integridad y confidencialidad de la información institucional. Tales deficiencias ponen en riesgo la continuidad operativa, la seguridad de los datos críticos y limitan la capacidad de respuesta y expansión tecnológica del Congreso de la República.
- Frente a estos desafíos, es crucial alcanzar la certificación de los Centros de Datos bajo las normas ISO 27001:2022, NTP/ISO N° 22237 y ANSI/ITIA 942. Este proceso incluirá un rediseño acorde a las especificaciones técnicas de estos estándares internacionales y una validación final para garantizar operaciones alineadas con las mejores prácticas internacionales.
- Debido al exponencial incremento del cibercrimen y amplia variedad de nuevas amenazas cibernéticas, tales como ataques masivos de ransomware, estafas de phishing, robo de información, robo de credenciales, ataques dirigidos y más, el Congreso de la República viene integrándose en un proceso de mejoramiento continuo de sus actividades, encaminándose a la transformación digital. Es por ello por lo que parte de uno de los lineamientos de la gestión, es la ciberseguridad. El Congreso de la República necesita garantizar que sus activos de información no se vean afectados por alguna amenaza cibernética externa o interna, es por esto, que se requiere contratar la suscripción de una plataforma de CYBER SOC delegada, que permita realizar un monitoreo y correlacionamiento continuo de eventos de seguridad, a fin de PREVENIR, DETECTAR y RESPONDER ante cualquier incidente cibernético, a través de una plataforma de CYBER SOC que permita delegar las actividades propias de una gestión proactiva en ciberseguridad a un equipo de profesionales con un seguimiento activo 24x7.

**7. CARACTERÍSTICAS DEL SERVICIO A REALIZAR**

La plataforma deberá cubrir la seguridad, correlacionamiento de eventos de seguridad, detección y respuesta ante incidentes tipo SOAR para la totalidad de los servidores de misión crítica y determinados activos estratégicos, brindando a través de una plataforma de CYBER SOC delegada la coadministración de los eventos de seguridad de la institución la deberá ejecutarse por un periodo de setecientos treinta (730) calendario garantizando el MONITOREO 24X7X360, la DETECCIÓN y RESPUESTA EFECTIVA ante ataques cibernéticos sobre un total de 100 SERVIDORES (Físicos y Virtuales), integrando las fuentes necesarias (antivirus, antispam, correo, firewalls y/o componentes de red) para mejorar la tasa de detección y respuesta.

**7.1. ARQUITECTURA DE LA PLATAFORMA DE DETECCIÓN Y RESPUESTA**

- El fabricante de la plataforma ofertada de Cyber SOC debe adjuntar reporte de auditoría de tipo SOC 3 para los productos de detección y respuesta ofertados. La plataforma de Cyber SOC delegada debe ser provista en modalidad de Software as a Service (SaaS) desde un SOC Data Center que cuente con infraestructura certificada en conformidad con las normas ISO/IEC 27001:2022, 27017:2015, 27018:2019, 27701:2019, 22301:2019, 20000-1:2018, 9001:2015 y CSA STAR CCM v4.0.
- La plataforma deberá soportar mínimamente las siguientes plataformas de sistemas operativos Windows Server 2012 R2 (32-bit / 64-bit), Windows Server 2016 / 2019 (32-bit / 64-bit), Windows Server 2022 (32-bit / 64-bit), CentOS 7 and greater, Red Hat 8 and 9.
- La plataforma debe presentarse como un sistema integrado tipo SOAR integrando tecnologías y plataformas requeridas que se gobiernen desde una sola consola de orquestación automatizada con acceso basado en roles que permita la COADMINISTRACIÓN por parte del equipo del Congreso de la República.

Edificio Julia Alberto Sánchez Sánchez,  
Jr. Huallaga N° 358 - Of. 220 - Lima, Perú  
Central Telefónica: 311-7777

www.congreso.gob.pe



**ÁREA DE INFRAESTRUCTURA TECNOLÓGICA**

Decenio de la Igualdad de Oportunidades para Mujeres y Hombres  
Año de la Recuperación y Consolidación de la economía peruana

- La plataforma debe proveer capacidades de detección y respuesta administrada a través del equipo del fabricante permitiendo la eficiencia y efectividad del proceso.

La plataforma base tipo SOAR debe permitir la integración con la infraestructura de TI y seguridad existente, logrando que la plataforma administrada por el equipo de analistas de SOC del fabricante identifique rápidamente actividades maliciosas y sospechosas en los principales vectores de amenazas críticas: endpoint, red y nube, para brindar una defensa avanzada contra ciberamenazas las 24 horas, los 7 días de la semana durante el tiempo que dure la suscripción.

La plataforma deberá trabajar preferentemente sobre un esquema basado en agente, el cual sólo demande del acceso seguro a una plataforma de Cyber SOC gestionada la cual opere desde un Data Center en la nube.

- La plataforma debe proporcionar una capacidad segura, liviana y fácil de implementar para capturar la telemetría de seguridad desde los puntos finales a través de un agente ligero que no supere los ocho (08) MB de tamaño a fin de que el equipo de profesionales que trabaja en el SOC Data Center clasifique, correlacione y registre datos de forma eficiente y efectiva.

La plataforma debe garantizar la seguridad de la información del activo protegido a través de la configuración de un agente que no pueda aceptar conexión entrante, que no sea compatible con el control remoto, ni con la capacidad de ejecutar contenido generado por el usuario en endpoints (puntos finales) o servidores.

La plataforma debe garantizar la seguridad de las comunicaciones usando el protocolo TLS v1.2 permitiendo solo los siguientes conjuntos de cifrado fuertes:

- o TLS\_ECDHE\_RSA\_WITH\_CHACHA20\_POLY1305\_SHA256,
- o TLS\_ECDHE\_RSA\_WITH\_AES\_128\_GCM\_SHA256,
- o TLS\_ECDHE\_RSA\_WITH\_AES\_256\_GCM\_SHA384,
- o TLS\_RSA\_WITH\_AES\_128\_GCM\_SHA256,
- o TLS\_RSA\_WITH\_AES\_256\_GCM\_SHA384

La plataforma debe admitir la autenticación de dos factores (2FA) para salvaguardar el acceso a la consola.

- La plataforma debe permitir la coadministración efectiva por parte del Congreso de la República a través de la integración de un sistema de acceso basado en roles considerando mínimamente:

- o Rol de propietario, habilitando control total sobre la plataforma
- o Rol visualizador, habilitando funciones de seguimiento y generación de informes sobre todos los eventos generados y procesados
- o Rol resolutor de incidentes, habilitando funciones de seguimiento, generación de informes, aislamiento y liberación de host afectados.

- La plataforma debe poder definir una relación de usuarios que serán notificados a través de correo electrónico y/o vía telefónica específicamente sobre:

- o Amenazas críticas o emergencias en el momento que ocurren
- o Instrucciones de remediación y/o fortalecimiento de configuraciones
- o Advertencia y/o detección de vulnerabilidades y/o riesgos latentes

La plataforma debe integrar capacidades de SIEM Less para el monitoreo y correlacionamiento de eventos de seguridad de hosts, firewalls, antivirus, directorio activo, correo electrónico y/o componentes de red, incorporando la detección de infracciones basadas en las técnicas de Mitre Attack, la actividad y los servicios de la red, las herramientas sospechosas y la detección de archivos maliciosos para brindar una solución de seguridad integral.

La plataforma debe contar con una aplicación que brinde la posibilidad de recopilar y analizar eventos en CEF (formato de evento común) y LEEF (formato extendido de evento de registro) a través de Syslog.

- La plataforma debe tener una arquitectura multitenant que le permita crear instancias de gobierno independiente asignadas a usuarios clave dentro de la organización.

Edificio Luis Alberto Sánchez Sánchez,  
Jr. Huallegua N° 358 - Of. 220 - Lima, Perú  
Central Telefónica: 3117777

www.congreso.gob.pe





#### ÁREA DE INFRAESTRUCTURA TECNOLÓGICA

“Decenio de la Igualdad de Oportunidades para Mujeres y Hombres”  
“Año de la recuperación y consolidación de la economía peruana”

- La plataforma debe permitir crear reportes bajo demanda y programarlos para su envío automático al correo electrónico.
- La plataforma debe permitir la creación de informes de inventario e informes ejecutivos hasta con una antigüedad de noventa (90) días.

#### 7.2. CAPACIDADES DE DETECCIÓN Y RESPUESTA DE CIBERATAQUES

- La plataforma de Cyber SOC debe integrar a través del agente capacidades de detección avanzada de infracciones reconociendo tácticas, técnicas y procedimientos (TTP) del adversario de acuerdo con el marco MITRE ATT&CK. La plataforma de Cyber SOC deberá estar diseñada específicamente para buscar TTP sobre el dispositivo local Windows, Mac y Linux en varias categorías, incluidas mínimamente descubrimiento, persistencia, evasión de defensa, ejecución, acceso a credenciales, escalada de privilegios y movimiento lateral.
- La plataforma de Cyber SOC deben incluir funciones de búsqueda a través de sistemas de cacería de amenazas avanzadas y feeds de búsqueda de inteligencia de amenazas automatizadas considerando mínimamente las siguientes metodologías de prueba de búsqueda de amenazas como: Browser visit, DNS Cache Entry, Driver File Hash, Driver File Name, File Hash, File Name, Event in log source, Event in log category, Event ID in log, Event type in log, Service state, User Account, Network connection, Process Hash, Process Name, Registry Key y YARA rules.  
La plataforma deberá mapear conexiones de red entrantes y salientes las cuales deberán ser registradas y analizadas para detectar amenazas en la red. La actividad maliciosa se identificará evaluando el puerto utilizado, la reputación y la geolocalización de la dirección IP y otras atribuciones disponibles.
- La plataforma deberá detectar ransomware verificando el sistema local en busca de actividades de cifrado permitiendo a los usuarios eliminar el proceso infractor o aislar el host afectado automáticamente, deteniendo los ataques de ransomware inmediatamente después de la detección.  
La plataforma deberá contar con un monitor de registro de eventos de punto final logrando ingerir los eventos relacionados con la seguridad escritos en el registro de eventos pudiendo agregar identificadores de eventos personalizados para monitorear aplicaciones personalizadas.
- La plataforma deberá contar con la capacidad de analizar registros de firewall enviando datos a Data Center SOC a través de Syslog para monitorear los eventos de seguridad registrados, la integración deberá realizarse a nivel de API.
- La plataforma debe integrar capacidades de detección de indicadores de compromiso (IoC), esta aplicación deberá ejecutar detecciones seleccionadas por el equipo del Data Center SOC a través de su equipo de investigación de amenazas y se puede actualizar según sea necesario sin que el administrador o el usuario deban realizar ninguna acción.
- La plataforma debe presentar un entorno de trabajo colaborativo evidenciando los diferentes eventos de detección basados en múltiples fuentes de información sobre amenazas. El Data Center SOC supervisará estas detecciones y las tratará con alta prioridad, y el equipo de investigación de amenazas seguirá supervisando las métricas de detección para ajustar los falsos positivos o los falsos negativos.
- La plataforma debe contar con la capacidad de detectar archivos maliciosos a través de su propio motor de detección de malware desarrollado como parte de la solución integrada, escaneando archivos escritos en el disco o ejecutados en busca de atributos maliciosos para proporcionar redundancia sobre la solución antimalware con la que ya cuenta la institución.
- La plataforma debe contar con la capacidad de detectar servicios de red sospechosos que se ejecutan en servidores y estaciones de trabajo. Si bien existen múltiples servicios de red disponibles para uso legítimo, las detecciones sospechosas se definen como puertos y servicios conocidos que se aprovechan

Edificio Luis Alberto Sánchez Sánchez  
Jr. Hualtaya N° 358 - Of. 220 - Lima, Perú  
Central Telefónica: 311-7737



**ÁREA DE REESTRUCTURA TECNOLÓGICA**

Decreto de la Iguz  
Año de la recup

de oportunidades para Mujeres y Hombr  
ción y consolidación de la economía peruana

con fines maliciosos por lo que es de vital importancia la evaluación de cada uno de estos servicios.

La plataforma debe contar con la posibilidad de detectar herramientas sospechosas y/o programas que puedan afectar negativamente la seguridad del sistema y la red. Las herramientas sospechosas detectadas deben investigarse y clasificarse como utilidades de piratería, descifradores de contraseñas u otras herramientas utilizadas por atacantes con fines maliciosos.

- La plataforma debe poder configurarse para habilitar la monitorización de registros de unidades USB (Medios extraíbles) para mapear cuando un dispositivo USB se conecta y se desconecta.

La plataforma debe contar con capacidades de respuesta ante ataques en curso, aislando dispositivos en la red que tengan instalado un agente, el aislamiento del host se realizará como consecuencia de un análisis y/o activación automática de un playbook de respuesta a incidentes para evitar la propagación de código malicioso al impedir que una máquina vulnerada se comuniquen con otros dispositivos de red en internet o la red del cliente. La máquina aislada mantendrá la conectividad con la plataforma correspondiente y permitirá que el Data Center SOC o equipo responsable en la institución reconecten el dispositivo.

- La plataforma debe contar con capacidades de respuesta y remediación a través del agente, logrando ejecutar la eliminación de archivos, eliminación de claves y valores del registro, terminación de procesos, desinstalación de software, parada de servicios, eliminación de tareas programadas.

La plataforma deberá mostrar por cada activo protegido el detalle de las potencias brechas de seguridad en función a la cantidad de eventos maliciosos y eventos sospechosos especificando la telemetría y detalle de cada evento analizado.

- La plataforma deberá mostrar todos los eventos detectados en orden cronológico permitiendo visualizar objetivos, tácticas y técnicas previstas por los atacantes ayudando a interrumpir rápidamente un proceso de ataque reduciendo el tiempo de permanencia, cada evento en el tiempo deberá de mostrar la fecha y hora exacta de la detección, la IP local, el puerto, IP remota el puerto remoto el país y el detalle de la conexión o telemetría del evento.

- La plataforma deberá mostrar información detallada del servidor y/o estación custodiada en línea con información detallada del inventario del activo permitiendo conocer:

- o Configuración del sistema y configuración de red
- o Detalle de los servicios (Nombre, tipo, estado y ubicación)
- o Software instalado (Fabricante, usuario, versión, tamaño y fecha de instalación)
- o Usuarios y sesiones activas
- o Status de aplicación de políticas de contraseñas
- o Recursos compartidos
- o Estado de la red (Netstat) y tabla ARP
- o Status de Update y Upgrade

**7.3. CAPACIDADES DE PREVENCIÓN Y REDUCCIÓN DE SUPERFICIE DE ATAQUE CIBERNETICO**

- La solución propuesta para este escenario tiene por objetivo añadir capacidades de prevención proactiva contra ataques cibernéticos a la plataforma de Cyber SOC delegada a través de la reducción proactiva y continua de la superficie de ataque externa e interna en la entidad.

**7.3.1. GESTIÓN COLABORATIVA Y PRESENTACIÓN DE RESULTADOS DE POSTURA DE SEGURIDAD EN EL TIEMPO**

La reducción de la superficie de ataque se hará efectiva a través de la ejecución de ejercicios de hacking ético, pentesting y la priorización de vulnerabilidades, configuraciones débiles y anomalías.

Edificio Luis Alberto Sánchez Sánchez  
Jr. Huallaga N° 358 - Of. 220 - Lima, Perú  
Central Telefónica: 311-7777

www.congreso.gob.pe



**ÁREA DE INFRAESTRUCTURA TECNOLÓGICA**

Dispositivo de la Igualdad de oportunidades para Mujeres y Hombres  
Año de la recuperación y consolidación de la economía peruana

- La reducción de la superficie de ataque interna y externa deberá ser presentada a través de una plataforma web de entorno colaborativo que permita documentar e interactuar a todos los integrantes del equipo del POSTOR y a los del equipo del Congreso de la República en las tareas de remediación de vulnerabilidades y riesgos, mapeando fechas, tareas y asignaciones.
- La plataforma web utilizada para ejecutar las actividades de reducción de superficie de ataque deberá presentarse en modalidad cloud (SaaS).
- La plataforma deberá permitir documentar la actividad sobre cada vulnerabilidad y/o riesgo cibernético (identificado, permitiendo ingresar y actualizar información referida a la descripción, solución, tipo de vulnerabilidad, nivel de severidad, información adicional, relación con el activo específico afectado, relación con otras vulnerabilidades, actividades realizadas, usuarios responsables de cada actividad, captura de pantalla y/o evidencia de remediación aplicada y cierre o mitigación formal de riesgo).
- La plataforma web utilizada para ejecutar las actividades de reducción de superficie de ataque deberá poder modelar el siguiente proceso para la remediación de las vulnerabilidades detectadas empezando desde la detección de la vulnerabilidad, documentando el informe en la plataforma, asignando tareas específicas de corrección de la vulnerabilidad al equipo del Congreso de la República, soportando consultas, preguntas y soporte a incidentes del equipo del congreso de la República, documentando la corrección y/o remediación aplicada en ambiente de producción, para finalmente cerrar el caso.

**7.3.2. MONITOREO Y REDUCCIÓN CONTINUA DEL NIVEL DE EXPOSICIÓN AL RIESGO EXTERNO**

- La plataforma utilizada deberá permitir la automatización de las pruebas de penetración e identificación de riesgos sobre los activos publicados.
- La plataforma debe estar desarrollada sobre un marco de mejora continua en el tiempo, brindando detalles de las remediaciones, aplicar por cada vulnerabilidad o riesgo asociado al activo.
- La plataforma deberá realizar automáticamente el filtrado de salida para garantizar que la organización esté restringiendo efectivamente el tráfico de salida innecesario, evitando de esta manera que un determinado acceso pueda permitir que un actor malicioso exfiltrar datos del sistema de la organización.
- La plataforma deberá auditar los intentos de autenticación para detectar el uso de credenciales de usuario comprometidas. El objetivo es que, de manera automática, se intente validar dichas credenciales para identificar los accesos y sistemas en los que puedan ser explotadas. Este es un proceso comúnmente utilizado por atacantes y probadores de penetración durante la escalada de privilegios, por lo que resulta crucial que la plataforma ejecute esta validación en primera instancia.
- La plataforma deberá auditar y validar la escalada de privilegios y movimiento lateral usando un conjunto válido de credenciales identificando áreas valiosas dentro de su organización. Esto es llevado a cabo a través de una variedad de métodos y herramientas a fin de poder ejecutar netstat de forma recursiva en múltiples hosts, proporcionando salida y representación visual del flujo de datos (o conexiones de red) dentro del entorno.
- La plataforma deberá poder detectar y documentar la exfiltración de datos a través de la simulación y registro de esta actividad para ayudar al equipo de informática del Congreso de la República para ajustar configuraciones y cerrar brechas de seguridad.
- La plataforma deberá poder hacer uso de acceso elevado e intentar cargar código malicioso en sistemas remotos en un intento de probar la protección de punto final de la organización a fin de afinar los controles antivirus.

Edificio Luis Alberto Sánchez Sánchez  
Jr. Huallaga N° 358 - Of. 220 - Lima, Perú  
Central Telefónica: 3119777

www.congreso.gob.pe



**ÁREA DE INFRAESTRUCTURA TECNOLÓGICA**

Diseño de la infraestructura de oportunidades para Mujeres y Hombres  
Año de la recuperación y consolidación de la economía peruana

- La plataforma deberá poder generar un informe ejecutivo y un informe técnico acerca de una vulnerabilidad y automatizar la prueba de penetración documentando la capacidad de respuesta que se tuvo frente a ésta.
- La plataforma deberá poder configurarse para analizar objetivos externos publicados a internet u objetivos internos como servidores y/o aplicaciones.
- La plataforma deberá presentar informes de penetración y remediación de forma trimestral evidenciando la evolución de los ejercicios.

**7.3.3. MONITOREO Y REDUCCIÓN CONTINUA DEL NIVEL DE EXPOSICIÓN AL RIESGO INTERNO**

- La plataforma deberá ser de tipo SaaS con una arquitectura basada en agente ligero al cual no supere los 20 MB de tamaño para su óptimo desempeño.
- La plataforma deberá implementar una gestión avanzada de vulnerabilidades, configuraciones alineadas a cumplimiento normativo como ISO y NIST además los activos en busca de anomalías.

La plataforma deberá estar basada en la gestión avanzada de vulnerabilidades internas trabajando sobre una metodología de priorización de riesgos SSVC la cual consiste en un sistema que ayuda a analizar las vulnerabilidades para tomar decisiones que contribuyan a prevenir incidentes de seguridad y contener sus consecuencias.

- La plataforma deberá presentar la priorización de vulnerabilidades según su nivel de explotabilidad mínimamente con los siguientes criterios: fácilmente explotable, explotable en la red, explotación pública disponible, explotación con alto movimiento lateral.

- La plataforma deberá tener la capacidad de relacionar las vulnerabilidades con ataques de alta fidelidad, las vulnerabilidades de los kits de explotación que se puedan utilizar para explotar la debilidad. Esto debe permitir predecir un ataque específico arrojando las coordenadas exactas para mitigarlo.

La plataforma deberá contemplar el descubrimiento de activos de TI de forma automática y permitir generar alertas de uso indebido de aplicaciones o software a los responsables.

- La plataforma deberá gestionar de forma integral la corrección de errores de configuración y controles de seguridad para fortalecer los sistemas.

La plataforma deberá identificar, clasificar, distribuir e instalar parches de actualización para mitigar los riesgos de seguridad considerando parches sobre Windows, Linux, macOS y todas las aplicaciones instaladas sobre los hosts tales como navegadores, bases de datos, componentes, etc.

- La plataforma deberá evaluar el cumplimiento normativo mínimamente de NIST CSF, ISO, STIG y SOC-2 a través de la validación que realice el agente instalado sobre los servidores y/o estaciones seleccionadas.

La plataforma debe cubrir mínimamente la siguiente lista de puntos de referencia para su módulo de cumplimiento:

- Tiempo mínimo de la contraseña.
- Permitir estados de espera cuando el equipo o servidor inicio sesión.
- Requerir una contraseña cuando una computadora se activa.
- Criptografía del sistema para el forzado de una fuerte protección de claves para las claves de usuario almacenadas en la computadora.
- La clave debe cumplir los requerimientos de complejidad.
- Desactivar la prevención de ejecución de datos para el ejecutable de ayuda HTML.
- Requerir contraseña al conectarse.
- Habilitar la autenticación del cliente del asignador de extremos de RPC.
- Requerir autenticación de usuario para conexiones remotas mediante autenticación de nivel de red.
- Requerir el uso de inicio rápido.
- Desactivar la prevención de ejecución de datos para Explorer.

Edificio Luis Alberto Sánchez Sánchez,  
Jr. Huayta N° 358 - Of. 220 - Lima, Perú  
Central Telefónica: 311-7777

www.congreso



**ÁREA DE INFRAESTRUCTURA TECNOLÓGICA**

Plano de la igualdad de oportunidades para Mujeres y Hombres  
Año de la recuperación y consolidación de la economía peruana

- o Hacer cumplir el historial de contraseñas.
- o Seguridad de la red: nivel de autenticación de LAN Manager.
- o Control del comportamiento del Registro de eventos cuando el archivo de registro alcanza su tamaño máximo (Seguridad).
- o Inicio de sesión interactivo: límite de inactividad de la máquina.
- o Desactiva las notificaciones de aplicaciones en la pantalla de bloqueo.
- o Permitir el acceso remoto a la interfaz Plug and Play.
- o No procesar la lista de ejecutar una vez para la configuración del equipo.
- o No enumerar usuarios conectados en equipos unidos a un dominio.
- o Umbral de bloqueo de cuenta.
- o Seguridad de red: seguridad de sesión mínima para clientes basados en NTLM SSP (incluido RPC seguro).
- o Acceso a la red: no permitir la enumeración anónima de cuentas y recursos compartidos SAM.
- o No procesar la lista de ejecución heredada para la configuración del equipo.
- o Impedir la instalación de dispositivos extraíbles.
- o Longitud mínima de la contraseña.
- o Criptografía del sistema: use algoritmos compatibles con FIPS para el cifrado, el hash y la firma.
- o Control de cuentas de usuario: eleve solo las aplicaciones de UIAccess que están instaladas en ubicaciones seguras.
- o Acceso a la red: rutas y subrutas de registro accesibles de forma remota.
- o Miembro del dominio: cifre o firme digitalmente los datos del canal seguro (siempre).
- o Control de cuentas de usuario: Comportamiento del aviso de elevación para usuarios estándar.
- o Control de cuentas de usuario: detecte instalaciones de aplicaciones y solicite la elevación.
- o Cuentas: estado de la cuenta de invitado
- o Acceso a la red: restrinja el acceso anónimo a canalizaciones con nombre y recursos compartidos.
- o Acceso a la red: no permitir la enumeración anónima de cuentas SAM.
- o Acceso a la red: no permitir aplicar permisos a usuarios anónimos.
- o Control de cuentas de usuario: ejecute todos los administradores en modo de aprobación de administrador.
- o Control de cuentas de usuario: eleve solo los ejecutables que estén firmados y validados
- La plataforma deberá consolidar y presentar el análisis y búsqueda de vulnerabilidades, configuraciones erróneas alineadas a cumplimiento NIST, anomalías de postura que deriven del uso de procesador, red, memoria, puertos, servicios, usuarios, perfiles, etc. y otros riesgos de seguridad.
- La plataforma debe integrar un módulo que ejecute acciones para alinear políticas de uso de los activos tales como:
  - o Bloquear una aplicación por determinado tiempo.
  - o Permitir la ejecución de aplicaciones en determinados intervalos de tiempo.
  - o Bloquear y determinar el acceso a dispositivos por determinado intervalo de tiempo.
  - o Enviar un script.
  - o Gestionar un proceso.
  - o Gestionar el status de un servicio.
  - o Gestionar un registro.
  - o Instalar o desinstalar una aplicación por determinados periodos de tiempo.
  - o Evaluar la actividad de la red.
  - o Evaluar la transferencia de archivos.
  - o Validar que programas inician sesión.

Edificio Luis Alberto Sánchez Sánchez  
Jr. Huallaga N° 358 - Of. 220 - Lima, Perú  
Central Telefónica: 311 7777

www.congreso.gob.pe



**ÁREA DE INFRAESTRUCTURA TECNOLÓGICA**

Decisión de la Ig:  
Año de la recur

l de oportunidades para Mujeres y Hombr  
ción y consolidación de la economía peruana

- Borrar un archivo.
- Mover un archivo a cuarentena.

La plataforma deberá automatizar la creación de informes completamente personalizables y listos para auditorías, presentando mínimamente informe de inventario o exposición de activos, informes de incumplimiento de políticas de uso de software, informes de vulnerabilidades con su respectivo nivel de riesgo basado en múltiples criterios, informes de aplicación de parches sobre sistemas operativos y aplicaciones instaladas, informes de anomalías con indicadores de ataque (IoA) e indicadores de compromiso (IoC) e informes de cumplimiento de la NIST y/o ISO, evidenciando la reducción del riesgo en el tiempo.

**7.4. CAPACIDADES DE PREDICTIBILIDAD DE ATAQUES**

El servicio ofertado deberá incluir el acceso, administración y reportes a una plataforma de Cyber Threat Intelligence capaz de poder implementar capacidades de predictibilidad de ataques cibernéticos dirigidos y no dirigidos a través del monitoreo continuo de dark web y diversos canales utilizados por hackers y ciberdelincuentes.

La plataforma deberá ser presentada en modalidad de Software as a Service (SaaS) sin requerir de infraestructura física adicional para su normal desempeño.

- La plataforma deberá detectar credenciales comprometidas de la institución, las credenciales que se recuperan pueden estar relacionadas con clientes externos, afiliados de terceros, aplicaciones comerciales y aplicaciones de TI internas.

La plataforma deberá reconocer robo de credenciales de botnets las cuales han sido robadas por los servidores de críme logrando determinar el origen de la fuente, ya sea por configuraciones incorrectas y/o robo a través de herramientas de malware identificando el nombre de la botnet responsable y técnicas de ingeniería social utilizadas.

- La plataforma deberá reconocer credenciales de hacktivismo las cuales han sido filtradas en fuentes de cibercrimen y hacktivistas como foros, sitios de pagado, P2P, sitios web oscuros, etc.

La plataforma deberá monitorear la actividad de hacktivismo en redes sociales, sitios de pagado, chats IRC, etc. para saber si existen grupos de hacktivismo que buscan atacar activos tecnológicos de la institución.

- La plataforma debe permitir identificar y detectar vulnerabilidades y ataques de día 0/1 día que afectan el software y hardware utilizado por la institución.

La plataforma deberá integrar capacidades de predictibilidad basada en la recopilación de datos de fuentes abiertas, cerradas y privadas a través del acceso a una base de datos con el cual los especialistas en inteligencia realizarán búsquedas en la Darknet profunda y redes relacionadas (Contenido Darknet, Contenido Deepweb, Plataformas de chat encriptado (Telegram y otros), Hacker forums, FTP servers, Marketplaces y otros lugares no divulgados) para encontrar indicios o evidencias de amenazas existentes o emergentes que puedan atender contra el Congreso de la República.

La plataforma deberá presentar detalles de los hallazgos del módulo de credenciales, entregando mínimamente los siguientes datos:

- Categorización según el nivel de criticidad y/o prioridad de las credenciales encontradas.
- Usuario y contraseña comprometida.
- Tipo de botnet relacionada.
- URL afectada y/o plataforma o servicio afectado.
- Palabras clave utilizadas para la captura.
- Tipo de credencial.
- Clasificación.
- Relación con plataforma de correo.
- Última actualización.
- Fecha de reporte.
- Fecha de violación o captura.

Edificio Luis Alberto Sánchez Sánchez  
Jr. Huallaga N° 358 - Of. 220 - Lima, Perú  
Central Telefónica: 311-7777

www.congreso.gob.pe



**ÁREA DE INFRAESTRUCTURA TECNOLÓGICA**

Decenio de la igualdad de oportunidades para Mujeres y Hombres  
Año de la recuperación y consolidación de la economía peruana

- La plataforma deberá permitir la creación de alertas para todos sus módulos.
- La plataforma deberá poder afinar la búsqueda a través de filtros, parámetros y clasificación por dominio, IP o palabra para todos sus módulos.
- La plataforma deberá poder integrar datos de amenazas STIX/TAXII e intercambio de información con el SIEM o SOAR que la institución implemente.
- La plataforma deberá documentar más de 10 años de datos históricos sobre amenazas.
- La plataforma deberá presentar complementos disponibles para SIEM, XSOAR y TIP.
- La plataforma deberá administrar un sistema dinámico de puntuación de riesgos para alimentar programas de gestión de vulnerabilidades a través de API.
- La plataforma deberá integrar puntuación y clasificación de amenazas de malware.
- La plataforma deberá integrar en sus procesos la entrega verificada por humanos a fin de minimizar falsos positivos.
- La plataforma deberá integrar una asociación continua con Cyber Threat Alliance (CTA).
- La plataforma deberá tener una arquitectura modular que permita activar diferentes funcionalidades en el tiempo según los requerimientos de profundización e investigación a medida, estas funcionalidades deberán comprender mínimamente el compromiso de credenciales, protección de dominio, fuga de datos, hacktivismo, tarjetas de crédito, monitoreo de la organización en la dark web, exploración de amenazas, monitoreo de la organización en redes sociales e indicadores de ataque.

**7.5. PRESENTACIÓN OBLIGATORIA DENTRO DE LA PROPUESTA:**

- El Postor dentro de su propuesta, deberá acreditar fehacientemente el cumplimiento de las especificaciones técnicas solicitadas, numeral 7. **ESPECIFICACIONES TÉCNICAS MÍNIMAS (7.1, 7.2, 7.3, 7.4)**, catálogos y/o brochure y/o folletería y/o instructivos y/o ficha técnica y/o manuales y/o capturas de pantalla de las plataformas en funcionamiento.

Las características principales a verificar serán las siguientes:

Compatibilidad con sistemas operativos especificados, integración con fuentes de datos de seguridad (firewalls, antivirus, correo, directorio activo, componentes de red), autenticación de dos factores (2FA), protocolos de comunicación segura, aislamiento del agente (sin conexiones entrantes ni control remoto), coadministración basada en roles (propietario, visualizador, resolutor de incidentes), capacidades avanzadas de detección y respuesta (SOAR) integradas con MITRE ATT&CK, reducción de la superficie de ataque mediante pruebas de penetración y priorización de vulnerabilidades, monitoreo 24x7 de eventos de seguridad con alertas en tiempo real, respuesta automatizada a incidentes (aislamiento de hosts comprometidos, remediación de amenazas), certificaciones internacionales (ISO/IEC 27001, 27017, 27018, CSA STAR, SOC 3), generación de reportes (inventario, vulnerabilidades, eventos detectados), modalidad SaaS desde un SOC Data Center certificado, capacidad de análisis predictivo mediante Cyber Threat Intelligence (dark web, día 0/1 día), cumplimiento de normativas internacionales (ISO, NIST, STIG).

**7.6. CARACTERÍSTICAS DE LA SEGURIDAD GESTIONADA**

- El servicio de seguridad gestionada deberá contemplar de forma integral la gestión proactiva de toda la plataforma de Cyber SOC delegada, incluyendo la gestión tipo MDR correlacionando los eventos de equipos, servidores, componentes de red, antivirus y firewall, correo electrónico, directorio activo y demás plataforma de seguridad convenientes.

Edificio Luis Alberto Sánchez Sánchez,  
Jr. Hualagá N° 358 - Of. 220 - Lima, Perú  
Central Telefónica: 311-7777

www.congreso.gob.pe



**ÁREA DE INFRAESTRUCTURA TECNOLÓGICA**

Decenio de la Igualdad de Oportunidades para Mujeres y Hombres  
Año de la recuperación y consolidación de la economía peruana

- El servicio de seguridad gestionada deberá contemplar la gestión proactiva de todas las capacidades de prevención, detección, respuesta y predictibilidad que oferte la plataforma Cyber SOC delegada.
- El servicio de seguridad gestionada deberá presentar un plan de acción con las salvaguardas y estrategias recomendadas para el cumplimiento progresivo de los controles de seguridad idóneos alineados a la NIST.
- El servicio de seguridad gestionada deberá destinar un recurso (Especialista) local en las instalaciones del Congreso que se comunicará por correo electrónico y otros medios para coordinar las siguientes actividades:
  - Consolidar y presentar los resultados obtenidos de la plataforma tipo SOAR (Cyber SOC) para brindar capacidades de detección y respuesta ante ataques cibernéticos, mostrando evidencia del correlacionamiento de eventos de múltiples fuentes, alertas sobre servicios o aplicaciones sospechosas, conexiones con redes ciberterroristas e infracciones de seguridad revisadas en el tiempo con su respectiva telemetría.
  - Consolidar y presentar los resultados obtenidos de la plataforma y/o tecnología utilizada para las capacidades de prevención con respecto al hacking, pentesting y reducción de superficie de ataque interna y externa, adjuntando información sobre la gestión de riesgos basado en vulnerabilidades, configuraciones débiles y anomalías.
  - Absolución de consultas técnicas y soporte a incidentes reportados en la institución.
  - Elaboración e implementación de directivas y estrategias de concienciación en ciberseguridad a través de webinars, ponencias de activación, micro formación y ejercicios de suplantación de identidad y phishing para los usuarios de la institución.
- El servicio de seguridad gestionada deberá considerar actividades de reducción de superficie de ataque interna y externa a fin de mitigar los riesgos y reducir rápidamente su superficie de ataque por lo que el servicio debe considerar una gestión continua de vulnerabilidades con capacidad de detectar, evaluar, priorizar y remediar riesgos de seguridad más allá de las vulnerabilidades y exposiciones comunes (CVE) evidenciando:
  - Detección y clasificación de vulnerabilidades por Host y por aplicaciones con detalle de antigüedad, grupos específicos, ataques relacionados, Explotabilidad, vulnerabilidades remediadas, mitigadas, excluidas y programadas para remediación.
  - Detalles de los activos expuestos (Programas instalados).
  - El servicio de seguridad gestionada asumirá la remediación integral de los riesgos, aplicando parches, corrigiendo configuraciones, anomalías y definiendo políticas de uso de software a través de la desinstalación y/o bloqueo efectivo de aplicaciones, toda actividad deberá quedar documentada en la plataforma que corresponda para futuras auditorías. Todas las actividades que no se alcance a realizar deberán estar debidamente justificadas con la aprobación de los responsables de la institución y cogerán prioridad en el siguiente mes de objetivos.

**7.7. NIVELES DE SERVICIOS ESTABLECIDOS (SLA)**

- El Cyber SOC escalará un evento de interés a un incidente de forma automática o manual; los incidentes generarán una notificación por EMAIL o un ticket de mesa de ayuda cuando la Integración esté habilitada.
- El Cyber SOC escalará aún más un incidente mediante una llamada telefónica al usuario o, si es necesario, aislando el dispositivo y notificando al usuario. Cuando se detecte una ejecución potencialmente maliciosa en un dispositivo, el Cyber SOC lo gestionará como un incidente de Gravedad 1 hasta que la organización indique lo contrario.

Edificio Luis Alberto Sánchez Sánchez  
Jr. Hualagá N° 358 - Of. 220 - Lima, Perú  
Central Telefónica: 311-7777

www.congreso.gob.pe





**ÁREA DE INFRAESTRUCTURA TECNOLÓGICA**

Ministerio de la Igualdad de Oportunidades para Mujeres y Hombres  
Año de la recuperación y consolidación de la economía peruana

- Después de que el primer evento sospechoso/malicioso se convierta en un incidente, los analistas buscan otros eventos o incidentes inusuales y que lo corroboren. No recomendamos archivar los eventos.  
Las aplicaciones sirven como recopiladores de eventos; el Cyber SOC evalúa regularmente los eventos en las aplicaciones para buscar cualquier instancia que deba escalar a un incidente o crear una regla lógica para generar notificaciones automáticamente.
- El tiempo de detección: los patrones de telemetría y la zona horaria del usuario son elementos clave para los analistas del Cyber SOC y afectan la acción que tomarán. El Cyber SOC considera la zona horaria de la organización y las ejecuciones fuera del horario laboral en su proceso de toma de decisiones.
- El Cyber SOC iniciará una investigación en profundidad luego de cualquier incidente/evento de Gravedad 1 para determinar si el historial de incidentes y los eventos en las aplicaciones presentan algún otro indicio de un entorno violado. Según lo que encuentre, el SOC aislará los dispositivos si:
  - El cliente no responde la llamada para confirmar que las acciones están autorizadas.
  - El SOC no puede determinar con 100 % de certeza que alguna etapa de un ataque no está en curso en función de los incidentes y eventos encontrados en el panel del cliente en ese momento.

NIVELES DE GRAVEDAD – EVENTOS / INCIDENTES				
SEVERIDAD	IMPACTO	DESCRIPCIÓN	RESPUESTA TÍPICA (DETECCIÓN/ NOTIFICACIÓN/ ACCIÓN)	SLA (ACUERDO DE NIVEL DE SERVICIO)
SEV1	CRÍTICA URGENTE	Compromiso del sistema confirmado; ataque en curso.	2 min. / 5 min. / 10 min.	60 min.
SEV1	CRÍTICA	Fallo en cuarentena del antivirus; actividad maliciosa o sospechosa detectada en ejecución de archivos inusuales, conexiones con IPs de mala reputación o países monitoreados.	2 min. / 5 min. / 20 min.	60 min.
SEV2	IMPORTANTE	Actividad inusual detectada sin compromiso confirmado de sistemas, se detectó una alerta y ningún componente de los sistemas están comprometidos.	2 min. / 10 min. / según sea necesario	No aplica
SEV3	MENOR	El sistema muestra intentos de inicio de sesión fallidos u otros eventos generados por la red del cliente sistemas o usuarios y	2 min. / 10 min. / según sea necesario	No aplica

Edificio Luis Alberto Sánchez Sánchez  
Jr. Huallaga N° 358 – Of. 220 – Lima, Perú  
Central Telefónica: 3117777

www.congreso.gob.pe



**ÁREA DE INFRAESTRUCTURA TECNOLÓGICA**

Defensoría de la Igualdad de Oportunidades para Mujeres y Hombres  
Unidad de Promoción y Consolidación de la Economía Peruana

		no forman parte de una amenaza de ciberseguridad.		
SEV4	INFORMATIVA	No se observa ningún efecto malicioso en el sistema.	2 min. / según sea necesario / según sea necesario	No aplica
<b>CONEXIONES DE RED TERRORISTA CIBERNÉTICA</b>				
<b>DETECTAR</b>	<b>ANALIZAR</b>	<b>REMEDIACIÓN / MITIGACIÓN</b>	<b>ACCIONES</b>	
<b>Cyber SOC</b>	<b>Cyber SOC</b>	<b>Cyber SOC</b>	<b>Cyber SOC Local</b>	<b>Cyber SOC</b>
Conexión RDP sospechosa.	Analizar detalles. Revisar la línea de tiempo. Identificar otros eventos sospechosos.	Si se detecta un inicio de sesión exitoso, notifique al socio de TI. Si no está autorizado, aisle el dispositivo.  Si se detecta fuerza bruta pero no inicio de sesión exitoso detectado, notificar Socio de TI.	Si no está autorizado, cambie todos los usuarios, contraseñas con acceso al dispositivo. Ejecute un escaneo de antivirus completo. Investigar raíz causa. Aplicar políticas de acceso estrictas.  Coloque RDP detrás de VPN. Actualizar sistema. Aplicar políticas de acceso estrictas.	EMAIL/TICKET LLAMADA AISLAR
Conexión SQL sospechosa	Analizar detalles. Revisar la línea de tiempo. Identificar otros eventos sospechosos.	Si la conexión es exitosa, notifique al socio de TI. Si no está autorizado, aisle el dispositivo.  Si la conexión está autorizada, notifique al socio de TI.	Si no está autorizado, cambie todos los usuarios, contraseñas con acceso al dispositivo. Ejecute un escaneo de antivirus completo. Aplicar estrictas políticas de acceso.  Ejecute un escaneo de antivirus completo, aplicar estrictas políticas de acceso.	EMAIL/TICKET LLAMADA AISLAR
Conexiones entrantes sospechosas en 445 o 25 (SMB/SAMBA/Usos compartido de archivos de Windows) o 139 (Servicio de sesión NetBIOS)	Analizar detalles. Revisar la línea de tiempo. Identificar cualquier otro evento sospechoso.	Si la conexión es exitosa, notifique al personal de TI. Si no está autorizado, aisle el dispositivo.	Si no está autorizado, cambie todos los usuarios, contraseñas con acceso al dispositivo. Ejecute un escaneo de antivirus completo. Investigar la causa raíz de compromiso.	EMAIL/TICKET LLAMADA AISLAR

Edificio Luis Alberto Sánchez Sánchez,  
Jr. Huallaga N° 358 - Of. 220 - Lima, Perú  
Central Telefónica: 311-7177

www.congreso.gob.pe



**AREA DE INFRAESTRUCTURA TECNOLÓGICA**

Decenio de la Igualdad de oportunidades para Mujeres y Hombres  
Año de la recuperación y consolidación de la economía peruana

			Aplicar políticas de acceso estrictas.	
		Si la conexión está autorizada, notifique al socio de TI.	Si el Socio responde a nuestra llamada y confirma autorizado, o actual incidente o incidentes anteriores son resueltos antes de la convocatoria el SOC no aislará el dispositivo.	EMAIL/TICKET LLAMADA

SERVICIOS DE CYBERSOC					
Servicio		SLA		Reportes y Accesos	
Monitoreo de salud de la plataforma		Disponibilidad diaria 24x7x365		Detección de casos de uso establecidos. Resumen semanal. Consolidado mensual del servicio.	
Monitoreo avanzado tiempo real y correlación de eventos de seguridad		Disponibilidad diaria 24x7x365		Detección de casos de uso establecidos. Resumen semanal. Consolidado mensual del servicio.	
Cyber Threat Intelligence (Inteligencia de Ciberseguridad)		Disponibilidad diaria 24x7x365		Informe de Inteligencia periódico.	
Threat Hunting		Disponibilidad diaria 24x7x365		Atención de casos de seguridad avanzados	
Alerta Temprana		Disponibilidad diaria 24x7x365		Envío de alertas de acuerdo con la matriz de comunicación.	
Portal de Supervisión		Disponibilidad diaria 24x7x365		Acceso al Dashboard personalizado de reporte.	
Advanced Security Incident Response (Respuesta Avanzada a Incidentes)					
Preparación	Tiempo promedio de detección e inicio del análisis	Tiempo promedio de contención	Tiempo promedio de reparación	Tiempo promedio de resolución	Análisis de repercusiones
Permanente	< 30 minutos	< 45 minutos	< 3 horas	< 6 horas	Dentro de las 48 horas de resuelto el incidente.
Tiempos de Atención Off-Site					
Disponibilidad 24 x 7 x 365					
2 horas de atención como plazo máximo en Lima Metropolitana					

Edificio Luis Alberto Sánchez Sánchez  
Jr. Huallaga N° 358 - Of. 220 - Lima, Perú  
Central Telefónica: 3119177

www.congreso.gob.pe



CONGRESO  
REPUBLICA

AREA DE

INFRAESTRUCTURA TECNOLÓGICA

Decenio de la Igualdad de Oportunidades para Mujeres y Hombres  
Año de la recuperación y consolidación de la economía peruana

Registro de tickets de mesa de ayuda	
Tiempo máximo de registro del incidente, desde que son reportados	15 minutos



Edificio Luis Alberto Sánchez Sánchez  
Jr. Huallaga N° 358 - Of. 220 - Lima, Perú  
Central Telefónica: 311-7777



**ÁREA DE INFRAESTRUCTURA TECNOLÓGICA**

Diseño de la igualdad de oportunidades para Mujeres y Hombres  
Año de la recuperación y consolidación de la economía peruana

**8. OTRAS CONSIDERACIONES**

Es responsabilidad del contratista adoptar todas las medidas de seguridad para la ejecución del servicio, no siendo responsabilidad de la Entidad cualquier accidente que pudiera presentarse por la no observancia de lo que norma al respecto.

**9. REQUISITOS DEL PROVEEDOR Y SU PERSONAL**

**9.1. Requisitos del proveedor**

El postor deberá tener su Registro Nacional de Proveedores (RNP) vigente, a fin de poder contratar con el estado.

✓ El postor deberá tener Registro Único de Contribuyente (R.U.C.)

✓ El postor deberá contar con al menos 2 certificaciones de soluciones de Ciberseguridad.

El postor deberá tener un centro de Atención al Cliente 24x7 de tipo call center. El postor adjudicado deberá ser distribuidor autorizado de la solución ofertada.

✓ La empresa deberá disponer de todos los equipos y herramientas de trabajo necesarios a ser utilizados durante la prestación del servicio.

✓ El ejecutor deberá contar con un sólido equipo de trabajo, el mismo que deberá garantizar el desarrollo del trabajo solicitado en el plazo y horarios establecidos.

**Acreditación centro de atención al cliente:**

Para acreditar certificaciones de soluciones de ciberseguridad se aceptarán copias simples de los certificados oficiales emitidos por la entidad autorizada o documentos de designación formal.

Para acreditar el centro de atención al cliente 24x7, el postor deberá presentar una declaración jurada que certifique la disponibilidad de un centro de atención al cliente con servicio continuo (24x7).

Estos documentos deberán ser presentados al momento de perfeccionamiento del contrato.

**9.2. Requisitos del Personal propuesto:**

El proveedor debe acreditar que cuenta con los siguientes especialistas:

• **Un (01) jefe de Proyectos.**

Formación Académica, capacitación y otros:

- Ingeniero titulado en Computación o Sistemas o Electrónica o Redes y Comunicaciones de Datos o Ingeniería Informática, con colegiatura vigente al realizar el servicio.
- Certificación vigente en gestión de proyectos PMP o Scrum Master Certified.
- Certificación en Ciberseguridad Lead Cybersecurity Professional Certificate (LCSPC).
- Participación en curso o taller "Gestión de Ciber Crisis" con un mínimo de 08 horas lectivas.

Experiencia:

- Experiencia no menor de tres (03) años como Jefe o Gestor de Proyectos de soluciones de Ciberseguridad.

• **Un (01) Operador de Servicio**

Formación Académica, capacitación y otros:

Edificio Luis Alberto Sánchez Sánchez,  
Jr. Huallaga N° 358 - Of. 220- Lima, Perú  
Central Telefónica: 3113777



**ÁREA DE INFRAESTRUCTURA TECNOLÓGICA**

Diccionario de la lengua  
Año de la recuperación y consolidación de la economía peruana

- o Técnico profesional en redes y comunicaciones y/o telecomunicaciones.
- o Certificación técnica vigente en CEH V12 - Certified Ethical Hacker
- o Participación en curso o taller "Gestión de Ciber Crisis" con un mínimo de 08 horas lectivas.

**Experiencia:**

- o Experiencia no menor de tres (03) años como especialista en soluciones de Ciberseguridad.

El jefe de Proyectos será el responsable para realizar las coordinaciones con el Área de Infraestructura Tecnológica de la institución.

El jefe de Proyectos participará en la ejecución del servicio, y realizará las coordinaciones necesarias para que los operarios u otro personal operativo pueda ingresar a la entidad en forma adicional.

**Acreditación:**

Los documentos que acrediten el perfil señalado corresponden a lo siguiente:

- La formación académica se acreditará con copia simple del título profesional.
- La experiencia se acreditará con cualquiera de los siguientes documentos: (i) copia simple de contratos o (ii) constancias o (iii) certificados o (iv) cualquier otra documentación que, de manera fehaciente demuestre la experiencia del personal propuesto.
- En el caso de la colegiatura y la experiencia del personal, solo será acreditada al momento del inicio de la participación efectiva del profesional en la ejecución del contrato.
- Las acreditaciones de las certificaciones solicitadas para el personal propuesto deberán ser presentadas como parte de los documentos requeridos para el perfeccionamiento del contrato.

En caso de reemplazo del personal, este deberá tener un perfil igual o superior al previsto en los términos de referencia, el mismo que deberá ser aprobado por el área usuaria del servicio. Asimismo, este evento deberá ser comunicado previamente y de manera formal por mesa de partes del Congreso de la República.

**10. PLAZO DE EJECUCIÓN DEL SERVICIO**

El plazo para la ejecución del servicio es de seiscientos treinta (730) días calendario, contados a partir del día siguiente de la implementación del servicio.

El plazo máximo para la implementación del servicio será de treinta (30) días calendario, contados desde el día siguiente de la firma del contrato. Este proceso deberá concluir con la suscripción de un acta de culminación de implementación, documento que marcará el inicio oficial del periodo de ejecución del servicio, conforme a los plazos establecidos.

**11. PLAN DE TRABAJO**

El contratista deberá entregar en un plazo máximo de quince (15) días calendario contados a partir del día siguiente de la firma del contrato, el plan de trabajo que incluya el cronograma de actividades para la implementación del "Servicio de suscripción de plataforma de Cyber SOC delegada tipo Soar para el monitoreo, prevención, detección y respuesta ante incidentes cibernéticos con seguridad gestionada para el Congreso de la República".

Edificio Luis Alberto Sánchez Sánchez  
Jr. Huallaga N° 358 - Of. 220 - Lima, Perú  
Central Telefónica: 311-7777

www.congreso.gob.pe



CONGRESO  
REPUBLICA

### ÁREA DE INFRAESTRUCTURA TECNOLÓGICA

Proyecto de la igualdad de oportunidades para Mujeres y Hombres  
Año de la recuperación y consolidación de la economía peruana

## 12. ENTREGABLES

ENTREGABLE	PLAZO DE ENTREGA
Primer Entregable: Informe de Implementación de la Solución	Como máximo a los 7 días calendarios contados a partir de suscrita el acta de culminación de la implementación del servicio.
Segundo Entregable: Informe anual del servicio - 1er año	Como máximo a los 7 días calendario culminado los 365 días calendarios de iniciado el servicio.
Tercer Entregable: Informe anual del servicio - 2do año	Como máximo a los 7 días calendario culminado los 730 días calendarios de iniciado el servicio.

## 13. FORMA DE PAGO

El pago se efectuará en tres (03) armadas después de emitida la conformidad por parte del Área de Infraestructura Tecnológica y refrendado por el Departamento de Tecnologías de la Información, efectuándose según siguiente detalle:

Entregable	Porcentaje de pago	Condición de pago
01	40% del monto total de la prestación	A la conformidad del Primer Entregable.
02	30% del monto total de la prestación	A la conformidad del Segundo Entregable.
03	30% del monto total de la prestación	A la conformidad del Tercer Entregable.

Asimismo, para el pago el contratista deberá presentar:  
- comprobante de pago

## 14. CONFORMIDAD DE LA PRESTACIÓN DEL SERVICIO

La conformidad será emitida por el Área de Infraestructura Tecnológica y refrendada por el Departamento de Tecnologías de la Información luego de la recepción y revisión de los entregables.

### 14.1. DEL PRIMER ENTREGABLE.

La conformidad será emitida por el Área de Infraestructura Tecnológica y refrendada por el Departamento de Tecnologías de la Información luego de:

- La entrega del Acuerdo de Nivel de Servicios - ANS,
- La entrega del Plan de Trabajo y Cronograma de Actividades.
- La verificación del cumplimiento de las actividades correspondientes a la prestación principal.
- La recepción y validación del informe técnico correspondiente a la etapa de instalación, configuración y pruebas de la solución.

### 14.2. DEL SEGUNDO Y TERCER ENTREGABLE.

La conformidad del segundo y tercer entregable será emitida por el Área de Infraestructura Tecnológica y refrendada por el Departamento de Tecnologías de la Información previa recepción y validación del informe anual del servicio.

Edificio Luis Alberto Sánchez Sánchez,  
Jr. Huallaga N° 358 - Of. 220 - Lima, Perú  
Central Telefónica: 311-7777



ÁREA DE

INFRAESTRUCTURA TECNOLÓGICA

Diseño de la lig  
Año de la recu

rd de oportunidades para Mujeres y Hombr  
ción y consolidación de la economía peruana

### 15. PENALIDADES

En caso de retraso injustificado del contratista en la ejecución de las prestaciones objeto del contrato, la entidad le aplicará automáticamente una penalidad por mora por cada día de retraso. La penalidad se considerará de acuerdo a lo estipulado en el Artículo 162° del Reglamento de la Ley de Contrataciones del Estado.

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

Donde F tiene los siguientes valores:

- Para plazos menores o iguales a sesenta (60) días, para bienes, servicios en general, consultorías y ejecución de obras:  $F = 0.40$ .
- Para plazos mayores a sesenta (60) días:
  - Para bienes, servicio y consultorías:  $F = 0.25$ .
  - Para obras:  $F = 0.15$ .

Tanto el monto como el plazo se refieren, según corresponda, a la ejecución total del servicio o a la obligación parcial, de ser el caso, que fuera materia de retraso. Se considera justificado el retraso, cuando el contratista acredite, de modo objetivamente sustentado, que el mayor tiempo transcurrido no le resulta imputable. En calificación del retraso como justificado, no da lugar al pago de gastos generales de ningún tipo.

### 16. OTRAS PENALIDADES

En caso se incurra en el incumplimiento de las prestaciones relacionadas al servicio, las penalidades se considerarán de acuerdo a lo estipulado en el artículo 163 del Reglamento de la Ley de Contrataciones del Estado.

- De acuerdo con el artículo 163 del Reglamento se pueden establecer penalidades distintas al retraso o mora en la ejecución de la prestación, las cuales deben ser objetivas, razonables, congruentes y proporcionales con el objeto de la contratación.
- Para dicho efecto, se debe incluir un listado detallado de 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.

N°	SUPUESTOS DE APLICACIÓN DE PENALIDAD	FORMA DE CÁLCULO	PROCEDIMIENTO
1	Por día de atraso en la entrega del Informe de Implementación de la Solución.	1 % de una UIT por cada día de atraso.	Mediante acta de culminación de la implementación del servicio.
2	Por día de atraso en la entrega del Acuerdo de Nivel de Servicio - ANS (Service Level Agreement - SLA)	1 % de una UIT por cada día de atraso.	Mediante informe del área usuaria.

Edificio Luis Alberto Sánchez Sánchez,  
Jr. Huallegá N° 358 - Of. 220 - Lima, Perú  
Central Telefónica: 311-7777





**ÁREA DE INFRAESTRUCTURA TECNOLÓGICA**

Diseño de la Igualdad de oportunidades para Mujeres y Hombres  
Año de la recuperación y consolidación de la economía peruana

N°	SUPUESTOS DE APLICACIÓN DE PENALIDAD	FORMA DE CÁLCULO	PROCEDIMIENTO
3	Por día de atraso en la entrega del Plan de trabajo	1 % de una UIT por cada día de atraso	Mediante informe del área usuaria.
4	Por día de atraso en la entrega Informe anual del servicio.	1 % de una UIT por cada día de atraso.	Mediante informe del área usuaria.

**17. RESPONSABILIDAD POR VICIOS OCULTOS**

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

*El plazo máximo de responsabilidad del contratista es de un (1) año contado a partir de la conformidad otorgada por LA ENTIDAD.*

**18. CONFIDENCIALIDAD**

El contratista se compromete a mantener en reserva y a no revelar a terceros, sin previa autorización escrita del Congreso de la República, toda información que le sea suministrada por ésta última, y/o sea obtenida en el ejercicio de las actividades a desarrollarse o conozca directa o indirectamente durante el proceso de selección o para la realización de sus tareas, excepto en cuanto resultare estrictamente necesario para el cumplimiento del presente Contrato.

El contratista deberá mantener a perpetuidad la confidencialidad y reserva absoluta en el manejo de cualquier información y documentación a la que se tenga acceso a consecuencia del procedimiento de selección y la ejecución del contrato, quedando prohibida revelar a terceros.

Dicha obligación comprende la información que se entrega, como también la que se genera durante la realización de las actividades previas a la ejecución del contrato, durante su ejecución y la producida una vez que se haya concluido el contrato.

Dicha información puede consistir en informes, recomendaciones, cálculos, documentos y demás datos compilados o recibidos por el contratista.

Asimismo, aun cuando sea de índole pública, la información vinculada al procedimiento de contratación, incluyendo su ejecución y conclusión, no podrá ser utilizada por el contratista para fines publicitarios o de difusión por cualquier medio sin obtener la autorización correspondiente del Congreso de la República.

**19. 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,*

Edificio Luis Alberto Sánchez Sánchez  
Jr. Huallaga N° 358 - Of. 220 - Lima, Perú  
Central Telefónica: 311-7777



ÁREA DE

INFRAESTRUCTURA TECNOLÓGICA

Decano de la Igu  
Año de la recu

id de oportunidades para Mujeres y Hombr  
ción y consolidación de la economía peruana

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.

20. SOLUCIÓN DE CONTROVERSIAS

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

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

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

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

21. LUGAR DE EJECUCIÓN

Jirón Huallaga 358 - Cercado de Lima - Lima. Horario de atención desde las 9:00 hasta las 17:00 horas.

22. SISTEMA DE CONTRATACION

El sistema de contratación es de suma alzada.

**NOTA:** Los requisitos de calificación establecidos en el numeral 23 de los terminos de referencia, se establecen en el numeral 3.2 de la Sección Especifica de las presentes bases.

**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>Ingeniero titulado en Computación o Sistemas o Electrónica o Redes y Comunicaciones de Datos o Ingeniería Informática del personal clave requerido como Jefe de Proyectos.</p> <p>Técnico profesional en redes y comunicaciones y/o telecomunicaciones del personal clave requerido como Operador de Servicio.</p> <p><u>Acreditación:</u></p> <p>El Título será verificado por el comité de selección en el Registro Nacional de Grados Académicos y Títulos Profesionales en el portal web de la Superintendencia Nacional de Educación Superior Universitaria - SUNEDU a través del siguiente link: <a href="https://enlinea.sunedu.gob.pe/">https://enlinea.sunedu.gob.pe/</a> o en el Registro Nacional de Certificados, Grados y Títulos a cargo del Ministerio de Educación a través del siguiente link: <a href="https://titulosinstitutos.minedu.gob.pe/">https://titulosinstitutos.minedu.gob.pe/</a>, según corresponda.</p> <p><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> <p><i>Incluir o eliminar, según corresponda. Sólo deberá incluirse esta nota cuando la formación académica sea el único requisito referido a las calificaciones del personal clave que se haya previsto. Ello a fin que la Entidad pueda verificar los grados o títulos requeridos en los portales web respectivos.</i></p> <p>En caso el Título 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>Mínimo de ocho (08) horas lectivas, en participación en curso o taller "Gestión de Ciber Crisis" del personal clave requerido como Jefe de Proyectos.</p> <p>Mínimo de ocho (08) horas lectivas, en participación en curso o taller "Gestión de Ciber Crisis" del personal clave requerido como Operador de Servicio.</p> <p><u>Acreditación:</u></p> <p>Se acreditará con copia simple de constancias o certificados, según corresponda.</p> <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>
<b>B.4</b>	<b>EXPERIENCIA DEL PERSONAL CLAVE</b>

	<p><b>Requisitos:</b></p> <p>Experiencia no menor de tres (03) años como jefe o gestor de proyectos de soluciones de Ciberseguridad, del personal clave requerido como Jefe de Proyectos.</p> <p>Experiencia no menor de tres (03) años como especialista en soluciones de Ciberseguridad, del personal clave requerido como Operador de Servicio.</p> <p><u>De presentarse experiencia ejecutada paralelamente (traslape), para el cómputo del tiempo de dicha experiencia sólo se considerará una vez el periodo traslapado.</u></p> <p><b>Acreditación:</b></p> <p>La experiencia del personal clave se acreditará con cualquiera de los siguientes documentos: (i) copia simple de contratos y su respectiva conformidad o (ii) constancias o (iii) certificados o (iv) cualquier otra documentación que, de manera fehaciente demuestre la experiencia del personal propuesto.</p> <div data-bbox="365 619 1364 1144"> <p><b>Importante</b></p> <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> </div>
C	<p><b>EXPERIENCIA DEL POSTOR EN LA ESPECIALIDAD</b></p> <p><b>Requisitos:</b></p> <p>El postor debe acreditar un monto facturado acumulado equivalente a S/ 1'500,000.00 (Un Millón Quinientos Mil con 00/100 Soles), por la contratación de servicios iguales o similares al objeto de la convocatoria, durante los ocho (8) años anteriores a la fecha de la presentación de ofertas que se computarán desde la fecha de la conformidad o emisión del comprobante de pago, según corresponda.</p> <p>Se consideran servicios similares a los siguientes: servicios de soluciones de seguridad y ciberseguridad, soluciones de monitoreo, automatización y respuesta ante incidentes de seguridad informática.</p> <p><b>Acreditación:</b></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>9</sup>, correspondientes a un máximo de veinte (20) contrataciones.</p>

<sup>9</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".

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

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

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

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

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

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

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

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

#### Importante

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

#### Importante

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

#### CAPÍTULO IV FACTORES DE EVALUACIÓN

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

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

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

#### Importante

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

## CAPÍTULO V PROFORMA DEL CONTRATO

### Importante

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

Conste por el presente documento, la contratación del **SERVICIO DE SUSCRIPCIÓN PARA UNA PLATAFORMA DE CORRELACIONADOR DE EVENTOS (SIEM) Y CYBER SOC DELEGADA TIPO SOAR PARA EL MONITOREO, PREVENCIÓN, DETECCIÓN Y RESPUESTA ANTE INCIDENTES CIBERNÉTICOS CON SEGURIDAD GESTIONADA PARA EL CONGRESO DE LA REPUBLICA**, que celebra de una parte el **CONGRESO DE LA REPUBLICA**, en adelante LA ENTIDAD, con RUC N° 20161749126, con domicilio legal en JR. HUALLAGA NRO. 358 LIMA - LIMA - LIMA, representada por [...], identificado con DNI N° [...], y de otra parte [...], con RUC N° [...], con domicilio legal en [...], inscrita en la Ficha N° [...] Asiento N° [...] del Registro de Personas Jurídicas de la ciudad de [...], debidamente representado por su Representante Legal, [...], con DNI N° [...], según poder inscrito en la Ficha N° [...], Asiento N° [...] del Registro de Personas Jurídicas de la ciudad de [...], a quien en adelante se le denominará EL CONTRATISTA en los términos y condiciones siguientes:

### CLÁUSULA PRIMERA: ANTECEDENTES

Con fecha [...], el comité de selección adjudicó la buena pro del **CONCURSO PÚBLICO N°002-2025-CR-1** para la contratación del **SERVICIO DE SUSCRIPCIÓN PARA UNA PLATAFORMA DE CORRELACIONADOR DE EVENTOS (SIEM) Y CYBER SOC DELEGADA TIPO SOAR PARA EL MONITOREO, PREVENCIÓN, DETECCIÓN Y RESPUESTA ANTE INCIDENTES CIBERNÉTICOS CON SEGURIDAD GESTIONADA PARA EL CONGRESO DE LA REPUBLICA**, 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 SUSCRIPCIÓN PARA UNA PLATAFORMA DE CORRELACIONADOR DE EVENTOS (SIEM) Y CYBER SOC DELEGADA TIPO SOAR PARA EL MONITOREO, PREVENCIÓN, DETECCIÓN Y RESPUESTA ANTE INCIDENTES CIBERNÉTICOS CON SEGURIDAD GESTIONADA PARA EL CONGRESO DE LA REPUBLICA**.

### 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>10</sup>

LA ENTIDAD se obliga a pagar la contraprestación a EL CONTRATISTA en [INDICAR MONEDA], en PAGOS PARCIALES con periodicidad quincenal, 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

<sup>10</sup> En cada caso concreto, dependiendo de la naturaleza del contrato, podrá adicionarse la información que resulte pertinente a efectos de generar el pago.

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:

El plazo para la ejecución del servicio es de setecientos treinta (730) días calendarios, contados a partir del día siguiente de la implementación del servicio.

El plazo máximo para la implementación del servicio será de treinta (30) días calendario, contados desde el día siguiente de la firma del contrato. Este proceso deberá concluir con la suscripción de un acta de culminación de implementación, documento que marcará el inicio oficial del período de ejecución del servicio, conforme a los plazos establecidos.

En concordancia con lo establecido en el expediente de contratación.

#### **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."*

##### **Importante**

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

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

LA ENTIDAD puede solicitar la ejecución de las garantías cuando EL CONTRATISTA no las hubiere



renovado antes de la fecha de su vencimiento, conforme a lo dispuesto por el literal a) del numeral 155.1 del artículo 155 del Reglamento de la Ley de Contrataciones del Estado.

**CLÁUSULA NOVENA: CONFORMIDAD DE LA PRESTACIÓN DEL SERVICIO**

La conformidad de la prestación del servicio se regula por lo dispuesto en el artículo 168 del Reglamento de la Ley de Contrataciones del Estado. La conformidad será otorgada por el Área de Infraestructura Tecnológica del Departamento de Tecnología de la Información emitiendo la conformidad de la prestación efectuada, en el plazo máximo de siete (7) días de producida la recepción.

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

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

**CLÁUSULA DÉCIMA: DECLARACIÓN JURADA DEL CONTRATISTA**

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

**CLÁUSULA UNDÉCIMA: RESPONSABILIDAD POR VICIOS OCULTOS**

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

El plazo máximo de responsabilidad del contratista es de UN (1) año contado a partir de la conformidad otorgada por LA ENTIDAD.

**CLÁUSULA DUODÉCIMA: PENALIDADES**

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

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

Donde:

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

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

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

Importante

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

#### **OTRAS PENALIDADES**

N°	SUPUESTOS DE APLICACIÓN DE PENALIDAD	FORMA DE CÁLCULO	PROCEDIMIENTO
1	Por día de atraso en la entrega del Informe de Implementación de la Solución.	1 % de una UIT por cada día de atraso.	Mediante informe del área usuaria
2	Por día de atraso en la entrega del Acuerdo de Nivel de Servicio – ANS (Service Level Agreement - SLA)	1 % de una UIT por cada día de atraso.	Mediante informe del área usuaria
3	Por día de atraso en la entrega del Plan de trabajo	1 % de una UIT por cada día de atraso.	Mediante informe del área usuaria
4	Por día de atraso en la entrega Informe anual del servicio.	1 % de una UIT por cada día de atraso.	Mediante informe del área usuaria

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

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

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

#### **CLÁUSULA DÉCIMA TERCERA: RESOLUCIÓN DEL CONTRATO**

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

#### **CLÁUSULA DÉCIMA CUARTA: RESPONSABILIDAD DE LAS PARTES**

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

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

#### **CLÁUSULA DÉCIMA QUINTA: ANTICORRUPCIÓN**

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

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

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

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

**CLÁUSULA DÉCIMA SEXTA: MARCO LEGAL DEL CONTRATO**

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

**CLÁUSULA DÉCIMA SÉTIMA: SOLUCIÓN DE CONTROVERSIAS<sup>11</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 Laudo arbitral emitido es inapelable, definitivo y obligatorio para las partes desde el momento de su notificación, según lo previsto en el numeral 45.21 del artículo 45 de la Ley de Contrataciones del Estado.

**CLÁUSULA DÉCIMA OCTAVA: FACULTAD DE ELEVAR A ESCRITURA PÚBLICA**

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

**CLÁUSULA DÉCIMA NOVENA: DOMICILIO PARA EFECTOS DE LA EJECUCIÓN CONTRACTUAL**

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

DOMICILIO DE LA ENTIDAD: JR. HUALLAGA NRO. 358 LIMA - LIMA - LIMA

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

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

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

\_\_\_\_\_  
"LA ENTIDAD"

\_\_\_\_\_  
"EL CONTRATISTA"

**Importante**

*Este documento puede firmarse digitalmente si ambas partes cuentan con firma digital, según la Ley N° 27269, Ley de Firmas y Certificados Digitales<sup>12</sup>.*

<sup>11</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).

<sup>12</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°002-2025-CR-1**  
Presente.-

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

Nombre, Denominación o Razón Social :			
Domicilio Legal :			
RUC :	Teléfono(s) :		
MYPE <sup>13</sup>	SI	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>14</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>13</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>14</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°002-2025-CR-1**  
Presente.-

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

Datos del consorciado 1				
Nombre, Denominación o Razón Social :				
Domicilio Legal :				
RUC :	Teléfono(s) :			
MYPE <sup>15</sup>		Sí	No	
Correo electrónico :				

Datos del consorciado 2				
Nombre, Denominación o Razón Social :				
Domicilio Legal :				
RUC :	Teléfono(s) :			
MYPE <sup>16</sup>		Sí	No	
Correo electrónico :				

Datos del consorciado ...				
Nombre, Denominación o Razón Social :				
Domicilio Legal :				
RUC :	Teléfono(s) :			
MYPE <sup>17</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>15</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>16</sup> Ibídem.

<sup>17</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>18</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>18</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°002-2025-CR-1**  
Presente.-

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

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

[CONSIGNAR CIUDAD Y FECHA]

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

**Importante**

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



ANEXO N° 3

DECLARACIÓN JURADA DE CUMPLIMIENTO DE LOS TÉRMINOS DE REFERENCIA

Señores  
**COMITÉ DE SELECCIÓN**  
**CONCURSO PÚBLICO N°002-2025-CR-1**  
Presente.-

Es grato dirigirme a usted, para hacer de su conocimiento que luego de haber examinado las bases y demás documentos del procedimiento de la referencia y, conociendo todos los alcances y las condiciones detalladas en dichos documentos, el postor que suscribe ofrece el servicio de **SERVICIO DE SUSCRIPCIÓN PARA UNA PLATAFORMA DE CORRELACIONADOR DE EVENTOS (SIEM) Y CYBER SOC DELEGADA TIPO SOAR PARA EL MONITOREO, PREVENCIÓN, DETECCIÓN Y RESPUESTA ANTE INCIDENTES CIBERNÉTICOS CON SEGURIDAD GESTIONADA PARA EL CONGRESO DE LA REPUBLICA**, 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°002-2025-CR-1**  
Presente.-

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

**El plazo para la ejecución del servicio es de setecientos treinta (730) días calendarios, contados a partir del día siguiente de la implementación del servicio.**

**El plazo máximo para la implementación del servicio será de treinta (30) días calendario, contados desde el día siguiente de la firma del contrato. Este proceso deberá concluir con la suscripción de un acta de culminación de implementación, documento que marcará el inicio oficial del período de ejecución del servicio, conforme a los plazos establecidos.**

[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°002-2025-CR-1**  
Presente.-

Los suscritos declaramos expresamente que hemos convenido en forma irrevocable, durante el lapso que dure el procedimiento de selección, para presentar una oferta conjunta al **CONCURSO PÚBLICO N°002-2025-CR-1**.

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

a) Integrantes del consorcio

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

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

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

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

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

1. OBLIGACIONES DE [NOMBRE, DENOMINACIÓN O RAZÓN SOCIAL DEL CONSORCIADO 1] [%]<sup>19</sup>

[DESCRIBIR LAS OBLIGACIONES DEL CONSORCIADO 1]

2. OBLIGACIONES DE [NOMBRE, DENOMINACIÓN O RAZÓN SOCIAL DEL CONSORCIADO 2] [%]<sup>20</sup>

[DESCRIBIR LAS OBLIGACIONES DEL CONSORCIADO 2]

TOTAL OBLIGACIONES 100%<sup>21</sup>

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

<sup>20</sup> Consignar únicamente el porcentaje total de las obligaciones, el cual debe ser expresado en número entero, sin decimales.

<sup>21</sup> Este porcentaje corresponde a la sumatoria de los porcentajes de las obligaciones de cada uno de los integrantes del consorcio.

[CONSIGNAR CIUDAD Y FECHA]

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

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

**Importante**

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

**ANEXO N° 6**

**PRECIO DE LA OFERTA**

Señores  
**COMITÉ DE SELECCIÓN**  
**CONCURSO PÚBLICO N°002-2025-CR-1**  
Presente.-

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

CONCEPTO	PRECIO TOTAL
SERVICIO DE SUSCRIPCIÓN PARA UNA PLATAFORMA DE CORRELACIONADOR DE EVENTOS (SIEM) Y CYBER SOC DELEGADA TIPO SOAR PARA EL MONITOREO, PREVENCIÓN, DETECCIÓN Y RESPUESTA ANTE INCIDENTES CIBERNÉTICOS CON SEGURIDAD GESTIONADA PARA EL CONGRESO DE LA REPUBLICA	
<b>TOTAL</b>	

El precio de la oferta es 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**

- *En caso que el postor reduzca su oferta, según lo previsto en el artículo 68 del Reglamento, debe presentar nuevamente este Anexo.*
- *El postor que goce de alguna exoneración legal, debe indicar que su oferta no incluye el tributo materia de la exoneración, debiendo incluir el siguiente texto:*  
*"Mi oferta no incluye [CONSIGNAR EL TRIBUTO MATERIA DE LA EXONERACIÓN]."*

ANEXO N° 8

EXPERIENCIA DEL POSTOR EN LA ESPECIALIDAD

Señores  
COMITÉ DE SELECCIÓN  
CONCURSO PÚBLICO N°002-2025-CR-1  
Presente.-

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

N°	CLIENTE	OBJETO DEL CONTRATO	N° CONTRATO / O/S / COMPROBANTE DE PAGO	FECHA DEL CONTRATO O CP <sup>22</sup>	FECHA DE LA CONFORMIDAD DE SER EL CASO <sup>23</sup>	EXPERIENCIA PROVENIENTE <sup>24</sup> DE:	MONEDA	IMPORTE <sup>25</sup>	TIPO DE CAMBIO VENTA <sup>26</sup>	MONTO FACTURADO ACUMULADO <sup>27</sup>
1										
2										
3										
4										

<sup>22</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>23</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>24</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>25</sup> Se refiere al monto del contrato ejecutado incluido adicionales y reducciones, de ser el caso.

<sup>26</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>27</sup> Consignar en la moneda establecida en las bases.

N°	CLIENTE	OBJETO DEL CONTRATO	N° CONTRATO / O/S / COMPROBANTE DE PAGO	FECHA DEL CONTRATO O CP <sup>22</sup>	FECHA DE LA CONFORMIDAD DE SER EL CASO <sup>23</sup>	EXPERIENCIA PROVENIENTE <sup>24</sup> DE	MONEDA	IMPORTE <sup>25</sup>	TIPO DE CAMBIO VENTA <sup>26</sup>	MONTO FACTURADO ACUMULADO <sup>27</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°002-2025-CR-1  
Presente.-

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

[CONSIGNAR CIUDAD Y FECHA]

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

**Importante**

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

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



ANEXO N° 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°002-2025-CR-1**  
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.*