

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> <ul style="list-style-type: none"> • Abc 	Se refiere a consideraciones importantes a tener en cuenta por el comité de selección y por los proveedores.
4	<div>Advertencia</div> <ul style="list-style-type: none"> • Abc 	Se refiere a advertencias a tener en cuenta por el comité de selección y por los proveedores.
5	<div>Importante para la Entidad</div> <ul style="list-style-type: none"> • Xyz 	Se refiere a consideraciones importantes a tener en cuenta por el comité de selección y deben ser eliminadas una vez culminada la elaboración de las bases.

CARACTERÍSTICAS DEL DOCUMENTO:

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

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

INSTRUCCIONES DE USO:

- 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



COFIDE
EL BANCO DE DESARROLLO DEL PERÚ

**BASES INTEGRADAS DE CONCURSO PÚBLICO PARA LA
CONTRATACIÓN DE SERVICIOS EN GENERAL**

**CONCURSO PÚBLICO
N° 007-2024-COFIDE**

**CONTRATACIÓN DE SERVICIO DE GESTIÓN Y
OPERACIÓN DE LA CIBERSEGURIDAD**

DEBER DE COLABORACIÓN

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

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

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

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

SECCIÓN GENERAL

DISPOSICIONES COMUNES DEL PROCEDIMIENTO DE SELECCIÓN

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

CAPÍTULO I ETAPAS DEL PROCEDIMIENTO DE SELECCIÓN

1.1. REFERENCIAS

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

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

1.2. CONVOCATORIA

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

1.3. REGISTRO DE PARTICIPANTES

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

Importante

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

1.4. FORMULACIÓN DE CONSULTAS Y OBSERVACIONES A LAS BASES

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

Importante

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

1.5. ABSOLUCIÓN DE CONSULTAS, OBSERVACIONES E INTEGRACIÓN DE BASES

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

Importante

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

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

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

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

Advertencia

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

Importante

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

1.7. FORMA DE PRESENTACIÓN DE OFERTAS

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

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

Importante

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

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

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

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

1.8. PRESENTACIÓN Y APERTURA DE OFERTAS

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

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

Importante

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

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

1.9. EVALUACIÓN DE LAS OFERTAS

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

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

1.10. CALIFICACIÓN DE OFERTAS

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

1.11. SUBSANACIÓN DE LAS OFERTAS

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

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

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

1.12. RECHAZO DE LAS OFERTAS

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

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

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

1.13. OTORGAMIENTO DE LA BUENA PRO

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

1.14. CONSENTIMIENTO DE LA BUENA PRO

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

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

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

Importante

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

CAPÍTULO II

SOLUCIÓN DE CONTROVERSIAS DURANTE EL PROCEDIMIENTO DE SELECCIÓN

2.1. RECURSO DE APELACIÓN

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

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

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

Importante

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

2.2. PLAZOS DE INTERPOSICIÓN DEL RECURSO DE APELACIÓN

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

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

CAPÍTULO III DEL CONTRATO

3.1. PERFECCIONAMIENTO DEL CONTRATO

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

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

3.2. GARANTÍAS

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

3.2.1. GARANTÍA DE FIEL CUMPLIMIENTO

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

3.2.2. GARANTÍA DE FIEL CUMPLIMIENTO POR PRESTACIONES ACCESORIAS

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

Importante

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

3.2.3. GARANTÍA POR ADELANTO

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

3.3. REQUISITOS DE LAS GARANTÍAS

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

Importante

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

Advertencia

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

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

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

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

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

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

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

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

3.4. EJECUCIÓN DE GARANTÍAS

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

3.5. ADELANTOS

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

3.6. PENALIDADES

3.6.1. PENALIDAD POR MORA EN LA EJECUCIÓN DE LA PRESTACIÓN

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

3.6.2. OTRAS PENALIDADES

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

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

3.7. INCUMPLIMIENTO DEL CONTRATO

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

3.8. PAGOS

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

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

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

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

Advertencia

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

3.9. DISPOSICIONES FINALES

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

SECCIÓN ESPECÍFICA

CONDICIONES ESPECIALES DEL PROCEDIMIENTO DE SELECCIÓN

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

CAPÍTULO I GENERALIDADES

1.1. ENTIDAD CONVOCANTE

Nombre : CORPORACIÓN FINANCIERA DE DESARROLLO S.A. – COFIDE

RUC N° : 20100116392

Domicilio legal : Augusto Tamayo Nro. 160 – San Isidro

Teléfono: : 615-4000

Correo electrónico: : mrecabarren@cofide.com.pe

1.2. OBJETO DE LA CONVOCATORIA

El presente procedimiento de selección tiene por objeto la contratación del servicio de gestión y operación de la ciberseguridad.

1.3. EXPEDIENTE DE CONTRATACIÓN

El expediente de contratación fue aprobado mediante Acta de Aprobación de Expediente N° 075-2024-GGHA el 26 de diciembre de 2024.

1.4. FUENTE DE FINANCIAMIENTO

Recursos Directamente Recaudados.

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 treinta y nueve (39)

meses en concordancia con lo establecido en el expediente de contratación.

1.9. COSTO DE REPRODUCCIÓN Y ENTREGA DE BASES

Los participantes registrados tienen el derecho de recabar un ejemplar de las bases, para cuyo efecto deben cancelar S/ 5.00 (cinco con 00/100 Soles) en la cuenta corriente N° 193-0245964-0-83, código CCI N° 002 193 0002 4596 4083 11, del Banco de Crédito del Perú (BCP), luego acercarse al Departamento de Compras de COFIDE a recoger las bases, previa presentación del voucher de depósito.

Importante

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

1.10. BASE LEGAL

- Texto Único Ordenado de la Ley N° 30225, Ley de Contrataciones del Estado aprobado mediante Decreto Supremo N° 082-2019-EF.
- Reglamento de la Ley N° 30225, Ley de Contrataciones del Estado aprobado por el Decreto Supremo N° 344-2018-EF.
- Ley N° 31953 - Ley de Presupuesto del Sector Público para el Año Fiscal 2024.
- Ley N° 31954 - Ley de Equilibrio Financiero del Presupuesto del Sector Público del Año Fiscal 2024
- Ley N° 31955, Ley de Endeudamiento del sector público para el año fiscal 2024.
- Directiva N° 004-2019-OSCE/CD, mediante el cual se indica las disposiciones sobre el contenido del Resumen Ejecutivo del Estudio de Mercado.
- Ley N° 31955, Ley de Endeudamiento del sector público para el año fiscal 2024.
- Ley N° 28411, Ley General del Sistema Nacional de Presupuesto, sus modificatorias y normas complementarias
- Ley 27444, Ley del Procedimiento Administrativo General y sus modificatorias.
- Ley N° 27806, Ley de Transparencia y de Acceso a la Información Pública.
- Decreto Supremo N° 004-2019-JUS, TUO de la Ley N° 27444 – Ley del Procedimiento Administrativo General.
- Resolución N° D000112-2022-OSCE-PRE, Modifica la directiva N° 001-20219-OSCE/CD Bases Solicitud de Expresión de Intereses estándar para los Procedimientos de Selección a Convocar en el Marco de la Ley 30225.
- Directivas vigentes aprobadas por el OSCE

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

CAPÍTULO II DEL PROCEDIMIENTO DE SELECCIÓN

2.1. CALENDARIO DEL PROCEDIMIENTO DE SELECCIÓN

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

Importante

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

2.2. CONTENIDO DE LAS OFERTAS

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

2.2.1. Documentación de presentación obligatoria

2.2.1.1. Documentos para la admisión de la oferta

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

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

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

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

Advertencia

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

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

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

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

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

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

Importante

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

2.2.1.2. Documentos para acreditar los requisitos de calificación

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

2.2.2. Documentación de presentación facultativa:

- a) Incorporar en la oferta los documentos que acreditan los “Factores de Evaluación” establecidos en el Capítulo IV de la presente sección de las bases, a efectos de obtener el puntaje previsto en dicho Capítulo para cada factor.

Advertencia

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

2.3. REQUISITOS PARA PERFECCIONAR EL CONTRATO

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

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

Datos Bancarios	
Nombre del Banco	
Nombre del Titular de la Cuenta	

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

N° de Cuenta																				
N° de CCI																				
Tipo de Cuenta	Corriente				Ahorros				Otra: <i>Especificar</i>											
Moneda	PEN																USD			
N° de Cuenta de Detracción - Banco de la Nación																				
Correo electrónico de cobranzas (<i>para notificación del pago</i>)																				

- e) Copia de la vigencia del poder del representante legal de la empresa que acredite que cuenta con facultades para perfeccionar el contrato, cuando corresponda.
- f) Copia de DNI del postor en caso de persona natural, o de su representante legal en caso de persona jurídica.⁵

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 – PIDE⁶ y siempre que el servicio web se encuentre activo en el Catálogo de Servicios de dicha plataforma, no corresponderá exigir los documentos previstos en los literales e) y f).

- g) Domicilio para efectos de la notificación durante la ejecución del contrato.
- h) Autorización de notificación de la decisión de la Entidad sobre la solicitud de ampliación de plazo mediante medios electrónicos de comunicación ⁷ (**Anexo N° 12**).
- i) Detalle de los precios unitarios del precio ofertado⁸.
- j) Estructura de costos⁹.
- k) Detalle del precio de la oferta de cada uno de los servicios que conforman el paquete¹⁰.
- l) Curriculum Vitae documentado del personal NO CLAVE designado, según lo señalado en el numeral 5) de los términos de referencia, previstos en el capítulo III de la Sección específica de las bases.
- m) Informes que acrediten el liderazgo en soluciones en el mercado americano y/o europeo de al menos 2 años consecutivos en los últimos 4 años, según lo señalado en el numeral 6.3.4) de los términos de referencia, previstos en el capítulo III de la Sección Específica de las Bases.¹¹
- n) Documento que acredite contar con las certificaciones y Membresías señaladas en el numeral 7.1 de los términos de referencia, previstos en el capítulo III de la Sección Específica de las Bases.
- o) Anexo COFIDE 1.
- p) Anexo COFIDE 2.

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*

⁵ CONSULTA 43, formulada por SECURESOFT CORPORATION S.A.C.; Se confirma que en caso su representante no cuente con DNI, podrá presentar copia del Carnet de Extranjería.

⁶ 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/>

⁷ En tanto se implemente la funcionalidad en el SEACE, de conformidad con la Primera Disposición Complementaria Transitoria del Decreto Supremo N° 234-2022-EF.

⁸ Incluir solo en caso de la contratación bajo el sistema a suma alzada.

⁹ Incluir solo cuando resulte necesario para la ejecución contractual, identificar los costos de cada uno de los rubros que comprenden la oferta.

¹⁰ Incluir solo en caso de contrataciones por paquete.

¹¹ CONSULTA 55, formulada por SECURESOFT CORPORATION S.A.C.; Conforme a lo señalado por el área usuaria, se confirma que la documentación de sustento se podrá presentar en su idioma original. Haciendo presente que el postor ganador será responsable de la exactitud y veracidad de dichos documentos.

CONSULTA 56, formulada por SECURESOFT CORPORATION S.A.C.; Conforme a lo señalado por el área usuaria, se confirma que se podrá adjuntar informes o alguna evidencia que sustente el liderazgo de la tecnología ofertada emitido por empresas reconocidas como evaluadoras o consultoras o investigadoras de tecnologías de la información, como por ejemplo: Gartner, Forrester, Radicati, etc.

la Directiva "Participación de Proveedores en Consorcio en las Contrataciones del Estado".

- En los contratos periódicos de prestación de servicios en general que celebren las Entidades con las micro y pequeñas empresas, estas últimas pueden otorgar como garantía de fiel cumplimiento el diez por ciento (10%) del monto del contrato, porcentaje que es retenido por la Entidad durante la primera mitad del número total de pagos a realizarse, de forma prorrateada en cada pago, con cargo a ser devuelto a la finalización del mismo, conforme lo establece el numeral 149.4 del artículo 149 del Reglamento y numeral 151.2 del artículo 151 del Reglamento. Para dicho efecto los postores deben encontrarse registrados en el REMYPE, consignando en la Declaración Jurada de Datos del Postor (Anexo N° 1) o en la solicitud de retención de la garantía durante el perfeccionamiento del contrato, que tienen la condición de MYPE, lo cual será verificado por la Entidad en el link <http://www2.trabajo.gob.pe/servicios-en-linea-2-2> opción consulta de empresas acreditadas en el REMYPE.*
- En los contratos derivados de procedimientos de selección por relación de ítems, cuando el monto del ítem adjudicado o la sumatoria de los montos de los ítems adjudicados sea igual o menor a doscientos mil Soles (S/ 200,000.00), no corresponde presentar garantía de fiel cumplimiento de contrato ni garantía de fiel cumplimiento por prestaciones accesorias, conforme a lo dispuesto en el literal a) del artículo 152 del Reglamento.*

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 Haya¹².*
- La Entidad no puede exigir documentación o información adicional a la consignada en el presente numeral para el perfeccionamiento del contrato.*

2.4. PERFECCIONAMIENTO DEL CONTRATO

El contrato se perfecciona con la suscripción del documento que lo contiene. Para dicho efecto el postor ganador de la buena pro, dentro del plazo previsto en el artículo 141 del Reglamento, debe presentar la documentación requerida en mesa de partes de COFIDE sito en Calle Augusto Tamayo N° 160, San Isidro.

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 mensuales, posterior a la recepción de la documentación exigida en el numeral 10.3 Entregables de la Etapa Operativa, luego de otorgada la conformidad del servicio por parte del área

¹² Según lo previsto en la Opinión N° 009-2016/DTN.

usuaria; para efectos del pago de las contraprestaciones ejecutadas por el contratista, la Entidad deberá contar con la siguiente documentación:

- Entregables según especificaciones técnicas o términos de referencia.
- Informe de supervisión del servicio del departamento de TI
- Acta de conformidad del servicio
- Comprobante de pago.

Dicha documentación se debe presentar al Departamento de Tecnologías de la información en formato digital (PDF), vía url y correo electrónico a las siguientes direcciones:

- <https://facilita.gob.pe/t/4897>
- entregablesti@cofide.com.pe

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

1. OBJETO

Contratar un Servicio de Gestión y Operación de la Ciberseguridad como plataforma integrada, generando reducción de costos de operación, optimizando la calidad que comprende la estandarización de los servicios que componen el catálogo, mediante los requisitos y Acuerdos de Niveles de Servicio (SLAs del texto en inglés) establecidos, y reduciendo los riesgos de seguridad de la información.

2. FINALIDAD PÚBLICA

La presente contratación pública tiene como finalidad garantizar la continuidad y seguridad de los servicios de nuestra plataforma tecnológica, buscando elevar los niveles de eficiencia y satisfacción de los usuarios internos y externos de COFIDE.

Por la naturaleza del valor de los activos de información, por las mejores prácticas de seguridad y continuidad del Negocio, es que se requiere la contratación de un Servicio de Gestión y Operación de la Ciberseguridad

Este servicio está alineado con los lineamientos de políticas y Objetivos Estratégicos Institucionales previstos en el Plan Estratégico Institucional:

Eje Estratégico 2	Objetivo Estratégico Institucional
Organización Moderna y Sustentable	OEI6: Lograr la Excelencia Operativa

3. PROCESO DE ESTANDARIZACIÓN

No aplica

4. NÚMERO MÁXIMO DE CONSORCIADOS

El número máximo de consorciados es de tres (03).

El porcentaje mínimo de participación en la ejecución del contrato, para el integrante del consorcio que acredite mayor experiencia, es de 80%.

5. EQUIPO DE TRABAJO

El POSTOR deberá contar como mínimo con el siguiente personal, cabe mencionar que este detalle no limita a la empresa a colocar mayor cantidad o calidad de personal, de acuerdo con la eficiencia para el cumplimiento del servicio, **presentar el CV documentado del personal a la firma del contrato que no son PERSONAL CLAVE.**

Servicio	Rol	Formación	Experiencia	Capacitación y/o Certificación	
Gobierno y gestión del servicio	PERSONAL CLAVE	Titulado en las carreras de Ingeniería Electrónica	Mínimo 6 años en Gestión de Proyectos de TI y/o Seguridad	Por lo menos 01 de los siguientes cursos:	Por lo menos 01 de las siguientes certificaciones, como por ejemplo:

Servicio	Rol	Formación	Experiencia	Capacitación y/o Certificación	
	<p>(01) director del Proyecto¹³</p> <p><u>Función:</u> Responsable del servicio a nivel ejecutivo. Punto de escalamiento ante cualquier incumplimiento del servicio. Responsable de la correcta ejecución de la transición de entrada</p> <p>El personal podrá residir fuera del Perú y realizar servicio remoto.</p>	<p>o Ingeniería de Sistemas o Ingeniería Informática y de Sistemas o en Ingeniería de Cómputo y Sistemas o Ingeniería Informática o Ingeniería de Sistemas de Información o Ingeniería de Software</p>	<p>Gestionada, como Jefe o Gestor o Coordinador o Encargado o Director o Gerente o Subgerente</p>	<p>Curso, diplomado o programa en gerencia y/o gestión de proyectos, de mínimo 100 horas.</p>	<p>- Certificación PMP vigente - Certificación PRINCE2 vigente - Certificación en ISO 27032 Gerente de Ciberseguridad vigente - Certificación en Experto en Gestión de Proyectos PMI. - Certificación en SCRUM Master Professional Certificate.</p>
	<p>PERSONAL CLAVE (01) Líder de CSIRT¹⁴</p> <p><u>Función:</u> Profesional encargado de liderar el equipo de respuesta ante incidentes. Responsable de comunicación a alto nivel gerencial.</p>	<p>Profesional Titulado o Bachiller en Ingeniería Electrónica o Ingeniería de Sistemas o en Tecnologías de la Información o en Ingeniería de Cómputo y Sistemas o Ingeniería Informática o Ingeniería de Sistemas de Información o Ingeniería de Software</p>	<p>Mínimo de cuatro (4) años en proyectos de plataformas de Seguridad, CyberSOC o Ciberseguridad o Servicio de Respuesta ante Incidentes, como Jefe o Líder o Coordinador</p>	<p>Por lo menos 03 de los siguientes cursos: -Curso, diplomado o programa de ITIL, de mínimo 20 horas. - Curso, diplomado o programa de ISO/IEC 27001 Auditor Líder, de mínimo 30 horas. -Curso, diplomado o programa de Transformación Digital, de mínimo 30 horas. - Curso, diplomado o programa de respuesta ante incidentes, de mínimo 50 horas.</p>	<p>Por lo menos 01 de las siguientes certificaciones, como por ejemplo: -CompTIA Security+, vigente -(ISC) Certified Information Systems Security Professional (CISSP), vigente -Lead Cybersecurity Professional Certificate (LCSPC), vigente -Certificación en PECB Certified ISO/IEC 27001 Lead Implementer, vigente</p>

¹³ **CONSULTA 29**, formulada por DIGIWARE S.A.C; Conforme a lo señalado por el área usuaria, se acepta en parte lo solicitado; por lo que, para el Director del proyecto, se aceptará que:

* Personal se encuentre ubicado fuera de Perú.

* Servicio remoto.

Así como las siguientes certificaciones relacionadas al perfil:

- Certificación en Experto en Gestión de Proyectos PMI.

- Certificación en SCRUM Master Professional Certificate.

Que, no se aceptarán las demás certificaciones, debido a que no se ha podido validar que las mismas se encuentren efectivamente relacionadas al perfil.

¹⁴ **CONSULTA 30**, formulada por DIGIWARE S.A.C; Conforme a lo señalado por el área usuaria, se recuerda que las consultas y observaciones deberán ser formuladas de forma clara y precisa, siendo que en la presente consulta no indica a que sección del perfil se debe realizar el cambio solicitado (Formación y/o experiencia y/o capacitación y/o certificación); por lo tanto, no se acepta lo solicitado.

Servicio	Rol	Formación	Experiencia	Capacitación y/o Certificación	
				- Curso, diplomado o programa de atención de ciberamenazas, de mínimo 30 horas.	
	PERSONAL CLAVE (01) Líder de CyberSOC ¹⁵ Función: Profesional encargado de liderar el equipo de CyberSOC. Responsable del servicio a nivel operativo. Punto de escalamiento ante cualquier incumplimiento del servicio. Responsable de la correcta ejecución del servicio.	Profesional Titulado o Bachiller en Ingeniería Electrónica o en Telecomunicaciones o en Redes y Comunicaciones o Sistemas o en Tecnologías de la Información o en Cómputo y Sistemas o Informática o de Sistemas de Información o Ingeniería de Seguridad	Mínimo de seis (6) años en servicios especializados de CyberSOC, Security Advisor o Ciberinteligencia como Especialista o Analista Técnico o Jefe o Líder	Por lo menos 02 de los siguientes cursos: - Curso, diplomado o programa de Seguridad de Sistemas de Información, de mínimo 100 horas. - Curso, diplomado o programa de Certified Information Security Manager (CISM), de mínimo 20 horas. - Curso, diplomado o programa de Certified Information Systems Security Professional (CISSP), de mínimo 40 horas. - Curso, diplomado o programa en gestión de servicio de SOC o CyberSOC, de mínimo 50 horas.	Por lo menos 02 de las siguientes certificaciones, como por ejemplo: -CompTIA Security+, vigente - EC-Council Certified Security Analyst (ECSA), vigente -(ISC) Certified Information Systems Security Professional (CISSP), vigente -Lead Cybersecurity Professional Certificate (LCSPC), vigente -Certificación Ethical Hacker, vigente
	PERSONAL CLAVE (01) Service Manager ¹⁶ Función:	Profesional Titulado en Ingeniería Electrónica o en Telecomuni	Mínimo de seis (6) años en gestionar o liderar o supervisar servicios de	Por lo menos 02 de los siguientes cursos: - Curso, diplomado o	Por lo menos 01 de las siguientes certificaciones, como, por ejemplo: - Certificación en ISO 27001

¹⁵ **CONSULTA 31**, formulada por DIGIWARE S.A.C; Conforme a lo señalado por el área usuaria, se recuerda que las consultas y observaciones deberán ser formuladas de forma clara y precisa, siendo que en la presente consulta no indica a que sección del perfil se debe realizar el cambio solicitado (Formación y/o experiencia y/o capacitación y/o certificación); por lo tanto, no se acepta lo solicitado.

¹⁶ **CONSULTA 32**, formulada por DIGIWARE S.A.C; Conforme a lo señalado por el área usuaria, se recuerda que las consultas y observaciones deberán ser formuladas de forma clara y precisa, siendo que en la presente consulta no indica a que sección del perfil se debe realizar el cambio solicitado (Formación y/o experiencia y/o capacitación y/o certificación); por lo tanto, no se acepta lo solicitado.

Servicio	Rol	Formación	Experiencia	Capacitación y/o Certificación	
	Responsable del servicio a nivel ejecutivo. Punto de contacto de COFIDE con relación al servicio. Responsable del cumplimiento contractual y de la correcta ejecución del servicio	caciones o en Redes y Comunicaciones o Sistemas o en Tecnologías de la Información o en Cómputo y Sistemas o Informática o de Sistemas de Información o Ingeniería de Seguridad	ciberseguridad como Especialista o Analista Técnico o Jefe o Líder	programa de Seguridad de Sistemas de Información, de mínimo 100 horas. - Curso, diplomado o programa de Certified Information Security Manager (CISM), de mínimo 20 horas. - Curso, diplomado o programa de Certified Information Systems Security Professional (CISSP), de mínimo 40 horas. - Curso, diplomado o programa en Gestión de Servicios de Tecnologías de la Información, de mínimo 40 horas. - Curso y/o Diplomado y/o programa de Especialización en Gestión de Proyectos, de mínimo 100 horas. ¹⁷	implementador líder, vigente - ISO 27032 Gerente de Ciberseguridad, vigente - Certificación ITIL v3 o v4 Foundation, vigente - Certificación de Ciberseguridad o Seguridad Informática o Seguridad de la Información, vigente.
S1 - Servicio de evaluación de Seguridad TI	Gestor de riesgos sobre activos TI Función: Profesional encargado de liderar la evaluación de las soluciones de seguridad de COFIDE. Valida y aprueba el trabajo realizado por los analistas	Bachiller en las carreras de en las carreras de Ingeniería Informática y/o telecomunicaciones y redes y/o Ingeniería de Sistemas e Informática y/o Ingeniería	Mínimo 2 años en proyectos de Ciberseguridad de TI, Seguridad de la Información, Seguridad Informática, Configuración de seguridad en redes y nube, Soporte o Implementación de	Por lo menos 01 de los siguientes cursos: -Cursos en gestión de riesgos de seguridad de la información -Cursos en gestión de infraestructuras TI -Cursos en soluciones de seguridad	Por lo menos 01 de las siguientes certificaciones, como, por ejemplo: -GIAC Certified Forensic Analyst (GCFA) -Certified Ethical Hacker CEH -Certified Penetration Testing Engineer - CPTE -Certified Secure Web Application Engineer - CSWAE.

¹⁷ **CONSULTA 42 y 47**, formuladas por SECURESOFTECH CORPORATION S.A.C.; Conforme a lo señalado por el área usuaria y, con ocasión a la integración de las bases, se acepta lo solicitado, por lo que se acepta como una opción adicional el curso, diplomado o programa de Especialización en Gestión de Proyectos, de mínimo 100 horas; dado que las funciones solicitadas para este personal también son de gestión.

Servicio	Rol	Formación	Experiencia	Capacitación y/o Certificación	
		electrónica y/o Ingeniería Informático y/o Ingeniería Industrial y/o Ingeniería de Sistemas y/o Ingeniería de Sistemas Empresariales y/o Ingeniería Informática y de Sistemas.	Soluciones de Seguridad Informática y/o Ciberseguridad .	- Curso Certificación en el marco de trabajo para los sistemas de seguridad de la NIST - Curso, diplomado o programa de Certified Information Systems Security Professional (CISSP)	- Fortinet NG Firewall - Kaspersky Cybersecurity Training - McAfee NSP IPS - McAfee Web Gateway - Fortinet NSE4 - Technical Certified Protect Deployment. - Certified Professional - Threat Management and Defense - Certified Endpoint Security - Otros certificados relacionados a Herramientas de Ciberseguridad o Seguridad TI.
	Analista(s) de riesgos TI Función: Profesionales encargados de realizar el análisis de las soluciones de seguridad, encontrar las brechas y plantear planes de acción	Bachiller y/o¹⁸ Titulado Técnico en las carreras de Informática y/o telecomunicaciones y redes y/o Sistemas e Informática y/o electrónica y/o Informático y/o Industrial y/o Sistemas y/o Ingeniería de Tecnologías de Información y Sistemas.	Mínimo 1 año en proyectos de Ciberseguridad de TI, Seguridad de la Información, Seguridad Informática, Configuración de seguridad en redes y nube, Soporte o Implementación de Soluciones de Seguridad Informática y/o Ciberseguridad .	Por lo menos 01 de los siguientes cursos: - Cursos en gestión de riesgos de seguridad de la información - Cursos en gestión de infraestructuras TI - Cursos en soluciones de seguridad - Curso de Vulnerability Management	Por lo menos 01 de las siguientes certificaciones, como, por ejemplo: - CEH - CPTE - CSWAE - Certificación herramientas de escaneo de vulnerabilidades - Fortinet NG Firewall - Kaspersky Cybersecurity Training - McAfee NSP IPS - Technical Certified Protect Deployment. - Network Security Expert Certification - Certified Professional - Threat Management and Defense - Certified Endpoint Security - Otros certificados relacionados a Herramientas de Ciberseguridad o Seguridad TI.
S2 - Servicio de Gestión de	Analista(s) de operación de equipos y	Bachiller y/o¹⁹ Titulado	Mínimo 1 año en gestión y operación de	Cursos de operación y/o administración	Por lo menos 01 certificación del fabricante de los

¹⁸ **CONSULTA 50**, formulada por SECURESOFT CORPORATION S.A.C.; Conforme a lo señalado por el área usuaria y, con ocasión a la integración de las bases, se acepta lo solicitado; por lo que, se acepta como formación del Analista(s) de riesgos TI el grado de bachiller, al tratarse de un alcance superior al mínimo solicitado de Titulado Técnico.

¹⁹ **CONSULTA 51**, formulada por SECURESOFT CORPORATION S.A.C.; Conforme a lo señalado por el área usuaria y, con ocasión a la integración de las bases, se acepta lo solicitado; por lo que, se acepta como formación del Analista(s) de operación de equipos y soluciones de seguridad el grado de bachiller, al tratarse de un alcance superior al mínimo solicitado de Titulado Técnico.

Servicio	Rol	Formación	Experiencia	Capacitación y/o Certificación	
los Equipos o Activos o Soluciones de Seguridad	soluciones de seguridad Función: Profesionales encargados de la ejecución de los cambios y requerimientos en las plataformas que estén bajo administración del PROVEEDOR.	Técnico en las carreras de Informática y/o telecomunicaciones y redes y/o Sistemas e Informática y/o electrónica y/o Informático y/o Industrial y/o Sistemas y/o Ingeniería de Sistemas.	equipos y soluciones de seguridad (WAF, WAN, Firewall, IPS, IDS, entre otros), Soporte o Implementación de Soluciones de Seguridad Informática y/o Ciberseguridad .	de equipos y soluciones de seguridad de las marcas que se van a operar por lo menos 40 horas	productos que el Contratista operará (Fortinet y/o Kaspersky y/o Forcepoint y/o Trellix y/o McAfee)
S3 - Servicios de Detección Avanzada	Gestor de Seguridad Función: Supervisor del equipo SOC gestiona el monitoreo y análisis de los eventos y la respuesta a los incidentes	Bachiller en las carreras de Ingeniería Informática y/o telecomunicaciones y redes y/o Ingeniería de Sistemas e Informática y/o Ingeniería electrónica y/o Ingeniería Informático y/o Ingeniería Industrial y/o Ingeniería de Sistemas y/o Ingeniería Informática y de Sistemas.	Mínimo 2 años en: -Identificación, clasificación, análisis de eventos de seguridad -Identificación y gestión de incidentes de seguridad -Gestión y operación de soluciones SIEM - Soporte o Implementación de Soluciones de Seguridad Informática y/o Ciberseguridad .	Por lo menos 01 de los siguientes cursos: -Cursos de identificación y clasificación de eventos de seguridad y/o Cursos de gestión de incidentes y/o - Cursos para el desarrollo de casos de uso y/o Cursos de implementación y operación del SIEM y/o Cursos en soluciones de seguridad	Contar con al menos 01 de las certificaciones en tecnologías/productos tipo SIEM y de seguridad, como, por ejemplo: -RSA NetWitness Logs & Network Certified Administrator. -Certified Product Specialis: Security Information and Event Management (SIEM) -- McAfee: Security Information and Event Management 10 course. -Certified Enterprise Security Manager – SIEM. -Certified Professional - Threat Management and Defense -Certified Endpoint Security -Otros certificados relacionados a tecnologías/productos SIEM.
	Analista(s) de seguridad Función: Encargados del monitoreo y análisis de eventos de seguridad.	Bachiller en las carreras de Ingeniería Informática y/o telecomunicaciones y	Mínimo 2 años en cualquiera de los 3 criterios mencionados: -Identificación, clasificación, análisis de	Por lo menos 01 de los siguientes cursos: Cursos de identificación y clasificación de eventos de	Entre los Analistas de seguridad asignados, cuenten cada uno con al menos una certificación en tecnologías o

Servicio	Rol	Formación	Experiencia	Capacitación y/o Certificación	
	Brindan soporte nivel 0 y 1 ante los incidentes que se presenten	redes y/o Ingeniería de Sistemas e Informática y/o Ingeniería electrónica y/o Ingeniería Informático y/o Ingeniería Industrial y/o Ingeniería de Sistemas y/o Ingeniería Electrónica y Telecomunicaciones.	eventos de seguridad -Identificación y gestión de incidentes de seguridad -Gestión y operación de soluciones SIEM - Soporte o Implementación de Soluciones de Seguridad Informática y/o Ciberseguridad .	seguridad por lo menos 40 horas y/o Cursos de gestión de incidentes por lo menos 40 horas y/o Cursos para el desarrollo de casos de uso por lo menos 40 horas y/o Cursos de implementación y operación del SIEM por lo menos 40 horas y/o Cursos en soluciones de seguridad por lo menos 40 horas y/o curso de CISSP de 40 horas y/o maestría en dirección de sistemas y tecnología de la información	productos tipo SIEM, como por ejemplo: - Fortinet: SIEM - McAfee: Security Information and Event Management 10 course. -Certified Enterprise Security Manager – SIEM. -Otros certificados de productos tipo SIEM
S4 - Servicios Respuesta a Incidentes como Servicio	Especialista en gestión de incidentes Función: Encargados de la respuesta a incidentes graves de Ciberseguridad, brindan el nivel 3 de respuesta	Bachiller en las carreras de Ingeniería Informática y/o telecomunicaciones y redes y/o Ingeniería de Sistemas e Informática y/o Ingeniería electrónica y/o Ingeniería Informático y/o Ingeniería Industrial y/o Ingeniería de Sistemas	Mínimo 2 años liderando SOCs y/o equipos de gestión de incidentes - Soporte o Implementación de Soluciones de Seguridad Informática y/o Ciberseguridad .	Por lo menos 01 de los siguientes cursos: -Cursos de identificación y clasificación de eventos de seguridad - Cursos de gestión (identificación, clasificación, generación de planes, respuesta, contención, erradicación y recuperación) de incidentes -Cursos en soluciones de seguridad	Contar con al menos 01 de las certificaciones, como, por ejemplo: -Certificado ISO 27035 Incident Manager -Gestión y respuesta ante incidentes -Lead Cybersecurity Professional Certificate (LCSPC) - EXIN Business Continuity Management Foundation -Certificación en seguridad de la información. -Certified Endpoint Security -Otros certificados relacionados a Gestión y respuesta ante incidentes.
	Analista(s) de respuesta a incidentes	Bachiller y/o ²⁰ Titulado	Mínimo 1 año en:	Por lo menos 01 de los	Contar con al menos 01 certificación, como, por ejemplo:

²⁰ CONSULTA 52, formulada por SECURESOFT CORPORATION S.A.C.; Conforme a lo señalado por el área usuaria y, con ocasión a la integración de las bases, se acepta lo solicitado; por lo que, se acepta como formación del Analista(s) de respuesta a incidentes el grado de bachiller, al tratarse de un alcance superior al mínimo solicitado de Titulado Técnico.

Servicio	Rol	Formación	Experiencia	Capacitación y/o Certificación	
	Función: Encargados de la respuesta a incidentes graves de Ciberseguridad, brindan el nivel 2 de respuesta	Técnico en las carreras de Informática y/o telecomunicaciones y redes y/o Sistemas e Informática y/o electrónica y/o Informático y/o Industrial y/o Sistemas y/o Ingeniería Empresarial y de Sistemas.	- Operaciones de SOCs (incidentes de seguridad de la información) - Soporte o Implementación de Soluciones de Seguridad Informática y/o Ciberseguridad .	siguientes cursos: -Cursos de gestión (identificación, clasificación, generación de planes, respuesta, contención, erradicación y recuperación) de incidentes por lo menos 40 horas -Cursos en soluciones de seguridad por lo menos 40 horas -Seguridad informática de 25 horas	- Certificado ISO 27035 Incidente Manager - Gestión y respuesta ante incidentes -Lead Cybersecurity Professional Certificate (LCSPC) -Certificado ISO 27032 -Certificado ISO 27001 -Certified Information systems Security Professional -CISSP -Network Security Expert Certification -Certified Professional - Threat Management and Defense -Certified Targeted Attack Protection --Otros certificados relacionados a Gestión y respuesta ante incidentes.
S5 -Servicio de escaneo, análisis e identificación de vulnerabilidades de las aplicaciones web	Analista(s) de soluciones de escaneo e identificación de vulnerabilidades de aplicaciones web Profesionales encargados de la ejecución de los escaneos e identificación de vulnerabilidades de aplicaciones web	Bachiller y/o ²¹ Titulado Técnico en las carreras de Informático y/o Industrial y/o Informático y de sistemas y/o Industrial Sistemas e Informática y/o Ingeniería de Tecnologías de Información y Sistemas.	Mínimo 1 año en: - Gestión y análisis de vulnerabilidades de aplicaciones web con soluciones de seguridad tipo WAS -Soporte o Implementación de Soluciones de Seguridad Informática y/o Ciberseguridad .	Cursos de operación y/o administración de soluciones de análisis de vulnerabilidades de aplicaciones WEB (WAS) de la marca que se van a operar	Por lo menos 01 certificación del fabricante del producto que el proveedor operará
S6 -Servicio de ciberinteligencia	Analista(s) de monitoreo de ciberinteligencia Profesionales encargados del monitoreo de amenazas en la	Bachiller y/o Titulado Técnico en las carreras de Informático y/o Industrial	Mínimo 1 año en: - Monitoreo de CyberSOC o monitoreo de amenazas de seguridad o ciberseguridad	Por lo menos 01 de los siguientes cursos: Cursos de identificación y clasificación de eventos de	Contar con al menos 01 certificación, como, por ejemplo: - Certificado ISO 27035 Incidente Manager - Gestión y respuesta ante

²¹ **CONSULTA 53**, formulada por SECURESOFT CORPORATION S.A.C.; Conforme a lo señalado por el área usuaria y, con ocasión a la integración de las bases, se acepta lo solicitado; por lo que, se acepta como formación del Analista(s) de soluciones de escaneo e identificación de vulnerabilidades de aplicaciones web el grado de bachiller, al tratarse de un alcance superior al mínimo solicitado de Titulado Técnico.

Servicio	Rol	Formación	Experiencia	Capacitación y/o Certificación	
	deep y dark web, así como de otros vectores de ciberseguridad.	y/o Informático y de y/o Industrial Sistemas e Informática y/o Ingeniería de Sistemas ²²	-Soporte o Implementación de Soluciones de Seguridad Informática y/o Ciberseguridad .	seguridad por lo menos 40 horas y/o Cursos de gestión de incidentes por lo menos 40 horas y/o Cursos para el desarrollo de casos de uso por lo menos 40 horas y/o Cursos de implementación y operación del SIEM por lo menos 40 horas y/o Cursos en soluciones de seguridad por lo menos 40 horas y/o curso de CISSP de 40 horas y/o maestría en dirección de sistemas y tecnología de la información	incidentes -Lead Cybersecurity Professional Certificate (LCSPC) -Certificado ISO 27032 -Certificado ISO 27001 -Certified Information systems Security Professional -CISSP -Network Security Expert Certification -Certified Professional - Threat Management and Defense -Certified Targeted Attack Protection --Otros certificados relacionados a monitoreo de amenazas de ciberseguridad.

Equipo de Trabajo

6. DESCRIPCIÓN DEL SERVICIO

COFIDE requiere contratar el Servicio de Gestión y Operación de la Ciberseguridad el cual está constituido por un conjunto de servicios de Seguridad informática, Centro de Operaciones de Seguridad (SOC) y Ciberseguridad. Estos se encuentran enmarcados en un modelo que busca optimizar la calidad de los servicios de protección de la infraestructura de TI y la información digital, beneficiando a todas las partes interesadas y tomando en cuenta la complejidad de operación característica de COFIDE.

Los servicios de Gestión y Operación de Ciberseguridad son seis (06) comprende las siguientes prestaciones:

Ítem	Nombre del servicio	Frecuencia	Descripción del servicio
S1	Servicio de evaluación de Seguridad TI	Anual Una única vez a demanda ²³	Identificación de riesgos de seguridad basados en el inventario de activos IT y su ciclo de vida (gabinete)
S2	Servicio de Gestión de los Equipos o Soluciones de Seguridad	Continua	Operación de los activos de seguridad de la empresa (propios)

²² CONSULTA 48, formulada por SECURESOFT CORPORATION S.A.C.; Conforme a lo señalado por el área usuaria y, con ocasión a la integración de bases, se acepta lo solicitado; por lo que, se acepta la carrera de Ingeniería de Sistemas como formación para el Analista de Monitoreo de Ciberseguridad.

CONSULTA 49, formulada por SECURESOFT CORPORATION S.A.C.; Conforme a lo señalado por el área usuaria y, con ocasión a la integración de las bases, se acepta lo solicitado; por lo que, se acepta como formación del Analista de Monitoreo de Ciberseguridad el grado de bachiller, al tratarse de un alcance superior al mínimo solicitado de Titulado Técnico.

²³ CONSULTA 54, formulada por SECURESOFT CORPORATION S.A.C.; Conforme a lo señalado por el área usuaria y, con ocasión a la integración de las bases, se confirma que la frecuencia para este servicio será de una única vez como se indica en el detalle del punto 6.1 de los términos de referencia (p. 28 de las bases administrativas)

S3	Servicios de Detección Avanzada	Continua	Monitoreo y alerta temprana sobre activos de la empresa
S4	Servicios Respuesta a Incidentes	Continua	Gestión de incidentes
S5	Servicio de Identificación de las Vulnerabilidades en Aplicaciones	Continua (a demanda)	Identificación de las Vulnerabilidades en Aplicaciones
S6	Servicio de Ciberinteligencia	Continua	Monitoreo y alerta temprana sobre uso de palabras o frases clave (actividades en la web)

Servicios de Ciberseguridad

Objeto de la Contratación

Los Servicio de Gestión y Operación de la Ciberseguridad materia de la presente contratación que se detallan a continuación:

- a. **S1-Servicio de evaluación de Seguridad TI.** Servicio diseñado para la identificación de riesgos de seguridad basados en el inventario de activos TI (equipos y soluciones de seguridad), su ciclo de vida y la información de contexto del activo
- b. **S2-Servicio de Gestión de los Equipos o Soluciones de Seguridad.** Servicio dimensionado para establecer y ejecutar un marco de trabajo para que se realice la configuración o se coordine, con COFIDE u otros Contratistas participantes para que se configuren, los firewalls, IPS, IDS, entre otros equipos de seguridad perimetral y soluciones de seguridad.
- c. **S3-Servicios de Detección Avanzada.** Este servicio se realizará mediante el uso de la tecnología de correlación de eventos que permite la gestión de los logs y los flujos generados/consumidos por los dispositivos para la detección de eventos de seguridad. El servicio considera un método de detección avanzado en base a casos de uso de ciberseguridad, el mismo que brindará información de la eficiencia de cada caso de uso aplicado.
- d. **S4-Servicios Respuesta a Incidentes como Servicio.** La dimensión del servicio abarca lo siguiente:
 - Proveer un modelo de anticipación y respuesta frente a crisis derivadas de incidentes graves de seguridad.
 - Diseñar todos los mecanismos necesarios de contención, análisis, respuesta, erradicación y recuperación como parte de la gestión de incidentes de seguridad.
 - Análisis forense digital y de seguridad.
- e. **S5-Servicio de Identificación de las Vulnerabilidades en Aplicaciones.** El Servicio consiste en realizar un Hacking ético a las aplicaciones que incluya: Un análisis de vulnerabilidades automatizado mediante uso de soluciones, cuyo resultado sea un informe de auditoría, y una reauditoría para certificar la corrección de vulnerabilidades.
- f. **S6-Servicios de Ciberinteligencia.** Servicio que consiste en el uso de una solución para identificar amenazas y riesgos respecto de la reputación, marcas y/o conceptos importantes de COFIDE, de tal modo que se brinde visibilidad más allá del ciclo de vida de los ataques, añadiendo contexto y prioridad a las amenazas globales.

6.1 SERVICIO DE EVALUACIÓN DE SEGURIDAD TI (S1)

Servicio diseñado para la identificación de riesgos de seguridad basados en el inventario de activos TI (equipos y soluciones de seguridad), su ciclo de vida y la información de contexto del activo.

El servicio S1 se ejecutará a demanda dentro de los primeros dos (02) años del servicio e inicia a partir de la firma del **Acta de inicio del servicio S1** que considera la evaluación de los activos de seguridad de TI.

Se evalúa la información de contexto del activo TI (marca, modelo, serie, rol del activo, ubicación dentro del mapa de red de componentes TI, información de la configuración),

arrojando como resultado una hoja de ruta para la mejora de los activos TI en términos de seguridad, lo cual puede incluir mejores prácticas de configuración de los activos, ampliación de las capacidades de los activos, la adquisición de nuevos activos o reemplazo de los activos existentes. Este servicio se cotiza por la cantidad de activos TI a evaluar.

A continuación, la cantidad de activos a considerar:

EMPRESA	CANTIDAD DE ACTIVOS
COFIDE	10 11 ²⁴

Cantidad de Activos del servicio S1

Este servicio se podrá realizar de manera remota o si el caso lo amerita en gabinete, es decir en las instalaciones del COFIDE, con la información detallada de los activos TI y debe contar con las siguientes características:

6.1.1.Escalabilidad

La escalabilidad permitirá integrar otros activos al servicio mediante un nuevo requerimiento a o adenda al contrato, solo puede ser posible mientras esté en la Etapa Operativa del Servicio y antes de que inicie la evaluación de activo TI de COFIDE programado.

6.1.2.Seguridad

El Contratista deberá contar con los procedimientos y los mecanismos de seguridad física y lógica que reduzcan los riesgos de interrupción de la prestación de los servicios de Gestión y Operación de Ciberseguridad para COFIDE, lo cual se acreditará con los certificados o procedimientos respectivos del servicio.

6.1.3.Políticas del Servicio.

Este servicio considera las siguientes políticas:

- Trabajar con el total de los activos TI proporcionados por COFIDE.
- El postor puede aplicar la metodología que considere conveniente basado en cumplir con el objetivo del servicio y los SLAs.²⁵
- Los tiempos de las actividades serán coordinadas en la etapa de planificación y en ella se definirán las ventanas de recopilación de información
- Elaborar un informe de acciones correctivas y de mejora según la metodología empleada que tenga como fundamento el plan de tratamiento de riesgos de Ciberseguridad, asociada a las normativas ISO 31000 o ISO 27001.
- Los resultados de la prestación de este servicio serán compartidos por el contratista mediante un acceso privado a un repositorio compartido o en nube al cual tendrán acceso COFIDE, de tal manera que la información se encuentre en todo momento protegida de accesos no autorizados.

6.1.4.Características de los Componentes del Servicio

El detalle de las actividades a desarrollar para la evaluación de riesgos de los activos TI, se presentan a continuación:

- Preparación e inicio.** Se presentará el plan de trabajo y los requerimientos necesarios para la ejecución del servicio. Esta fase contempla lo siguiente:
 - Presentación del equipo de trabajo.
 - Establecimiento de los mecanismos de comunicación y seguimiento.

Resultados

- Cronograma con el detalle de actividades para ejecutar el servicio.

²⁴ CONSULTA 44, formulada por SECURESOFTECH CORPORATION S.A.C.; Conforme a lo señalado por el área usuaria, se acepta lo solicitado, por lo que se confirma que para el presente servicio se considerarán los activos que se encuentran dentro del punto 6.1.5. de los términos de referencia, los cuales suman 11.

²⁵ CONSULTA 2, formulada por DIGIWARE S.A.C.; Conforme a lo señalado por el área usuaria, se aclara que los SLAs del Servicio 1, solo serán medidos en la etapa de remediación de acuerdos a los SLAs de la gestión de requerimientos.

- Agenda de entrevistas con el personal de COFIDE.
- Estructura de los documentos base para ejecutar el servicio.

b. Levantamiento de información. El Contratista asignará un equipo de trabajo para recoger toda la información necesaria que permita cumplir con los objetivos del servicio. Para ello El Contratista debe considerar las siguientes actividades:

- Levantamiento de Información de los activos que forman parte del alcance.
- Elaboración de entrevistas con cada responsable del activo TI para completar la información, entender las estrategias establecidas en el área de Tecnologías de la Información y con objetivos a alcanzar.
- Entendimiento de las necesidades y objetivos necesarios y establecidos para COFIDE

Resultados

Inventario de activos con detalles técnicos.

c. Análisis y evaluación de riesgos. El Contratista debe considerar para la evaluación las medidas concretas aplicadas a cada activo y su exposición. Para esta etapa el Contratista evalúa la situación actual de cada activo TI a partir de los datos e información del contexto recogida en la etapa de levantamiento de información y desarrolla las siguientes actividades:

- Revisión de obsolescencia en base a marca, modelo, versión de software y upgrade.
- Revisión de configuración de los activos en base a buenas prácticas.
- Revisión del mapa de red, diseño y arquitectura.
- Análisis del estado de los activos (Sistema Operativo, Parches, Licenciamiento, etc.).
- Análisis de la infraestructura tecnológica (Obsolescencia, uso, etc).
- Definición de escenarios de riesgos.
- Integración y análisis de resultados.
- Ponderación de riesgos.
- Elaboración de Documentación Inicial (Diagramas e Informes).

Resultados

Identificación de riesgos y limitaciones de los activos respecto a su ciclo de vida.

6.1.5.Línea Base S1

El servicio será dimensionado tomando en cuenta los activos TI definidos, la línea base para el servicio de Evaluación de Seguridad TI, donde también está incluido las consolas de gestión de algunos activos que se indican a continuación:

Item	Activo	Cantidad	Marca	Modelo
01	Firewall Perimetral – Data Center Principal (FortiAnalyzer)	1 (HA - Activo/pasivo)	FORTINET	FORTIGATE 400E
02	Firewall Interno (FortiAnalyzer)	1 (HA - Activo/pasivo)	FORTINET	FORTIGATE 600F
03	IPS SENSOR (Appliance Físico)	1	TRELLIX	NS7500
04	Antispam (Proofpoint Email Protección SaaS)	1	PROOFPOINT	SAAS
06	Detección avanzada de amenazas y de respuesta automatizada	1	KARSPERSKY	Next XDR Expert
07	WAF (SaaS)	1	FORTINET	Forticloud
08	NAC (Appliance Virtual)	1	FORTINET	FNVMCA

09	Active Directory (AD)	3 (HA - Activo/Activo)	MICROSOFT	AD
10	Firewall Perimetral – Data Center de Contingencia (FortiAnalyzer)	1	FORTINET	FORTIGATE 60F

Línea base del servicio S1

Consideraciones

- El Contratista deberá contar con personal calificado, con experiencia y conocimiento para realizar la evaluación de riesgos de seguridad de los activos TI.
- De requerir recursos tecnológicos (hardware o software) para ejecutar el servicio, el Contratista deberá proporcionarlo a su equipo de trabajo asignado.

6.1.6.Facilidades Mínimas

Los recursos mínimos requeridos para este servicio son:

a. Procesos o Metodologías

Metodología para la apreciación de riesgos de activos TI.

b. Personal

El Contratista deberá contar como mínimo con el equipo solicitado en el numeral 5.

EQUIPO DE TRABAJO para este servicio.

El Contratista deberá presentar al menos un personal especializado con los roles indicados, es responsabilidad del contratista de incrementar los recursos humanos, bajos los roles indicados, para atender la demanda del servicio según los SLAs establecidos y los requisitos del servicio

6.1.7.Tecnologías

- Correo electrónico corporativo del Contratista para coordinaciones.
- Sistemas de videoconferencia para realizar las coordinaciones.
- Estaciones de trabajo para los recursos humanos proporcionado por el Contratista.
- Acceso a Internet.

Nota: El Contratista debe demostrar que posee propiedad sobre el hardware y/o software a utilizar. En el caso de utilizar servicios arrendados deberá demostrar que posee acceso al servicio.

6.1.8.Responsabilidades de El Contratista

El Contratista deberá garantizar que cuenta con los recursos que permitan ejecutar el servicio solicitado de forma efectiva, para lo cual deberá cumplir con las siguientes responsabilidades:

- Asignar un grupo de trabajo que cuente con los conocimientos y experiencia para la ejecución del servicio de evaluación de riesgos de los activos TI.
- Planificar las etapas de evaluación de riesgos de los activos TI y sus limitaciones respecto de su ciclo de vida.
- Garantizar que el servicio se realizará considerando la evaluación de una muestra de activos por tipología.
- Agendar con la debida anticipación las entrevistas con el personal de COFIDE en la etapa de levantamiento de información de los activos TI.
- Presentar un informe para la mejora de los activos TI en términos de seguridad, que incluye la ampliación de las capacidades de los activos, la adquisición de nuevos activos o reemplazo de los activos existentes, en función de los riesgos identificados de ser necesario.
- Seguimiento mensual de ejecución plan de mitigación de riesgos identificados, planes de acción y recomendaciones de mejora

6.1.9.Responsabilidades de COFIDE

Se detallan a continuación para el servicio las responsabilidades de COFIDE:

a. Durante la implementación o transición del servicio:

Remitir información adecuada y correcta de los inventarios actualizados de los activos TI y su contexto.
Designar el personal de contacto autorizado para el servicio.

b. Durante el servicio:

Designar a las personas con responsabilidad suficiente, que serán autorizadas para servir como coordinadores del servicio.

6.2 SERVICIO DE GESTIÓN DE LOS EQUIPOS O SOLUCIONES DE SEGURIDAD (S2)

Servicio dimensionado para establecer y ejecutar un marco de trabajo para que se realice la configuración o se coordine, con COFIDE u otros Contratistas de COFIDE participantes para que se configuren, los firewalls, IPS, NAC, entre otros equipos de seguridad y soluciones de seguridad.²⁶

Este servicio se realiza por requerimiento y los resultados se informan con una frecuencia mensual durante el período de ejecución del servicio y considera para la gestión aquellos activos que son de seguridad y gestionados por COFIDE. El resultado del servicio es la generación de un informe con las configuraciones realizadas. Este servicio se cotiza por la cantidad de activos TI a operar. A continuación, presentamos la cantidad de activos a considerar para este servicio:

EMPRESA	CANTIDAD DE ACTIVOS
COFIDE	06

Cantidad de Activos del servicio S2

Este servicio se realiza desde las instalaciones del Contratista usando una conexión remota (VPN Site-to-Site redundante) hacia los equipos a operar, con la información detallada de los activos TI seleccionados y debe contar con las siguientes características:

6.2.1 Escalabilidad

La escalabilidad deberá basarse en los siguientes aspectos: Tecnología, Procesos y Personas.

- a. Tecnología:** COFIDE tienen planificado incorporar nuevos servicios a la Gestión y Operación de Ciberseguridad, por lo tanto, el servicio debe estar soportado para permitir el crecimiento en la cantidad de los activos, usuarios y requerimientos de operación que se pueden atender por cada servicio.
- b. Procesos y Personas:** COFIDE puede requerir servicios adicionales, relacionados con los servicios de Gestión y Operación de Ciberseguridad (por ejemplo, actualizaciones en la arquitectura desplegada debido a migraciones en los activos que se están monitoreando) e incluso servicios complementarios, de conformidad con lo dispuesto en la Ley de Contrataciones del Estado y su Reglamento. Estas consultorías no forman parte de alcance inicial, lo que se sostiene es que COFIDE está en la potestad de solicitar al Contratista incrementos de activos (o usuarios) al servicio.

6.2.2 Seguridad

El Contratista deberá contar con los procedimientos y los mecanismos de seguridad física y lógica que reduzcan los riesgos de interrupción de la prestación de los servicios de Gestión y

²⁶ **CONSULTA 7**, formulada por DIGIWARE S.A.C.; Que, conforme a lo señalado por el área usuaria, se aclara que el servicio 2 es de gestión de equipos, siendo que ejecutar un marco de trabajo para que se realice la configuración o se coordine, se encuentra referido a los procedimientos de atención de los equipos o activos indicados en este servicio.

CONSULTA 8, formulada por DIGIWARE S.A.C.; Conforme a lo señalado por el área usuaria, se confirma la gestión de los activos y se valida que el alcance se encuentra indicado en el punto 6.2.5. Línea Base S2 de los términos de referencia.

CONSULTA 9, formulada por DIGIWARE S.A.C.; Conforme a lo señalado por el área usuaria, se precisa que la cantidad de incidentes por año que se tuvieron en la 6.2.5 Línea Base S2 (FW, NDR, NAC, WAF, Antispam, IPS, EDR) es de un promedio de 20 incidentes reportados y atendidos por el servicio al año.

CONSULTA 10, formulada por DIGIWARE S.A.C.; Conforme a lo señalado por el área usuaria, se precisa que cualquier incremento del alcance inicial será considerado como un servicio adicional o complementario y contratado según normativa de contrataciones del Estado.

Operación de Ciberseguridad para COFIDE, lo cual se acreditará con los certificados o procedimientos respectivos del servicio.

6.2.3 Políticas del Servicio.

Este servicio considera las siguientes políticas:

- a. Custodiar las credenciales de acceso a los equipos que les han sido asignados para operación de manera confidencial. Esto significa llevar un control de a quiénes se ha distribuido las credenciales de acceso, la firma de convenios de confidencialidad entre otros elementos de control.
- b. Informar de cambios de personal con accesos privilegiados a los equipos de COFIDE y ejecutar un procedimiento de control de cambio de claves.
- c. Realizar el registro, clasificación y atención de los requerimientos de operación sobre los equipos y soluciones de seguridad que le hayan sido encargados.
- d. Analizar el impacto de los requerimientos de operación solicitados por COFIDE y dar retroalimentación antes de ejecutar el requerimiento. Todo cambio debe ser validado por COFIDE y los roles de la estructura organizacional del proyecto establecida para tal fin.
- e. Reportar los resultados de la ejecución del requerimiento solicitado.
- f. Los resultados de la prestación de este servicio serán almacenados en un portal de almacenamiento en nube proporcionado por el POSTOR, al cual tendrá acceso COFIDE.

6.2.4 Características de los Componentes del Servicio

El alcance específico para cada uno de los componentes ha sido organizado de la siguiente manera:

a. Gestión de la infraestructura de Seguridad

- Supervisión.
- Soporte especializado para los equipos y las soluciones de seguridad indicadas en los alcances por cada empresa.
- Administración delegada la cual tiene como funcionalidades la atención de requerimientos y atención de incidentes.

b. Monitorización de Seguridad

- Envío de reportes mensuales.
- Envío de reporte de los incidentes ocurridos con los equipos y las soluciones de seguridad gestionados.
- Atención proactiva 24x7 con calidad de servicio.
- Contar con un soporte especializado.
- Gestión a través de herramienta de tickets y correo electrónico.
- Gestión de requerimientos, incidentes reactivos/proactivos y gestión de cambios, a través de un único Centro de Gestión.

c. Planes de mejora

- Seguridad gestionada: lo cual incluye depuración de reglas, depuración de accesos web, actualización de firmware, integración de funcionalidades nuevas, entre otros.
- Documentos: Planes de mejora ejecutados, informes requeridos por COFIDE, tickets generados, entre otros.

6.2.5 Línea Base S2

El servicio será dimensionado tomando en cuenta los activos que son equipos o soluciones de seguridad definidos por COFIDE. El servicio contempla como línea base los siguientes activos definidos:

Item	Activo	Cantidad	Marca	Modelo
------	--------	----------	-------	--------

01	Firewall Perimetral – Data Center Principal (FortiAnalyzer) ²⁷	1 (HA - Activo/pasivo)	FORTINET	FORTIGATE 400E
02	Firewall Interno (FortiAnalyzer)	1 (HA - Activo/pasivo)	FORTINET	FORTIGATE 600F
03	IPS SENSOR (Appliance Físico)	1	TRELLIX	NS7500
04	Detección avanzada de amenazas y de respuesta automatizada (XDR)	1	KARSPERSKY	Next XDR Expert
05	WAF (SaaS)	1	FORTINET	Forticloud
06	NAC (Appliance Virtual)	1	FORTINET	FNVNCA

Línea base del servicio S2

6.2.6 Facilidades Mínimas

Los recursos mínimos requeridos por este servicio son:

a. Procesos o Metodologías

- Metodología para la atención de requerimientos de operación del servicio

b. Personal

El Contratista deberá contar como mínimo con el equipo solicitado en el numeral 5.

EQUIPO DE TRABAJO para este servicio.

El Contratista deberá presentar al menos un personal especializado con los roles indicados, es responsabilidad del contratista de incrementar los recursos humanos, bajos los roles indicados, para atender la demanda del servicio según los SLAs establecidos y los requisitos del servicio

6.2.7 Tecnologías

- a. Correo electrónico corporativo del Contratista para coordinaciones.
- b. Sistemas de llamadas para realizar las coordinaciones.
- c. Estaciones de trabajo para los recursos humanos proporcionado por el Contratista.²⁸
- d. Acceso a Internet.

Nota: El Contratista debe demostrar que posee propiedad sobre el hardware y/o software a utilizar. En el caso de utilizar servicios arrendados deberá demostrar que posee acceso al servicio.

6.2.8 Responsabilidades de El Contratista

El Contratista deberá garantizar que cuenta con los recursos que permitan ejecutar el servicio solicitado de forma efectiva, para lo cual deberá cumplir con las siguientes responsabilidades:

- a. Asignar un grupo de trabajo que cuente con los conocimientos y experiencia para la ejecución del servicio de Gestión de los equipos y soluciones de seguridad.
- b. Garantizar la calidad de los servicios y equipos considerados en la presente propuesta.
- c. Tomar medidas proactivas para detectar actividades maliciosas antes de que puedan causar un daño, en lugar de enfocarse en medidas reactivas una vez que tiene lugar una amenaza.
- d. Realizar la vigilancia constante del perímetro y las operaciones internas, para identificar y hacer tratamiento a las brechas de seguridad.
- e. Garantizar la atención proactiva de incidentes 7x24 con calidad de servicio especializada.
- f. Realizar el servicio cada vez que COFIDE realice un requerimiento y reportar los resultados con una frecuencia mensual durante el período del contrato.
- g. Presentar un informe con los resultados de la gestión del mantenimiento, supervisión y atención de requerimientos de los equipos y en el primer mes la sugerencia de arrendar equipos o soluciones que se integren al modelo del servicio.

²⁷ **CONSULTA 6**, formulada por DIGIWARE S.A.C.; Conforme a lo señalado por el área usuaria, se confirma que son 02 firewall en HA (activo/pasivo).

²⁸ **CONSULTA 11**, formulada por DIGIWARE S.A.C.; Conforme a lo señalado por el área usuaria, se confirma que los equipos de trabajo para los recursos humanos del contratista, deberán ser provistos por este.

6.2.9 Responsabilidades de COFIDE

Se detallan a continuación para el servicio las responsabilidades de COFIDE:

a. Durante la implementación o transición del servicio:

1. Remitir los inventarios actualizados de los activos que son equipos o soluciones de seguridad parte del alcance del servicio
2. Designar personal de contacto autorizado para el servicio.

b. Durante el servicio:

1. Facilitar el acceso a gestión de los equipos y soluciones de seguridad en las sedes de COFIDE, en caso se requiera.
2. Designar a las personas con responsabilidad suficiente, que serán autorizadas para servir como coordinadores para casos de garantía.

6.3 SERVICIOS DE DETECCIÓN AVANZADA (S3)

Este servicio mediante el uso de la tecnología de correlación de eventos permite la gestión de los logs y los flujos generados/consumidos por los dispositivos para la detección de eventos de seguridad. El servicio considera un método de detección avanzado en base a casos de uso de ciberseguridad, el mismo que brindará información de la eficiencia de cada caso de uso aplicado. Este servicio se realiza con una frecuencia diaria (24x7) durante el período de ejecución del servicio y considera la detección de amenazas, identificación de amenazas o actividades sospechosas en la red que pudieran afectar a los activos TI. El resultado del servicio es un informe que considera los siguientes aspectos:

- a. El Monitoreo y Detección que se lleva a cabo de múltiples fuentes con el objetivo de detectar hechos o elementos significativos que puedan afectar negativamente al normal funcionamiento del negocio de COFIDE.
- b. El Análisis e Interpretación que se integra y trata la información obtenida transformándola en conocimiento válido para la toma de decisiones. Dicha información se obtiene tomando medidas intencionales para detectar actividades maliciosas antes de que puedan causar daño.
- c. Una de las principales tareas del servicio de SOC es clasificar las alertas conforme se van recibiendo.
- d. Ocurrencias de servicios de SOC, en el cual se incluye el estado de la plataforma, estadísticas de la solución, estadísticas de los eventos de seguridad detectados, status de tickets asignados, estadísticas de amenazas a nivel mundial, estadísticas de amenazas a nivel del cliente, conclusiones y recomendaciones enfocados al servicio.
- e. El servicio SOC es responsable de garantizar que los posibles incidentes de seguridad se identifiquen, analicen, defiendan, investiguen y se realice la contención de manera oportuna y diligente de acuerdo con lo establecido en el presente documento.
- f. Los servicios de SOC deben contar con personal que tenga un amplio conocimiento y experiencia de las herramientas y tecnología a su disposición.

Este servicio se cotiza por la cantidad de activos involucrados en el servicio (nodos y/o dispositivos) y/o la estimación de la cantidad de Eventos por Segundo (EPS) que los activos involucrados en el servicio pueden generar, así como los casos de uso configurados, la cantidad de servidores y las licencias de soluciones SIEM (Security Information and Event Management). A continuación, presentamos la cantidad de activos y la cantidad de EPS²⁹:

²⁹ **CONSULTA 14**, formulada por DIGIWARE S.A.C.; Conforme a lo señalado por el área usuaria, se aclara que el alcance del SERVICIO DE DETECCIÓN AVANZADA (S3), solo hace referencia a soluciones SIEM, siendo que si el proveedor desea adicionar más soluciones para cumplir con el alcance del servicio, estas serán consideradas como válidas.

CONSULTA 15, formulada por DIGIWARE S.A.C.; Conforme a lo señalado por el área usuaria, se precisa que no se está confirmando la inclusión de soluciones SOAR en el servicio, solo se hace referencia a soluciones SIEM, si el proveedor desea adicionar más soluciones para cumplir con el alcance del servicio, estas serán consideradas como válidas.

CONSULTA 16, formulada por DIGIWARE S.A.C.; Conforme a lo señalado por el área usuaria, se precisa que no se confirma la inclusión de soluciones SOAR en el servicio; sin perjuicio de ello, si el proveedor desea adicionar más soluciones para la ejecución del servicio, estas serán consideradas como válidas.

EMPRESA	CANTIDAD DE ACTIVOS ³⁰	CANTIDAD DE EPS ESTIMADOS
COFIDE	40 12	2000

Cantidad de Activos y EPS del Servicio S3

Este servicio se realiza en las instalaciones de El Contratista y con una conexión remota hacia los equipos colectores y/o su motor de correlación instalados en el centro de datos de COFIDE, COFIDE proporcionará el espacio físico en su gabinete con conexión eléctrica y comunicación a los equipos que forman parte del servicio. Los equipos colectores se encargan de recolectar logs desde los activos TI seleccionados y debe contar con las siguientes características:

6.3.1 Escalabilidad

La escalabilidad deberá basarse en los siguientes aspectos: Tecnología, Procesos y Personas.

- Tecnología:** COFIDE tienen planificado incorporar al Servicio de Gestión y Operación de la Ciberseguridad más componentes y/o mejorar posturas de seguridad, por lo tanto, este debe estar soportado para permitir el crecimiento en la cantidad de los activos, usuarios y requerimientos de operación que se requiera atender por cada servicio.
- Procesos y Personas:** COFIDE podría requerir servicios adicionales, relacionados con el Servicio de Gestión y Operación de la Ciberseguridad (por ejemplo, actualizaciones en la arquitectura desplegada debido a migraciones en los activos que se están monitoreando) e incluso servicios complementarios, de conformidad con lo dispuesto en la Ley de Contrataciones del Estado y su Reglamento. Estas consultorías no forman parte de alcance inicial, lo que se sostiene es COFIDE está en la potestad de solicitar al Contratista incrementos de activos (o usuarios) al servicio

6.3.2 Disponibilidad

La arquitectura desplegada y sus componentes deberán ofrecer una disponibilidad de acuerdo con la sección de los “Niveles de Servicio”. El Contratista del Servicio de Gestión y Operación de la Ciberseguridad facilitará el acceso a la información en un esquema 24x7.

6.3.3 Seguridad

El Contratista deberá contar con los procedimientos y los mecanismos de seguridad física y lógica que reduzcan los riesgos de interrupción de la prestación del Servicio de Gestión y Operación de la Ciberseguridad para COFIDE, lo cual se acreditará con los certificados o procedimientos respectivos del servicio.

6.3.4 Políticas del Servicio.

Este servicio considera las siguientes políticas:

- De no llegar a cubrir los EPS incluidos en la línea base COFIDE podrá agregar equipos y/o activos al servicio sin costo adicional, hasta cubrir la brecha presentada en coordinación y revisión entre COFIDE y el POSTOR.
- Realizar la recolección de los logs de los diversos activos que han sido seleccionados para ser monitoreados.
- Realizar la normalización de los logs recolectados.
- Almacenar hasta un (01) año de información histórica.
- Presentar como mínimo tres (03) meses de información en línea de eventos de seguridad, los cuales están incluidos en los 12 meses de retención histórica.
- Realizar correlación de eventos de seguridad mediante el uso de una solución tecnológica.
- El servicio debe ser prestado en la modalidad 24x7 de manera continua.

³⁰ **CONSULTA 57**, formulada por SECURESOFTECH CORPORATION S.A.C.; Se confirma al postor que, este servicio se considerará los activos que se encuentran dentro del punto 6.3.6 el cual suman 12. Conforme a lo señalado por el área usuaria, se acepta lo solicitado, por lo que se confirma que para el presente servicio se considerarán los activos que se encuentran dentro del punto 6.3.6. de los términos de referencia, los cuales suman 12.

La información obtenida y procesada por este servicio, debe estar almacenada en los data center redundantes en territorio nacional y/o extranjero del contratista.³¹

El Contratista accederá a la información obtenida y procesada resultante del monitoreo de activos a través de una conexión VPN toda vez que la información se encuentre distribuida o a través de una conexión cifrada TLS 1.2.

- h. Toda la información generada y procesada por la infraestructura utilizada es propiedad de COFIDE, siendo además confidencial.
- i. El Contratista deberá implementar los mecanismos físicos y lógicos de seguridad para garantizar que la información que produzca este servicio se mantenga confidencial, íntegra y disponible.
- j. Es importante tener en cuenta que para los componentes de las infraestructuras utilizadas para la prestación de este servicio y que son administrados por El Contratista, se debe considerar una actualización de estos durante el periodo del servicio.³²
- k. El Contratista debe preferir la instalación de componentes que generen ahorros de costo en la prestación del servicio sin perder las funcionalidades requeridas.
- l. Comunicar a COFIDE los eventos de seguridad, y de ser el caso los incidentes de seguridad que se hayan identificado.
- m. Asesorar a COFIDE en la remediación de los eventos de seguridad identificados.
- n. Elaborar un informe que contenga los eventos de seguridad encontrados producto del monitoreo realizado a los activos de TI, las coordinaciones realizadas y de ser el caso los incidentes de seguridad detectados.
- o. Los resultados de la prestación de este servicio serán almacenados en un portal al cual tendrá acceso como máximo tres (03) usuarios de COFIDE
- p. Analizar la criticidad de los incidentes de seguridad.
- q. Elaborar y actualizar el plan de respuesta a incidentes.
- r. Ejecutar medidas de contención de incidentes y mitigación de los impactos.
- s. Ejecutar medidas de contención de incidentes y mitigación de los impactos de los activos considerados en el presente servicio.
- t. Considerar soluciones líderes en el mercado americano y/o europeo. Adjuntar informes que acrediten el liderazgo de al menos dos años consecutivos de los últimos cuatro años **la cual debe ser presentada a la firma de contrato**³³

6.3.5 Características de los componentes del Servicio

La tecnología utilizada para este servicio es a través de una solución SIEM que brindará visibilidad para poder identificar, comprender y dar respuesta sobre las amenazas. El modelo operativo de la solución comprende un alcance de preparación, detección, triage, y priorización de los eventos de seguridad. Los eventos de seguridad que supongan vulnerabilidades y/o amenazas, deberán ser comunicados a COFIDE para que se coordine y planifique su remediación y/o mitigación. De ser el caso, este servicio puede activar el servicio de respuesta a incidentes (S4) para que realice un análisis, contención, erradicación, recuperación y seguimiento del incidente identificado. Esta solución debe contar con las siguientes características:

- a. El servicio se realizará mediante el uso de herramientas especializadas que intercepten y/o recopilen el tráfico y/o información de los datos.

³¹ CONSULTA 21, formulada por DIGIWARE S.A.C.; Conforme a lo señalado por el área usuaria, se confirma que la redundancia solo es para la infraestructura donde se aloja la tecnología del SOC y no del colector.

³² CONSULTA 17, formulada por DIGIWARE S.A.C.; Conforme a lo señalado por el área usuaria, se aclara que el alcance del servicio indica que "se debe considerar una actualización" como mínimo durante el periodo del servicio; sin embargo, si el servicio requiere realizar más actualizaciones como parte del alcance, estas se deberán ejecutar para mitigar las vulnerabilidades con estas actualizaciones.

³³ CONSULTA 12 y 13, formulada por DIGIWARE S.A.C.; Conforme a lo señalado por el área usuaria, se aclara que el requerimiento es mínimo y obligatorio, si la solución cumple con mayores certificaciones para asegurar los controles de seguridad, estos serán aceptados.

CONSULTA 45, formulada por SECURESOFT CORPORATION S.A.C.; Conforme a lo señalado por el área usuaria, se confirma que la documentación de sustento se podrá presentar en su idioma original. Haciendo presente que el postor ganador será responsable de la exactitud y veracidad de dichos documentos.

CONSULTA 46, formulada por SECURESOFT CORPORATION S.A.C.; Conforme a lo señalado por el área usuaria, se confirma que se podrá adjuntar informes o alguna evidencia que sustente el liderazgo de la tecnología ofertada emitido por empresas reconocidas como evaluadoras o consultoras o investigadoras de tecnologías de la información, como por ejemplo: Gartner, Forrester, Radicati, etc.

- b. Todos los componentes del SIEM deben estar alojados en el data center del POSTOR o en nube.
- c. COFIDE proporcionara recursos virtuales en su data center sólo de recolección (colector) de forma transitoria y reenvío de información hacia el SIEM del POSTOR en su data center o en nube. El postor deberá incluir la arquitectura en detalle de la solución a proponer en la que se señale todos los componentes que la conforman, explicando la función de cada uno de los mismos.³⁴
- d. Recopilar los logs de todos los activos que deben ser monitoreados y realizar una gestión adecuada de los mismos de forma continua y por el personal capacitado.
- e. Reportar de manera inmediata cuando no pueda recolectar los logs desde los activos.
- f. El licenciamiento debe ser flexible y capaz de trabajar por número de nodos o activos o dispositivos o volumen/consumo (EPS). La cantidad de EPS no debe ser una limitante para la escalabilidad.
- g. Hacer el correcto análisis de datos, eventos de seguridad y de tráfico.
- h. La solución SIEM debe admitir información para enriquecimiento de contexto de soluciones de análisis de vulnerabilidades del mercado tales como: Nessus y/o Qualys y/o Tenable y/o Rapid7. Esta capacidad debe estar habilitada.³⁵
- i. Casos de uso configurados al inicio de la operación por activos
- j. Actualizar, de ser el aplicable, los casos de uso configurados.
- k. Contar con inteligencia de correlación par tener un mejor análisis de eventos de seguridad contrastando bitácoras de dos o más dispositivos en ambientes seguros.³⁶
- l. El equipo del SOC debe garantizar un monitoreo 24x7 para la atención a cualquier problema.
- m. Asesorar en la mitigación de riesgos generados por posibles amenazas, la activación de la gestión de incidentes de seguridad o a la contención y remediación de los mismos cuando estos se materializan.
- n. Analizar de manera oportuna las anomalías de tráfico observando patrones en bitácoras o flujos de datos.³⁷
- o. Admitir el marco MITRE ATT&CK en la solución SIEM para identificar y categorizar las amenazas, así como reglas predefinidas asignadas a las tácticas y técnicas.
- p. Tener plantillas de búsqueda de caza de amenazas predefinidas.³⁸
- q. El almacenamiento de datos en la nube del fabricante de la solución debe estar cifrado mediante protocolo AES-256 o criptografía sólida según las buenas prácticas de seguridad.

Para la consecución de estos objetivos, el SOC se deberá dividir por niveles en función del grado de especialización de los analistas que lo conforman, considerando como mínimo lo siguiente, para este servicio S3:

- **En el nivel 0:** Mesa de ayuda.
- **En el nivel 1:** Se encuentran los analistas de alertas, que monitorizan continuamente las alertas que recibe el SOC. Los analistas evalúan estas alertas de seguridad y, si alcanzan el umbral predefinido según la política del SOC, se escalan al nivel 2.

³⁴ **CONSULTA 23**, formulada por DIGIWARE S.A.C; Conforme a lo señalado por el área usuaria, se confirma que COFIDE cuenta con los siguientes requisitos para VM, donde se alojará el recolector (4 Core CPU Recommended clock speed: 2.8 GHZ or higher, 16 GB ram, 500 gb SSD), se aclara que no se esta solicitando capacidades de SOAR.

³⁵ **CONSULTA 18**, formulada por DIGIWARE S.A.C; Conforme a lo señalado por el área usuaria, se confirma que este punto hace referencia a tener la capacidad, mas no forma parte de la implementación.

³⁶ **CONSULTA 19**, formulada por DIGIWARE S.A.C; Conforme a lo señalado por el área usuaria, se aclara que este punto hace referencia a Inteligencia de correlación del SIEM para el análisis de eventos de seguridad contrastando bitácoras de dos o más dispositivos en ambientes seguros, si el proveedor desea adicionar más soluciones tecnológicas para cumplir con el alcance del servicio, estas serán consideradas como válidas.

³⁷ **CONSULTA 20**, formulada por DIGIWARE S.A.C; Conforme a lo señalado por el área usuaria, se aclara que el punto de referencia indica "Analizar de manera oportuna las anomalías de tráfico observando patrones en bitácoras o flujos de datos", no se menciona analizar comportamiento de usuarios que es lo que realiza UEBA; por lo que, no se acepta lo solicitado.

³⁸ **CONSULTA 22**, formulada por DIGIWARE S.A.C; Conforme a lo señalado por el área usuaria, se confirma que este punto hace referencia a tecnología de threat hunting; siendo que las demás funcionalidades indicadas serán aceptadas como opcionales.

Tanto el nivel 0 y 1 hacen uso de playbooks o guía para el manejo de incidentes de seguridad. Los niveles 2 y 3 corresponden al Servicios de Respuesta a incidentes (S4) y pueden ser activados por el Servicio de Detección Avanzada (S3).

6.3.6 Línea Base S3

La línea base para el servicio de detección avanzada será dimensionado por la cantidad de activos definidos y los Eventos por Segundo (EPS) que genera cada activo.

El servicio contempla como línea base el siguiente alcance:

Requerimiento	1er parámetro		2do parámetro	
	Unidad de Medida	Cantidad	Unidad de Medida	Cantidad
Detección avanzada a través de una solución SIEM	Activo	10	EPS	2000

Línea Base del servicio S3

El detalle de los activos es el siguiente:

Item	Activo	Cantidad	Marca	Modelo	Casos de uso
01	Firewall Perimetral – Data Center Principal (FortiAnalyzer)	1 (HA - Activo/pasivo)	FORTINET	FORTIGATE 400E	02
02	Firewall Interno (FortiAnalyzer) ³⁹	1 (HA - Activo/pasivo)	FORTINET	FORTIGATE 600F	02
03	IPS SENSOR (Appliance Físico)	1	TRELLIX	NS7500	02
04	Antispam (Proofpoint Email Protección SaaS)	1	PROOFPOINT	SAAS	01
05	Detección avanzada de amenazas y de respuesta automatizada	1	KARSPERSKY	Next XDR Expert	02
06	WAF (SaaS)	1	FORTINET	Forticloud	02
07	NAC (Appliance Virtual)	1	FORTINET	FNVMCA	01
08	Database Firewall (Appliance Virtual)	1	IMPERVA	SECURESPHERE X2500	02
09	Solución de detección y respuesta de red (NDR)	1	FORTINET	1000F	02
10	Active Directory (AD) ⁴⁰	3 (HA - Activo/Activo)	MICROSOFT	AD	02

Detalle de Línea base del servicio S3

³⁹ **CONSULTA 3**, formulada por DIGIWARE S.A.C.; Conforme a lo señalado por el área usuaria, se confirma que son 02 firewall en HA (activo/pasivo).

⁴⁰ **CONSULTA 1**, formulada por DIGIWARE S.A.C.; Conforme a lo señalado por el área usuaria, se aclara que son 03 Active Directory (AD) en replica.

6.3.7 Facilidades Mínimas

Los recursos mínimos requeridos por este servicio son:

a. Procesos o Metodologías

- Metodología para la evaluación de eventos de seguridad.
- Metodología para analizar los resultados de la correlación.
- Metodología para configurar los casos de uso nuevos.
- Metodología para establecer los plazos de retención de información idóneos.
- Metodología para comunicar las alertas de los eventos de seguridad.
- Metodología para activar el servicio de gestión de incidentes.

b. Personal

El Contratista deberá contar como mínimo con el equipo solicitado en el numeral 5. **EQUIPO DE TRABAJO** para este servicio.

El Contratista deberá presentar al menos un personal especializado con los roles indicados, es responsabilidad del contratista de incrementar los recursos humanos, bajos los roles indicados, para atender la demanda del servicio según los SLAs establecidos y los requisitos del servicio

c. Tecnologías

- Software y/o hardware y/o servicio en la nube para la recolección, homologación y almacenamiento de logs, realización de la correlación y una consola que permita configurar las reglas (casos de uso).
- Consola de administración: Hardware ubicado en el SOC del Contratista que almacena los logs o servicio en nube.
- Conectividad para acceso al software y/o hardware de monitoreo.
- Estaciones de trabajo para los recursos humanos proporcionado por el Contratista.
- Correo electrónico corporativo del Contratista para coordinaciones.
- Sistemas de videoconferencia para realizar las coordinaciones de colaboración.

Nota: El Contratista debe demostrar que posee propiedad sobre el hardware y software a utilizar. En el caso de utilizar servicios arrendados deberá demostrar que posee acceso al servicio.

6.3.8 Responsabilidades de El Contratista

El Contratista deberá garantizar que cuenta con los recursos que permitan ejecutar el servicio solicitado de forma efectiva, para lo cual deberá cumplir con las siguientes responsabilidades:

- a. Garantizar la conformación de un equipo multidisciplinario con amplio conocimiento en la detección y análisis de amenazas, y en la gestión y respuesta de estas, en base al entorno y contexto de COFIDE y su sector de actividad.
- b. Garantizar la calidad de los servicios y equipos considerados para este servicio.
- c. Establecer un método de detección avanzando en base a casos de uso de Ciberseguridad, el mismo que brindará información de la eficiencia de cada caso de uso aplicado.
- d. Realizar el servicio de forma mensual durante el período de contrato,
- e. Presentar un Informe que considera los aspectos de Monitoreo, Detección, Análisis e Interpretación de los resultados a partir del cual se podrán tomar decisiones.
- f. Asesorar a COFIDE para hacer frente a una posible situación que compromete la seguridad de la información digital y de la infraestructura TI.
- g. Garantizar que la tecnología utilizada para este servicio es a través de una solución SIEM que detecte las amenazas o actividades sospechosas.

6.3.9 Responsabilidades de COFIDE

Se detallan a continuación para el servicio las responsabilidades de COFIDE:

a. Durante la implementación o transición del servicio:

- Remitir los inventarios actualizados de los activos.
- Designar personal de contacto autorizado para el servicio.

b. Durante el servicio:

1. Dar las facilidades de acceso al personal de El Contratista que realizará el despliegue, instalación, configuración y mantenimiento de los componentes necesarios para la operación del SIEM en la sede de COFIDE en caso se requiera.
2. Designar a las personas con responsabilidad suficiente, que serán autorizadas para servir como coordinadores para casos de garantía.
3. Garantizar la conectividad para la gestión remota.

6.4 SERVICIO DE RESPUESTA A INCIDENTES COMO SERVICIO (S4)

La dimensión del servicio abarca lo siguiente:

- a. Proveer un modelo de anticipación y respuesta frente a crisis derivadas de incidentes graves de seguridad.
- b. El Contratista debe ofertar el servicio de respuesta ante incidentes de seguridad informática, con el objetivo de coadyuvar a COFIDE en la mitigación, contención y solución de las incidencias.
- c. Diseñar todos los mecanismos necesarios de contención, análisis, respuesta, erradicación y recuperación como parte de la gestión de incidentes de seguridad.
- d. Debe contar con un equipo de respuesta ante incidentes de seguridad informática CSIRT (Computer Security Incident Response Team). Las instalaciones y el personal que operan el CSIRT del Contratista, deben estar ubicados en la ciudad de Lima, Perú.
- e. Análisis forense digital y de seguridad.

Este servicio se activa bajo demanda en el transcurso del período del servicio. El servicio asigna una cantidad de horas para la gestión de incidentes para COFIDE por cada año que dura el servicio. El resultado del servicio es un informe por ocurrencia del análisis de incidentes, las medidas de contención y respuesta implementadas y el estado de recuperación de los servicios o activos. Este servicio se cotiza por la cantidad de horas asignadas para la atención de incidentes. A continuación, presentamos las horas contempladas para este servicio:

COFIDE	HORAS PARA GESTIÓN DE INCIDENTES (ANUAL)
Total horas del Servicio S4	80

Cantidad de Horas del servicio S4

Este servicio se realiza fundamentalmente desde las instalaciones de El Contratista con una conexión remota hacia los activos COFIDE que han sido afectados por el incidente, excepcionalmente cuando el incidente no pueda ser superado de manera remota, el Contratista deberá coordinar con COFIDE para desarrollar la gestión de incidentes de manera presencial en las locaciones donde se encuentran los activos afectados. El servicio debe contar con las siguientes características:

6.4.1 Políticas del Servicio.

Este servicio debe basarse en las siguientes políticas:

- a. Realizar el registro, clasificación y atención de los incidentes de seguridad.
- b. Asesorar y participar en evaluación de los daños ocasionados por los incidentes de seguridad.
- c. Asesorar y participar en la etapa de erradicación y recuperación del incidente a COFIDE.
- d. Reportar los resultados de la gestión de incidentes notificados.
- e. El servicio debe ser prestado en la modalidad 24x7.
- f. El Contratista accederá a la información obtenida y procesada resultante de la gestión de incidentes.
- g. Toda la información generada y procesada es propiedad de COFIDE, siendo además confidencial.
- h. El Contratista deberá implementar los mecanismos físicos y lógicos de seguridad para garantizar que la información que produzca este servicio se mantenga confidencial, íntegra y disponible.

- i. Comunicar a COFIDE cualquier información relevante que permita gestionar de manera adecuada el incidente notificado.
- j. Asesorar a COFIDE en las medidas a tomar respecto de la gestión de incidentes.
- k. Elaborar un informe que contenga las actividades realizadas para la gestión de los incidentes notificados.
- l. Informar a COFIDE en cuanto se advierta la ocurrencia de un incidente de Ciberseguridad que presente un impacto significativo adverso significativo verificado o presumible de:
 - Pérdida o hurto de información de la empresa o de clientes.
 - Fraude interno o externo
 - Impacto negativo en la imagen o reputación de la empresa
 - Interrupción de operaciones.
- m. Los resultados de la prestación de este servicio serán almacenados en un portal del POSTOR al cual tendrá acceso el personal de COFIDE con las medidas de seguridad requeridas.
- n. El equipo de respuesta ante incidentes del contratista debe estar registrado como miembro del FIRST (Forum of Incident Response and Security Teams).

6.4.2 Características de los Componentes del Servicio

El servicio estará compuesto por las siguientes etapas basado en un enfoque CSIRT:

- a. **Presentación del plan de atención de incidentes.** El Contratista deberá definir en el plan lo siguiente:
 - Conocimiento de la infraestructura y de la red de COFIDE.
 - Clasificación y jerarquía de los activos de acuerdo con el valor del negocio.
 - Roles, responsabilidades y partes interesadas dentro de la organización encargados de los riesgos, activos, así como de la detección de incidentes, la operación, la continuidad y la disponibilidad del servicio. El CONTRATISTA debe considerar la revisión del actual **PROCEDIMIENTO DE GESTIÓN DE INCIDENTES DE SEGURIDAD DIGITAL** para la propuesta de la organización del servicio.
 - Definir los incidentes por tipo y niveles de impacto en base al criterio de taxonomía o clasificación que se vaya a utilizar asociado a los activos de información de COFIDE. En la fase de transición el Contratista deberá coordinar con COFIDE la obtención de la clasificación de los activos de información.
 - El servicio debe tener la capacidad de analizar, mediante el uso de Sandboxing u ambientes propios para tal fin, el malware encontrado.
- b. **Reporte y solicitud de apoyo para la atención de incidentes.** El reporte de un incidente de seguridad será notificado a través del proceso o canal establecido entre el Contratista y COFIDE, posterior al reporte en caso corresponda que se requiera apoyo en la contención y mitigación del incidente, podrá hacer uso del servicio solicitando el apoyo por cualquier canal de comunicación (telefónico, correo, aplicativo).
El Contratista cuando lo requiera podrá solicitar el apoyo de las personas involucradas en el incidente reportado con el fin de las validaciones, aprobaciones y correcta ejecución de actividades.
- c. **Participación en la contención y mitigación del incidente.** El Contratista deberá participar de las actividades que se deben realizar como parte de la respuesta de la atención del incidente reportado siguiendo estos pasos:
 - Realizar una evaluación inicial.
 - Generar recomendaciones para contener el daño y minimizar el riesgo.
 - Identificar el tipo y la gravedad del ataque.
 - Generar recomendaciones para proteger las pruebas en caso de requerir un análisis forense.
 - Generar recomendaciones para recuperar los sistemas.
 - Participar en la compilación y organización de la documentación del incidente.
 - Participar en la valoración de los daños del incidente.

- Revisar las directivas de respuesta y actualización.

Para el análisis y respuesta a los incidentes, el SOC deberá considerar como mínimo los niveles 2 y 3, en función del grado de especialización de los analistas que lo conforman, lo que se precisa a continuación:

- **En el nivel 2:** Los analistas determinan si los datos o el sistema se han visto afectados y, de ser así, recomendarán una respuesta.
- **En el nivel 3:** Se cuenta con profesionales capacitados, que se encargan de resolver los incidentes, pero también de buscar posibles incidentes con el fin de prevenirlos.

6.4.3 Línea Base S4

El servicio contempla como línea base el siguiente alcance:

Requerimiento	Unidad de medida	Cantidad
Atención de incidentes de seguridad	horas anuales	80

Línea base del servicio S4

Nota: Las horas que no puedan ser utilizadas por COFIDE para la gestión de incidentes, podrán ser utilizadas para capacitaciones en temas relacionados a seguridad de información realizadas por El Contratista.

6.4.4 Facilidades Mínimas

Los recursos mínimos requeridos para este servicio son:

a. Procesos o Metodologías

- Metodología para la gestión de incidentes, en sus diferentes etapas, lo que debe incluir como mínimo la identificación, clasificación, análisis, elaboración de planes de respuesta, planes de contención, planes de erradicación y planes de restauración.

b. Personal

El Contratista deberá contar como mínimo con el equipo solicitado en el numeral 5.

EQUIPO DE TRABAJO para este servicio.

El Contratista deberá presentar al menos un personal especializado con los roles indicados, es responsabilidad del contratista de incrementar los recursos humanos, bajos los roles indicados, para atender la demanda del servicio según los SLAs establecidos y los requisitos del servicio. Para el cumplimiento de los objetivos de este servicio el Contratista podrá adicionar al equipo los roles que considere necesario para la gestión integral de los incidentes, por ejemplo, podría requerir un especialista en análisis forense, un especialista en threat hunting u otro rol.

6.4.5 Tecnologías

- Software especializado, según requiera cada incidente (por ejemplo, software de volcado de memoria, de recuperación de datos, etc.).
- Estaciones de trabajo para los recursos humanos proporcionado por el Contratista.
- Correo electrónico corporativo del Contratista para coordinaciones.
- Sistemas de videoconferencia para realizar las coordinaciones.

Nota: El Contratista debe demostrar que posee propiedad sobre el hardware y software a utilizar. En el caso de utilizar servicios arrendados deberá demostrar que posee acceso al servicio.

6.4.6 Responsabilidades de El Contratista

El Contratista deberá garantizar que cuenta con los recursos que permitan ejecutar el servicio solicitado de forma efectiva, para lo cual deberá cumplir con las siguientes responsabilidades:

- Garantizar la conformación de un equipo multidisciplinario con amplio conocimiento y experiencia para la ejecución del servicio de respuesta a incidentes.
- Garantizar la calidad de los servicios y equipos considerados en la prestación del servicio.

- c. Diseñar un modelo de anticipación y respuesta frente a crisis derivadas de incidentes graves de seguridad.
- d. Diseñar todos los mecanismos necesarios de contención, análisis, remediación y recuperación que se produzcan en los incidentes de seguridad.
- e. Presentar un informe de la gestión realizada por cada incidente que se produzca que incluya: las medidas de contención y respuesta implementadas y el estado de recuperación de los servicios o activos.

6.4.7 Responsabilidades de COFIDE

Se detallan a continuación para el servicio las responsabilidades de COFIDE:

a. Durante la implementación o transición del servicio:

- Designar personal de contacto autorizado para el servicio.
- Entregar la información requerida.

b. Durante el servicio:

- Dar las facilidades de acceso al personal de El Contratista para la atención de incidentes reportados en la sede de COFIDE, en caso se requiera.
- Designar a las personas con responsabilidad suficiente, que serán autorizadas para servir como coordinadores para casos de garantía.
- Garantizar la conectividad para la gestión remota.

6.5 Servicio de Identificación de Vulnerabilidades en Aplicaciones (S5)

6.5.1 Descripción y Alcance del Servicio

El Servicio consiste en realizar un Hacking ético a las aplicaciones que incluya: Un análisis de vulnerabilidades automatizado y/o a demanda mediante uso de soluciones, cuyo resultado sea un informe de auditoría. Este servicio se realiza (hacking ético) una vez por año a demanda durante el período de ejecución del servicio y considera para el análisis de vulnerabilidades aquellos activos que son aplicaciones internas y externas. Este servicio se cotiza por la cantidad de activos TI a evaluar a demanda. A continuación, presentamos la cantidad de activos por año:

Ítem	Tipo de activo	Cantidad activos a escanear anual (hacking ético)
1	Aplicaciones web Interfaz de programación de aplicaciones – API	10

Cantidad de Activos del servicio S5

Este servicio se realiza desde las instalaciones del Contratista y del cliente con la información detallada de los activos que son aplicaciones internas y externas seleccionadas por COFIDE y debe contar con las siguientes características:

a. Seguridad

El Contratista deberá contar con los procedimientos y los mecanismos de seguridad física y lógica que reduzcan los riesgos de interrupción de la prestación de los servicios de Gestión y Operación de Ciberseguridad, lo cual se acreditará con los certificados o procedimientos respectivos del servicio.

6.5.2 Políticas del Servicio.

Este servicio considera las siguientes políticas:

- a. Realizar el escaneo de vulnerabilidades sobre el inventario de aplicaciones presentado.
- b. La infraestructura utilizada para realizar el escaneo y el almacenamiento de los resultados del escaneo deben estar ubicados, de preferencia, dentro de las instalaciones los centros de datos del contratista o en la nube.
- c. Para el escaneo interno será mediante el uso de una sonda de escaneo desplegada en las instalaciones de COFIDE, quien proporcionará los recursos virtuales.
- d. El Contratista accederá a la información resultante del escaneo de vulnerabilidades a través del portal de la herramienta o solución a utilizar.

- e. Toda la información generada y procesada por la infraestructura utilizada es propiedad de COFIDE, siendo además confidencial.
- f. El Contratista deberá implementar los mecanismos físicos y lógicos de seguridad para garantizar que la información que produzca este servicio se mantenga confidencial, íntegra y disponible.
- g. Es importante tener en cuenta que para los componentes de las infraestructuras utilizadas para la prestación de este servicio y que son administrados por El Contratista, se debe considerar mantener actualizado toda la infraestructura implementada y mitigar las vulnerabilidades que conlleven durante el periodo del servicio.
- h. El Contratista debe preferir la instalación de componentes que generen ahorros de costo en la prestación del servicio sin perder las funcionalidades requeridas.
- i. En caso El Contratista requiera una infraestructura basada en máquinas virtuales, deberá establecer la configuración de los recursos de la máquina virtual requerida.
- j. En caso El Contratista proponga infraestructura basada en hardware deberá establecer la cantidad de unidades raqueables y consumo de energía requeridos.
- k. Asesorar a COFIDE en la remediación de vulnerabilidades identificadas.⁴¹
- l. Elaborar un informe que contenga los resultados de las vulnerabilidades encontradas producto del escaneo de las aplicaciones consideradas por COFIDE.
- m. Los resultados de la prestación de este servicio serán compartidos por el contratista mediante un acceso privado a un repositorio compartido o en nube al cual solo tendrán acceso el personal asignado por COFIDE.
- n. Las vulnerabilidades detectadas en el hacking ético deben de disponer de trazabilidad, a fin de que se disponga de las evidencias respectivas

6.5.3 Características de los Componentes del Servicio

El servicio debe enfocarse en realizar la detección de las vulnerabilidades mediante el uso de herramientas tecnológicas de seguridad, la funcionalidad de la herramienta debe permitir cómo mínimo lo siguiente:

- a. Investigación de fuentes públicas.
- b. Sondeo de los puntos de entrada de las aplicaciones.
- c. Sondeo de servicios y software.
- d. Sondeo de métodos HTTP usados.
- e. Configuración de autenticación de la aplicación.
- f. Verificación de controles Cliente-Side (De lado del cliente).
- g. La evaluación de controles utilizados para la autenticación
- h. Manejo de sesiones y validación de datos de entrada.
- i. Identificación de problemas de configuración, transmisión insegura de datos y divulgación de información sensible.
- j. Escaneo externo de los activos que son aplicaciones.
- k. Escaneo interno mediante el uso de una sonda de escaneo desplegada en las instalaciones de COFIDE.
- l. Verificación de la validación de datos de entrada.
- m. Envío de alertas y la identificación de vulnerabilidades de la misma forma que si se detectará de forma proactiva.
- n. Investigación de vulnerabilidades por versión de software
- o. Clasificación de las vulnerabilidades basado en el criterio de explotación (para ayudar a priorizar amenazas realmente explotables de las que no), identificando aquellas que son potencialmente de mayor riesgo para la empresa y hacer el seguimiento del estado de las vulnerabilidades.
- p. El informe entregado deberá indicar la severidad de las vulnerabilidades encontradas, (baja, media, alta o extrema)
- q. Deberá detectar, identificar, evaluar y dar recomendaciones para la remediación de los 10 riesgos principales de OWASP, como inyección de SQL, secuencias de comandos entre sitios (XSS), entidades externas XML (XXE), autenticación interrumpida y configuraciones incorrectas, también las amenazas de WASC, las debilidades de CWE y los CVE asociados en aplicaciones web.
- r. Se deberá determinar y mostrar el nivel de explotabilidad de cada vulnerabilidad encontrada.

⁴¹ **CONSULTA 24**, formulada por DIGIWARE S.A.C; Conforme a lo señalado por el área usuaria, se confirma que los hallazgos tienen como producto la recomendación y/o asesoramiento sobre las vulnerabilidades reportadas y no involucra la aplicación y/o remediación.

- s. Se deberá verificar para el cumplimiento de las mejores prácticas de OWASP Top Ten (Open Web Application Security Project).
- t. Permitir escaneos en profundidad dinámicos para descubrir, catalogar todas las aplicaciones web y APIs en el perímetro de la red empresarial, redes internas e instancias en la nube.
- u. Proporcionar información relativa al activo afectado, categoría de la vulnerabilidad, métodos de remediación, del mismo modo que si se tratara de una auditoría.
- v. Admitir la capacidad de volver a probar una vulnerabilidad específica que se haya detectado antes en la aplicación web
- w. Permitir gestionar múltiples escaneos de aplicaciones web combinando múltiples escáneres para acelerar el proceso de escaneo y obtener resultados de forma más rápida.
- x. Escanear aplicaciones web de gran tamaño haciendo uso de un mecanismo de escaneo progresivo, que debe permitir escanear en etapas incrementales y evitar cualquier restricción que pueda generarse al intentar escanear una aplicación de una sola vez.

6.5.4 Facilidades Mínimas

Los recursos mínimos que requiere este servicio son:

a. Procesos o Metodologías

- Metodología para el análisis y evaluación de vulnerabilidades de aplicaciones.

b. Personal

- El Contratista es responsable de incrementar los recursos humanos, bajos los roles indicados, para atender la demanda del servicio según los SLAs establecidos y los requisitos del servicio

c. Tecnologías

- Software y/o hardware para el escaneo de vulnerabilidades en aplicaciones
- Máquina de salto para el acceso a información interna de la red.
- Conectividad para acceso al software y/o hardware de escaneo.
- Estaciones de trabajo para los recursos humanos proporcionado por el Contratista.
- Correo electrónico corporativo del Contratista para coordinaciones.
- Sistemas de videoconferencia para realizar las coordinaciones.
- Infraestructura o servicio de recopilación de vulnerabilidades: Solución (hardware o software) que permite realizar el escaneo de aplicaciones para la identificación de vulnerabilidades.
- Consola de Administración de vulnerabilidades: Recopila las vulnerabilidades producto del escaneo de vulnerabilidades de las aplicaciones.

Nota: El Contratista debe demostrar que posee propiedad sobre el hardware y software a utilizar. En el caso de utilizar servicios arrendados deberá demostrar que posee acceso al servicio.

El Contratista por confidencialidad de la información deberá contener información únicamente con COFIDE; con lo que la herramienta deberá ser únicamente dedicada para COFIDE.

6.5.5 Responsabilidades del Contratista

El Contratista deberá garantizar que cuenta con los recursos que permitan ejecutar el servicio solicitado de forma efectiva, para lo cual deberá cumplir con las siguientes responsabilidades:

- a. Asignar un grupo de trabajo que cuente con los conocimientos y experiencia para la ejecución del servicio de identificación de vulnerabilidades en aplicaciones expuestas.
- b. Contar con los procedimientos y los mecanismos de seguridad física y lógica que reduzcan los riesgos de operación para COFIDE.
- c. Acreditar que cuenta con los certificados y procedimientos relacionados a la prestación del servicio.
- d. Garantizar que los recursos tecnológicos utilizados envían alertas, en la cual se detalle el tipo de vulnerabilidad encontrada.
- e. De existir algún inconveniente mayor el Contratista asumirá la responsabilidad por el error en el sistema instalado.
- f. Presentar un informe técnico con los resultados del hacking ético de vulnerabilidades para los activos evaluados.

6.5.6 Responsabilidades de COFIDE

Se detallan a continuación para el servicio las responsabilidades de COFIDE:

- a. Durante la implementación o transición del servicio:
 - Remitir los inventarios actualizados de los activos que son aplicaciones.
 - Designar personal de contacto autorizado para el servicio.
- b. Durante el servicio:
 - Dar las facilidades de acceso al personal de El Contratista que realizará el hacking ético en las sedes de COFIDE, en caso se requiera.
 - Designar a las personas con responsabilidad suficiente, que serán autorizadas para servir como coordinadores para casos de garantía.
 - Garantizar la conectividad para la gestión remota.
 - Deberá otorgar el acceso al personal del Contratista al servidor o IP privada donde se encuentran las aplicaciones internas a evaluar.

6.6 SERVICIO DE CIBERINTELIGENCIA (S6)

Servicio que consiste en el uso de una solución para identificar amenazas y riesgos respecto de la reputación, marcas y/o conceptos importantes de COFIDE, de tal modo que se brinde visibilidad más allá del ciclo de vida de los ataques, añadiendo contexto y prioridad a las amenazas globales. Este servicio se realiza de forma continua 24x7 y al cierre de cada mes se entrega un informe con los resultados del monitoreo. Para la ejecución del servicio se considera como entrada un conjunto de palabras (frase clave) que deben ser definidas por COFIDE en la fase de transición antes de que el servicio entre en operación. El resultado del servicio es un informe que considera: la identificación de manera temprana de ciberamenazas, las coordinaciones realizadas con COFIDE afectadas, las recomendaciones para mitigar las amenazas y de ser el caso las acciones ejecutadas por parte de El Contratista o de COFIDE para mitigar el impacto de las ciberamenazas. Este servicio se cotiza por la cantidad o set de palabras (palabra raíz) establecidas y personalizadas por COFIDE. A continuación, presentamos La cantidad de palabras:

Ítem	Cantidad de palabras o set de palabras mínimas (4 para marca y 1 dominio)
1	5

Cantidad de Palabras o set de Palabras para el Servicio S6

Este servicio se realiza en las instalaciones del Contratista, con la información de la cantidad de palabras establecidas por COFIDE y debe contar con las siguientes características:

6.6.1 Seguridad

El Contratista deberá contar con los procedimientos y los mecanismos de seguridad física y lógica que reduzcan los riesgos de interrupción de la prestación de los servicios de Ciberseguridad (SOC) para COFIDE, lo cual se acreditará con los certificados o procedimientos respectivos del servicio.

6.6.2 Políticas del Servicio.

Este servicio considera las siguientes políticas:

- a. En la fase de transición del servicio COFIDE deberá indicar las palabras por cada categoría.
- b. El Contratista utilizará infraestructura propia o servicios para la búsqueda de amenazas en el Internet basado en los sets de palabras definidos.
- c. Una vez que se identifique una amenaza, El Contratista deberá comunicar inmediatamente la situación a COFIDE.
- d. El Contratista asesorará a COFIDE en las medidas de remediación a aplicar (no incluye temas legales)
- e. El Contratista podrá representar a COFIDE, previa autorización de ésta, en el proceso de dar de baja a la amenaza identificada. ⁴²

⁴² CONSULTA 25, formulada por DIGIWARE S.A.C; Conforme a lo señalado por el área usuaria, se confirma que COFIDE podrá entregar una carta y/o similar de autorización para que el contratista pueda hacer uso de la representación y gestionar los takedowns si este lo requiere para cubrir este alcance.

- f. El Contratista hará seguimiento a las amenazas que se encuentren activas, para ello llevará un registro de las amenazas identificadas y resueltas.
- g. El Contratista hará seguimiento a la resolución de amenazas que hayan quedado bajo responsabilidad de COFIDE.
- h. El Contratista hará seguimiento a las amenazas que se encuentren activas, para ello llevará un registro de las amenazas identificadas y resueltas o dados de baja, por el equipo de ciberinteligencia
- i. Los resultados de la prestación de este servicio serán almacenados en un portal o una plataforma cloud al cuál tendrán acceso COFIDE.

6.6.3 Características de los Componentes del Servicio

Para cubrir los requisitos planteados del presente servicio de Ciberinteligencia, El Contratista debe poner a disposición de COFIDE una efectiva detección ante amenazas que contemple lo siguiente:

- a. La entrega de capacidades equivalentes a un equipo multidisciplinario con amplio conocimiento en la detección y análisis de amenazas en el Internet, y en la gestión y respuesta de estas, en base al entorno y contexto de COFIDE y su sector de actividad.
- b. Uso de herramientas, de alto valor tecnológico de terceros y/o propietarias, configuradas en función a las palabras clave establecidas para la búsqueda de ciberamenazas.
- c. Evolución continua de todos los elementos del servicio (procesos, herramientas, fuentes, etc.) en base a la experiencia, buenas prácticas y estándares del mercado
- d. Cobertura completa en base al ciclo de vida de detección, análisis, mitigación de la exposición a las amenazas y de ser el caso el cierre de la amenaza.
 - **Detección:** Identificación proactiva y seguimiento 24x7.
 - **Análisis:** Evaluación exhaustiva de la información procesable (amenazas identificadas)
 - **Mitigación:** Bloqueo en navegadores y bloques en red.
 - **Cierre:** Retirada de contenidos, cierre de sites y takedown
- e. Capacidad de llevar a cabo la identificación temprana, desde la creación del dominio similar a su marca y su uso en correos electrónicos, portales, perfiles, apps, y que intenta falsificar la identidad de la organización, y así tomar acciones para desactivarlos.
- f. Contar con inteligencia accionable que permita tomar acciones en tiempo y forma para la protección de su marca.
- g. Monitoreo de discusiones en comunidades de actores de amenazas de tipo foros, fuentes abiertas, Deep Web, Dark Web.
- h. El servicio de Ciberinteligencia debe mostrar información relevante de las amenazas identificadas, como mínimo:
 - Breve descripción de las vulnerabilidades reveladas, amenazas, rastros de compromiso, así como la actividad actual de ciberdelincuencia y ciberespionaje contra los activos de COFIDE.
 - Análisis de actividades en foros ocultos.
- i. El servicio permitirá enviar solicitudes de takedown al proveedor del servicio **(180 solicitudes como máximo para todo el periodo del servicio)**⁴³ y este deberá preparar la documentación para la solicitud de eliminación a la autoridad local/regional pertinente (CERT, registrador, etc.) que tenga los derechos legales necesarios para cerrar el dominio. El servicio deberá informar a través de notificaciones en cada paso del proceso hasta que el recurso solicitado se elimine con éxito.
- j. El servicio de Takedown que forma parte del servicio debe cubrir los siguientes puntos como mínimo:
 - Eliminación de dominios maliciosos o de phishing
 - Eliminación de aplicaciones móviles falsas

Nota: El servicio de eliminación debe tener una cobertura mundial.
- k. Monitoreo de comunidades clandestinas que permitan identificar actividades ilícitas desde foros publicos y comunidades de intercambio de archivos centradas en delitos cibernéticos, piratería, fraude y extremismo/terrorismo. Se debe extraer de lo observado la dirección IP, la ubicación (ciudad/país), el proveedor de alojamiento, timestamp
- l. Identificar datos expuestos de COFIDE, código fuente o sistemas vulnerables dentro de conjuntos de datos de código abierto e infraestructura pública. Como parte del servicio de Ciberinteligencia el Contratista debe contemplar los siguientes tipos de amenazas: Dominios sospechosos, typosquatting, uso no autorizado de marca, seguimiento de

⁴³ CONSULTA 4 y 5, formuladas por DIGIWARE S.A.C.; Conforme a lo señalado por el área usuaria y, con ocasión a la integración de las bases, se precisa que se considerará un máximo de 180 solicitudes de TAKEDOWN por todo el periodo del servicio.

identidad digital, counterfeit, exposición de información, hacktivismo, robos de credenciales, entre otros. Es obligatorio que El Contratista resuelva la amenaza relevante (takedown) en la medida que este en sus manos realizar la resolución y si no se puede resolver directamente por El Contratista, deberá asesorar en el desarrollo de la eliminación de la amenaza. El número de resoluciones de amenazas es ilimitado. Se deben resolver todas aquellas que se consideren relevantes. El Contratista deberá proponer a COFIDE para su aprobación los criterios para la clasificación de las amenazas.

6.6.4 Facilidades Mínimas

Los recursos mínimos requeridos para este servicio son:

a. Procesos o Metodologías

- Metodología para identificar la relevancia de las palabras clave a utilizar.
- Metodología para realizar la Ciberinteligencia y encontrar ciberamenazas.

b. Personal

El Contratista es responsable de incrementar los recursos humanos, bajos los roles indicados, para atender la demanda del servicio según los SLAs establecidos y los requisitos del servicio

c. Tecnologías

- Software y/o hardware y/o servicios especializados para la detección de ciberamenazas en el Internet.
- Estaciones de trabajo para los recursos humanos proporcionado por el Contratista.
- Acceso a Internet.
- Correo electrónico corporativo del Contratista para coordinaciones.
- Sistemas de videoconferencia para realizar las coordinaciones.

Nota: El Contratista debe demostrar que posee propiedad sobre el hardware y software a utilizar. En el caso de utilizar servicios arrendados deberá demostrar que posee acceso al servicio.

6.6.5 Responsabilidades del CONTRATISTA

El Contratista deberá garantizar que cuenta con los recursos que permitan ejecutar el servicio solicitado COFIDE de forma efectiva, para lo cual deberá cumplir con las siguientes responsabilidades:

- a.** Identificar riesgos en los activos de información de COFIDE y brindar visibilidad más allá del ciclo de vida de los ataques, añadiendo contexto y prioridad a las amenazas globales a través de boletines de ciberseguridad.
- b.** Presentar un Informe del servicio que considere: la identificación de ciberamenazas y su clasificación, además las medidas correctivas desarrolladas y la asesoría brindada a COFIDE para minimizar el impacto de la amenaza.
- c.** Realizar la documentación de la respuesta brindada para mitigar el impacto de las ciberamenazas en COFIDE

6.6.6 Responsabilidades de COFIDE

Se detallan a continuación para el servicio las responsabilidades de COFIDE:

a. Durante la implementación o transición del servicio:

- Designar personal de contacto autorizado para el servicio.

b. Durante el servicio:

- Designar a las personas con responsabilidad suficiente, que serán autorizadas para servir como coordinadores.
- Garantizar la conectividad para la gestión remota.

6.7 ETAPAS DEL SERVICIO

El plazo de ejecución de las etapas del servicio se contabilizará a partir del día siguiente de la fecha indicada en el **Acta de Inicio del servicio**, la cual debe ser firmada como máximo en los primeros (10) días calendarios contados a partir del día siguiente de la firma de contrato.

Los servicios pasan por cuatro (04) etapas, totalizando treinta y nueve (39) meses para todas estas etapas, según muestra el cronograma siguiente:

ETAPA	MESES DE LAS ETAPAS												
	(UN MES)	(UN MES)	(UN MES)	MES 1	MES 2	MES 3	MES 4	...	MES 8	...	MES 33	MES 34	MES 35
Planificación	Planificación												
Implementación		Implementación											
Operativa				Etapa de Gestión y Operación del Servicio									
Transición de Salida													Transición de Salida

Etapas del Servicio

A continuación, se describen de forma general cada una de las etapas:

Etapas de Planificación: Etapa de planeamiento inicial correspondiente a la preparación de la infraestructura del servicio de Ciberseguridad. Así mismo, se realizará el establecimiento de lineamientos, políticas y procedimientos para las etapas de transición (entrada y salida) y de operación del servicio de Ciberseguridad. Duración de un (01) mes como máximo contabilizados a partir del día siguiente de la fecha indicada en el **Acta de Inicio del servicio**.

Etapas de Implementación: Periodo en el cual el Contratista ejecutará las actividades necesarias para la toma de control de la operación de los servicios de Ciberseguridad. Corresponde a la conformación de los recursos requeridos para la ejecución de los servicios. Durante esta etapa, el PROVEEDOR deberá cumplir con las condiciones requeridas para implementar el servicio, pruebas y activación en un plazo máximo de dos (02) meses como máximo contados a partir del día siguiente de culminado la **Etapas de Planificación**. El PROVEEDOR es responsable de la ejecución de esta etapa del Servicio y debe presentar informes de estado del avance semanal. El esfuerzo de esta etapa no generara costos adicionales al servicio y debe ser asumida por el PROVEEDOR. Culminado esta etapa, se debe generar el **Acta de inicio de la Etapa operativa**.

Etapas Operativa: Duración de treinta y seis (36) meses.

Etapas de Transición de Salida: Periodo de tiempo en el cual el Contratista ejecutará las actividades necesarias para el traslado o migración de los recursos contemplados en el presente servicio. Esta fase se ejecutará dentro de la **Etapas Operativa**. Duración de dos (02) meses como máximo

6.7.1 Etapas de Planificación

Es esta etapa se cuenta con la participación del Contratista del “Servicio de Gestión y Operación de la Ciberseguridad” y COFIDE para definir todo lo necesario para la operación del servicio, con la finalidad de permitir y garantizar una correcta ejecución de la implementación y la operación. Ello incluye, la ejecución de las actividades para la elaboración de planes, procedimientos, formatos, instructivos, políticas y controles. Cuando El Contratista del Servicio de Gestión y Operación de la Ciberseguridad cumpla con el envío de los entregables y se otorguen la respectiva conformidad, sin observaciones ni salvedades, esta fase se da por concluida.

6.7.2 Etapas de Implementación

a. Políticas y Estrategias

Se debe desarrollar la implementación de los servicios cumpliendo las siguientes políticas y estrategias generales:

- Todos los servicios deben incluir como mínimo actividades de coordinación y confirmación en la fase de transición, es decir antes de la ejecución de los servicios.
- En la etapa de planeamiento del Servicio El Contratista deberá desarrollar un Plan de Implementación a detalle.
- Para aquellos servicios que requieren de una conexión VPN hacia los Centros de Datos de COFIDE, El Contratista debe realizar pruebas de conectividad de los enlaces de comunicación desde su Centro de Operaciones de Seguridad (SOC principal y redundante).

- Para aquellos Servicios de Gestión y Operación de la Ciberseguridad que requieran la instalación, despliegue y configuración de componentes (Hardware, software y/o servicios) sobre la infraestructura del cliente (propia, arrendada o en la nube), deberá implementarse durante en esta etapa, El Contratista realizará dichas instalaciones y configuraciones durante los fines de semana, días feriados no laborales u horas no laborales en una ventana de tiempo coordinada entre El Contratista y COFIDE a fin de minimizar el impacto en la operativa de COFIDE.⁴⁴
- El Contratista deberá considerar que para el despliegue de los Servicios Gestión y Operación de Ciberseguridad que modifiquen la infraestructura (propias, arrendadas y en la nube) de COFIDE, estas modificaciones deberán estar activas y configuradas en la infraestructura que corresponda de manera anticipada. Para garantizar el correcto funcionamiento de los equipos y soluciones El Contratista deberá realizar pruebas o pilotos, en coordinación con COFIDE.
- El Contratista en coordinación con COFIDE elaborará un plan de contingencia y plan de Rollback en caso las configuraciones realizadas ocasionen un daño o los componentes no se ejecuten de forma adecuada.

b. Plan de despliegue de Servicios

El Contratista debe cumplir con las siguientes actividades generales en tres fases:

- **Preparación:** Ejecutar las actividades de la planificación, coordinación y alistar los recursos necesarios (metodologías, personas, tecnología e infraestructura) para los servicios de Gestión y Operación de Ciberseguridad.
- **Implementación:** Realizar las coordinaciones, y de ser el caso la ejecución, el despliegue, instalación y configuración de los componentes (Hardware, software y/o servicios) requeridos para los servicios de Ciberseguridad. Los servicios (del S1 al S6) deben estar desplegados e instalados en el plazo de dos (02) meses como máximo contados a partir del día siguiente de culminado la **Etapas de Planificación**, estos servicios comienzan su operación y al finalizar el mes El Contratista puede realizar la facturación (para aquellos servicios que sean mensuales).
- **Aceptación de las coordinaciones:** En esta fase El Contratista y COFIDE se ponen de acuerdo respecto de las metodologías, procesos e información a utilizar durante la ejecución.
- **Pruebas de Recepción:** Es la fase de verificación del correcto despliegue de los servicios de Ciberseguridad que modifiquen la infraestructura (propias, arrendadas y en la nube) de COFIDE.

6.7.3 Etapa Operativa

6.7.3.1 Descripción y Alcance de los Servicios

El Contratista debe implementar los servicios de Operación y servicios de Gestión que permitan mantener la continuidad de los servicios de Ciberseguridad, atender los requerimientos que se derivan de la administración de infraestructura desplegada; y administrar los incidentes y/o problemas que puedan impactar en los niveles de servicio acordados descritos en la sección de acuerdo de nivel de servicio. Los Servicios de Gestión y Operación están constituidos de la manera siguiente:

- El Contratista debe utilizar herramientas automatizadas (software y hardware) para la atención de incidentes y requerimientos, lo que incluye el Portal de atención de requerimientos e incidentes del proyecto.
- Los servicios de operación deben estar basados en buenas prácticas o estándares internacionales de seguridad y calidad como ISO 27001 e ISO 9001. El postor debe tener de forma mandatoria ambas certificaciones.
- La Gestión de Eventos Operacionales considera las siguientes etapas: monitoreo, detección, análisis, identificación, categorización y registro de eventos, que son recibidos por rutinas de operación, alertas automatizadas y reporte de eventos; interacciones operativas, informe de ejecución de tareas y procesos. Este servicio debe ser prestado en modalidad 24x7.
- Se deberá proveer un Portal de Información, donde se podrá acceder a visualizar información de alto nivel de acuerdo con su perfil de acceso. Este acceso será otorgado hasta a tres (3) usuarios y el portal debe proveer vistas relacionadas a la

⁴⁴ CONSULTA 27, formulada por DIGIWARE S.A.C; Conforme a lo señalado por el área usuaria, se confirma que la implementación puede ser ejecutada de lunes a viernes de 8am a 6pm y de ser necesario, feriados y fines de semana sobre las configuraciones que tengan impacto sobre la operativa de COFIDE.

gestión y monitoreo de los servicios en un formato ITIL (Eventos, Incidentes, Capacidad, etc.).

- Monitoreo del tiempo de respuesta de los servicios S3 de Gestión de los Equipos o Soluciones de Seguridad y Servicios de Respuesta a incidentes S4, midiendo periódicamente los tiempos de respuesta de estos, de acuerdo a lo establecido en el acuerdo de nivel de servicio.
- Monitoreo de Eventos de la infraestructura montada por El Contratista: Eventos que deben ser reportados de manera automática a una consola centralizada que debe recibir información de los agentes de monitoreo de los servidores, información sobre logs de las infraestructuras proveídas y utilizadas por El Contratista.
- Monitoreo del Desempeño y Capacidad de la infraestructura montada por El Contratista: Eventos que informan sobre el desborde de umbrales de desempeño de almacenamiento de información; y umbrales de capacidad de unidades de disco.
- Administración de Cambios: Registro, seguimiento, colección de las aprobaciones y actualización hasta la atención de los Cambios Operacionales.
- Atención de Requerimientos: Atención de Requerimientos identificados de manera clara y precisa en tiempos de acuerdo con los niveles de servicio acordados; los requerimientos factibles de atender deben ser los usuales para el negocio, de bajo riesgo y que se encuentran debidamente documentados. Se precisa que el registro de requerimientos debe ser atendido en modalidad 24x7.
- Gestión de Incidentes y Problemas Operacionales: Registro, escalamiento, seguimiento y actualización hasta la resolución de los Incidentes y Problemas Operacionales clasificados de acuerdo con el impacto, usando una metodología como ITIL v3/v4 para la administración de Incidentes y Problemas. Así mismo debe estar alineada a las buenas prácticas de NIST.

En esta fase, COFIDE o un tercero contratado por COFIDE, podrán realizar verificaciones del servicio tales como:

- Nivel de adherencia a los procedimientos e instructivos definidos.
- Cumplimiento de los niveles de servicio brindados por El Contratista del servicio, para lo cual El Contratista del servicio de Ciberseguridad debe brindar la información que solicite El Contratista del modelo de gobierno del servicio de Gestión y Operación del servicio de Ciberseguridad.

6.7.3.2 Políticas del Servicio

- Mantener la confidencialidad de la información de configuración, accesos, información recopilada y derivada durante la prestación del servicio
- Para mantener la operatividad de los servicios que prestará El Contratista, éste deberá garantizar el buen uso de los enlaces VPN que se le proporcionen.

Para la administración de los Servicios de la Gestión y Operación se deberá contar con políticas base, que constituirán las reglas básicas para su atención.

a. Política de Monitoreo de Servicios

- El Contratista debe poseer umbrales de capacidad y desempeño que garanticen la continuidad de los servicios de Ciberseguridad, por ejemplo:
 - ✓ Disco: Alerta Menor al 90% de capacidad, Alerta Crítica al 95% de capacidad, Alerta Fatal al 98% de capacidad.
 - ✓ Almacenamiento: Alerta Menor al 90% de capacidad, Alerta Crítica al 95% de capacidad, Alerta Fatal al 98% de capacidad.

Nota: Estos umbrales de capacidad de desempeño aplican para aquellos componentes que intervienen en servicios que recopilan, generan y almacenan información.

El Contratista podrá establecer umbrales de capacidad y desempeño adicionales los cuales garantizan los niveles de servicio necesarios.

El Contratista debe contar con un sistema que alerte los límites de capacidad de almacenamiento y disco.

b. Política de Cambios

- El Contratista deberá valorar los riesgos que implica cada cambio solicitado por COFIDE. Para ello, deberá calcularlo considerando el impacto del negocio y la probabilidad de falla del cambio solicitado.
- La gestión de accesos a los portales debe ser brindada como parte de un modelo restringido de “auto servicio”, el mismo que deberá ser automatizado por El Contratista.
- Los planes de vuelta atrás o ‘rollback’ deberán ser considerados en cualquier cambio cuyo impacto pueda afectar los niveles de servicio.

c. Política de Incidentes y Problemas

- **Incidente:** Interrupción no planificada en los Servicios contratados o reducción de la calidad de los servicios. Ejemplo: Una falla en un ítem de configuración (CI) puede no impactar en el servicio, sin embargo, puede ser catalogado como un incidente.
- **Problema:** Es un incidente o múltiples incidentes de causa desconocida y síntomas comunes. Es decir, un problema es cualquier evento resultante en la pérdida o potencial pérdida de la disponibilidad o funcionamiento de los servicios de Ciberseguridad. Esto incluye errores relacionados con las conectividades VPN, hardware, software y servicios contratados. Un correcto proceso de administración de problemas debe poder identificar, registrar, rastrear problemas que tengan impacto en la entrega de los servicios reconociendo recurrencia, abordando procedimientos y conteniendo o minimizando el impacto.
Si la necesidad del negocio así lo amerita, el personal autorizado de COFIDE tendrá la potestad de establecer la severidad de un incidente en un determinado momento, si así lo considera pertinente.
La Prioridad puede ser modificada durante el ciclo de vida de un problema si se determina que el impacto de negocio fue subestimado o sobrestimado
Se acordarán reuniones periódicas para la revisión de los Incidentes y Problemas acontecidos.

d. Centro de Monitoreo y Herramientas

- Registrar todos los eventos y alertas sobre la ejecución de los servicios como evidencia para la apertura de los incidentes o problemas sobre la prestación de los servicios y de ser el caso realizar el escalamiento oportuno.
- Monitoreo en Línea los umbrales de capacidad, en los servicios que correspondan. Asimismo, monitorear la disponibilidad por conectividad y funcionamiento de la infraestructura necesaria para la prestación de los servicios.
- Diferenciación de los eventos por tipo color para un manejo simple pero eficiente, considerando hasta cuatro (04) tipos de eventos.
- Debe permitir acceder a la consola de monitoreo, en modo de sólo lectura, para hasta tres (03) personas de COFIDE.⁴⁵ El acceso a esta consola se realizará por medio del enlace por internet y debe permitir visualizar el estado de cada uno de los servicios.

e. Punto Único de Contacto y Herramienta de Gestión

- Un punto de Contacto que se encargue exclusivamente de gestionar los Servicios de la Operación que atiende a COFIDE. El objetivo es concentrar la atención con un Centro Único de Contacto para evitar la degradación de la calidad del servicio y posible impacto en la continuidad de la operación, este servicio es 24x7. En caso de cambio de turno de personal, El Contratista debe asegurar que el status de incidentes problemas y cambios se trasmita adecuadamente, y no afecte la calidad del servicio de COFIDE
- Modo de Comunicación:

⁴⁵ **CONSULTA 26**, formulada por DIGIWARE S.A.C; Conforme a lo señalado por el área usuaria, se aclara que este punto hace referencia a la consola de monitoreo (dashboard) donde se podrá visualizar al menos: Cumplimiento de SLAs, gestión de eventos, gestión de incidentes, gestión de solicitudes, gestión de cambios, entre otros relacionados con el servicio. Se definirá el alcance de la vista en la etapa de implementación. Finalmente, se precisa que la consola es independiente del SIEM.

- ✓ Teléfono:
 - Incidentes, Consultas, coordinaciones.
 - Grabar todas las llamadas, retención 30 días.
 - Se precisa que el 100% del total de llamadas establecidas se deben grabar y retener por un periodo de 30 días.
- ✓ Web: Incidentes y requerimientos.
- ✓ Correo: Coordinaciones y consultas. Contingencia del Portal de atención de requerimientos e incidentes del proyecto para generación de requerimientos.
- ✓ Recibir los requerimientos a través del Portal de atención de requerimientos e incidentes del proyecto 24x7. La herramienta que permite gestionar los Incidentes, Problemas, Cambios y Requerimientos será el Portal de atención de requerimientos e incidentes del proyecto que se encontrará en línea 24x7 para la verificación y seguimiento de las solicitudes de COFIDE. El horario de atención de los requerimientos atendidos por el Centro Único de Contacto será de lunes a viernes entre las 08:00hrs hasta las 18:00hrs, excluyendo sábados, domingos y feriados.
- ✓ Registrar los incidentes, cambios y requerimientos en una herramienta que se encuentre alineada a ITIL v3 o superior para asegurar las mejores prácticas de la gestión los servicios de Ciberseguridad. En caso los Incidentes se conviertan en un problema el registro debe asociarse al registro de Problema para mejorar el seguimiento de las acciones que se están realizando para la solución correspondiente. En caso de que al ejecutarse la atención de un Cambio o Requerimiento, este presente inconveniente, la herramienta debe permitir asociar un incidente o problema para contar con las causas derivadas de un cambio realizado.
- ✓ Los usuarios TI que se encuentren relacionados al servicio de manera directa (Gerentes de Proyectos, Especialistas, Analistas, Operadores y Coordinadores por parte de El Contratista; y Gerentes de Proyecto y personal TI relacionados con el Proyecto por parte de COFIDE) tendrán una vista para visualizar los incidentes, problemas, requerimientos y/o cambios. La finalidad debe ser contar con una sola vista para simplificar su uso y minimizar el error en el registro, además de acelerar el proceso de registro.
- ✓ La herramienta de gestión de Incidentes, Problemas, Cambios y Requerimientos debe permitir anotar como mínimo la hora de registro del ticket, hora de inicio de solución, hora fin de solución y hora de cierre de ticket. Además, debe permitir anotar los estados de atención, es decir si está en proceso de atención, pendiente por atender, o resuelto. La cantidad de licencias para el acceso a la herramienta de incidentes, problemas, requerimientos y/o cambios, para el personal de COFIDE es de tres (03) usuarios concurrentes.
- ✓ La herramienta de gestión de Incidentes, Problemas, Cambios y Requerimientos debe permitir registrar la prioridad basada en el impacto y urgencia.

6.7.3.3 Responsabilidades de El Contratista

- a. Contar con personal para el Centro Único de Contacto 24x7, con los analistas que atenderán los Incidentes, Cambios y Requerimientos.
- b. Proporcionar en uso el equipamiento y software para la Administración de Eventos del servicio.
- c. Proporcionar en uso el equipamiento y software para la Administración de Incidentes y Problemas Operacionales y Administración de Cambios.
- d. Asignar el o los administradores de las herramientas de Monitoreo de los servicios de Ciberseguridad.

- e. Asignar el o los administradores de las herramientas de Gestión de Incidentes, Problemas, Requerimientos y Cambios.
- f. Proporcionar los elementos necesarios para la comunicación entre el personal TI de COFIDE y el Centro Único de Contacto
- g. Contar con una central telefónica y garantizar su correcta operación.
- h. Implementar la herramienta de gestión de requerimientos e incidentes (Portal de atención de requerimientos e incidentes del proyecto).

6.7.3.4 Resumen de licenciamiento

En el siguiente cuadro se define la responsabilidad de la provisión de las licencias de software:

Software	COFIDE	Contratista de Ciberseguridad
Sistema de gestión de requerimientos e Incidentes		X
Sistema de Monitoreo de toda la infraestructura desplegada para la prestación de los servicios		X
Cualquier otro software necesario para la Gestión de la operación.		X

Responsabilidad de licencias del servicio de operación

6.7.3.5 Responsabilidades de COFIDE

- a. Proporcionar las credenciales e información de los equipos a operar.
- b. Reportar oportunamente los requerimientos incidentes y problemas que se observe sobre los servicios.
- c. Coordinar con los responsables de los Centros de Datos para que se le brinde facilidades El Contratista, a fin de que pueda instalar y configurar la infraestructura necesaria para la prestación del servicio de Ciberseguridad. Esto incluye la autorización para crear máquinas virtuales, instalar físicamente equipos y configurar conexiones de VPN.

6.7.4 Etapa de Transición de salida

La duración de la fase de transición de salida será como mínimo de dos (02) meses los cuales están incluidos dentro de los (36) meses de El Contrato. Esta fase se dará de no continuar el mismo Contratista brindando el servicio y por tanto el contrato finalice en el tercer año. Se ha establecido la siguiente política y estrategia de migración:

6.7.4.1 Política y Estrategia de Migración

El Contratista deberá desarrollar en forma coordinada con COFIDE, un plan de transición de salida para cada uno de los servicios, manteniendo la secuencia de migración de servicios. Cualquier cambio será autorizado por COFIDE.

La migración deberá ser desarrollada en un periodo de tiempo coordinado entre El Contratista, el nuevo Contratista y COFIDE. Se realizará en general los fines de semana, días feriados no laborables u horas no laborables, a fin de minimizar el impacto en los negocios.

Se han definido dos (02) etapas para la transición de salida, estas son:

a. Etapas de Preparación

La etapa de Preparación tiene como finalidad ejecutar todas las actividades y coordinaciones necesarias para iniciar la salida Servicio de Ciberseguridad. Las actividades para realizar durante esta etapa serán las siguientes:

- Reuniones de coordinación entre COFIDE, el Contratista y el futuro Contratista.
- Programa de actividades de migración para el traslado de los servicios.
- Programar los periodos de trabajo para el traslado de los servicios, los cuales tendrán que ser presentados en un Plan a más tardar (30) días calendarios antes del inicio de la salida de servicios.

b. Etapas de Traslado de Servicios

La etapa de Traslado de Servicios tiene como finalidad ejecutar todas las actividades necesarias para el correcto traslado de los servicios hacia el nuevo Contratista.

Las actividades para realizar durante esta etapa serán las siguientes:

- Migración del Servicio de Gestión de los Equipos o Soluciones de Seguridad.
- Migración del Servicio de Detección Avanzada.
- Migración del Servicio de Respuesta a Incidentes.

Los cronogramas específicos para cada actividad serán desarrollados por los Gerentes de Proyecto de COFIDE y El Contratista, y deberán culminarse a más tardar quince (15) días calendarios, antes del inicio de la salida de los servicios.

El plan detallado para el servicio de transición de salida será revisado en conjunto con COFIDE para que se realice una migración y traslado de servicios de una manera ordenada y coordinada.

6.7.4.2 Responsabilidades de El Contratista

- a. El Contratista deberá aplicar las mejores prácticas en la realización de las tareas incluidas en el plan de trabajo presentado para ser llevadas a buen término, con la seguridad y confiabilidad, minimizando todos los riesgos dentro de los alcances de la presente propuesta.
- b. El Contratista será responsable del mantenimiento, salvaguarda y respaldo de las configuraciones y datos (Sistema Operativo, redes y aplicaciones) de la infraestructura y componentes que él despliegue y de los que COFIDE haya decidido poner bajo su custodia, hasta su entrega a un nuevo Contratista que comunique COFIDE en su oportunidad. En el caso que la entrega al nuevo Contratista sobrepase la fecha de culminación de El Contrato establecido, el cambio de fecha se gestionará a través del proceso de control de cambios para la ampliación del servicio.
- c. Deberá brindar las facilidades técnicas y de acceso al Centro de Datos al futuro Contratista, en caso se requiera.
- d. El Contratista deberá mantener las últimas copias de respaldo de la información de las configuraciones y de los datos generados por la infraestructura del Contratista. Las copias de respaldo del actual contratista deberán ser trasladadas al nuevo Contratista.

6.8 ACUERDO DE NIVELES DE SERVICIO

6.8.1 Horario de Atención

HORARIO DE DISPONIBILIDAD DEL SERVICIO						
	S1	S2	S3	S4	S5	S6
Días de Disponibilidad	L-V	L-D	L-D	L-D	L-D	L-D
Hora Inicio	9 a.m.	24x7	24x7	24x7	24x7	24x7

Hora Fin	6 p.m.					
Periodo de vigencia	36 meses					

6.8.2 Definiciones

- **Tiempo de Respuesta oportuna**, se refiere al tiempo transcurrido desde el registro de la atención en el centro de servicios o punto de contacto del proveedor, hasta la asignación y atención del especialista encargado en atender la solicitud. Durante esta interacción se indicará la prioridad.
- **Prioridad**, Se refiere al sentido de urgencia que se debe tomar en consideración a la solicitud reportada.
 - ✓ **Prioridad Alta**: Evento con interrupción y/o alto impacto en la operación del servicio. No se cuenta con solución alterna inmediata.
 - ✓ **Prioridad Media**: Evento con importante impacto en la operación del servicio. Se cuenta con solución alterna inmediata.
 - ✓ **Prioridad baja**: Incidente con bajo impacto en la operación del servicio.
- **Tiempo de solución oportuna**⁴⁶, para el caso de incidentes es el tiempo transcurrido entre la comunicación al PROVEEDOR de la existencia del mal funcionamiento del servicio por parte de COFIDE (llamada de servicio) y la disponibilidad y puesta en funcionamiento del servicio a satisfacción del COFIDE. Para el caso del requerimiento se considera el tiempo transcurrido entre la solicitud al PROVEEDOR (correo electrónico) y la confirmación de dicha atención por parte de COFIDE.

6.8.3 Niveles del Servicio

GESTIÓN DE INCIDENTES ⁴⁷			
	Prioridad Alta	Prioridad Media	Prioridad Baja
Horario atención	L-D 24 x 7	L-V 9 x 5	L-V 9 x 5
Tiempo de respuesta ⁴⁸	30 minutos 60 minutos	60 minutos 120 minutos	120 minutos 180 minutos
Tiempo de solución oportuna	8 horas	24 horas	48 horas

⁴⁶ **CONSULTA 33**, formulada por SECURESOFTE CORPORATION S.A.C.; Conforme a lo señalado por el área usuaria, se precisa que:

(i) el Tiempo de Solución Oportuna para los incidentes aplica para todos los eventos relacionado a la atención de incidentes del servicio (Infraestructura y/o tecnología y/o seguridad).

(ii) para incidentes se considera desde que se recibe la Respuesta Oportuna hasta que se realiza la resolución del incidente. Se aclara al postor que, para los requerimiento se considera desde que se recibe la Respuesta Oportuna hasta que se realiza la resolución del requerimiento.

⁴⁷ **CONSULTA 35**, formulada por SECURESOFTE CORPORATION S.A.C.; Conforme a lo señalado por el área usuaria, respecto a la gestión de incidentes:

(i) Se aclara que el Tiempo de Solución Oportuna para los incidentes aplica para todos los eventos relacionado a la atención de incidentes del servicio (Infraestructura y/o tecnología y/o seguridad)

(ii) Se confirma que para la solución de un incidente donde haya la intervención o escalamiento a la marca y/o de un tercero, el ticket de atención debe ser excluido de la medición ya que los tiempos no podrán ser definidos por el contratista. El contratista será el responsable de hacer seguimiento hasta la resolución del incidente.

(iii) Se confirma que se considerará que si para la solución del incidente se tiene dependencia del cliente o de un tercero, el ticket de atención deberá ser excluido de la medición ya que los tiempos no podrán ser definidos por el contratista. El contratista será el responsable de hacer seguimiento hasta la resolución del incidente.

⁴⁸ **CONSULTA 34**, formulada por SECURESOFTE CORPORATION S.A.C.; Conforme a lo señalado por el área usuaria y, con ocasión a la integración de las bases, con la finalidad de fomentar una mayor pluralidad de postores, se acepta lo solicitado; por lo que se considera los siguientes tiempos de respuesta para la gestión de incidentes:

Tiempo de respuesta:

Prioridad Alta=60 minutos

Prioridad Media=120 minutos

Prioridad Baja=180 minutos.

Periodo de vigencia	36 meses
Número de atenciones contratadas	Ilimitadas

GESTIÓN DE REQUERIMIENTOS			
	Prioridad Alta	Prioridad Media	Prioridad Baja
Horario atención	L-D 24 x 7	L-V 9 x 5	L-V 9 x 5
Tiempo de respuesta	01 horas	3 horas	6 horas
Tiempo de solución oportuna	24 horas	72 horas	144 horas
Periodo de vigencia	36 meses		
Número de atenciones contratadas	Ilimitadas		

6.8.4 Umbrales de Niveles de Servicio⁴⁹

Indicador	Fórmula de medición mensual	Umbral
Respuesta oportuna de Incidentes	Cantidad de incidentes respondidos oportunamente / Cantidad total de incidentes	60%
Respuesta oportuna de requerimientos	Cantidad de requerimientos respondidos oportunamente / Cantidad total de requerimientos	60%
Solución oportuna de Incidentes Prioridad Alta	Cantidad de incidentes prioridad Alta resueltos oportunamente / Cantidad total de incidentes prioridad Alta	100%
Solución oportuna de requerimientos Prioridad Alta	Cantidad de requerimientos prioridad Alta resueltos oportunamente / Cantidad total de requerimientos prioridad Alta	80%
Solución oportuna de Incidentes Otras Prioridades	Cantidad de incidentes prioridad Media y Baja resueltos oportunamente / Cantidad total de incidentes prioridad Media y Baja	60%
Solución oportuna de requerimientos Otras Prioridades	Cantidad de requerimientos prioridad Media y Baja resueltos oportunamente / Cantidad total de requerimientos prioridad Media y Baja	50%

Nota: El servicio deberá incluir un dashboard en línea desde la cual podrá visualizar el cumplimiento de los SLA del servicio y la gestión de tickets de requerimientos e incidencias.

7. CONDICIONES DEL SERVICIO

⁴⁹ **CONSULTA 36**, formulada por SECURESOFT CORPORATION S.A.C.; Conforme a lo señalado por el área usuaria, no se acepta lo solicitado, se precisa que para asegurar la calidad del servicio y minimizar el impacto de incidentes sobre la operativa de COFIDE, se considera que el umbral de cumplimiento del 100% para la solución oportuna de incidentes de prioridad alta es justificable.

7.1 DEL POSTOR:

- El POSTOR del servicio deberá contar con al menos dos (02) certificaciones para empresas de Ciberseguridad indicadas a continuación:

Ítem	Certificado	Detalle
1	ISO 9001:2015 50	Contar con certificado vigente emitido por una entidad autorizada que cuente con el siguiente alcance: Diseño, comercialización, implementación, administración, soporte, monitoreo, consultoría, servicios especializados y capacitación de soluciones en seguridad de la información; además de la gestión del centro de operaciones de seguridad CYBERSOC en Perú.
2	ISO 22301:2019	Contar con certificado vigente emitido por una entidad autorizada que cuente con el siguiente alcance: Servicios de monitoreo, soporte y administración remota de plataformas de ciberseguridad en Perú
3	ISO 27001:2013	Contar con certificado vigente emitido por una entidad autorizada que cuente con el siguiente alcance: Diseño, comercialización, implementación, administración, soporte, monitoreo, consultoría, servicios especializados y capacitación de soluciones en seguridad de la información; además de la gestión de los centros de operaciones de seguridad CYBERSOC en Perú
4	Certificado de Madurez del CyberSOC	Contar con certificado vigente con un nivel mínimo de madurez de 4 sobre 5, emitido por una entidad autorizada que cuente con el siguiente alcance: Organización de centros de operaciones de seguridad, personal, procesos, tecnología y servicios (monitoreo de seguridad, gestión de incidente de seguridad, inteligencia de amenazas, búsqueda de amenazas y gestión de vulnerabilidades)

Nota: Presentar los certificados a la firma del contrato

- El POSTOR del servicio debe contar con al menos con dos (02) membresías de comunidades de Ciberseguridad indicadas a continuación:

Ítem	Comunidad	Detalle
1	FIRST	Contar con certificación vigente que indique la membresía al Foro de Incident Response and Security Teams
2	APWG	Contar con certificación o carta que indique o confirme que la empresa es miembro o corresponsal acreditado de APWG (Unificando la Respuesta Global al Delito Cibernético)
3	FS-ISAC	Contar con certificación o carta que indique o confirme que la empresa es miembro o corresponsal acreditado del Centro de Análisis e Intercambio de Información de Servicios Financieros (FS-ISAC) para el

⁵⁰ **CONSULTA 58**, formulada por SECURESOFT CORPORATION S.A.C.; Conforme a lo señalado por el área usuaria, se acepta parcialmente lo solicitado, debido a que el servicio está alineado directamente a la gestión y operación de un Cybersoc a nivel de ciberseguridad, y la calidad de los productos y servicios está implícito en el requerimiento general, se retira de las certificaciones obligatorias el certificado ISO 9001

Ítem	Comunidad	Detalle
		intercambio de inteligencia en ciberseguridad en tiempo real.
4	CYBERSECURITY TECH ACCORD	Contar con certificación o carta que indique o confirme que la empresa es miembro o corresponsal acreditado o signataria del Acuerdo Tecnológico de Ciberseguridad para respaldar la confianza y la seguridad en el mundo en línea y foro para colaboración entre los signatarios.
5	Global Cyber Alliance ⁵¹	Contar con certificación o carta que indique o confirme que la empresa es miembro o corresponsal acreditado o signataria de Global Cyber Alliance

Nota: Presentar un documento o carta que avale lo solicitado a la firma del contrato

- El POSTOR podrá realizar una visita técnica y/o sesión remota para el levantamiento de información, no se aceptarán costos adicionales al servicio que el POSTOR no haya incluido por desconocimiento o falta de información. Los participantes interesados en realizar la visita técnica deberán coordinarla con el señor Daniel Mora Balta del Departamento de TI de COFIDE, ubicado en calle Augusto Tamayo 160 San Isidro – Lima al correo **dmora@cofide.com.pe** o al teléfono 01615400 anexo 4016, para el levantamiento de información y estudio de campo que le permita, adicionalmente a la información proporcionada, presentar y sustentar su propuesta.
- Realizar las coordinaciones con COFIDE para el despliegue e instalación de la infraestructura en los equipos y soluciones que son gestionados por terceros.
- Aplicar las mejores prácticas en la realización de las tareas incluidas en el plan de trabajo presentado para ser llevadas a buen término, con la seguridad y confiabilidad, minimizando todos los riesgos dentro de los alcances de la presente propuesta.
- Las instalaciones de El Contratista deben cumplir con las condiciones de energía, ambiente, espacio, infraestructura de redes, soporte para cableado y seguridad adecuados para el desarrollo de los servicios.
- Ser responsable por el mantenimiento, salvaguarda y respaldo de las configuraciones (Hardware, software y/o servicios) utilizadas para la ejecución de los servicios.
- Es responsable por los períodos en que los servicios estén fuera de línea por problemas causados por las actividades relacionadas al traslado e instalación de equipos. Los seguros por siniestro y transporte son responsabilidad de El Contratista.

7.2 DE COFIDE:

- COFIDE brindará las facilidades al postor ganador, para que desarrollen sus actividades durante el periodo del servicio contratado.
- Entregar toda la información solicitada por El Contratista.
- Brindar información acerca de las redes y componentes TI.
- Coordinar de manera diligente con El Contratista con el fin de atender cualquier requerimiento de información y de ser el caso dar conformidad sobre las metodologías propuestas y la recepción definitiva del servicio.
- Brindar todas las facilidades de acceso y permisos necesarios al Contratista para que se puedan realizar las actividades de la fase de transición de entrada señaladas

7.3 SEGURIDAD DE LA INFORMACIÓN

- De conformidad a la Directiva de Seguridad de la Información N°011.04.2022 "Relación

⁵¹ CONSULTA 28, formulada por DIGIWARE S.A.C; Conforme a lo señalado por el área usuaria y, con ocasión a la integración de bases, se confirma que se aceptará una membresía de Global Cyber Alliance.

con Proveedores”, el CONTRATISTA debe cumplir:

Protección de Activos

En caso de requerir conexiones para la implementación y/o soporte y/u operación del servicio, El CONTRATISTA:

- Es el responsable de la seguridad del servicio ofrecido y deberá contar con medidas de seguridad (firewall, protección contra software malicioso, control de fugas de información, entre otros), que permitan asegurar la confidencialidad, integridad y disponibilidad de la información de COFIDE.
- Debe coordinar con el equipo de Tecnologías de Información de COFIDE el otorgamiento de accesos y su posterior revocación al finalizar el servicio u contrato.
- Debe coordinar con el equipo de Tecnologías de Información de COFIDE el método de acceso permitido, políticas de usuarios y contraseñas, autorización de accesos a usuarios y sus respectivos privilegios, control físico y lógico para la restricción de acceso a la información sensible, así como mantener actualizada la lista de personas autorizadas.

Acuerdo de Confidencialidad

EL CONTRATISTA debe cumplir con el acuerdo de confidencialidad, en virtud del cual se obliga a no copiar, difundir, aplicar, ni comunicar a terceros información, base de datos ni cualquier otro aspecto relacionado a COFIDE a la que tenga acceso durante la ejecución del servicio. En el caso de que EL CONTRATISTA incumpla el pacto de confidencialidad, COFIDE a su sola discreción podrá resolver el contrato, sin perjuicio de adoptar las acciones legales que correspondan.

8. GESTIÓN DEL PERSONAL

No Aplica.

9. OTRAS PENALIDADES

El incumplimiento de umbrales indicados en el numeral **6.2.4** traerá como consecuencia las siguientes penalidades.

9.1 Para tiempos de respuesta y solución⁵²

Supuesto de aplicación de penalidad	Forma de cálculo	Procedimiento
Respuesta oportuna de Incidentes (todas las Prioridades)	10% * 1UIT	El cálculo se realiza si no cumple con el umbral del Respuesta oportuna de Incidentes (60%)

⁵² **CONSULTA 37**, formulada por SECURESOFT CORPORATION S.A.C.; Conforme a lo señalado por el área usuaria, se aclara que el cálculo de las penalidades es un estándar definido por COFIDE, el mismo que se encuentra alineado a la normativa de contrataciones del Estado, y se encuentran calculados a un porcentaje de una (01) UIT siendo proporcional, la necesidad de COFIDE es contar con un servicio disponible y de calidad teniendo en cuenta la criticidad de la Seguridad de Información de COFIDE.

Asimismo, se hace presente que, según la experiencia de anteriores contratos de COFIDE, la aplicación de tal penalidad no ha resultado ser irracional ni desproporcional, contrario a ello se busca fomentar que el contratista cumpla a cabalidad con lo requerido por la Entidad. Por lo tanto; no se acepta lo solicitado.

CONSULTA 38, formulada por SECURESOFT CORPORATION S.A.C.; Conforme a lo señalado por el área usuaria, se aclara que el cálculo de las penalidades es un estándar definido por COFIDE, se encuentra alineado a la normativa de contrataciones del Estado, y están calculadas a un porcentaje de una (01) UIT, siendo proporcional, la necesidad de COFIDE es contar con un servicio disponible y de calidad teniendo en cuenta la criticidad de la Seguridad de Información de COFIDE.

Asimismo, se precisa que para asegurar la calidad del servicio y minimizar el impacto de incidentes sobre la operativa de COFIDE, se considera que el umbral de cumplimiento del 100% para la solución oportuna de incidentes de prioridad alta es justificable. Se hace presente que, según la experiencia de anteriores contratos de COFIDE, la aplicación de tal penalidad no ha resultado ser irracional ni desproporcional, contrario a ello se busca fomentar que el contratista cumpla a calidad con lo requerido por la Entidad. Por lo tanto; no se acepta lo solicitado.

CONSULTA 39, 40 y 41, formulada por SECURESOFT CORPORATION S.A.C.; Conforme a lo señalado por el área usuaria, se aclara que el cálculo de las penalidades es un estándar definido por COFIDE, esta alineado a la normativa de contrataciones del Estado, y estas están calculadas a un porcentaje de una (01) UIT siendo proporcional, la necesidad de COFIDE es contar con un servicio disponible y de calidad teniendo en cuenta la criticidad de la Seguridad de Información de COFIDE.

Asimismo, se hace presente que, según la experiencia de anteriores contratos de COFIDE, la aplicación de tal penalidad no ha resultado ser irracional ni desproporcional, contrario a ello se busca fomentar que el contratista cumpla a calidad con lo requerido por la Entidad. Por lo tanto; no se acepta lo solicitado.

Respuesta oportuna de Requerimientos (todas las Prioridades)	5% * UIT	El cálculo se realiza si no cumple con el umbral del Respuesta oportuna de Requerimientos (60%)
Solución oportuna de Incidentes Prioridad Alta	20% * UIT	El cálculo se realiza si no cumple con el umbral del Solución oportuna de Incidentes Prioridad Alta (100%)
Solución oportuna de Requerimientos Prioridad Alta	10% * UIT	El cálculo se realiza si no cumple con el umbral del Solución oportuna de Requerimientos Prioridad Alta (80%)
Solución oportuna de Incidentes Otras Prioridades	10% * UIT	El cálculo se realiza si no cumple con el umbral del Solución oportuna de Incidentes Otras Prioridades (60%)
Solución oportuna de Requerimientos Otras Prioridades	5% * UIT	El cálculo se realiza si no cumple con el umbral del Solución oportuna de Requerimientos Otras Prioridades (50%)

Consideraciones:

- Las definiciones de Tiempo de respuesta oportuna, Prioridad del incidente y Tiempo de solución oportuna, se describen en el **numeral 6.8.2**
- Los niveles de servicio se describen en el **numeral 6.8.3**
- Los umbrales de nivel de servicio se describen en el **numeral 6.8.4**

10. ENTREGABLES

10.1 Entregables de Etapa de Planificación

Los entregables se deben enviar en un plazo máximo de **un (01) mes** contado a partir del día siguiente de la fecha indicada en el **Acta de Inicio del servicio**

ENTREGABLES GENERALES	CONTENIDO
Plan de proyecto	- Cronograma de actividades de implementación
Plan de riesgos	- Matriz de Riesgos del Proyecto (identificación, control y mitigación).
Plan de pruebas	- Protocolo de inspección y pruebas de recepción (incluye formatos).
Actas	- Acta de inicio del servicio

ENTREGABLES POR SERVICIO	CONTENIDO
S1 - Servicio de evaluación de Seguridad TI	- Plan para desarrollar procedimientos y formatos necesarios para la evaluación de seguridad de los activos TI.
S2 - Servicio de Gestión de los Equipos o	- Plan para desarrollar procedimientos y formatos necesarios para realizar la gestión y operación de los equipos o soluciones de seguridad.

Soluciones de Seguridad	
S3 - Servicios de Detección Avanzada	<ul style="list-style-type: none"> - Plan para instalar, configurar y desplegar los componentes necesarios para la operación del sistema SIEM, el cual permita realizar la detección avanzada. - Plan para desarrollar procedimientos y formatos necesarios para realizar la detección avanzada.
S4 - Servicios Respuesta a Incidentes como Servicio	<ul style="list-style-type: none"> - Plan para desarrollar procedimientos y formatos necesarios para realizar la respuesta a incidentes como servicio.
S5-Servicio de Identificación de las Vulnerabilidades en Aplicaciones.	<ul style="list-style-type: none"> - Plan para desarrollar procedimientos y formatos necesarios para realizar la respuesta a incidentes como servicio.
S6-Servicios de Ciberinteligencia.	<ul style="list-style-type: none"> - Plan para desarrollar procedimientos y formatos necesarios para realizar la respuesta a incidentes como servicio.
Todos los servicios	<ul style="list-style-type: none"> - Ficha técnica de los equipos y soluciones que presentarán en los servicios

10.2 Entregables de Etapa de Implementación

Los entregables se deben enviar dentro de **los quince (15) días calendarios** de iniciado la **Etapa de Operación** indicado en el **Acta de inicio de Etapa Operativa del Servicio**.

ENTREGABLES POR SERVICIO	CONTENIDO
S1 - Servicio de evaluación de Seguridad TI	<ul style="list-style-type: none"> - Actas de entrevistas con el personal de COFIDE. - Inventario de activos con detalles técnicos - Metodología para la apreciación de riesgos de activos TI. - Estructura de los documentos base para ejecutar el servicio.
S2 - Servicio de Gestión de los Equipos o Soluciones de Seguridad	<ul style="list-style-type: none"> - Metodología para la atención de requerimientos de operación. - Configuración de la conectividad mediante VPN para acceso hacia los equipos y soluciones de seguridad.
S3 - Servicios de Detección Avanzada	<ul style="list-style-type: none"> - Metodología para la evaluación de eventos de seguridad. - Metodología para analizar los resultados de la correlación. - Metodología para configurar los casos de uso nuevos. - Metodología para establecer los plazos de retención de información idóneos. - Metodología para comunicar las alertas de los eventos de seguridad. - Metodología para activar el servicio de gestión de incidentes. - Infraestructura configurada para la detección avanzada (SIEM). - Configuración de la conectividad mediante VPN para acceso al software y/o hardware de monitoreo. - Procedimiento para realizar la integración del SIEM en los equipos y soluciones que son gestionados por los proveedores de COFIDE.
S4 - Servicios Respuesta a	<ul style="list-style-type: none"> - Metodología para la gestión de incidentes, en sus diferentes etapas, lo que debe incluir como mínimo la

Incidentes como Servicio	identificación, clasificación, análisis, elaboración de planes de respuesta, planes de contención, planes de erradicación y planes de restauración.
S5-Servicio de Identificación de las Vulnerabilidades en Aplicaciones.	<ul style="list-style-type: none"> - Inventario de activos con detalles técnicos - Metodología para el análisis y evaluación de vulnerabilidades de aplicaciones. - Metodología para analizar los resultados de la evaluación. - Infraestructura de escaneo configuradas (sondas, máquinas de salto, entre otros). - Configuración de la conectividad mediante VPN para acceso al software y/o hardware de escaneo.
S6-Servicios de Ciberinteligencia.	<ul style="list-style-type: none"> - Actas de definición de palabras claves con el personal de COFIDE. - Metodología para identificar amenazas y riesgos respecto de la reputación, marcas y/o conceptos importantes de COFIDE.
Todos los servicios	<ul style="list-style-type: none"> - Acceso al Portal de atención de requerimientos e incidentes del proyecto. - Acceso al Portal de información (dashboard). - Manual o procedimiento para uso de herramienta de Gestión de Servicios - Formato del informe de gestión mensual, el cual reporta el uso de los servicios y los niveles de servicio alcanzados, así como las recomendaciones para la mejora de estos.

10.3 Entregables de Etapa Operativa

Tendrá un plazo de **treinta y seis (36) meses** contados a partir de la fecha indicada en el **Acta de Inicio de Etapa Operativa del servicio**.

Los entregables se deben enviar como dentro de **los siete (07) días calendarios** posteriores al mes del servicio.

ENTREGABLES POR SERVICIO	CONTENIDO	PLAZO MAXIMO
S1 - Servicio de evaluación de Seguridad TI	<ul style="list-style-type: none"> - Informe técnico con los resultados de la evaluación de riesgos, el cual debe indicar los riesgos identificados, planes de acción y recomendaciones de mejora. - Inventario de los activos evaluados durante la ejecución del servicio. - Informe ejecutivo con el detalle de las fases ejecutadas. - Plan de mitigación de riesgos identificados, planes de acción y recomendaciones de mejora. - Acta de inicio del servicio S1 - Informe de seguimiento de remediaciones (Mensual durante toda la etapa Operativa del servicio). 	<p>Una vez por año dentro de los cinco (05) primeros meses de cada aniversario e inicia a partir de Acta de inicio del servicio S1</p> <p>Una vez a demanda dentro de los primeros dos (02) años del servicio e inicia a partir de la firma del Acta de inicio del servicio S1 que considera la evaluación de los activos de</p>

		seguridad de TI. ⁵³
S2 - Servicio de Gestión de los Equipos o Soluciones de Seguridad	<ul style="list-style-type: none"> - Informe con los resultados de la gestión de la atención de incidentes, mantenimiento, supervisión y atención de requerimientos de los equipos o soluciones que se integren al modelo del servicio en los casos que aplique, incluir plan de mejoras y recomendaciones 	Mensual a partir del mes siguiente a la fecha indicada en el Acta de Inicio de Etapa Operativa del servicio
S3 - Servicios de Detección Avanzada	<ul style="list-style-type: none"> - Informe que considera los aspectos de Monitoreo, Detección, Análisis e Interpretación de los resultados a partir del cual se podrán tomar decisiones, incluir plan de acción y recomendaciones de mejora. 	Mensual a partir del mes siguiente a la fecha indicada en el Acta de Inicio de Etapa Operativa del servicio
S4 - Servicios Respuesta a Incidentes como Servicio	<ul style="list-style-type: none"> - Informe de la gestión realizada por cada incidente que se produzca que incluya: las medidas de contención y respuesta implementadas y el estado de recuperación de los servicios o activos y el análisis forense que determine las causas del incidente de ser necesario. - Informe de análisis forense del incidente significativo adverso que identifique las causas y las medidas para su gestión si este fuera necesario. 	Mensual a partir del mes siguiente a la fecha indicada en el Acta de Inicio de Etapa Operativa del servicio
S5-Servicio de Identificación de las Vulnerabilidades en Aplicaciones.	<ul style="list-style-type: none"> - Informe técnico con los resultados del hacking ético de vulnerabilidades para los activos evaluados, incluir plan de acción y recomendaciones de mejora. 	Una vez por año a demanda e inicia a partir de Acta de Inicio de Etapa Operativa del servicio
S6-Servicios de Ciberinteligencia.	<ul style="list-style-type: none"> - Informe del servicio que considere: la identificación de ciberamenazas y su clasificación, además las medidas correctivas desarrolladas y la asesoría brindada a COFIDE para minimizar el impacto de la amenaza, incluir plan de acción y recomendaciones de mejora. 	Mensual a partir del mes siguiente a la fecha indicada en el Acta de Inicio de Etapa Operativa del servicio
Todos los servicios	<p>Presentación (resumen ejecutivo) de los resultados de la gestión de todos los servicios del periodo mensual. Cantidad de problemas, incidentes y requerimientos recibidos por teléfono, mail, Portal de atención de requerimientos e incidentes del proyecto.</p> <ul style="list-style-type: none"> - Cumplimiento de indicadores corporativos (SLA's) - Cuadro de control de semáforo. - Gráficos de rendimiento y tendencias. - Planes de acción correctivo con fecha de compromiso dentro de los plazos del contrato. 	Mensual a partir del mes siguiente a la fecha indicada en el Acta de Inicio de Etapa Operativa del servicio

⁵³ **CONSULTA 59**, formulada por SECURESOFT CORPORATION S.A.C.; Conforme a lo señalado por el área usuaria, se confirma que el plazo máximo para el Servicio de evaluación de Seguridad TI será de una única vez como se indica en el detalle del punto 6.1 (p. 28 de las bases administrativas).

	- Consumos efectivos de capacidades contra la Línea Base.	
--	---	--

10.4 Entregables de Etapa de Transición de salida

ENTREGABLES POR SERVICIO	CONTENIDO	PLAZO MAXIMO
Todos los servicios	- Presentar un plan de capacitación para el nuevo Contratista del servicio de por lo menos cuatro (04) horas de capacitación para un máximo de cinco (05) personas en los roles de Service Manager y Operación del Servicio. Este plan de capacitación será programado de común acuerdo entre COFIDE y El Contratista. Esta capacitación se realizará de manera virtual y será realizada por el personal del Contratista. Las sesiones de capacitación podrán ser grabadas para futura referencia.	Dos (02) meses antes de culminar el periodo de la Etapa Operativa del servicio

Nota: Los entregables se deben presentar en formato fuente, es decir documento en Word, Excel, PowerPoint, Visio o Project, según corresponda, en formato de impresión (PDF)

Los entregables serán remitidos a la Mesa de Partes Virtual de COFIDE, a través del siguiente enlace <https://facilita.gob.pe/t/4897> y vía correo electrónico al siguiente email:

- entregablesti@cofide.com.pe

11. PLAZO DEL SERVICIO

El periodo del servicio operativo tendrá un plazo de **treinta y seis (36) meses** contados a partir de la fecha indicada en el **Acta de Inicio de Etapa Operativa del servicio**.

12. FORMA DE PAGO

El pago se ejecutará de manera mensual en cuotas iguales posterior a la recepción de la documentación exigida en el **numeral 10.3 Entregables de Etapa Operativa**, luego de otorgada la conformidad del servicio por parte del área usuaria; para efectos del pago de las contraprestaciones ejecutadas por el contratista, la Entidad deberá contar con la siguiente documentación:

- Entregables según especificaciones técnicas o términos de referencia.
- Informe de supervisión del servicio del departamento de TI
- Acta de conformidad del servicio
- Comprobante de pago.

13. GARANTÍA

No aplica.

14. DEPENDENCIA ENCARGADA DE DAR LA CONFORMIDAD DEL SERVICIO

La conformidad del servicio será otorgada por la Gerencia de Gestión Humana y Administración, previo VºBº del Subgerente del Dpto. de Tecnologías de Información, así como por la Gerencia de Riesgos, previo VºBº del responsable de Seguridad de la Información

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	CAPACIDAD TÉCNICA Y PROFESIONAL												
B.1	EQUIPAMIENTO ESTRATÉGICO												
	<p><u>Requisitos:</u></p> <p><u>Requisitos:</u> El equipamiento estratégico requerido por cada servicio es como se detalla a continuación:</p> <table> <tr> <th data-bbox="336 701 483 734">Servicio</th><th data-bbox="491 701 1396 734">Facilidades Tecnológicas Mínimas</th></tr> <tr> <td data-bbox="336 736 483 1249">General</td><td data-bbox="491 736 1396 1249"> <ul style="list-style-type: none"> - El Contratista deberá contar con un Centro de Operaciones y Seguridad (SOC), donde se encuentren monitoreando las 24 horas del día, los 7 días a la semana y los 365 los días del año durante la vigencia del contrato, este Centro de Operaciones y Seguridad deberá estar dentro del territorio nacional, y deberá contar con un Centro de Operaciones y Seguridad como contingencia fuera del país para asegurar la alta disponibilidad. Así mismo el Centro de Operaciones y Seguridad (SOC) deberá contar con un sistema de gestión ON LINE el cual mediante un Dashboard personalizable (el cual se podrá mostrar en un Pc, laptop, u teléfono inteligente) permitirá a COFIDE hacer un seguimiento de los eventos, indicadores de gestión para cumplimiento del SLA, reportes de fallas, atención a nuevas solicitudes o tratamiento de reclamos, así como también la atención y solución de averías, y solicitudes derivadas del servicio sin necesidad de cursar comunicación al proveedor. La ENTIDAD deberá contar con acceso para al menos tres (3) usuarios al sistema de gestión ON LINE. </td></tr> <tr> <td data-bbox="336 1252 483 1406">S1</td><td data-bbox="491 1252 1396 1406"> <ul style="list-style-type: none"> - Correo electrónico corporativo del Contratista para coordinaciones. - Sistemas de videoconferencia para realizar las coordinaciones. - Estaciones de trabajo para los recursos humanos proporcionado por el Contratista. - Acceso a Internet. </td></tr> <tr> <td data-bbox="336 1408 483 1529">S2</td><td data-bbox="491 1408 1396 1529"> <ul style="list-style-type: none"> - Estaciones de trabajo para los recursos humanos proporcionado por el Contratista. - Conectividad para acceso hacia los equipos y soluciones de seguridad de COFIDE </td></tr> <tr> <td data-bbox="336 1532 483 1899">S3</td><td data-bbox="491 1532 1396 1899"> <ul style="list-style-type: none"> - Máquina virtual: Software y/o hardware y/o servicio en la nube para la recolección, homologación y almacenamiento de logs, realización de la correlación y una consola que permita configurar las reglas (casos de uso). - Consola de administración: Hardware ubicado en el SOC del Contratista que almacena los logs. - Conectividad para acceso al software y/o hardware de monitoreo. - Estaciones de trabajo para los recursos humanos proporcionado por el Contratista. - Correo electrónico corporativo del Contratista para coordinaciones. - Sistemas de videoconferencia para realizar las coordinaciones. </td></tr> <tr> <td data-bbox="336 1901 483 2069">S4</td><td data-bbox="491 1901 1396 2069"> <ul style="list-style-type: none"> - Software especializado, según requiera cada incidente (por ejemplo, software de volcado de memoria, de recuperación de datos, etc.). - Estaciones de trabajo para los recursos humanos proporcionado por el Contratista. - Correo electrónico corporativo del Contratista para coordinaciones. - Sistemas de videoconferencia para realizar las coordinaciones. </td></tr> </table>	Servicio	Facilidades Tecnológicas Mínimas	General	<ul style="list-style-type: none"> - El Contratista deberá contar con un Centro de Operaciones y Seguridad (SOC), donde se encuentren monitoreando las 24 horas del día, los 7 días a la semana y los 365 los días del año durante la vigencia del contrato, este Centro de Operaciones y Seguridad deberá estar dentro del territorio nacional, y deberá contar con un Centro de Operaciones y Seguridad como contingencia fuera del país para asegurar la alta disponibilidad. Así mismo el Centro de Operaciones y Seguridad (SOC) deberá contar con un sistema de gestión ON LINE el cual mediante un Dashboard personalizable (el cual se podrá mostrar en un Pc, laptop, u teléfono inteligente) permitirá a COFIDE hacer un seguimiento de los eventos, indicadores de gestión para cumplimiento del SLA, reportes de fallas, atención a nuevas solicitudes o tratamiento de reclamos, así como también la atención y solución de averías, y solicitudes derivadas del servicio sin necesidad de cursar comunicación al proveedor. La ENTIDAD deberá contar con acceso para al menos tres (3) usuarios al sistema de gestión ON LINE. 	S1	<ul style="list-style-type: none"> - Correo electrónico corporativo del Contratista para coordinaciones. - Sistemas de videoconferencia para realizar las coordinaciones. - Estaciones de trabajo para los recursos humanos proporcionado por el Contratista. - Acceso a Internet. 	S2	<ul style="list-style-type: none"> - Estaciones de trabajo para los recursos humanos proporcionado por el Contratista. - Conectividad para acceso hacia los equipos y soluciones de seguridad de COFIDE 	S3	<ul style="list-style-type: none"> - Máquina virtual: Software y/o hardware y/o servicio en la nube para la recolección, homologación y almacenamiento de logs, realización de la correlación y una consola que permita configurar las reglas (casos de uso). - Consola de administración: Hardware ubicado en el SOC del Contratista que almacena los logs. - Conectividad para acceso al software y/o hardware de monitoreo. - Estaciones de trabajo para los recursos humanos proporcionado por el Contratista. - Correo electrónico corporativo del Contratista para coordinaciones. - Sistemas de videoconferencia para realizar las coordinaciones. 	S4	<ul style="list-style-type: none"> - Software especializado, según requiera cada incidente (por ejemplo, software de volcado de memoria, de recuperación de datos, etc.). - Estaciones de trabajo para los recursos humanos proporcionado por el Contratista. - Correo electrónico corporativo del Contratista para coordinaciones. - Sistemas de videoconferencia para realizar las coordinaciones.
Servicio	Facilidades Tecnológicas Mínimas												
General	<ul style="list-style-type: none"> - El Contratista deberá contar con un Centro de Operaciones y Seguridad (SOC), donde se encuentren monitoreando las 24 horas del día, los 7 días a la semana y los 365 los días del año durante la vigencia del contrato, este Centro de Operaciones y Seguridad deberá estar dentro del territorio nacional, y deberá contar con un Centro de Operaciones y Seguridad como contingencia fuera del país para asegurar la alta disponibilidad. Así mismo el Centro de Operaciones y Seguridad (SOC) deberá contar con un sistema de gestión ON LINE el cual mediante un Dashboard personalizable (el cual se podrá mostrar en un Pc, laptop, u teléfono inteligente) permitirá a COFIDE hacer un seguimiento de los eventos, indicadores de gestión para cumplimiento del SLA, reportes de fallas, atención a nuevas solicitudes o tratamiento de reclamos, así como también la atención y solución de averías, y solicitudes derivadas del servicio sin necesidad de cursar comunicación al proveedor. La ENTIDAD deberá contar con acceso para al menos tres (3) usuarios al sistema de gestión ON LINE. 												
S1	<ul style="list-style-type: none"> - Correo electrónico corporativo del Contratista para coordinaciones. - Sistemas de videoconferencia para realizar las coordinaciones. - Estaciones de trabajo para los recursos humanos proporcionado por el Contratista. - Acceso a Internet. 												
S2	<ul style="list-style-type: none"> - Estaciones de trabajo para los recursos humanos proporcionado por el Contratista. - Conectividad para acceso hacia los equipos y soluciones de seguridad de COFIDE 												
S3	<ul style="list-style-type: none"> - Máquina virtual: Software y/o hardware y/o servicio en la nube para la recolección, homologación y almacenamiento de logs, realización de la correlación y una consola que permita configurar las reglas (casos de uso). - Consola de administración: Hardware ubicado en el SOC del Contratista que almacena los logs. - Conectividad para acceso al software y/o hardware de monitoreo. - Estaciones de trabajo para los recursos humanos proporcionado por el Contratista. - Correo electrónico corporativo del Contratista para coordinaciones. - Sistemas de videoconferencia para realizar las coordinaciones. 												
S4	<ul style="list-style-type: none"> - Software especializado, según requiera cada incidente (por ejemplo, software de volcado de memoria, de recuperación de datos, etc.). - Estaciones de trabajo para los recursos humanos proporcionado por el Contratista. - Correo electrónico corporativo del Contratista para coordinaciones. - Sistemas de videoconferencia para realizar las coordinaciones. 												

	<table> <tr> <td>S5</td><td> <ul style="list-style-type: none"> - Software especializado para el escaneo de las vulnerabilidades de las aplicaciones - Estaciones de trabajo para los recursos humanos proporcionado por el Contratista. - Correo electrónico corporativo del Contratista para coordinaciones. - Sistemas de videoconferencia para realizar las coordinaciones. </td></tr> <tr> <td>S6</td><td> <ul style="list-style-type: none"> - Software especializado para identificar amenazas y riesgos respecto de la reputación, marcas y/o conceptos importantes de COFIDE - Estaciones de trabajo para los recursos humanos proporcionado por el Contratista. - Correo electrónico corporativo del Contratista para coordinaciones. - Sistemas de videoconferencia para realizar las coordinaciones. </td></tr> </table> <p><u>Acreditación:</u></p> <p>Copia de documentos que sustenten la propiedad, la posesión, el compromiso de compra venta o alquiler u otro documento que acredite la disponibilidad del equipamiento estratégico requerido.</p> <div> <p>Importante</p> <p><i>En el caso que el postor sea un consorcio los documentos de acreditación de este requisito pueden estar a nombre del consorcio o de uno de sus integrantes.</i></p> </div>	S5	<ul style="list-style-type: none"> - Software especializado para el escaneo de las vulnerabilidades de las aplicaciones - Estaciones de trabajo para los recursos humanos proporcionado por el Contratista. - Correo electrónico corporativo del Contratista para coordinaciones. - Sistemas de videoconferencia para realizar las coordinaciones. 	S6	<ul style="list-style-type: none"> - Software especializado para identificar amenazas y riesgos respecto de la reputación, marcas y/o conceptos importantes de COFIDE - Estaciones de trabajo para los recursos humanos proporcionado por el Contratista. - Correo electrónico corporativo del Contratista para coordinaciones. - Sistemas de videoconferencia para realizar las coordinaciones.
S5	<ul style="list-style-type: none"> - Software especializado para el escaneo de las vulnerabilidades de las aplicaciones - Estaciones de trabajo para los recursos humanos proporcionado por el Contratista. - Correo electrónico corporativo del Contratista para coordinaciones. - Sistemas de videoconferencia para realizar las coordinaciones. 				
S6	<ul style="list-style-type: none"> - Software especializado para identificar amenazas y riesgos respecto de la reputación, marcas y/o conceptos importantes de COFIDE - Estaciones de trabajo para los recursos humanos proporcionado por el Contratista. - Correo electrónico corporativo del Contratista para coordinaciones. - Sistemas de videoconferencia para realizar las coordinaciones. 				
B.3	CALIFICACIONES DEL PERSONAL CLAVE				
B.3.1	FORMACIÓN ACADÉMICA				
	<p><u>Requisitos:</u></p> <p>Director del Proyecto: Titulado en las carreras de Ingeniería Electrónica o Ingeniería de Sistemas o Ingeniería Informática y de Sistemas o en Ingeniería de Cómputo y Sistemas o Ingeniería Informática o Ingeniería de Sistemas de Información o Ingeniería de Software</p> <p>Líder del CSIRT: Profesional Titulado o Bachiller en Ingeniería Electrónica o Ingeniería de Sistemas o en Tecnologías de la Información o en Ingeniería de Cómputo y Sistemas o Ingeniería Informática o Ingeniería de Sistemas de Información o Ingeniería de Software</p> <p>Líder del CyberSOC: Profesional Titulado o Bachiller en Ingeniería Electrónica o en Telecomunicaciones o en Redes y Comunicaciones o Sistemas o en Tecnologías de la Información o en Cómputo y Sistemas o Informática o de Sistemas de Información o Ingeniería de Seguridad.</p> <p>Service Manager: Profesional Titulado en Ingeniería Electrónica o en Telecomunicaciones o en Redes y Comunicaciones o Sistemas o en Tecnologías de la Información o en Cómputo y Sistemas o Informática o de Sistemas de Información o Ingeniería de Seguridad</p> <p><u>Acreditación:</u></p> <p>El grado o título requerido será verificado por el comité de selección en el Registro Nacional de Grados Académicos y Títulos Profesionales en el portal web de la Superintendencia Nacional de Educación Superior Universitaria - SUNEDU a través del siguiente link: https://enlinea.sunedu.gob.pe/ o en el Registro Nacional de Certificados, Grados y Títulos a cargo del Ministerio de Educación a través del siguiente link: https://titulosinstitutos.minedu.gob.pe/, según corresponda.</p> <p>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.</p> <p>En caso el grado o título requerido no se encuentre inscrito en el referido registro, el postor debe presentar la copia del diploma respectivo a fin de acreditar la formación académica requerida.</p>				
B.3.2	CAPACITACIÓN				
	<u>Requisitos:</u>				

	<p>Director del Proyecto: Por lo menos 01 de los siguientes cursos: Curso, diplomado o programa en gerencia y/o gestión de proyectos, de mínimo 100 horas.</p> <p>Líder del CSIRT: Por lo menos 03 de los siguientes cursos: - Curso, diplomado o programa de ITIL, de mínimo 20 horas. - Curso, diplomado o programa de ISO/IEC 27001 Auditor Líder, de mínimo 30 horas. - Curso, diplomado o programa de Transformación Digital, de mínimo 30 horas. - Curso, diplomado o programa de respuesta ante incidentes, de mínimo 50 horas. - Curso, diplomado o programa de atención de ciberamenazas, de mínimo 30 horas.</p> <p>Líder del CyberSOC: Por lo menos 02 de los siguientes cursos: - Curso, diplomado o programa de Seguridad de Sistemas de Información, de mínimo 100 horas. - Curso, diplomado o programa de Certified Information Security Manager (CISM), de mínimo 20 horas. - Curso, diplomado o programa de Certified Information Systems Security Professional (CISSP), de mínimo 40 horas. - Curso, diplomado o programa en gestión de servicio de SOC o CyberSOC, de mínimo 50 horas.</p> <p>Service Manager: Por lo menos 02 de los siguientes cursos: - Curso, diplomado o programa de Seguridad de Sistemas de Información, de mínimo 100 horas. - Curso, diplomado o programa de Certified Information Security Manager (CISM), de mínimo 20 horas. - Curso, diplomado o programa de Certified Information Systems Security Professional (CISSP), de mínimo 40 horas. - Curso, diplomado o programa en Gestión de Servicios de Tecnologías de la Información, de mínimo 40 horas. - Curso y/o Diplomado y/o programa de Especialización en Gestión de Proyectos, de mínimo 100 horas.⁵⁴</p> <p><u>Acreditación:</u> Se acreditará con copia simple de constancias, certificados u otro documento, según corresponda.</p> <div style="border: 1px solid black; padding: 5px; margin-top: 10px;"> <p>Importante</p> <p><i>Se podrá acreditar la capacitación mediante certificados de estudios de postgrado, considerando que cada crédito del curso que acredita la capacitación equivale a dieciséis horas lectivas, según la normativa de la materia.</i></p> </div>
B.4	EXPERIENCIA DEL PERSONAL CLAVE

⁵⁴ **CONSULTA 42 y 47**, formuladas por SECURESOFTECH CORPORATION S.A.C.; Conforme a lo señalado por el área usuaria y, con ocasión a la integración de las bases, se acepta lo solicitado, por lo que se acepta como una opción adicional el curso, diplomado o programa de Especialización en Gestión de Proyectos, de mínimo 100 horas; dado que las funciones solicitadas para este personal también son de gestión.

	<p><u>Requisitos:</u></p> <p>Director del Proyecto: Mínimo 6 años en Gestión de Proyectos de TI y/o Seguridad Gestionada, como Jefe o Gestor o Coordinador o Encargado o Director o Gerente o Subgerente.</p> <p>Líder del CSIRT: Mínimo de cuatro (4) años en proyectos de plataformas de Seguridad, CyberSOC o Ciberseguridad o Servicio de Respuesta ante Incidentes, como jefe o Líder o Coordinador.</p> <p>Líder del CyberSOC: Mínimo de seis (6) años en servicios especializados de CyberSOC, Security Advisor o Ciberinteligencia como Especialista o Analista Técnico o jefe o Líder</p> <p>Service Manager: Mínimo de seis (6) años en gestionar o liderar o supervisar servicios de ciberseguridad como Especialista o Analista Técnico o Jefe o Líder</p> <p><u>De presentarse experiencia ejecutada paralelamente (traslape), para el cómputo del tiempo de dicha experiencia sólo se considerará una vez el periodo traslapado.</u></p> <p><u>Acreditación:</u></p> <p>La experiencia del personal clave se acreditará con cualquiera de los siguientes documentos: (i) copia simple de contratos y su respectiva conformidad o (ii) constancias o (iii) certificados o (iv) cualquier otra documentación que, de manera fehaciente demuestre la experiencia del personal propuesto.</p> <div> <p>Importante</p> <ul style="list-style-type: none"> • <i>Los documentos que acreditan la experiencia deben incluir los nombres y apellidos del personal clave, el cargo desempeñado, el plazo de la prestación indicando el día, mes y año de inicio y culminación, el nombre de la Entidad u organización que emite el documento, la fecha de emisión y nombres y apellidos de quien suscribe el documento.</i> • <i>En caso los documentos para acreditar la experiencia establezcan el plazo de la experiencia adquirida por el personal clave en meses sin especificar los días se debe considerar el mes completo.</i> • <i>Se considerará aquella experiencia que no tenga una antigüedad mayor a veinticinco (25) años anteriores a la fecha de la presentación de ofertas.</i> • <i>Al calificar la experiencia del personal, se debe valorar de manera integral los documentos presentados por el postor para acreditar dicha experiencia. En tal sentido, aun cuando en los documentos presentados la denominación del cargo o puesto no coincida literalmente con aquella prevista en las bases, se deberá validar la experiencia si las actividades que realizó el personal corresponden con la función propia del cargo o puesto requerido en las bases.</i> </div>
C	EXPERIENCIA DEL POSTOR EN LA ESPECIALIDAD

Requisitos:

El postor debe acreditar un monto facturado acumulado equivalente a S/ 5'640,000.00 (Cinco millones seiscientos cuarenta 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.

Se consideran servicios similares a los siguientes:

- Servicio de Licencias o Servicio de CYBERSOC o Administración y Monitoreo de Plataformas de Seguridad y Correlación Inteligente de Eventos de Seguridad
- Servicio de seguridad de red interna y perimetral
- Servicio de Soporte, Monitoreo y Administración de red interna y perimetral
- Consultoría, desarrollo, mantenimiento y/o soporte de soluciones tecnológicas de seguridad
- Servicios de RedTeam
- Servicio de monitoreo de eventos de seguridad (SOC)
- Servicio de CyberSOC o Cyber Defense Center
- Soporte, gestión, mantenimiento o monitoreo de equipamiento o plataformas de seguridad
- Servicio de seguridad Gestionada, Solución Integral Tecnológica de Ciberseguridad – SIEM
- Servicio de soporte de plataforma de seguridad y correlación, servicio de protección de tráfico web, sistema de correlación de eventos-SIEM

Acreditación:

La experiencia del postor en la especialidad se acreditará con copia simple de (i) contratos u órdenes de servicios, y su respectiva conformidad o constancia de prestación; o (ii) comprobantes de pago cuya cancelación se acredite documental y fehacientemente, con voucher de depósito, nota de abono, reporte de estado de cuenta, cualquier otro documento emitido por Entidad del sistema financiero que acredite el abono o mediante cancelación en el mismo comprobante de pago⁵⁵, correspondientes a un máximo de veinte (20) contrataciones.

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

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

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

⁵⁵ 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".

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

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

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

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

Importante

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

Importante

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

CAPÍTULO IV
FACTORES DE EVALUACIÓN

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

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

FACTOR DE EVALUACIÓN		PUNTAJE / METODOLOGÍA PARA SU ASIGNACIÓN
A. PRECIO		
<u>Evaluación:</u> Se evaluará considerando el precio ofertado por el postor. <u>Acreditación:</u> Se acreditará mediante el documento que contiene el precio de la oferta (Anexo N° 6).		La evaluación consistirá en otorgar el máximo puntaje a la oferta de precio más bajo y otorgar a las demás ofertas puntajes inversamente proporcionales a sus respectivos precios, según la siguiente fórmula: $P_i = \frac{O_m \times PMP}{O_i}$ i = Oferta P_i = Puntaje de la oferta a evaluar O_i = Precio i O_m = Precio de la oferta más baja PMP = Puntaje máximo del precio 100 puntos
PUNTAJE TOTAL		100 puntos⁵⁶

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.

⁵⁶ Es la suma de los puntajes de todos los factores de evaluación.

CAPÍTULO V PROFORMA DEL CONTRATO

Importante

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

Conste por el presente documento, la contratación del servicio de gestión y operación de la ciberseguridad, que celebra de una parte CORPORACIÓN FINANCIERA DE DESARROLLO S.A., en adelante LA ENTIDAD, con RUC N° 20100116392, con domicilio legal en Augusto Tamayo Nro. 160, distrito de San Isidro, provincia y departamento de 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° 007-2024-COFIDE** para la contratación de SERVICIO DE GESTIÓN Y OPERACIÓN DE LA CIBERSEGURIDAD, a [INDICAR NOMBRE DEL GANADOR DE LA BUENA PRO], cuyos detalles e importe constan en los documentos integrantes del presente contrato.

CLÁUSULA SEGUNDA: OBJETO

El presente contrato tiene por objeto SERVICIO DE GESTIÓN Y OPERACIÓN DE LA CIBERSEGURIDAD.

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 PAGO⁵⁷

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

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

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

⁵⁷ En cada caso concreto, dependiendo de la naturaleza del contrato, podrá adicionarse la información que resulte pertinente a efectos de generar el pago.

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

CLÁUSULA QUINTA: DEL PLAZO DE LA EJECUCIÓN DE LA PRESTACIÓN

El plazo de ejecución del presente contrato es de [.....], el mismo que se computa desde [CONSIGNAR SI ES DEL DÍA SIGUIENTE DEL PERFECCIONAMIENTO DEL CONTRATO, DESDE LA FECHA QUE SE ESTABLEZCA EN EL CONTRATO O DESDE LA FECHA EN QUE SE CUMPLAN LAS CONDICIONES PREVISTAS EN EL CONTRATO PARA EL INICIO DE LA EJECUCIÓN, DEBIENDO INDICAR LAS MISMAS EN ESTE ÚLTIMO CASO].

Importante

De preverse en los Términos de Referencia la ejecución de actividades de instalación, implementación u otros que deban realizarse de manera previa al inicio del plazo de ejecución, se debe consignar lo siguiente:

“El plazo para la [CONSIGNAR LAS ACTIVIDADES PREVIAS PREVISTAS EN LOS TÉRMINOS DE REFERENCIA] es de [.....], el mismo que se computa desde [INDICAR CONDICIÓN CON LA QUE DICHAS ACTIVIDADES SE INICIAN].”

CLÁUSULA SEXTA: PARTES INTEGRANTES DEL CONTRATO

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

CLÁUSULA SÉTIMA: GARANTÍAS

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

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

Importante

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

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

En el caso que corresponda, consignar lo siguiente:

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

Importante

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

de prestaciones accesorias, debe consignarse lo siguiente:

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

Importante

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

CLÁUSULA OCTAVA: EJECUCIÓN DE GARANTÍAS POR FALTA DE RENOVACIÓN

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

CLÁUSULA NOVENA: CONFORMIDAD DE LA PRESTACIÓN DEL SERVICIO

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

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

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

CLÁUSULA DÉCIMA: DECLARACIÓN JURADA DEL CONTRATISTA

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

CLÁUSULA UNDÉCIMA: RESPONSABILIDAD POR VICIOS OCULTOS

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

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

CLÁUSULA DUODÉCIMA: PENALIDADES

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

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

Donde:

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

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

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

OTRAS PENALIDADES

El incumplimiento de umbrales indicados en el numeral **6.2.4** traerá como consecuencia las siguientes penalidades.

9.2 Para tiempos de respuesta y solución

Supuesto de aplicación de penalidad	Forma de cálculo	Procedimiento
Respuesta oportuna de Incidentes (todas las Prioridades)	10% * 1UIT	El cálculo se realiza si no cumple con el umbral del Respuesta oportuna de Incidentes (60%)
Respuesta oportuna de Requerimientos (todas las Prioridades)	5% * UIT	El cálculo se realiza si no cumple con el umbral del Respuesta oportuna de Requerimientos (60%)
Solución oportuna de Incidentes Prioridad Alta	20% * UIT	El cálculo se realiza si no cumple con el umbral del Solución oportuna de Incidentes Prioridad Alta (100%)
Solución oportuna de Requerimientos Prioridad Alta	10% * UIT	El cálculo se realiza si no cumple con el umbral del Solución oportuna de Requerimientos Prioridad Alta (80%)
Solución oportuna de Incidentes Otras Prioridades	10% * UIT	El cálculo se realiza si no cumple con el umbral del Solución oportuna de Incidentes Otras Prioridades (60%)
Solución oportuna de Requerimientos Otras Prioridades	5% * UIT	El cálculo se realiza si no cumple con el umbral del Solución oportuna de Requerimientos Otras Prioridades (50%)

Consideraciones:

- Las definiciones de Tiempo de respuesta oportuna, Prioridad del incidente y Tiempo de solución oportuna, se describen en el **numeral 6.8.2**
- Los niveles de servicio se describen en el **numeral 6.8.3**
- Los umbrales de nivel de servicio se describen en el **numeral 6.8.4**

Importante

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

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

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

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

CLÁUSULA DÉCIMA TERCERA: RESOLUCIÓN DEL CONTRATO

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

CLÁUSULA DÉCIMA CUARTA: RESPONSABILIDAD DE LAS PARTES

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

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

CLÁUSULA DÉCIMA QUINTA: ANTICORRUPCIÓN

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

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

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

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

CLÁUSULA DÉCIMA SEXTA: MARCO LEGAL DEL CONTRATO

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

CLÁUSULA DÉCIMA SÉTIMA: SOLUCIÓN DE CONTROVERSIAS⁵⁸

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.

En virtud de ello, las PARTES convienen en sujetar dicho arbitraje a las siguientes reglas:

- El arbitraje será llevado a cabo por un Tribunal Arbitral compuesto de tres (3) miembros.
- El arbitraje se llevará a cabo de acuerdo al Reglamento del Centro de Arbitraje de la Cámara de Comercio de Lima (en adelante el "Centro").
- El lugar del arbitraje será en la ciudad de Lima, Perú y el idioma que se utilizará en el procedimiento arbitral será el castellano.
- Los gastos y costos correspondientes al arbitraje serán asumidos por la parte que no se vea favorecida con la decisión del Tribunal Arbitral.
- En caso de que alguna de las PARTES decidiera interponer recurso de anulación o cualquier otro tipo de recurso o acción contra el laudo arbitral ante el Poder Judicial, deberá constituir previamente a favor de la PARTE contraria, una Carta Fianza otorgada por un banco de primer orden con sede en Lima, equivalente al importe ordenado en el laudo arbitral, a la orden de "la PARTE contraria", la misma que será solidaria, irrevocable, incondicionada y de realización automática, ejecutable en caso que dicho recurso o acción, en fallo definitivo, no fuera declarado fundado. Dicha Carta Fianza deberá estar vigente durante el tiempo que dure el proceso promovido y será entregada en custodia a un notario de la ciudad de Lima.

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.

CLAUSULA DÉCIMA OCTAVA: PREVENCIÓN DE DELITOS, LAVADO DE ACTIVOS Y FINANCIAMIENTO DEL TERRORISMO

Es condición esencial en este contrato el cumplimiento por parte de EL CONTRATISTA, de las disposiciones previstas en la Ley N° 30424 "*Ley que regula la responsabilidad administrativa de las personas jurídicas en el proceso penal*" y sus modificatorias, del Decreto Legislativo N° 1106, "*Decreto Legislativo de Lucha Eficaz contra el Lavado de Activos y otros Delitos relacionados a la Minería Ilegal y Crimen Organizado*" y sus modificatorias, así como de las normas legales sobre el Sistema de Prevención del Lavado de Activos y Financiamiento del Terrorismo y de la Ley de Prácticas Corruptas en el Extranjero (Foreign Corrupt Practices Act); en adelante, "**las disposiciones en materia de PLAFT, Anticorrupción y Prevención de delitos**".

En ese sentido, EL CONTRATISTA, declara que:

- (i) Sus accionistas, directores, gerentes, funcionarios, representantes (entiéndase como cualquier persona que actúe por cuenta o interés suyo), colaboradores, y/o subcontratistas, cumplen estrictamente con las disposiciones en materia de PLAFT, Anticorrupción y Prevención de Delitos y que, a la fecha, ni este ni ninguna de las personas anteriormente señaladas, han incurrido en acciones y/o cometido actos que pudieran ser constitutivas de los delitos previstos en las disposiciones en materia de PLAFT, Anticorrupción y Prevención de Delitos.

⁵⁸ 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).

(ii) No han sido ni se encuentran condenados y/o investigados por acciones y/o actos que pudieran ser constitutivas de delitos previstos en las disposiciones en materia de PLAFT, Anticorrupción y Prevención de Delitos, a la celebración del presente contrato (o durante la ejecución del mismo).
(iii) Se compromete a remitir toda la información que COFIDE le pueda requerir en virtud a la Debida Diligencia en el conocimiento de EL CONTRATISTA, conforme a lo regulado en las normas legales sobre el Sistema de Prevención del Lavado de Activos y Financiamiento del Terrorismo. COFIDE guardará la confidencialidad y reserva sobre la información antes mencionada conforme a la normativa vigente aplicable.

Si durante la ejecución del contrato (y/o prestación del servicio), EL CONTRATISTA tomara conocimiento por cualquier medio de la ocurrencia de cualquier acción, conducta u otro acto que pueda constituir infracción a lo dispuesto en las disposiciones en materia de PLAFT, Anticorrupción y Prevención de Delitos, deberá informarlo de inmediato a COFIDE dentro del plazo de treinta (30) días calendario de conocida la ocurrencia a través de sus canales de comunicación formales.

Al respecto, EL CONTRATISTA se obliga a cumplir y hacer cumplir durante toda la vigencia del presente contrato (y/o durante la ejecución del servicio) las disposiciones en materia de PLAFT, Anticorrupción y Prevención de Delitos; por lo que se compromete a que ninguno de sus accionistas, directores, gerentes, funcionarios, representantes, colaboradores y/o subcontratistas, incurra en algún tipo de actividad, acción o conducta que pudiera contravenir lo dispuesto en las disposiciones en materia de PLAFT, Anticorrupción y Prevención de Delitos; en consecuencia, EL CONTRATISTA asume expresamente total y absoluta responsabilidad por las acciones, conductas, omisiones y/o cualquier acto cometida por éste y/o sus accionistas, directores, gerentes, funcionarios, representantes, colaboradores, y/o subcontratistas que infrinjan las disposiciones contenidas en las disposiciones en materia de PLAFT, Anticorrupción y Prevención de Delitos. Dicho supuesto de incumplimiento por parte de EL CONTRATISTA, configura una causal de [resolución automática y de pleno derecho] / [renuncia del encargo fiduciario] de conformidad con lo establecido en el numeral del presente contrato.

Finalmente, EL CONTRATISTA se compromete a mantener indemne a COFIDE frente a cualquier daño ocasionado por el incumplimiento de las disposiciones en materia de PLAFT, Anticorrupción y Prevención de Delitos, por parte de EL CONTRATISTA, o de sus accionistas, directores, gerentes, funcionarios, representantes, colaboradores, y/o subcontratistas, y reembolsará cualquier monto que COFIDE se viera obligado a abonar por mandato firme de alguna autoridad administrativa y/o judicial respecto de todo daño o perjuicio directo, multa, penalidad, sanción o costo que se derive del incumplimiento de las disposiciones en materia de PLAFT, Anticorrupción y Prevención de Delitos, así como también en caso la presente declaración resultase falsa y/o inexacta.

CLÁUSULA DÉCIMA NOVENA: FACULTAD DE ELEVAR A ESCRITURA PÚBLICA

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

CLÁUSULA VIGÉSIMA: DOMICILIO PARA EFECTOS DE LA EJECUCIÓN CONTRACTUAL

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

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

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

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

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

“LA ENTIDAD”

“EL CONTRATISTA”

Importante

Este documento puede firmarse digitalmente si ambas partes cuentan con firma digital, según la Ley N° 27269, Ley de Firmas y Certificados Digitales⁵⁹.

⁵⁹ 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° 007-2024-COFIDE

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 ⁶⁰		Sí		No	
Correo electrónico :					

Autorización de notificación por correo electrónico:

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

1. Solicitud de la descripción a detalle de todos los elementos constitutivos de la oferta.
2. Solicitud de reducción de la oferta económica.
3. Solicitud de subsanación de los requisitos para perfeccionar el contrato.
4. Solicitud para presentar los documentos para perfeccionar el contrato, según orden de prelación, de conformidad con lo previsto en el artículo 141 del Reglamento.
5. Respuesta a la solicitud de acceso al expediente de contratación.
6. Notificación de la orden de servicios⁶¹

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.

⁶⁰ 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.

⁶¹ 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° 007-2024-COFIDE

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 ⁶²		Sí	No	
Correo electrónico :				

Datos del consorciado 2				
Nombre, Denominación o Razón Social :				
Domicilio Legal :				
RUC :	Teléfono(s) :			
MYPE ⁶³		Sí	No	
Correo electrónico :				

Datos del consorciado ...				
Nombre, Denominación o Razón Social :				
Domicilio Legal :				
RUC :	Teléfono(s) :			
MYPE ⁶⁴		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.

⁶² 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.

⁶³ Ibídem.

⁶⁴ 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 servicios⁶⁵

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.

⁶⁵ 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° 007-2024-COFIDE
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° 007-2024-COFIDE

Presente.-

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

[CONSIGNAR CIUDAD Y FECHA]

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

Importante

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

ANEXO N° 4

DECLARACIÓN JURADA DE PLAZO DE PRESTACIÓN DEL SERVICIO

Señores

COMITÉ DE SELECCIÓN

CONCURSO PÚBLICO N° 007-2024-COFIDE

Presente.-

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

[CONSIGNAR CIUDAD Y FECHA]

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

ANEXO N° 5

PROMESA DE CONSORCIO

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

Señores
COMITÉ DE SELECCIÓN
CONCURSO PÚBLICO N° 007-2024-COFIDE
Presente.-

Los suscritos declaramos expresamente que hemos convenido en forma irrevocable, durante el lapso que dure el procedimiento de selección, para presentar una oferta conjunta al **CONCURSO PÚBLICO N° [CONSIGNAR NOMENCLATURA DEL PROCEDIMIENTO]**.

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

- a) Integrantes del consorcio
1. [NOMBRE, DENOMINACIÓN O RAZÓN SOCIAL DEL CONSORCIADO 1].
 2. [NOMBRE, DENOMINACIÓN O RAZÓN SOCIAL DEL CONSORCIADO 2].
- b) Designamos a [CONSIGNAR NOMBRES Y APELLIDOS DEL REPRESENTANTE COMÚN], identificado con [CONSIGNAR TIPO DE DOCUMENTO DE IDENTIDAD] N° [CONSIGNAR NÚMERO DE DOCUMENTO DE IDENTIDAD], como representante común del consorcio para efectos de participar en todos los actos referidos al procedimiento de selección, suscripción y ejecución del contrato correspondiente con [CONSIGNAR NOMBRE DE LA ENTIDAD].

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

- c) Fijamos nuestro domicilio legal común en [.....].
- d) Las obligaciones que corresponden a cada uno de los integrantes del consorcio son las siguientes:

1. OBLIGACIONES DE [NOMBRE, DENOMINACIÓN O RAZÓN SOCIAL DEL CONSORCIADO 1] [%]⁶⁶

[DESCRIBIR LAS OBLIGACIONES DEL CONSORCIADO 1]

2. OBLIGACIONES DE [NOMBRE, DENOMINACIÓN O RAZÓN SOCIAL DEL CONSORCIADO 2] [%]⁶⁷

[DESCRIBIR LAS OBLIGACIONES DEL CONSORCIADO 2]

TOTAL OBLIGACIONES 100%⁶⁸

[CONSIGNAR CIUDAD Y FECHA]

⁶⁶ Consignar únicamente el porcentaje total de las obligaciones, el cual debe ser expresado en número entero, sin decimales.
⁶⁷ Consignar únicamente el porcentaje total de las obligaciones, el cual debe ser expresado en número entero, sin decimales.
⁶⁸ Este porcentaje corresponde a la sumatoria de los porcentajes de las obligaciones de cada uno de los integrantes del consorcio.

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

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

Importante

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

ANEXO N° 6

PRECIO DE LA OFERTA

Señores
COMITÉ DE SELECCIÓN
CONCURSO PÚBLICO N° 007-2024-COFIDE
Presente.-

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

CONCEPTO	PRECIO TOTAL
TOTAL	

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

[CONSIGNAR CIUDAD Y FECHA]

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

Importante

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

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

ANEXO N° 8

EXPERIENCIA DEL POSTOR EN LA ESPECIALIDAD

Señores
COMITÉ DE SELECCIÓN
CONCURSO PÚBLICO N° 007-2024-COFIDE
Presente.-

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

Nº	CLIENTE	OBJETO DEL CONTRATO	Nº CONTRATO / O/S / COMPROBANTE DE PAGO	FECHA DEL CONTRATO O CP ⁶⁹	FECHA DE LA CONFORMIDAD DE SER EL CASO ⁷⁰	EXPERIENCIA PROVENIENTE ⁷¹ DE:	MONEDA	IMPORTE ⁷²	TIPO DE CAMBIO VENTA ⁷³	MONTO FACTURADO ACUMULADO ⁷⁴
1										
2										
3										
4										

⁶⁹ 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.

⁷⁰ 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.

⁷¹ 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”*.

⁷² Se refiere al monto del contrato ejecutado incluido adicionales y reducciones, de ser el caso.

⁷³ 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.

⁷⁴ Consignar en la moneda establecida en las bases.

Nº	CLIENTE	OBJETO DEL CONTRATO	N° CONTRATO / O/S / COMPROBANTE DE PAGO	FECHA DEL CONTRATO O CP ⁶⁹	FECHA DE LA CONFORMIDAD DE SER EL CASO ⁷⁰	EXPERIENCIA PROVENIENTE ⁷¹ DE:	MONEDA	IMPORTE ⁷²	TIPO DE CAMBIO VENTA ⁷³	MONTO FACTURADO ACUMULADO ⁷⁴
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° 007-2024-COFIDE
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° 007-2024-COFIDE
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.

ANEXO COFIDE 1

Señores

COMITÉ DE SELECCIÓN

CONCURSO PÚBLICO N° 007-2024-COFIDE

Presente.-

Yo, _____ identificado con DNI N° _____ en mi calidad de representante legal de la empresa _____, con RUC N° _____, y domicilio legal en _____ con _____ años de experiencia en el rubro _____, declaro, bajo juramento, lo siguiente:

1. Declaramos bajo juramento que conocemos que COFIDE es una empresa pública sujeta al cumplimiento del Reglamento de Gestión de Riesgos de LAFT, por lo que, en mi calidad de personal natural, y/o representante legal de la empresa, no cuento con antecedentes penales, ni me encuentro incluido en la lista emitida por la Oficina de Control de Activos Extranjeros del Departamento de Tesoro de los EEUU (OFAC), igualmente la empresa que represento a través del presente documento.
2. Declaramos bajo juramento los siguientes datos:

Nombres y Apellidos Representantes Empresa		Documento de Identidad		PEP (*) Sí/No
Nombres y Apellidos del Beneficiario Final del Proveedor		DNI		
Nombres y Apellidos del Representante Legal en el Perú		DNI		
Nombres y Apellidos de Accionistas, Socios o Asociados con más de 25% de capital social, aporte o participación sea directa o indirectamente.		DNI		
	Añadir las filas que se necesiten			

(*) Precisar sí o no, en caso sea Persona Expuesta Políticamente según Res. SBS N° 4349-2016.

3. Asimismo, en caso aplique, nos comprometemos a actualizar la información declarada cada dos años.

[CONSIGNAR CIUDAD Y FECHA]

Representante Legal de la Empresa o
Nombres y apellidos completos en caso de personal natural
(firma y sello)

ANEXO COFIDE 2

Señores
COMITÉ DE SELECCIÓN
CONCURSO PÚBLICO N° 007-2024-COFIDE
Presente.-

**DECLARACIÓN JURADA DE NO CONTAR CON INVESTIGACIONES EN CURSO,
ANTECEDENTES JUDICIALES, POLICIALES Y/O PENALES**

Yo, _____, identificado/a con Documento de Identidad (DNI/C.E./Pasaporte) N° _____,
con cargo _____, de la empresa _____ y con domicilio en _____, distrito de
_____, provincia _____ y departamento de _____, declaro de manera
voluntaria y bajo juramento que:

DECLARO BAJO JURAMENTO: (marcar con un aspa):

	SI	NO
Tener alguna investigación de cualquier naturaleza (delito y/o infracción) en curso a la fecha de la firma de la presente declaración.	<input type="checkbox"/>	<input type="checkbox"/>
Tener antecedentes judiciales.	<input type="checkbox"/>	<input type="checkbox"/>
Tener procesos judiciales abiertos y/o investigaciones judiciales a la fecha de la firma de la presente declaración.	<input type="checkbox"/>	<input type="checkbox"/>
Tener antecedentes Policiales.	<input type="checkbox"/>	<input type="checkbox"/>
Tener procesos Policiales abiertos y/o investigaciones policiales a la fecha de la firma de la presente declaración.	<input type="checkbox"/>	<input type="checkbox"/>
Tener antecedentes Penales.	<input type="checkbox"/>	<input type="checkbox"/>
Tener procesos Penales abiertos y/o investigaciones penales a la fecha de la firma de la presente declaración.	<input type="checkbox"/>	<input type="checkbox"/>

En caso de haber marcado Sí en los recuadros antes indicados, **completar el ADJUNTO AL ANEXO COFIDE 2.**

En relación a la información antes señalada, declaro que todo lo consignado en el presente documento es cierto, sometiéndome, de no ser así, a las acciones administrativas y de ley que correspondan.

Nombres y Apellidos completos:
Documento de Identidad / N°:
Cargo dentro de la empresa:
Fecha:
Firma (tal como figura en su Documento de Identidad):

ADJUNTO AL ANEXO COFIDE 2

INVESTIGACIONES, ANTECEDENTES JUDICIALES, POLICIALES y/o PENALES

A continuación, declarar las investigaciones de cualquier naturaleza (delito y/o infracción) vigentes, los antecedentes o procesos abiertos o investigación de carácter judicial, policial y/o penal en los que se encuentra como demandado/denunciado, colocando, **como mínimo**, los siguientes datos: delito materia de la demanda/denuncia, número de caso/expediente, fecha de inicio del proceso, dependencia y sede ante las cuales se sigue el proceso y, estado actual del proceso respectivo.

Yo, _____, identificado con (DNI/C.E./Pasaporte) N° _____, declaro bajo juramento contar con los siguientes antecedentes y/o investigaciones de carácter judicial, policial, penal y/o mantener los siguientes procesos abiertos:

[illegible]

En relación a la información antes señalada, declaro que todo lo consignado en el presente documento es cierto, sometiéndome, de no ser así, a las acciones administrativas y de ley que correspondan.

Nombres y Apellidos completos:

Documento de Identidad / N°:

Cargo dentro de la empresa:

Fecha:

Firma (tal como figura en su Documento de Identidad):

CODIGO DE ÉTICA Y CONDUCTA DE PROVEEDORES DE COFIDE



LINEAMIENTO ÉTICO Y DE CONDUCTA PARA PROVEEDORES DE COFIDE

1. Objetivo.-

El presente lineamiento tiene como objetivo que los proveedores que intervienen activamente en la cadena de suministro de COFIDE, tomen conocimiento de los estándares mínimos de comportamiento en materia de conducta ética, social y ambiental que esperamos que los proveedores cumplan cuando nos suministran bienes y servicios, asimismo tomen conocimiento del Código de Ética y Conducta de Cofide, que se encuentra publicado en la página web de Cofide, sus principios rectores y la adopción de pautas de conducta consistentes con la misma.

Para Cofide la relación con sus proveedores es fundamental para lograr sus objetivos, por lo tanto, es importante construir relaciones basadas en el respeto, la equidad y transparencia mutua; en ese sentido estos lineamientos, marcados por un ideal de cooperación, están orientados a un beneficio recíproco respetando las actividades y obligaciones de cada uno.

2. Ámbito de aplicación.-

Los lineamientos de ética y conducta son de aplicación a todas las personas naturales y a todos los accionistas, administradores, apoderados y representantes legales de personas jurídicas que representan a la empresa en el ejercicio de su cargo, y que mantengan una relación contractual de prestación de bienes y/o servicios con Cofide.

Asimismo, lo dispuesto en los presentes lineamientos se aplican en todos los casos, sin perjuicio de las condiciones y exigencias adicionales que puedan establecerse en la legislación aplicable, en las prácticas y normas de las diferentes leyes donde Cofide desarrolla sus actividades y contratos con cada proveedor.

El presente lineamiento debe leerse de forma conjunta con las condiciones contractuales pactadas entre COFIDE y el proveedor (términos de referencia, propuesta, cotización, contrato, orden de compra o servicio, entre otros documentos de la relación contractual).

3. Compromisos de los proveedores.-

Las pautas éticas que deben regir la actuación de los proveedores de Cofide a través del Código de Ética y Conducta de Cofide y el presente lineamiento, deberá ser aceptados por ellos al iniciar la relación contractual. Los compromisos éticos que deben cumplir los proveedores, accionistas, representantes o apoderados, y su personal, son los siguientes:

- 3.1 Desarrollar relaciones comerciales atendiendo a principios de ética empresarial y gestión transparente.
- 3.2 La protección del medio ambiente, y las buenas prácticas de Ecoeficiencia son prioritarias para COFIDE, los proveedores se comprometen a no realizar actuaciones que contravenga a la legislación aplicable, asimismo, se compromete a fomentar el respeto y protección del medio ambiente.
- 3.3 Promover la igualdad de oportunidades entre géneros y evitar la discriminación, salarial o de otro tipo, por razón de origen, raza, sexo, idioma, religión, opinión, condición económica o de cualquiera otra índole entre sus empleados/as.
- 3.4 Garantizar que la contratación de sus empleados se realiza respetando la legislación laboral y migratoria vigente, y demás disposiciones legales y reglamentarias de carácter laboral.
- 3.5 Promover a la interna el rechazo el trabajo forzoso u obligatorio y el trabajo infantil.
- 3.6 Respetar las normas de Protección al Consumidor y normas de la competencia, impulsando prácticas antimonopólicas y de lealtad comercial, asimismo se comprometen a no realizar publicidad engañosa sobre la actividad de sus negocios o terceros.



Firmado digitalmente por LOZANO
MEZA Yanira Margarita FAU
20100116392 soft
Motivo: Doy V° B°
Fecha: 26.09.2023 13:55:35 -05:00



- 3.7 Cumplir con la normativa de Seguridad y Salud ocupacional en sus instalaciones con su personal, y al prestar un servicio a Cofide, proporcionando a sus trabajadores un entorno seguro y libre de riesgos contra la salud y promoviendo la prevención de accidentes entre todo su personal.
 - 3.8 No ofrecer, prometer o realizar directa e indirectamente presentes, invitaciones, regalos, patrocinios o atenciones que, puedan llevar a establecer vínculos o compromisos que empañen la transparencia de las contrataciones, salvo objetos de propaganda de escaso valor (ej. merchandising). Como referencia, el monto deberá ser igual o menor a US\$ 10 (diez dólares EEUU) o su equivalente en la moneda local, al tipo de cambio vigente.
 - 3.9 Mantener un sistema adecuado de registros contables de todas las operaciones, gastos e ingresos que se realizan, sin omitir, ocultar, o alterar algún dato de la información, de manera que los registros contables reflejen fielmente la realidad.
 - 3.10 Cumplir con las políticas de Cofide relativas a la prevención de delitos, lavado de activos, financiamiento del terrorismo, soborno y extorsión, así como con las normas de conducta ética y moral, respetando las leyes aplicables sobre esta materia. El proveedor deberá cumplir a cabalidad con la cláusula de Prevención de Lavado de Activos y Financiamiento del Terrorismo (LA/FT) y Anti Corrupción de los contratos y ordenes de servicio/compra que emite Cofide.
 - 3.11 Actuar de manera honesta e íntegra, Cofide no tolerará la divulgación de información confidencial, la falsificación de documentos durante el proceso de selección y la ejecución del contrato. El proveedor deberá cumplir a cabalidad con la cláusula de Confidencialidad con que cuentan todos los contratos y ordenes de servicio/compra que emite Cofide.
 - 3.12 No prometer, ofrecer ni abonar de manera corrupta y/o soborno, directa ni indirectamente, dinero y otros bienes de valor, para: (i) influir sobre un acto o decisión de un profesional de COFIDE; (ii) obtener una ventaja indebida de COFIDE; o (iii) inducir a un profesional de COFIDE a ejercer influencia sobre un acto o decisión que pueda tener.
 - 3.13 Reportar de manera inmediata cuando noten cualquier incumplimiento comprobado o potencia a los presentes lineamientos y código de ética y conducta de Cofide.
 - 3.14 Declarar algún conflicto de interés que se presente antes de la contratación, como por ejemplo que un accionista o apoderado de la empresa sea familiar o familiar político de un colaborador de Cofide.
 - 3.15 Salvo COFIDE lo autorice expresamente en la relación contractual, no está permitido la utilización de subcontratistas por parte del proveedor, para aquellos casos que se prevea esta posibilidad, los proveedores deben garantizar que se cumplan los estándares del presente lineamiento ético.
4. Compromisos de Cofide hacia los proveedores.-
- De acuerdo al Código de Ética y Conducta de Cofide nos comprometemos a:
- 4.1. Seleccionar a proveedores con procesos competitivos e imparciales, que consideren criterios técnicos, económicos y éticos, evitando cualquier conflicto de interés, fraude o favoritismo en su selección, acorde con la normativa nacional vigente.
 - 4.2. Apoyar el desarrollo sostenible de los proveedores, la promoción del trabajo digno y el cumplimiento de las normas de carácter laboral, ambiental, sanitario y de seguridad.
 - 4.3. Respetar los contratos con los proveedores y emplear mecanismos aplicables para resolver controversias o situaciones de conflicto de interés, con base a la normativa aplicable, tanto interna como externa.
 - 4.4. Proteger toda información confidencial recibida de proveedores en términos de la relación contractual, no se revelará a terceros salvo consentimiento de los interesados, por obligación legal, o cumplimiento de resoluciones judiciales o administrativas.
 - 4.5. Proteger los datos de carácter personal que se capturen, almacenen o recopilen de proveedores.



5. Vulneración e incumplimientos del presente lineamiento.-

El incumplimiento por parte del proveedor de lo contenido en el presente lineamiento y el Código de Ética y Conducta de Cofide tendrá consecuencias en la relación contractual con COFIDE, tomando en cuenta la gravedad del incumplimiento, pudiendo llegar hasta la resolución del contrato con Cofide, sin perjuicio de otras acciones legales o administrativas que fueran de aplicación.

6. Sistema de gestión de prácticas cuestionables – Canal Ético.-

Cofide pone a disposición el canal ético, que es administrada por un tercero independiente y accesible a través de la página web de COFIDE. A través de este canal, se pueden reportar y/o informar posibles incumplimientos y/o posibles conductas irregulares o inusuales que puedan estar vinculados a conflicto de intereses, corrupción, lavado de activos u otros que implique perjuicio económico o reputacional para COFIDE. El denunciante puede mantener su anonimato; sin embargo, en caso desee brindar sus datos, estos serán guardados de manera estrictamente confidencial.

7. Consultas sobre el presente lineamiento ético.-

Las consultas relativas a la interpretación o aplicación de este lineamiento podrán hacerse llegar a través del correo mesadepartes@cofide.com.pe

Aprobado por: Gerencia de Gestión Humana y Administración

Fecha: 26/09/2023

Versión 3.0



Firmado digitalmente por FLORES
RODAS Violeta Karina FAU
20100116392 soft
Motivo: Soy el autor del documento
Fecha: 27.09.2023 16:37:17 -05:00

Pliego de Absolución de consultas y observaciones											
Nomenclatura del procedimiento de selección						CP N° 007-2024-COFIDE					
Objeto de la contratación						Servicio de Gestión y Operación de la Ciberseguridad					
Nro. Orden	RUC/Código	Nombre o Razón Social	Tipo Formulación	Sección	Numeral	Literal	Página	Consulta u Observación	Artículo y norma que se vulnera (en el caso de observaciones)	Análisis respecto de la consulta u observación	Precisión de aquello que se incorporará en las Bases a integrarse, de corresponder
1	20477770623	DIGIWARE DEL PERU S.A.C. - DIGIWARE S.A.C.	Consulta	General	6.3.6	N/A	38	Referente a el detalle de los activos Active Directory (AD) 3 (HA - Activo/Activo) MICROSOFT. Consulta: ¿La totalidad de AD a integrar es 6, teniendo en cuenta la arquitectura HA?		Conforme a lo señalado por el área usuaria, se aclara que son 03 Active Directory (AD) en replica.	
2	20477770623	DIGIWARE DEL PERU S.A.C. - DIGIWARE S.A.C.	Consulta	General	6.1	N/A	28	Dice: "b.El postor puede aplicar la metodología que considere conveniente basado en cumplir con el objetivo del servicio y los SLAs." Consulta: Sírvase a confirmar los SLA's para la consultoría, teniendo en cuenta que el numeral" 6.8.1 Horario de Atención" para S1 es de lunes a viernes de 9:00 am a 6:00pm.		Conforme a lo señalado por el área usuaria, se aclara que los SLAs del Servicio 1, solo serán medidos en la etapa de remediación de acuerdos a los SLAs de la gestion de requerimientos.	
3	20477770623	DIGIWARE DEL PERU S.A.C. - DIGIWARE S.A.C.	Consulta	General	6.3.6	N/A	38	Referente al detalle de los activos Firewall Interno (FortiAnalyzer) 1 (HA - Activo/pasivo) FORTINET - FORTIGATE 600F. Consulta: ¿La totalidad de firewalls a integrar son 2, teniendo en cuenta la arquitectura HA?		Conforme a lo señalado por el área usuaria, se confirma que son 02 firewall en HA (activo/pasivo).	
4	20477770623	DIGIWARE DEL PERU S.A.C. - DIGIWARE S.A.C.	Consulta	General	6.6.3	N/A	46	Dice: "El servicio permitirá enviar solicitudes de takedown al proveedor del servicio y este deberá preparar la documentación para la solicitud de eliminación a la autoridad local/regional pertinente (CERT, registrador, etc.)" Consulta: ¿Cuántos takedown espera al año durante el periodo del servicio?		Conforme a lo señalado por el área usuaria y, con ocasión a la integración de las bases, se precisa que se considerará un máximo de 180 solicitudes de TAKEDOWN por todo el periodo del servicio.	Se modifica literal i) del punto 6.6.3. de los términos de referencia del capítulo III de la Sección Especifica de las Bases, según el siguiente detalle: DICE: El servicio permitirá enviar solicitudes de takedown al proveedor del servicio ... DEBE DECIR: El servicio permitirá enviar solicitudes de takedown al proveedor del servicio (180 solitudes como maximo para todo el periodo del servicio) ...
5	20477770623	DIGIWARE DEL PERU S.A.C. - DIGIWARE S.A.C.	Consulta	General	6.6.3	N/A	46	Dice: "El servicio permitirá enviar solicitudes de takedown al proveedor del servicio y este deberá preparar la documentación para la solicitud de eliminación a la autoridad local/regional pertinente (CERT, registrador, etc.)". Consulta: De no tener un número aproximado de takedowns por año, ¿es posible aceptar 15 por año?		Conforme a lo señalado por el área usuaria y, con ocasión a la integración de las bases, se precisa que se considerará un máximo de 180 solicitudes de TAKEDOWN por todo el periodo del servicio.	Se modifica literal i) del punto 6.6.3. de los términos de referencia del capítulo III de la Sección Especifica de las Bases, según el siguiente detalle: DICE: El servicio permitirá enviar solicitudes de takedown al proveedor del servicio ... DEBE DECIR: El servicio permitirá enviar solicitudes de takedown al proveedor del servicio (180 solitudes como maximo para todo el periodo del servicio) ...
6	20477770623	DIGIWARE DEL PERU S.A.C. - DIGIWARE S.A.C.	Consulta	General	6.2.5	N/A	33	Referente a el detalle de los activos Firewall Perimetral ¿ Data Center Principal (FortiAnalyzer) 1 (HA - Activo/pasivo) FORTINET FORTIGATE 400E. Consulta: ¿La totalidad de firewalls a integrar son 2, teniendo en cuenta la arquitectura HA?		Conforme a lo señalado por el área usuaria, se confirma que son 02 firewall en HA (activo/pasivo)	
7	20477770623	DIGIWARE DEL PERU S.A.C. - DIGIWARE S.A.C.	Consulta	General	6.2	N/A	32	Dice: "Servicio dimensionado para establecer y ejecutar un marco de trabajo para que se realice la configuración o se coordine con COFIDE u otros Contratistas de COFIDE participantes para que se configuren los firewalls, IPS, NAC, entre otros equipos de seguridad y soluciones de seguridad." Consulta: Por favor, confirmar que" ejecutar un marco de trabajo para que se realice la configuración o se coordine " hace referencia al acompañamiento y no la gestión de activos.		Que, conforme a lo señalado por el área usuaria, se aclara que el servicio 2 es de gestión de equipos, siendo que ejecutar un marco de trabajo para que se realice la configuración o se coordine, se encuentra referido a los procedimientos de atención de los equipos o activos indicados en este servicio.	

8	20477770623	DIGIWARE DEL PERU S.A.C. - DIGIWARE S.A.C.	Consulta	General	6.2	N/A	32	<p>Dice: "Servicio dimensionado para establecer y ejecutar un marco de trabajo para que se realice la configuración o se coordine, con COFIDE u otros Contratistas de COFIDE participantes para que se configuren, los firewalls, IPS, NAC, entre otros equipos de seguridad y soluciones de seguridad."</p> <p>Consulta: De confirmar la gestión de los activos, se pide validar que el alcance es el de la línea "6.2.5 Línea Base S2" para la gestión de estos activos.</p>		Conforme a lo señalado por el área usuaria, se confirma la gestión de los activos y se valida que el alcance se encuentra indicado en el punto 6.2.5. Línea Base S2 de los términos de referencia.	
9	20477770623	DIGIWARE DEL PERU S.A.C. - DIGIWARE S.A.C.	Consulta	General	6.2	N/A	32	<p>Dice: "Servicio dimensionado para establecer y ejecutar un marco de trabajo para que se realice la configuración o se coordine, con COFIDE u otros Contratistas de COFIDE participantes para que se configuren, los firewalls, IPS, NAC, entre otros equipos de seguridad y soluciones de seguridad."</p> <p>Consulta: De confirmar la gestión de los activos, por favor, indicar cuántos casos de incidentes por año tuvieron en la 6.2.5 Línea Base S2 (FW, NDR, NAC, WAF, Antispam, IPS, EDR).</p>		Conforme a lo señalado por el área usuaria, se precisa que la cantidad de incidentes por año que se tuvieron en la 6.2.5 Línea Base S2 (FW, NDR, NAC, WAF, Antispam, IPS, EDR) es de un promedio de 20 incidentes reportados y atendidos por el servicio al año.	
10	20477770623	DIGIWARE DEL PERU S.A.C. - DIGIWARE S.A.C.	Consulta	General	6.2	N/A	32	<p>Dice: "Servicio dimensionado para establecer y ejecutar un marco de trabajo para que se realice la configuración o se coordine, con COFIDE u otros Contratistas de COFIDE participantes para que se configuren, los firewalls, IPS, NAC, entre otros equipos de seguridad y soluciones de seguridad."</p> <p>Consulta: Confirmar que cualquier incremento de gestión de activos que salga de la "6.2.5 Línea Base S2 " no forma parte del alcance inicial y debe ser cotizado a demanda como uno nuevo.</p>		Conforme a lo señalado por el área usuaria, se precisa que cualquier incremento del alcance inicial será considerado como un servicio adicional o complementario y contratado según normativa de contrataciones del Estado.	
11	20477770623	DIGIWARE DEL PERU S.A.C. - DIGIWARE S.A.C.	Consulta	General	6.2.7	N/A	34	<p>Dice: "c. Estaciones de trabajo para los recursos humanos proporcionado por el Contratista."</p> <p>Consulta: Confirmar que los equipos de trabajo para los recursos humanos del contratista ganador, serán ofertados COFIDE, caso contrario, confirmar que el contratista debe proveerlos.</p>		Conforme a lo señalado por el área usuaria, se confirma que los equipos de trabajo para los recursos humanos del contratista, deberán ser provistos por este.	
12	20477770623	DIGIWARE DEL PERU S.A.C. - DIGIWARE S.A.C.	Consulta	General	6.3	N/A	34	<p>Dice: "l.Considerar soluciones líderes en el mercado americano y/o europeo. Adjuntar informes que acrediten el liderazgo de, al menos, dos años consecutivos de los últimos cuatro años, la cual debe ser presentada a la firma de contrato".</p> <p>Consulta: Confirmar que el inciso es obligatorio u opcional, de ser obligatorio se recomienda a COFIDE que además de ser solución líder, este deberá estar certificada por lo menos en SOC 2 tipo II, ISO 27001, 27017, 27018 y GDPR para asegurar que los controles de seguridad mantendrán la información almacenada de forma segura y manteniendo la privacidad.</p>		Conforme a lo señalado por el área usuaria, se aclara que el requerimiento es mínimo y obligatorio, si la solución cumple con mayores certificaciones para asegurar los controles de seguridad, estos serán aceptados.	

13	20477770623	DIGIWARE DEL PERU S.A.C. - DIGIWARE S.A.C.	Consulta	General	6.3	N/A	34	<p>Dice: "t.Considerar soluciones líderes en el mercado americano y/o europeo. Adjuntar informes que acrediten el liderazgo de, al menos, dos años consecutivos de los últimos cuatro años, la cual debe ser presentada a la firma de contrato".</p> <p>Consulta: Confirmar que el inciso es obligatorio u opcional, de ser obligatorio se recomienda a COFIDE que además de ser solución líder, este deberá estar certificada por lo menos en SOC 2 tipo II, ISO 27001, 27017, 27018 y GDPR para asegurar que los controles de seguridad mantendrán la información almacenada de forma segura y manteniendo la privacidad.</p>		Conforme a lo señalado por el área usuaria, se aclara que el requerimiento es mínimo y obligatorio, si la solución cumple con mayores certificaciones para asegurar los controles de seguridad, estos serán aceptados.	
14	20477770623	DIGIWARE DEL PERU S.A.C. - DIGIWARE S.A.C.	Consulta	General	6.3	N/A	34	<p>Dice: "Este servicio se cotiza por la cantidad de activos involucrados en el servicio (nodos y/o dispositivos) y/o la estimación de la cantidad de Eventos por Segundo (EPS) que los activos involucrados en el servicio pueden generar, así como los casos de uso configurados, la cantidad de servidores y las licencias de soluciones SIEM (Security Information and Event Management). A continuación, presentamos la cantidad de activos y la cantidad de EPS".</p> <p>Consulta: Confirmar que capacidades tecnológicas de SOC espera como parte del alcance: SIEM, SOAR, UEBA.</p>		Conforme a lo señalado por el área usuaria, se aclara que el alcance del SERVICIO DE DETECCIÓN AVANZADA (S3), solo hace referencia a soluciones SIEM, siendo que si el proveedor desea adicionar mas soluciones para cumplir con el alcance del servicio, estas serán consideradas como válidas.	
15	20477770623	DIGIWARE DEL PERU S.A.C. - DIGIWARE S.A.C.	Consulta	General	6.3	N/A	34	<p>Dice: "Este servicio se cotiza por la cantidad de activos involucrados en el servicio (nodos y/o dispositivos) y/o la estimación de la cantidad de Eventos por Segundo (EPS) que los activos involucrados en el servicio pueden generar, así como los casos de uso configurados, la cantidad de servidores y las licencias de soluciones SIEM (Security Information and Event Management). A continuación, presentamos la cantidad de activos y la cantidad de EPS"</p> <p>Consulta: De confirmar qué capacidades tecnológicas de SOC incluyen SOAR, por favor, indicar si se espera una integración de playbook para Detección avanzada de amenazas y de respuesta automatizada (XDR) - Kaspersky, Firewall Interno (Fortigate 600F), NAC (Appliance Virtual), Active Directory (AD), Database Firewall (Appliance Virtual) Imperva, WAF (SaaS) Fortinet, Solución de detección y respuesta de red (NDR) Fortinet 1000F o Línea base del servicio S3.</p>		Conforme a lo señalado por el área usuaria, se precisa que no se está confirmando la inclusión de soluciones SOAR en el servicio, solo se hace referencia a soluciones SIEM, si el proveedor desea adicionar mas soluciones para cumplir con el alcance del servicio, estas serán consideradas como válidas.	
16	20477770623	DIGIWARE DEL PERU S.A.C. - DIGIWARE S.A.C.	Consulta	General	6.3	N/A	34	<p>Dice: "Este servicio se cotiza por la cantidad de activos involucrados en el servicio (nodos y/o dispositivos) y/o la estimación de la cantidad de Eventos por Segundo (EPS) que los activos involucrados en el servicio pueden generar, así como los casos de uso configurados, la cantidad de servidores y las licencias de soluciones SIEM (Security Information and Event Management). A continuación, presentamos la cantidad de activos y la cantidad de EPS"</p> <p>Consulta: De confirmar qué capacidades tecnológicas de SOC incluyen SOAR, por favor, indicar qué tipo de playbooks deben implementarse (ejemplo notificación o contención automática).</p>		Conforme a lo señalado por el área usuaria, se precisa que no se confirma la inclusión de soluciones SOAR en el servicio; sin perjuicio de ello, si el proveedor desea adicionar más soluciones para la ejecución del servicio, estas serán consideradas como válidas.	

17	20477770623	DIGIWARE DEL PERU S.A.C. - DIGIWARE S.A.C.	Consulta	General	6.3	N/A	34	<p>Dice: "Es importante tener en cuenta que para los componentes de las infraestructuras utilizadas para la prestación de este servicio y que son administrados por El Contratista, se debe considerar una actualización de estos durante el período del servicio."</p> <p>Consulta: Por favor, confirmar que se acepta como alcance 01 o 02 mantenimientos por año para la actualización de los componentes de infraestructura.</p>		<p>Conforme a lo señalado por el área usuaria, se aclara que el alcance del servicio indica que "se debe considerar una actualización" como mínimo durante el periodo del servicio; sin embargo, si el servicio requiere realizar más actualizaciones como parte del alcance, estas se deberán ejecutar para mitigar las vulnerabilidades con estas actualizaciones.</p>	
18	20477770623	DIGIWARE DEL PERU S.A.C. - DIGIWARE S.A.C.	Consulta	General	6.3	N/A	34	<p>Dice: "La solución SIEM debe admitir información para enriquecimiento de contexto de soluciones de análisis de vulnerabilidades del mercado, tales como: Nessus y/o Qualys y/o Tenable y/o Rapid7. Esta capacidad debe estar habilitada."</p> <p>Consulta: Confirmar que este punto hace referencia a tener la capacidad, mas no forma parte de la implementación.</p>		<p>Conforme a lo señalado por el área usuaria, se confirma que este punto hace referencia a tener la capacidad, mas no forma parte de la implementación.</p>	
19	20477770623	DIGIWARE DEL PERU S.A.C. - DIGIWARE S.A.C.	Consulta	General	6.3	N/A	34	<p>Dice: "k.Contar con inteligencia de correlación par tener un mejor análisis de eventos de seguridad contrastando bitácoras de dos o más dispositivos en ambientes seguros."</p> <p>Consulta: Confirmar que este punto hace referencia a Inteligencia artificial y que la entidad debe tomar en cuenta plataformas que se basen en modelos avanzados de inteligencia artificial, aprendizaje automático y ciencia de datos. Sus funciones principales deben abarcar la capacidad de recopilar datos de fuentes locales y en la nube, analizarlos de manera eficiente y almacenarlos de forma segura.</p>		<p>Conforme a lo señalado por el área usuaria, se aclara que este punto hace referencia a Inteligencia de correlación del SIEM para el análisis de eventos de seguridad contrastando bitácoras de dos o más dispositivos en ambientes seguros, si el proveedor desea adicionar más soluciones tecnológicas para cumplir con el alcance del servicio, estas serán consideradas como válidas.</p>	
20	20477770623	DIGIWARE DEL PERU S.A.C. - DIGIWARE S.A.C.	Consulta	General	6.3	N/A	34	<p>Dice: "n.Analizar de manera oportuna las anomalías de tráfico observando patrones en bitácoras o flujos de datos."</p> <p>Consulta: Confirmar que este punto hace referencia UEBA y que las capacidades de análisis de comportamiento de usuarios y entidades (UEBA) deben generar automáticamente líneas de tiempo inteligentes para comportamiento normal y anormal, utilizando aprendizaje automático. Esto permitirá aplicar calificaciones de riesgo, manteniendo un historial que servirá de base para las investigaciones.</p>		<p>Conforme a lo señalado por el área usuaria, se aclara que el punto de referencia indica "Analizar de manera oportuna las anomalías de tráfico observando patrones en bitácoras o flujos de datos", no se menciona analizar comportamiento de usuarios que es lo que realiza UEBA; por lo que, no se acepta lo solicitado.</p>	
21	20477770623	DIGIWARE DEL PERU S.A.C. - DIGIWARE S.A.C.	Consulta	General	6.3	N/A	34	<p>Dice: "El servicio debe ser prestado en la modalidad 24x7 de manera continua. La información obtenida y procesada por este servicio, debe estar almacenada en los data center redundantes en territorio nacional y/o extranjero del contratista".</p> <p>Consulta: Confirmar que la redundancia solo es para la infraestructura donde se aloja le tecnología del SOC y no del colector. De requerir redundancia del colector, por favor, indicar si/no y el número de data center.</p>		<p>Conforme a lo señalado por el área usuaria, se confirma que la redundancia solo es para la infraestructura donde se aloja le tecnología del SOC y no del colector.</p>	

22	20477770623	DIGIWARE DEL PERU S.A.C. - DIGIWARE S.A.C.	Consulta	General	6.3	N/A	34	<p>Dice: "p.Tener plantillas de búsqueda de caza de amenazas predefinidas."</p> <p>Consulta: Confirmar que este punto hace referencia a tecnología de threat hunting. Además, debe permitir consultas simples mediante operadores lógicos, condicionales, comodines, rangos y términos negativos sin necesidad de utilizar lenguaje complejo, incluyendo operadores de WildCards y Expresiones Regulares. Se recomienda a COFIDE que la plataforma deberá permitir la construcción de búsquedas complejas mediante el uso de lenguaje natural en castellano. Por ejemplo: ¿Muestra el top 10 de usuarios que más veces se autenticaron en el último día en Windows.</p>		Conforme a lo señalado por el área usuaria, se confirma que este punto hace referencia a tecnología de threat hunting; siendo que las demás funcionalidades indicadas serán aceptadas como opcionales.	
23	20477770623	DIGIWARE DEL PERU S.A.C. - DIGIWARE S.A.C.	Consulta	General	6.3	N/A	34	<p>Dice: "COFIDE proporcionara recursos virtuales en su data center sólo de recolección (colector) de forma transitoria y reenvío de información hacia el SIEM del POSTOR en su data center o en nube. El postor deberá incluir la arquitectura en detalle de la solución a proponer en la que se señale todos los componentes que la conforman, explicando la función de cada uno de los mismos."</p> <p>Consulta: Confirmar que COFIDE cuenta con los siguientes requisitos para VM, donde se alojará el recolector (4 Core CPU Recommended clock speed: 2.8 GHZ or higher, 16 GB ram, 500 gb SSD), de requerir capacidades de SOAR se <u>necesita una segunda VM de similar capacidad.</u></p>		Conforme a lo señalado por el área usuaria, se confirma que COFIDE cuenta con los siguientes requisitos para VM, donde se alojará el recolector (4 Core CPU Recommended clock speed: 2.8 GHZ or higher, 16 GB ram, 500 gb SSD), se aclara que no se esta solicitando capacidades de SOAR.	
24	20477770623	DIGIWARE DEL PERU S.A.C. - DIGIWARE S.A.C.	Consulta	General	6.5	N/A	43	<p>Dice: "Asesorar a COFIDE en la remediación de vulnerabilidades identificadas".</p> <p>Consulta: Confirmar que los hallazgos tienen como producto la recomendación y/o asesoramiento sobre los encontrado y no involucra la aplicación y/o remediación.</p>		Conforme a lo señalado por el área usuaria, se confirma que los hallazgos tienen como producto la recomendación y/o asesoramiento sobre las vulnerabilidades reportadas y no involucra la aplicación y/o remediación.	
25	20477770623	DIGIWARE DEL PERU S.A.C. - DIGIWARE S.A.C.	Consulta	General	6.6	N/A	46	<p>Dice: "e.El Contratista podrá representar a COFIDE, previa autorización de ésta, en el proceso de dar de baja a la amenaza identificada."</p> <p>Consulta: Confirmar que COFIDE entregará una carta y/o similar de autorización para que el contratista pueda hacer uso de la representación y gestionar los takedowns.</p>		Conforme a lo señalado por el área usuaria, se confirma que COFIDE podrá entregar una carta y/o similar de autorización para que el contratista pueda hacer uso de la representación y gestionar los takedowns si este lo requiere para cubrir este alcance.	
26	20477770623	DIGIWARE DEL PERU S.A.C. - DIGIWARE S.A.C.	Consulta	General	6.7	N/A	48	<p>Dice: "Debe permitir acceder a la consola de monitoreo, en modo de sólo lectura, para hasta tres (03) personas de COFIDE."</p> <p>Consulta: Confirmar que COFIDE espera tener acceso al dashboard de alto nivel o que este punto hace referencia a la consola del SIEM.</p>		Conforme a lo señalado por el área usuaria, se aclara que este punto hace referencia a la consola de monitoreo (dashboard) donde se podrá visualizar al menos: Cumplimiento de SLAs, gestión de eventos, gestión de incidentes, gestión de solicitudes, gestión de cambios, entre otros relacionados con el servicio. Se definirá el alcance de la vista en la etapa de implementación. Finalmente, se precisa que la consola es independiente del SIEM.	
27	20477770623	DIGIWARE DEL PERU S.A.C. - DIGIWARE S.A.C.	Consulta	General	6.7	N/A	48	<p>Dice: El Contratista realizará dichas instalaciones y configuraciones durante los fines de semana, días feriados no laborales u horas no laborales en una ventana de tiempo coordinada entre El Contratista y COFIDE a fin de minimizar el impacto en la operativa de COFIDE.</p> <p>Consulta: La integración de las fuentes al SOC no interrumpe la disponibilidad de los servicios. Por favor, confirmar que la implementación puede ser ejecutada de lunes a viernes de 8am a 6pm y, de ser necesario, feriados y fines de semana.</p>		Conforme a lo señalado por el área usuaria, se confirma que la implementación puede ser ejecutada de lunes a viernes de 8am a 6pm y de ser necesario, feriados y fines de semana sobre las configuraciones que tengan impacto sobre la operativa de COFIDE.	

28	20477770623	DIGIWARE DEL PERU S.A.C. - DIGIWARE S.A.C.	Consulta	General	7	N/A	57	<p>Dice: "El POSTOR del servicio debe contar con al menos con dos (02) membresías de comunidades de Ciberseguridad indicadas a continuación".</p> <p>Consulta: Confirmar que COFIDE puede aceptar una membresía que no está dentro de las bases como Global Cyber Alliance.</p>		<p>Conforme a lo señalado por el área usuaria y, con ocasión a la integración de bases, se confirma que se aceptará una membresía de Global Cyber Alliance.</p>	<p>Se modifica numeral 7.1. de los términos de referencia, capítulo III de la Sección Específica de las Bases:</p> <p>Se agrega:</p> <p>5. Global Cyber Alliance: Contar con certificación o carta que indique o confirme que la empresa es miembro o corresponsal acreditado o signataria de Global Cyber Alliance</p>
29	20477770623	DIGIWARE DEL PERU S.A.C. - DIGIWARE S.A.C.	Consulta	General	5	N/A	20	<p>Dice: Personal Clave. (01) Director del proyecto.</p> <p>Consulta: Por favor, confirmar que se acepta:</p> <p>*Personal ubicado fuera de Perú.</p> <p>*Servicio remoto.</p> <p>*Certificaciones adicionales de alguna de las siguientes opciones relacionadas al perfil:</p> <p>1. CERTIPROF. Lead Cybersecurity Professional Certificate (LCSPP).</p> <p>2. CERTIPROF. SCRUM Master Professional Certificate.</p> <p>3. CERTIPROF. SCRUM Product Owner Professional Certificate.</p> <p>4. CERTIPROF. Líder ISO 27001:2013</p> <p>5. AXELOS. ITIL Foundation Examination.</p> <p>6. APMG INTERNATIONAL. COBIT 5 Foundation Examination.</p> <p>7. CORPORACIÓN UNIVERSITARIA DE ASTURIAS. Programa Internacional especializado en Gestión para la Seguridad de la Información.</p> <p>8. INSTITUTO EUROPEO DE POSGRADO. Experto en Gestión de Proyectos PMI.</p> <p>9. ISACA. CISM.</p> <p>10. ISACA. CRISC.</p> <p>11. BSG Institute. CISSP.</p> <p>12. IT SERVICE. ISO 27001 Auditor.</p>		<p>Conforme a lo señalado por el área usuaria, se acepta en parte lo solicitado; por lo que, para el Director del proyecto, se aceptará que:</p> <p>* Personal se encuentre ubicado fuera de Perú.</p> <p>* Servicio remoto.</p> <p>Así como las siguientes certificaciones relacionadas al perfil:</p> <p>- Certificación en Experto en Gestión de Proyectos PMI.</p> <p>- Certificación en SCRUM Master Professional Certificate.</p> <p>Que, no se aceptarán las demás certificaciones, debido a que no se ha podido validar que las mismas se encuentren efectivamente relacionadas al perfil.</p>	<p>Se modifica numeral 5) de los términos de referencia, capítulo III de la Sección Específica de las Bases:</p> <p>Se agrega:</p> <p>Funciones:</p> <p>(...) el personal podrá residir fuera del Perú y realizar servicio remoto.</p> <p>Capacitación y/o certificación:</p> <p>Por lo menos 01 de las siguientes certificaciones, como por ejemplo:</p> <p>- Certificación PMP vigente</p> <p>- Certificación PRINCE2 vigente</p> <p>- Certificación en ISO 27032 Gerente de Ciberseguridad vigente</p> <p>- Certificación en Experto en Gestión de Proyectos PMI.</p> <p>- Certificación en SCRUM Master Professional Certificate.</p>
30	20477770623	DIGIWARE DEL PERU S.A.C. - DIGIWARE S.A.C.	Consulta	General	5	N/A	20	<p>Dice:</p> <p>Personal Clave. (1) Líder de CSIRT.</p> <p>Consulta:</p> <p>Por favor, confirmar que se aceptarán adicionalmente, alguna de las siguientes opciones relacionadas al perfil:</p> <p>1. SKILLFRONT. ISO/IEC 27001 Information Security Associate - Accredited Professional Certification.</p> <p>2. ISC2. Official ISC2 Certified in Cybersecurity (CC) Self-Paced Training - 1M.</p> <p>3. ISC2. Certified in Cybersecurity.</p> <p>4. CERTIPROF. Scrum Foundation Professional Certificate.</p> <p>5. PECB. Certified ISO/IEC 27032 Lead Cybersecurity Manager.</p> <p>CENTRO NACIONAL DE SEGURIDAD DIGITAL. Equipo de respuesta ante incidentes de seguridad digital.</p> <p>6. CENTRO NACIONAL DE SEGURIDAD DIGITAL. Auditor Interno ISO 27001.</p> <p>7. CENTRO NACIONAL DE SEGURIDAD DIGITAL. Análisis de Vulnerabilidades Digitales.</p> <p>8. CENTRO NACIONAL DE SEGURIDAD DIGITAL. Taller de Implementación del SOC.</p> <p>9. CENTRO NACIONAL DE SEGURIDAD DIGITAL. Gestión de seguridad de la información ISO 27001.</p> <p>10. AXELOS. ITIL Foundation Certificate in IT Service Management.</p>		<p>Conforme a lo señalado por el área usuaria, se recuerda que las consultas y observaciones deberán ser formuladas de forma clara y precisa, siendo que en la presente consulta no indica a que sección del perfil se debe realizar el cambio solicitado (Formación y/o experiencia y/o capacitación y/o certificación); por lo tanto, no se acepta lo solicitado.</p>	

31	20477770623	DIGIWARE DEL PERU S.A.C. - DIGIWARE S.A.C.	Consulta	General	5	N/A	20	<p>Dice: Personal Clave. (1) Lider de CyberSOC.</p> <p>Consulta: Por favor, confirmar que se aceptarán adicionalmente, alguna de las siguientes opciones relacionadas al perfil: 1. DRAGON JAR. Diplomado de Seguridad Informática Ofensiva. 2. OPEN-SEC. Fundamentos de Seguridad Ofensiva. 3. AXELOS. ITIL Foundation Certificate in IT Service Management. 5. OPEN-SEC. Seguridad Ofensiva. 6. OPEN-SEC. Seguridad Ofensiva para Aplicaciones. 7. SCRUMSTUDY. Scrum Fundamentals Certified. 8. CERTIPROF. Cybersecurity Awareness Professional Certification. 9. CERTIPROF. ISO/IEC 27001:2022 Certified Lead Implementer I27001CLI.</p>		<p>Conforme a lo señalado por el área usuaria, se recuerda que las consultas y observaciones deberán ser formuladas de forma clara y precisa, siendo que en la presente consulta no indica a que sección del perfil se debe realizar el cambio solicitado (Formación y/o experiencia y/o capacitación y/o certificación); por lo tanto, no se acepta lo solicitado.</p>	
32	20477770623	DIGIWARE DEL PERU S.A.C. - DIGIWARE S.A.C.	Consulta	General	5	N/A	20	<p>Dice: Personal Clave. (1) Service Manager.</p> <p>Consulta: Por favor, confirmar que se aceptarán adicionalmente, alguna de las siguientes opciones relacionadas al perfil: 1. PROJECT MANAGEMENT INSTITUTE. Project Management Professional (PMP). 2. LOGPOINT. Certified Logpoint SOAR. 6. CERTIPROF. Scrum Study Fundamental Certified. 7. ILC INNOVATION LEARNING CENTER. Scrum Master y Herramientas Colaborativas para Gestionar Proyectos. 8. CERTIPROF. Cybersecurity Awareness Professional Certification. 9. ACADEMIA DE CIBERSEGURIDAD. Curso Internacional Gestión de un Cybersoc.</p>		<p>Conforme a lo señalado por el área usuaria, se recuerda que las consultas y observaciones deberán ser formuladas de forma clara y precisa, siendo que en la presente consulta no indica a que sección del perfil se debe realizar el cambio solicitado (Formación y/o experiencia y/o capacitación y/o certificación); por lo tanto, no se acepta lo solicitado.</p>	
33	20601317461	SECURESOFT CORPORATION S.A.C	Consulta	Específico	6.8.2	.	56	<p>DICE: Tiempo de solución oportuna: para el caso de incidentes es el tiempo transcurrido entre la comunicación al PROVEEDOR de la existencia del mal funcionamiento del servicio por parte de COFIDE (llamada de servicio) y la disponibilidad y puesta en funcionamiento del servicio a satisfacción del COFIDE. Para el caso del requerimiento se considera el tiempo transcurrido entre la solicitud al PROVEEDOR (correo electrónico) y la confirmación de dicha atención por parte de COFIDE.</p> <p>CONSULTA: -Favor de confirmar que el Tiempo de Solución Oportuna para los incidentes aplicada solo para los de Infraestructura y/o tecnología y no para los de seguridad. -Favor de confirmar si para incidentes se puede considerar desde que finaliza el Tiempo de Respuesta Oportuna hasta que se realiza la resolución del incidente. -Favor de confirmar si para los requerimiento se puede considerar desde que finaliza el Tiempo de Respuesta Oportuna hasta que se realiza la resolución del requerimiento.</p>		<p>Conforme a lo señalado por el área usuaria, se precisa que: (i) el Tiempo de Solución Oportuna para los incidentes aplica para todos los eventos relacionado a la atención de incidentes del servicio (Infraestructura y/o tecnología y/o seguridad). (ii) para incidentes se considera desde que se recibe la Respuesta Oportuna hasta que se realiza la resolución del incidente. Se aclara al postor que, para los requerimiento se considera desde que se recibe la Respuesta Oportuna hasta que se realiza la resolución del requerimiento.</p>	

34	20601317461	SECURESOFT CORPORATION S.A.C	Consulta	Específico	6.8.3	.	56	<p>DICE: Gestión de incidentes</p> <p>CONSULTA: Favor de indicar si se puede considerar los siguientes tiempos:</p> <p>Tiempo de respuesta: Prioridad Alta=60 minutos Prioridad Media=120 minutos Prioridad Baja=180 minutos.</p>	<p>Conforme a lo señalado por el área usuaria y, con ocasión a la integración de las bases, con la finalidad de fomentar una mayor pluralidad de postores, se acepta lo solicitado; por lo que se considera los siguientes tiempos de respuesta para la gestión de incidentes:</p> <p>Tiempo de respuesta: Prioridad Alta=60 minutos Prioridad Media=120 minutos Prioridad Baja=180 minutos.</p>	<p>Se modifica numeral 6.8.3 de los términos de referencia del capítulo III de la Sección Específica de las Bases, según el siguiente detalle: DICE: Tiempo de respuesta: Prioridad Alta=30 minutos Prioridad Media=60 minutos Prioridad Baja=120 minutos.</p> <p>DEBE DECIR: Tiempo de respuesta: Prioridad Alta=60 minutos Prioridad Media=120 minutos Prioridad Baja=180 minutos.</p>
35	20601317461	SECURESOFT CORPORATION S.A.C	Consulta	Específico	6.8.3	.	56	<p>DICE: Gestión de incidentes</p> <p>CONSULTA: - Favor de confirmar que el tiempo de solución oportuna aplica solo para incidentes de infraestructura y/o tecnología. - Favor de confirmar que para la solución de un incidente donde haya la intervención de marca y/o de un tercero, el ticket de atención debe ser excluido de la medición ya que los tiempos no podrán ser definidos por el postor. -Se debe considerar que si para la solución del incidente se tiene dependencia del cliente o de un tercero, el ticket de atención debe ser excluido de la medición ya que los tiempos no podrán ser definidos por Securesoft.</p>	<p>Conforme a lo señalado por el área usuaria, respecto a la gestión de incidentes: (i) Se aclara que el Tiempo de Solución Oportuna para los incidentes aplica para todos los eventos relacionado a la atención de incidentes del servicio (Infraestructura y/o tecnología y/o seguridad) (ii) Se confirma que para la solución de un incidente donde haya la intervención o escalamiento a la marca y/o de un tercero, el ticket de atención debe ser excluido de la medición ya que los tiempos no podrán ser definidos por el contratista. El contratista será el responsable de hacer seguimiento hasta la resolución del incidente. (iii) Se confirma que se considerará que si para la solución del incidente se tiene dependencia del cliente o de un tercero, el ticket de atención deberá ser excluido de la medición ya que los tiempos no podrán ser definidos por el contratista. El contratista será el responsable de hacer seguimiento hasta la resolución del incidente.</p>	
36	20601317461	SECURESOFT CORPORATION S.A.C	Consulta	Específico	6.8.4	.	56	<p>DICE: Umbrales de niveles de servicio</p> <p>CONSULTA: Favor de indicar si es posible considerar un umbral de cumplimiento del 90% para la solución oportuna de incidentes de prioridad alta.</p>	<p>Conforme a lo señalado por el área usuaria, no se acepta lo solicitado, se precisa que para asegurar la calidad del servicio y minimizar el impacto de incidentes sobre la operativa de COFIDE, se considera que el umbral de cumplimiento del 100% para la solución oportuna de incidentes de prioridad alta es justificable.</p>	
37	20601317461	SECURESOFT CORPORATION S.A.C	Consulta	Específico	9.1	.	59	<p>DICE: Respuesta oportuna de incidentes</p> <p>CONSULTA: Favor de indicar si es posible considerar la forma de cálculo de: 7%*1UIT.</p>	<p>Conforme a lo señalado por el área usuaria, se aclara que el cálculo de las penalidades es un estándar definido por COFIDE, el mismo que se encuentra alineado a la normativa de contrataciones del Estado, y se encuentran calculados a un porcentaje de una (01) UIT siendo proporcional, la necesidad de COFIDE es contar con un servicio disponible y de calidad teniendo en cuenta la criticidad de la Seguridad de Información de COFIDE.</p> <p>Asimismo, se hace presente que, según la experiencia de anteriores contratos de COFIDE, la aplicación de tal penalidad no ha resultado ser irracional ni desproporcional, contrario a ello se busca fomentar que el contratista cumpla a cabalidad con lo requerido por la Entidad. Por lo tanto; no se acepta lo solicitado.</p>	
38	20601317461	SECURESOFT CORPORATION S.A.C	Consulta	Específico	9.1	.	59	<p>DICE: Solución oportuna de incidentes prioridad alta</p> <p>CONSULTA: -Favor de indicar si es posible considerar la forma de cálculo de: 10%*1UIT. -Favor de indicar si es posible considerar un umbral de cumplimiento del 90%</p>	<p>Conforme a lo señalado por el área usuaria, se aclara que el cálculo de las penalidades es un estándar definido por COFIDE, se encuentra alineado a la normativa de contrataciones del Estado, y están calculadas a un porcentaje de una (01) UIT, siendo proporcional, la necesidad de COFIDE es contar con un servicio disponible y de calidad teniendo en cuenta la criticidad de la Seguridad de Información de COFIDE.</p> <p>Asimismo, se precisa que para asegurar la calidad del servicio y minimizar el impacto de incidentes sobre la operativa de COFIDE, se considera que el umbral de cumplimiento del 100% para la solución oportuna de incidentes de prioridad alta es justificable.</p> <p>Se hace presente que, según la experiencia de anteriores contratos de COFIDE, la aplicación de tal penalidad no ha resultado ser irracional ni desproporcional, contrario a ello se busca fomentar que el contratista cumpla a cabalidad con lo requerido por la Entidad. Por lo tanto; no se acepta lo solicitado.</p>	

39	20601317461	SECURESOFT CORPORATION S.A.C	Consulta	Específico	9.1	.	59	DICE: Solución oportuna de requerimientos prioridad alta CONSULTA: Favor de indicar si es posible considerar la forma de cálculo de: 7%*1UIT.		Conforme a lo señalado por el área usuaria, se aclara que el calculo de las penalidades es un estándar definido por COFIDE, esta alineado a la normativa de contrataciones del Estado, y estas estan calculadas a un porcentaje de una (01) UIT siendo proporcional, la necesidad de COFIDE es contar con un servicio disponible y de calidad teniendo en cuenta la criticidad de la Seguridad de Información de COFIDE. Asimismo, se hace presente que, según la experiencia de anteriores contratos de COFIDE, la aplicación de tal penalidad no ha resultado ser irracional ni desproporcional, contrario a ello se busca fomentar que el contratista cumpla a cabalidad con lo requerido por la Entidad. Por lo tanto; no se acepta lo solicitado.	
40	20601317461	SECURESOFT CORPORATION S.A.C	Consulta	Específico	9.1	.	59	DICE: Solución oportuna de incidentes otras prioridades CONSULTA: Favor de indicar si es posible considerar la forma de cálculo de: 7%*1UIT.		Conforme a lo señalado por el área usuaria, se aclara que el calculo de las penalidades es un estándar definido por COFIDE, está alineado a la normativa de contrataciones del Estado, y estan calculadas a un porcentaje de una (01) UIT siendo proporcional, la necesidad de COFIDE es contar con un servicio disponible y de calidad teniendo en cuenta la criticidad de la Seguridad de Información de COFIDE. Asimismo, se hace presente que, según la experiencia de anteriores contratos de COFIDE, la aplicación de tal penalidad no ha resultado ser irracional ni desproporcional, contrario a ello se busca fomentar que el contratista cumpla a cabalidad con lo requerido por la Entidad. Por lo tanto; no se acepta lo solicitado.	
41	20601317461	SECURESOFT CORPORATION S.A.C	Consulta	Específico	9.1	.	59	DICE: Solución oportuna de requerimientos otras prioridades CONSULTA: Favor de indicar si es posible considerar la forma de cálculo de: 3%*1UIT.		Conforme a lo señalado por el área usuaria, se aclara que el calculo de las penalidades es un estándar definido por COFIDE, está alineado a la normativa de contrataciones del Estado, y están calculadas a un porcentaje de una (01) UIT siendo proporcional, la necesidad de COFIDE es contar con un servicio disponible y de calidad teniendo en cuenta la criticidad de la Seguridad de Información de COFIDE. Asimismo, se hace presente que, según la experiencia de anteriores contratos de COFIDE, la aplicación de tal penalidad no ha resultado ser irracional ni desproporcional, contrario a ello se busca fomentar que el contratista cumpla a cabalidad con lo requerido por la Entidad. Por lo tanto; no se acepta lo solicitado.	
42	20601317461	SECURESOFT CORPORATION S.A.C	Consulta	Específico	5	.	22	DICE: PERSONAL CLAVE (01) Service Manager Por lo menos 02 de los siguientes cursos: - Curso, diplomado o programa de Seguridad de Sistemas de Información, de mínimo 100 horas. - Curso, diplomado o programa de Certified Information Security Manager (CISM), de mínimo 20 horas. - Curso, diplomado o programa de Certified Information Systems Security Professional (CISSP), de mínimo 40 horas. - Curso, diplomado o programa en Gestión de Servicios de Tecnologías de la Información, de mínimo 40 horas. CONSULTA: Favor de confirmar que se podrá aceptar como una opción adicional el curso, diplomado o programa de Especialización en Gestión de Proyectos, de mínimo 100 horas; dado que las funciones solicitadas para este personal también son de gestión.		Conforme a lo señalado por el área usuaria y, con ocasión a la integración de las bases, se acepta lo solicitado, por lo que se acepta como una opción adicional el curso, diplomado o programa de Especialización en Gestión de Proyectos, de mínimo 100 horas; dado que las funciones solicitadas para este personal también son de gestión.	Se modifica numeral 5 de los términos de referencia del capítulo III de la Sección Específica de las Bases, según el siguiente detalle: <u>Service Manager</u> Se agrega: Por lo menos 02 de los siguientes cursos: (...) -Curso y/o Diplomado y/o programa de Especialización en Gestión de Proyectos, de mínimo 100 horas
43	20601317461	SECURESOFT CORPORATION S.A.C	Consulta	Específico	2.3	f	17	DICE: 2.3. REQUISITOS PARA PERFECCIONAR EL CONTRATO f) Copia de DNI del postor en caso de persona natural, o de su representante legal en caso de persona jurídica. CONSULTA: Favor de confirmar que se aceptará también presentar copia de Carnet de Extranjería del representante legal como cumplimiento de este punto.		Se confirma que en caso su representante no cuente con DNI, podrá presentar copia del Carnet de Extranjería.	

44	20601317461	SECURESOFT CORPORATION S.A.C	Consulta	Específico	6.1	.	29	DICE: CANTIDAD DE ACTIVOS: 10 CONSULTA: Se solicita a la Entidad confirmar que para este servicio se considerará los activos que se encuentran dentro del punto 6.1.5. el cual suman 11.		Conforme a lo señalado por el área usuaria, se acepta lo solicitado, por lo que se confirma que para el presente servicio se considerarán los activos que se encuentran dentro del punto 6.1.5. de los términos de referencia, los cuales suman 11.	Se modifica numeral 6.1.5 de los términos de referencia, capítulo III de la Sección Específica de las Bases: DICE: CANTIDAD DE ACTIVOS:10 DEBE DECIR: CANTIDAD DE ACTIVOS:11
45	20601317461	SECURESOFT CORPORATION S.A.C	Consulta	Específico	6.3.4	t	36	DICE: Considerar soluciones líderes en el mercado americano y/o europeo. Adjuntar informes que acrediten el liderazgo de al menos dos años consecutivos de los últimos cuatro años la cual debe ser presentada a la firma de contrato. CONSULTA: Favor de confirmar que la documentación de sustento se podrá presentar en su idioma original.		Conforme a lo señalado por el área usuaria, se confirma que la documentación de sustento se podrá presentar en su idioma original. Haciendo presente que el postor ganador será responsable de la exactitud y veracidad de dichos documentos.	
46	20601317461	SECURESOFT CORPORATION S.A.C	Consulta	Específico	6.3.4	t	36	DICE: Considerar soluciones líderes en el mercado americano y/o europeo. Adjuntar informes que acrediten el liderazgo de al menos dos años consecutivos de los últimos cuatro años la cual debe ser presentada a la firma de contrato. CONSULTA: Favor de confirmar que se podrá adjuntar informes o alguna evidencia que sustente el liderazgo de la tecnología ofertada emitido por empresas reconocidas como evaluadoras o consultoras o investigadoras de tecnologías de la información, como por ejemplo: Gartner, Forrester, Radicati, etc.		Conforme a lo señalado por el área usuaria, se confirma que se podrá adjuntar informes o alguna evidencia que sustente el liderazgo de la tecnología ofertada emitido por empresas reconocidas como evaluadoras o consultoras o investigadoras de tecnologías de la información, como por ejemplo: Gartner, Forrester, Radicati, etc.	
47	20601317461	SECURESOFT CORPORATION S.A.C	Consulta	Específico	3.2	B.3.2	67	DICE: CAPACITACION Requisitos Service Manager Por lo menos 02 de los siguientes cursos: - Curso, diplomado o programa de Seguridad de Sistemas de Información, de mínimo 100 horas. - Curso, diplomado o programa de Certified Information Security Manager (CISM), de mínimo 20 horas. - Curso, diplomado o programa de Certified Information Systems Security Professional (CISSP), de mínimo 40 horas. - Curso, diplomado o programa en Gestión de Servicios de Tecnologías de la Información, de mínimo 40 horas. CONSULTA: Favor de confirmar que se podrá aceptar como una opción adicional el curso, diplomado o programa de Especialización en Gestión de Proyectos, de mínimo 100 horas; dado que las funciones solicitadas para este personal también son de gestión.		Conforme a lo señalado por el área usuaria, se acepta lo solicitado; por lo que, se acepta como una opción adicional el curso, diplomado o programa de Especialización en Gestión de Proyectos, de mínimo 100 horas; dado que las funciones solicitadas para este personal también son de gestión.	Se modifica numeral 5 de los términos de referencia del capítulo III de la Sección Específica de las Bases, según el siguiente detalle: Service Manager Se agrega: Por lo menos 02 de los siguientes cursos: (...) - Curso y/o Diplomado y/o programa de Especialización en Gestión de Proyectos, de mínimo 100 horas
48	20601317461	SECURESOFT CORPORATION S.A.C	Consulta	Específico	5	.	27	DICE: S6-Servicio de ciberinteligencia Analista de Monitoreo de Ciberinteligencia Formación Titulado Técnico en las carreras de Informático y/o Industrial y/o Informática y de y/o Industrial Sistemas e Informática CONSULTA: Favor de confirmar que se podrá aceptar la carrera de Ingeniería de Sistemas.		Conforme a lo señalado por el área usuaria y, con ocasión a la integración de bases, se acepta lo solicitado; por lo que, se acepta la carrera de Ingeniería de Sistemas como formación para el Analista de Monitoreo de Ciberseguridad.	Se modifica numeral 5 de los términos de referencia del capítulo III de la Sección Específica de las Bases, según el siguiente detalle: S6-Servicio de ciberinteligencia Analista de Monitoreo de Ciberinteligencia DICE: Formación Titulado Técnico en las carreras de Informático y/o Industrial y/o Informática y de y/o Industrial Sistemas e Informática DEBE DECIR:: Formación Titulado Técnico en las carreras de Informático y/o Industrial y/o Informática y/o Industrial Sistemas e Informática <u>y/o Ingeniería de Sistemas</u>

49	20601317461	SECURESOFT CORPORATION S.A.C	Consulta	Específico	5	.	27	DICE: S6-Servicio de ciberinteligencia Analista de Monitoreo de Ciberinteligencia Formación Titulado Técnico en las carreras de Informático y/o Industrial y/o Informático y de y/o Industrial Sistemas e Informática CONSULTA: Favor de confirmar que se podrá aceptar también el grado de Bachiller.		Conforme a lo señalado por el área usuaria y, con ocasión a la integración de las bases, se acepta lo solicitado; por lo que, se acepta como formación del Analista de Monitoreo de Ciberinteligencia el grado de bachiller, al tratarse de un alcance superior al mínimo solicitado de Titulado Técnico.	Se modifica numeral 5 de los términos de referencia del capítulo III de la Sección Específica de las Bases, según el siguiente detalle: S6-Servicio de ciberinteligencia Analista de Monitoreo de Ciberinteligencia DICE: Formación Titulado Técnico en las carreras de Informático y/o Industrial y/o Informático y de y/o Industrial Sistemas e Informática DEBE DECIR:: Formación Bachiller y/o Titulado Técnico en las carreras de Informático y/o Industrial y/o Informático y/o Industrial Sistemas e Informática y/o Ingeniería de Sistemas
50	20601317461	SECURESOFT CORPORATION S.A.C	Consulta	Específico	5	.	23	DICE: S1-Servicio de evaluación de Seguridad TI Analista(s) de riesgos TI Formación Titulado Técnico en las carreras de ¿... CONSULTA: Favor de confirmar que se podrá aceptar también el grado de Bachiller.		Conforme a lo señalado por el área usuaria y, con ocasión a la integración de las bases, se acepta lo solicitado; por lo que, se acepta como formación del Analista(s) de riesgos TI el grado de bachiller, al tratarse de un alcance superior al mínimo solicitado de Titulado Técnico.	Se modifica numeral 5 de los términos de referencia del capítulo III de la Sección Específica de las Bases, según el siguiente detalle: S1-Servicio de evaluación de Seguridad TI Analista(s) de riesgos TI Formación DICE: Titulado Técnico en las carreras de ... DEBE DECIR: <u>Bachiller y/o</u> Titulado Técnico en las carreras de...
51	20601317461	SECURESOFT CORPORATION S.A.C	Consulta	Específico	5	.	24	DICE: S2 - Servicio de Gestión de los Equipos o Activos o Soluciones de Seguridad Analista(s) de operación de equipos y soluciones de seguridad Formación Titulado Técnico en las carreras de ¿... CONSULTA: Favor de confirmar que se podrá aceptar también el grado de Bachiller.		Conforme a lo señalado por el área usuaria y, con ocasión a la integración de las bases, se acepta lo solicitado; por lo que, se acepta como formación del Analista(s) de operación de equipos y soluciones de seguridad el grado de bachiller, al tratarse de un alcance superior al mínimo solicitado de Titulado Técnico.	Se modifica numeral 5 de los términos de referencia del capítulo III de la Sección Específica de las Bases, según el siguiente detalle: S2 - Servicio de Gestión de los Equipos o Activos o Soluciones de Seguridad Analista(s) de operación de equipos y soluciones de seguridad Formación DICE: Titulado Técnico en las carreras de ... DEBE DECIR: <u>Bachiller y/o</u> Titulado Técnico en las carreras de...
52	20601317461	SECURESOFT CORPORATION S.A.C	Consulta	Específico	5	.	25	DICE: S4 - Servicios Respuesta a Incidentes como Servicio Analista(s) de respuesta a incidentes Formación Titulado Técnico en las carreras de ¿... CONSULTA: Favor de confirmar que se podrá aceptar también el grado de Bachiller.		Conforme a lo señalado por el área usuaria y, con ocasión a la integración de las bases, se acepta lo solicitado; por lo que, se acepta como formación del Analista(s) de respuesta a incidentes el grado de bachiller, al tratarse de un alcance superior al mínimo solicitado de Titulado Técnico.	Se modifica numeral 5 de los términos de referencia del capítulo III de la Sección Específica de las Bases, según el siguiente detalle: S4 - Servicios Respuesta a Incidentes como Servicio Analista(s) de respuesta a incidentes Formación DICE: Titulado Técnico en las carreras de ... DEBE DECIR: <u>Bachiller y/o</u> Titulado Técnico en las carreras de...
53	20601317461	SECURESOFT CORPORATION S.A.C	Consulta	Específico	5	.	26	DICE: S5 -Servicio de escaneo, análisis e identificación de vulnerabilidades de las aplicaciones web Analista(s) de soluciones de escaneo e identificación de vulnerabilidades de aplicaciones web Formación Titulado Técnico en las carreras de ¿... CONSULTA: Favor de confirmar que se podrá aceptar también el grado de Bachiller.		Conforme a lo señalado por el área usuaria y, con ocasión a la integración de las bases, se acepta lo solicitado; por lo que, se acepta como formación del Analista(s) de soluciones de escaneo e identificación de vulnerabilidades de aplicaciones web el grado de bachiller, al tratarse de un alcance superior al mínimo solicitado de Titulado Técnico.	Se modifica numeral 5 de los términos de referencia del capítulo III de la Sección Específica de las Bases, según el siguiente detalle: S5 -Servicio de escaneo, análisis e identificación de vulnerabilidades de las aplicaciones web Analista(s) de soluciones de escaneo e identificación de vulnerabilidades de aplicaciones web Formación DICE: Titulado Técnico en las carreras de ... DEBE DECIR: <u>Bachiller y/o</u> Titulado Técnico en las carreras de...
54	20601317461	SECURESOFT CORPORATION S.A.C	Consulta	Específico	6	.	27	DICE: DESCRIPCIÓN DEL SERVICIO S1-Servicio de evaluación de Seguridad TI Frecuencia: Anual CONSULTA: Favor de confirmar que la frecuencia para este servicio será de una única vez como se indica en el detalle del punto 6.1 de la página 28 de las bases.		Conforme a lo señalado por el área usuaria y, con ocasión a la integración de las bases, se confirma que la frecuencia para este servicio será de una única vez como se indica en el detalle del punto 6.1 de los términos de referencia (p. 28 de las bases administrativas)	Se modifica numeral 6.1 de los términos de referencia del capítulo III de la Sección Específica de las Bases, según el siguiente detalle: DICE: DESCRIPCIÓN DEL SERVICIO S1-Servicio de evaluación de Seguridad TI Frecuencia: Anual DEBE DECIR:: DESCRIPCIÓN DEL SERVICIO S1-Servicio de evaluación de Seguridad TI Frecuencia: <u>Una única vez a demanda</u>
55	20601317461	SECURESOFT CORPORATION S.A.C	Consulta	Específico	2.3	m	17	DICE: Informes que acrediten el liderazgo en soluciones en el mercado americano y/o europeo de al menos 2 años consecutivos en los últimos 4 años, según lo señalado en el numeral 6.3.4) de los términos de referencia, previstos en el capítulo III de la Sección Específica de las Bases CONSULTA: Favor de confirmar que la documentación de sustento se podrá presentar en su idioma original.		Conforme a lo señalado por el área usuaria, se confirma que la documentación de sustento se podrá presentar en su idioma original. Haciendo presente que el postor ganador será responsable de la exactitud y veracidad de dichos documentos.	

56	20601317461	SECURESOFT CORPORATION S.A.C	Consulta	Específico	2.3	m	17	<p>DICE: Informes que acrediten el liderazgo en soluciones en el mercado americano y/o europeo de al menos 2 años consecutivos en los últimos 4 años, según lo señalado en el numeral 6.3.4) de los términos de referencia, previstos en el capítulo III de la Sección Específica de las Bases</p> <p>CONSULTA: Favor de confirmar que se podrá adjuntar informes o alguna evidencia que sustente el liderazgo de la tecnología ofertada emitido por empresas reconocidas como evaluadoras o consultoras o investigadoras de tecnologías de la información, como por ejemplo: Gartner, Forrester, Radicati, etc.</p>		<p>Conforme a lo señalado por el área usuaria, se confirma que se podrá adjuntar informes o alguna evidencia que sustente el liderazgo de la tecnología ofertada emitido por empresas reconocidas como evaluadoras o consultoras o investigadoras de tecnologías de la información, como por ejemplo: Gartner, Forrester, Radicati, etc.</p>	
57	20601317461	SECURESOFT CORPORATION S.A.C	Consulta	Específico	6.3	.	35	<p>DICE: CANTIDAD DE ACTIVOS: 10</p> <p>CONSULTA: Se solicita a la Entidad confirmar que para este servicio se considerará los activos que se encuentran dentro del punto 6.3.6 el cual suman 12.</p>		<p>Se confirma al postor que, este servicio se considerará los activos que se encuentran dentro del punto 6.3.6 el cual suman 12.</p> <p>Conforme a lo señalado por el área usuaria, se acepta lo solicitado, por lo que se confirma que para el presente servicio se considerarán los activos que se encuentran dentro del punto 6.3.6. de los términos de referencia, los cuales suman 12.</p>	<p>Se modifica numeral 6.3.6. de los términos de referencia, capítulo III de la Sección Específica de las Bases:</p> <p>DICE: CANTIDAD DE ACTIVOS:10</p> <p>DEBE DECIR: CANTIDAD DE ACTIVOS:12</p>
58	20601317461	SECURESOFT CORPORATION S.A.C	Consulta	Específico	7.1	.	57	<p>DICE: El POSTOR del servicio deberá contar con al menos dos (02) certificaciones para empresas de Ciberseguridad indicadas a continuación: ISO 9001:2015</p> <p>CONSULTA: Favor de confirmar que el certificado ISO 9001 será considerado como opcional y no dentro de las 2 certificaciones obligatorias, debido a que el servicio está alineado directamente a la gestión y operación de un Cybersoc a nivel de ciberseguridad, y la calidad de los productos y servicios está implícito en el requerimiento general.</p>		<p>Conforme a lo señalado por el área usuaria, se acepta parcialmente lo solicitado, debido a que el servicio está alineado directamente a la gestión y operación de un Cybersoc a nivel de ciberseguridad, y la calidad de los productos y servicios está implícito en el requerimiento general, se retira de las certificaciones obligatorias el certificado ISO 9001</p>	<p>Se modifica numeral 7.1 de los términos de referencia, capítulo III de la Sección Específica de las Bases, se reitera la certificación ISO 9001:2015</p>
59	20601317461	SECURESOFT CORPORATION S.A.C	Consulta	Específico	10.3	.	62	<p>DICE: S1 - Servicio de evaluación de Seguridad TI Plazo Máximo Una vez por año dentro de los cinco (05) primeros meses de cada aniversario e inicia a partir de Acta de inicio del servicio S1</p> <p>CONSULTA: Favor de confirmar que el plazo máximo para este servicio será de una única vez como se indica en el detalle del punto 6.1 de la página 28 de las bases.</p>		<p>Conforme a lo señalado por el área usuaria, se confirma que el plazo máximo para el Servicio de evaluación de Seguridad TI será de una única vez como se indica en el detalle del punto 6.1 (p. 28 de las bases administrativas).</p>	<p>Se modifica numeral 10.3 de los términos de referencia, capítulo III de la sección específica de las bases, según el siguiente detalle:</p> <p>DICE: S1 - Servicio de evaluación de Seguridad TI Plazo Máximo Una vez por año dentro de los cinco (05) primeros meses de cada aniversario e inicia a partir de Acta de inicio del servicio S1</p> <p>DEBE DECIR: S1 - Servicio de evaluación de Seguridad TI Plazo Máximo Una vez a demanda dentro de los primeros dos (02) años del servicio e inicia a partir de la firma del Acta de inicio del servicio S1 que considera la evaluación de los activos de seguridad de TI.</p>