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

CONCURSO PÚBLICO Nº 04-2021-COFIDE
PRIMERA CONVOCATORIA

CONTRATACIÓN DE SERVICIO DE CIBERSEGURIDAD EN LOS SISTEMAS DE COFIDE

Firmado digitalmente por ATOCHE MACEDO Diego Gustavo FAU 20100116392 soft
Motivo: Soy el autor del documento
Fecha: 26.08.2021 11:38:38 -05:00

Firmado digitalmente por ANGULO IZQUIERDO Monica Rocio FAU 20100116392 soft
Motivo: Doy V° B°
Fecha: 26.08.2021 15:27:35 -05:00

Firmado digitalmente por HURTADO ARCE Zuley Geraldine FAU 20100116392 soft
Motivo: Doy V° B°
Fecha: 26.08.2021 17:16:46 -05:00

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.

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). Los demás documentos deben ser visados por el postor. En el caso de persona jurídica, por su representante legal, apoderado o mandatario designado para dicho fin y, en el caso de persona natural, por este o su apoderado. No se acepta el pegado de la imagen de una firma o visto. Las ofertas se presentan foliadas.

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

1.8. PRESENTACIÓN Y APERTURA DE OFERTAS

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

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

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

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

1.9. EVALUACIÓN DE LAS OFERTAS

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

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

1.10. CALIFICACIÓN DE OFERTAS

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

1.11. SUBSANACIÓN DE LAS OFERTAS

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

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

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

1.12. RECHAZO DE LAS OFERTAS

Previo al otorgamiento de la buena pro, el comité de selección revisa las ofertas económicas que cumplen los requisitos de calificación, de conformidad con lo establecido para el rechazo de ofertas, previsto en el artículo 68 del Reglamento, de ser el caso.

De rechazarse alguna de las ofertas calificadas, el comité de selección revisa el cumplimiento

de los requisitos de calificación de los postores que siguen en el orden de prelación, en caso las hubiere.

1.13. OTORGAMIENTO DE LA BUENA PRO

Definida la oferta ganadora, el comité de selección otorga la buena pro, mediante su publicación en el SEACE, incluyendo el cuadro comparativo y las actas debidamente motivadas de los resultados de la admisión, no admisión, evaluación, calificación, descalificación 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 accesoria, 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.
RUC Nº	:	20100116392.
Domicilio legal	:	Augusto Tamayo N° 160 San Isidro.
Teléfono:	:	615-4000.
Correo electrónico:	:	datoche@cofide.com.pe.

1.2. OBJETO DE LA CONVOCATORIA

El presente procedimiento de selección tiene por objeto la contratación del servicio de Ciberseguridad en los sistemas de COFIDE.

1.3. EXPEDIENTE DE CONTRATACIÓN

El expediente de contratación fue aprobado mediante Acta de aprobación el 16 de agosto del 2021.

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:

- 30 dias calendario para la etapa de Planificación.
- 60 días calendario para la etapa de Transición de Entrada.
- 36 meses para la etapa operativa.

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 el importe de S/. 3.00 (tres con 00/100 Soles) a nuestra Cta. Cte. 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

- Ley N° 31084 “Ley de Presupuesto del Sector Público para el Año Fiscal 2021”.
- Ley N° 31085 “Ley de Equilibrio Financiero del Presupuesto del Sector Público para el año fiscal 2021”.
- Ley N° 31086 “Ley de Endeudamiento del Sector Público para el año 2021”.
- Acuerdo de Directorio N° 003-2020/009-FONAFE, mediante el que FONAFE aprueba el Presupuesto del año 2021 de COFIDE.
- Resolución de Gerencia General Nº 002-GG-2021, mediante el cual se aprobó el Plan Anual de Contrataciones de la Corporación Financiera de Desarrollo S.A. - COFIDE, para el ejercicio presupuestal 2021.
- Resolución SBS N° 2660-2015, Reglamento de Gestión de Riesgos de Lavado de Activos y del Financiamiento del Terrorismo, y sus modificatorias.
- Ley N° 27693, Ley que crea la Unidad de Inteligencia Financiera - Perú (UIF - Perú)
- Ley N° 30424, Ley que regula la responsabilidad administrativa de las personas jurídicas y sus modificatorias.
- Decreto Supremo 002-2019-JUS - Reglamento de la Ley Nº 30424, Ley que regula la Responsabilidad Administrativa de las Personas Jurídicas.
- Manual de Prevención y Gestión de los Riesgos de Lavado de Activos y del Financiamiento del Terrorismo.
- Manual de Prevención de Delitos de COFIDE.
- Política de Gestión de Conflicto de Interés de COFIDE
- Lineamientos de ética y conducta del proveedor
- Política de Sostenibilidad de COFIDE
- Decreto Supremo Nº 103-2020-EF establecen disposiciones reglamentarias para la tramitación de los procedimientos de selección que se reinicien en el marco del Texto Único Ordenado de la Ley Nº 30225, mediante el cual se dispone adecuar protocolos sanitarios a los procedimientos de selección.
- Decreto Supremo N° 168-2020-EF establecen disposiciones en materia de contrataciones públicas para facilitar la reactivación de contratos de bienes y servicios y modificación el Reglamento de Ley de Contrataciones del Estado.
- Plan de seguimiento ante el COVID19 del Dpto. de Gestión Humana.

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

CAPÍTULO II
DEL PROCEDIMIENTO DE SELECCIÓN

2.1. CALENDARIO DEL PROCEDIMIENTO DE SELECCIÓN

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

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

2.2. CONTENIDO DE LAS OFERTAS

La oferta contendrá, además de un índice de documentos[1], 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 Nº 1)**

b) Documento que acredite la representación de quien suscribe la oferta.

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

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

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

Advertencia
De acuerdo con el artículo 4 del Decreto Legislativo N° 1246, las Entidades están prohibidas de exigir a los administrados o usuarios la información que puedan obtener directamente mediante la interoperabilidad a que se refieren los artículos 2 y 3 de dicho Decreto Legislativo. En esa medida, si la Entidad es usuaria de la Plataforma de Interoperabilidad del Estado – PIDE[2] 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 Nº 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 Nº 3**)

---

[1] La omisión del índice no determina la no admisión de la oferta.

[2] 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 Nº 4)**[3]

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 Nº 5**)

g) El precio de la oferta en SOLES debe registrarse directamente en el formulario electrónico del SEACE.

Adicionalmente se debe adjuntar el Anexo N° 6 en el caso de procedimientos convocados a precios unitarios, esquema mixto de suma alzada y precios unitarios, porcentajes u honorario fijo y comisión de éxito, según corresponda.

En el caso de procedimientos convocados a suma alzada únicamente se debe adjuntar el Anexo N° 6, cuando corresponda indicar el monto de la oferta de la prestación accesoria o que el postor goza de alguna exoneración legal.

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.

h) Ficha técnica de las herramientas, equipos y/o productos que utilizará durante la ejecución de todos los servicios.

i) Presentar el "Plan para la vigilancia, prevención y control de COVID-19 en el trabajo" de acuerdo con lo establecido a la R.M. N° 239-2020-MINSA (y sus posteriores adecuaciones).

j) Constancia de presentación del Plan para la vigilancia, prevención y control de COVID-19 en el trabajo en el sistema integrado para COVID-19 (SICOVID-19) o correo de presentación del Plan por Mesa de partes virtual del MINSA.

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:

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".

[3] 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.

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. Carta Fianza del 10% del monto del contrato. Detallando la nomenclatura del procedimiento (CP 004-2021-COFIDE) y el objeto del procedimiento (Servicio de Ciberseguridad en los Sistemas de COFIDE).
b) Contrato de consorcio con firmas legalizadas ante Notario de cada uno de los integrantes de ser el caso.

c) Información indicada a continuación:

Información Bancaria (*)																			
Nombre del Banco																			
N° de Cuenta																			
N° de CCI																			
Tipo de Cuenta	Corriente					Ahorros				Otra: *Especificar*									
Moneda	PEN									USD									
N° de Cuenta de Detracción - Banco de la Nación																			
Correo electrónico de cobranzas *(para notificación del pago)*																			

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

Advertencia

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

f) Domicilio para efectos de la notificación durante la ejecución del contrato.
g) Detalle de los precios unitarios del precio ofertado[5].
h) Documento que acredite que posee derecho de uso sobre el hardware y software a utilizar para la conexión remota para las tareas relacionadas a la gestión de los dispositivos o activos, lo cual debe ser acreditado con la factura de la compra del hardware y la licencia del software o mediante una Declaración Jurada si el software ha sido desarrollado por el contratista. En el caso de utilizar servicios arrendados deberá demostrar que posee acceso al servicio y la forma de acreditarlo será con la factura del arrendamiento del servicios o documento del fabricante.
i) Documento que incluya os precios unitarios para adiciones y reducciones de (activos y horas) de los diferentes servicios que componen el Servicio de Ciberseguridad
j) Nombre y apellido, número de celular y correo electrónico del responsable de seguridad y salud en el trabajo del contratista
k) CV documentado donde se detalle el cumplimiento de todo el personal solicitado en el numeral 4 del requerimiento incluido en el Capítulo III de las presentes bases.
l) Declaración jurada solicitada por COFIDE (Anexo COFIDE 1).
m) Declaración jurada del representante legal (Anexo COFIDE 2)

[4] 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/

[5] Incluir solo en caso de la contratación bajo el sistema a suma alzada.

Importante

- *En caso que el postor ganador de la buena pro sea un consorcio, las garantías que presente este para el perfeccionamiento del contrato, así como durante la ejecución contractual, de ser el caso, además de cumplir con las condiciones establecidas en el artículo 33 de la Ley y el artículo 148 del Reglamento, deben consignar expresamente el nombre completo o la denominación o razón social de los integrantes del consorcio, en calidad de garantizados, de lo contrario no podrán ser aceptadas por las Entidades. No se cumple el requisito antes indicado si se consigna únicamente la denominación del consorcio, conforme lo dispuesto en la Directiva "Participación de Proveedores en Consorcio en las Contrataciones del Estado".*

- *En los contratos periódicos de prestación de servicios en general que celebren las Entidades con las micro y pequeñas empresas, estas últimas pueden otorgar como garantía de fiel cumplimiento el diez por ciento (10%) del monto del contrato, porcentaje que es retenido por la Entidad durante la primera mitad del número total de pagos a realizarse, de forma prorrateada en cada pago, con cargo a ser devuelto a la finalización del mismo, conforme lo establece el numeral 149.4 del artículo 149 del Reglamento y numeral 151.2 del artículo 151 del Reglamento. Para dicho efecto los postores deben encontrarse registrados en el REMYPE, consignando en la Declaración Jurada de Datos del Postor (Anexo N° 1) o en la solicitud de retención de la garantía durante el perfeccionamiento del contrato, que tienen la condición de MYPE, lo cual será verificado por la Entidad en el link http://www2.trabajo.gob.pe/servicios-en-linea-2-2 opción consulta de empresas acreditadas en el REMYPE.*

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

Importante

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

- *De conformidad con el Reglamento Consular del Perú aprobado mediante Decreto Supremo N° 076-2005-RE para que los documentos públicos y privados extendidos en el exterior tengan validez en el Perú, deben estar legalizados por los funcionarios consulares peruanos y refrendados por el Ministerio de Relaciones Exteriores del Perú, salvo que se trate de documentos públicos emitidos en países que formen parte del Convenio de la Apostilla, en cuyo caso bastará con que estos cuenten con la Apostilla de la Haya[6].*

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

2.4. PERFECCIONAMIENTO DEL CONTRATO

El contrato se perfecciona con la suscripción del documento que lo contiene. Para dicho efecto el postor ganador de la buena pro, dentro del plazo previsto en el artículo 141 del Reglamento debe presentar la documentación requerida en la mesa de partes de COFIDE sito en Calle Augusto Tamayo Nº 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).

[6] Según lo previsto en la Opinión N° 009-2016/DTN.

2.5. FORMA DE PAGO

La Entidad realizará el pago de la contraprestación pactada a favor del contratista en 36 cuotas mensuales.

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

- Comprobante de pago (deberá ser remitido al email facturaselectronicas@cofide.com.pe, es el único correo formal para su presentación).
- Entregables según términos de referencia.
- Acta de conformidad emitida por la Gerencia Usuaria.

Dicha documentación de debe presentar en mesa de partes de COFIDE, sito en Calle Augusto Tamayo N° 160, San Isidro.

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

El presente proceso de selección tiene como objeto la contratación de un proveedor especializado que realice las operaciones sobre los equipos de seguridad y se encargue del monitoreo de los equipos con el objetivo de alertar de manera temprana y realizar la gestión del ciclo de vida completo de los incidentes de Ciberseguridad que se presenten desde la identificación, análisis, respuesta y recuperación ante incidentes.

2 FINALIDAD PÚBLICA

La presente contratación pública tiene como finalidad garantizar la continuidad y seguridad de los servicios y procesos de COFIDE.

El presente servicio se alinea con los objetivos estratégicos de la corporación:

Alcance	Objetivo Estratégico Institucional	Objetivo Estratégico de TI
Financiero	OEI5: Asegurar la sostenibilidad institucional de COFIDE	OE3: Gestionar los Servicios de TI de manera eficiente y oportuna para un adecuado soporte de la operación en COFIDE

3 INFRAESTRUCTURA DEL PROVEEDOR

Ver Anexo C.

4 EQUIPO DE TRABAJO

El perfil mínimo del personal requerido que garantice un adecuado servicio se detalla a continuación:

Servicio	Rol	Formación	Experiencia	Capacitación y/o Certificación	
Gobierno y gestión del servicio	**PERSONAL CLAVE** (01) Director del Proyecto	Titulado como Ingeniería electrónica,	Mínimo 3 años en proyectos de Cibersegurid	Por lo menos 01 de los	Por lo menos 01 de las siguientes certificaciones:

Servicio	Rol	Formación	Experiencia	Capacitación y/o Certificación	
	<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	Sistemas, Telecomunicaciones y Redes, Ingeniero Informático y/o Ingeniero Industrial y/o Ingeniero de Sistemas	ad de TI, Seguridad de la Información, Seguridad Informática, Configuración de seguridad en redes y nube.	siguientes cursos: -Diplomado en Gerencia de Proyectos o Diplomado en Seguridad Informática, o Curso en seguridad de la información o curso de Ciberseguridad de por lo menos 40 horas	Certificación PMP o ISO 21500 Gerente de Proyectos, vigente o Certificación PRINCE2 - Certificación en ISO 27001 implementador líder o Certificación en ISO 27032 Gerente de Ciberseguridad vigente o (ISACA)Certified Information Security Manager (CISM) o Certificado CISSP (vigente) -Otros certificados relacionados a Ciberseguridad o Gestión de Proyectos.
	(01) Arquitecto de Seguridad **<u>Función</u>**: Profesional encargado del diseño técnico de los servicios, debe entender la realidad de COFIDE y plantear la arquitectura más eficiente y que mayor protección brinde	Bachiller en las carreras de Ingeniería Informática y/o telecomunicaciones y redes y/o Ingeniería de Sistemas e Informática	Mínimo con 3 años en proyectos de Ciberseguridad de TI, Seguridad de la Información, Seguridad Informática, Configuración de seguridad en redes y nube.	Por lo menos 02 de los siguientes cursos: -Cursos de arquitectura de Ciberseguridad y/o cursos de seguridad de la información y/o cursos en Ciberseguridad -Cursos de seguridad informática -Cursos de seguridad en redes	Por lo menos 01 de las siguientes certificaciones: -CompTIA Security+, vigente -Analista de Seguridad Certificado - EC-Council Certified Security Analyst (ECSA), vigente -(ISC) Certified Information Systems Security Professional (CISSP), vigente -Certificación en el marco de trabajo para la Ciberseguridad de la NIST, vigente -SandBlast

Servicio	Rol	Formación	Experiencia	Capacitación y/o Certificación	
				- Capacitación por el fabricante de las marcas de los productos que ofrezca el Contratista para proveer cada uno de los servicios de Ciberseguridad.	Mobile Security Administrator -SandBlast Accredited Administrator -IDSA: Database Security Associate Certificate Exam (DBF) -Lead Cybersecurity Professional Certificate (LCSPC) -Certificación en ISO 27001 implementador líder -Otros certificados relacionados a Ciberseguridad.
	(01) Service Manager Punto único de contacto de COFIDE con relación al servicio. Responsable del cumplimiento contractual y de la correcta ejecución del servicio	Titulado como Ingeniería Informática y/o Ingeniero Industrial y/o Ingeniería de Computación y Sistemas y/o Ingeniería de Sistemas e Informática	Mínimo 2 años en proyectos de Ciberseguridad de TI, Seguridad de la Información, Seguridad Informática, Configuración de seguridad en redes y nube.	Por lo menos 01 de los siguientes cursos: -Cursos de Gerencia de Proyectos por lo menos 40 horas -Curso de preparación para la certificación internacional PMP por 48 horas lectivas - Curso en seguridad de la información o Ciberseguridad de por	Por lo menos 01 de las siguientes certificaciones: Certificación en ISO 27001 implementador líder o ISO 27032 Gerente de Ciberseguridad o Certificación ITIL v3 o v4 Foundation vigente o certificado CRISC o certificado CDPS o Certificate LCSPC o Certificación en seguridad de la información o Certificación en Advanced Threat Defense -Otros certificados relacionados a Ciberseguridad o

Servicio	Rol	Formación	Experiencia	Capacitación y/o Certificación	
				lo menos 40 horas -Cursos en Gestión de Servicios de Tecnologías de la Información por lo menos 40 horas	Gestion de Servicios TI.
S1 - Servicio de evaluación de Seguridad TI	Gestor de riesgos sobre activos TI Profesional encargado de liderar la evaluación de las soluciones de seguridad de COFIDE. Valida y aprueba el trabajo realizado por los analistas	Profesional titulado y/o Bachiller en las carreras de Ingeniería Informática y/o Ingeniero Industrial y/o ingeniero informático y de sistemas y/o Ingeniería de Sistemas Empresariales	Mínimo 3 años en proyectos de Ciberseguridad de TI, Seguridad de la Información, Seguridad Informática, Configuración de seguridad en redes y nube.	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 Certificación en el marco de trabajo para los sistemas de seguridad de la NIST	Por lo menos 01 de las siguientes certificaciones: -GIAC Certified Forensic Analyst (GCFA) -Certified Ethical Hacker CEH -Certified Penetration Testing Engineer - CPTE -Certified Secure Web Application Engineer - CSWAE. - 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

Servicio	Rol	Formación	Experiencia	Capacitación y/o Certificación	
					Herramientas de Ciberseguridad o Seguridad TI.
	Analista(s) de riesgos TI Profesionales encargados de realizar el análisis de las soluciones de seguridad, encontrar las brechas y plantear planes de acción	Titulado y/o Bachiller como Ingeniería Informática y/o Ingeniería Industrial y/o Ingeniería de Sistemas e Informática y/o Ingeniería de Sistemas y Computación	Mínimo 2 años en proyectos de Ciberseguridad de TI, Seguridad de la Información, Seguridad Informática, Configuración de seguridad en redes y nube.	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: -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 los Equipos o Soluciones de Seguridad	Analista(s) de operación de equipos y soluciones de seguridad Profesionales encargados de la ejecución de los cambios y requerimientos en las plataformas que estén bajo	Titulado y/o Bachiller como Ingeniero Informático y/o Ingeniero Industrial y/o Ingeniería Industrial Sistemas e Informática	Mínimo 2 años en gestión y operación de equipos y soluciones de seguridad (WAF, WAN, Firewall, IPS, IDS, entre otros)	Cursos de operación y/o administración de equipos y soluciones de seguridad de las marcas que se van a operar	Por lo menos 01 certificación del fabricante de los productos que el Contratista operará (Fortinet o Kaspersky o Forcepoint)

Servicio	Rol	Formación	Experiencia	Capacitación y/o Certificación	
	administración del PROVEEDOR.	Técnico en informática, computación o sistemas		por lo menos 40 horas	
S3 - Servicios de Detección Avanzada	Arquitecto de seguridad	Definido en los roles generales			
	PERSONAL CLAVE Gestor de Seguridad Líder del equipo SOC gestiona el monitoreo y análisis de los eventos y la respuesta a los incidentes	Titulado y/o Bachiller como Ingeniería Informática y/o Ingeniería Industrial y/o Ingeniería Electrónica y/o ingeniería de sistemas y/o Ingeniería Sistemas e Informática	Mínimo 3 años en: - Identificación, clasificación, análisis de eventos de seguridad - Identificación y gestión de incidentes de seguridad -Gestión y operación de soluciones SIEM	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	Titulado y/o Bachiller	Mínimo 2 años en	Por lo menos 01	Entre los Analistas de

Servicio	Rol	Formación	Experiencia	Capacitación y/o Certificación	
	Profesionales encargados del monitoreo y análisis de eventos de seguridad. Brindan soporte nivel 0 y 1 ante los incidentes que se presenten	como Ingeniería Informática y/o Ingeniería Industrial y/o Ingeniería Electrónica y/o Ingeniería de Sistemas y/o Ingeniería de Sistemas Computo y Telecomunicaciones y/o Técnico en informática, computación o sistemas y/o Técnico en redes y comunicaciones	cualquiera de los 3 criterios mencionados: - Identificación, clasificación, análisis de eventos de seguridad - Identificación y gestión de incidentes de seguridad -Gestión y operación de soluciones SIEM	de los siguientes cursos: Cursos de identificación y clasificación de eventos de 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	seguridad asignados, cuenten cada uno con al menos una certificación en tecnologías o 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

Servicio	Rol	Formación	Experiencia	Capacitación y/o Certificación	
				de la información	
S4 - Servicios Respuesta a Incidentes como Servicio	Especialista en gestión de incidentes Profesionales encargados de la respuesta a incidentes graves de Ciberseguridad, brindan el nivel 3 de respuesta	Titulado y/o Bachiller como Ingeniería Informática y/o Ingeniero Industrial y/o Ingeniería de Sistemas y/o Técnico en redes y comunicaciones	Mínimo 3 años liderando SOCs y/o equipos de gestión de incidentes	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 01de 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 Profesionales encargados de la respuesta a incidentes graves de Ciberseguridad, brindan el nivel 2 de respuesta	Titulado y/o Bachiller como Ingeniero Informático y/o Ingeniero Industrial y/o Ingeniero de sistemas y/o Técnico en informática, computación y/o sistemas y/o	Mínimo 2 años en operaciones de SOCs (incidentes de seguridad de la información)	Por lo menos 01 de los siguientes cursos: -Cursos de gestión (identificación, clasificación, generación de planes, respuesta, contención, erradicación y recuperaci	Contar con al menos 01 certificaciones, como por ejemplo: -Certificado ISO 27035 Incidente Manager - Gestión y respuesta ante incidentes -Lead Cybersecurity Professional Certificate (LCSPC) -Certificado ISO 27032

Servicio	Rol	Formación	Experiencia	Capacitación y/o Certificación	
		Técnico en redes y comunicaciones y/o Técnico en Computación e Informática		ón) de incidentes por lo menos 40 horas -Cursos en soluciones de seguridad por lo menos 40 horas -Seguridad informática de 25 horas	-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.

5 DESCRIPCIÓN DEL SERVICIO

5.1 Alcance del Servicio

El servicio de Ciberseguridad a contratar por COFIDE comprende la siguiente prestación principal:

Ítem	Descripción	Cantidad
Único	- S1 - Servicio de evaluación de Seguridad TI - S2 - Servicio de Gestión de los Equipos o Soluciones de Seguridad - S3 - Servicios de Detección Avanzada - S4 - Servicios Respuesta a Incidentes como Servicio	01 servicio

5.2 Situación Actual

COFIDE cuenta con una sede principal, ubicada en Calle Augusto Tamayo 160, San Isidro, que cuenta con un Centro de Cómputo Principal (CCP) propio, donde se realiza el procesamiento de datos e información de forma sistematizada.

COFIDE, como parte de su Plan de Continuidad de Negocio, también cuenta con un contrato de servicio de housing o alojamiento del Centro de Cómputo Alterno (CCA), el cual nos permite alojar equipamiento propio y arrendado, así como replicar desde CCP la operación e información crítica frente a cualquier eventualidad o recuperación de desastres. Este servicio

adicionalmente nos brinda enlaces de comunicaciones y servicios complementarios igualmente necesarios para la operación de ambos Centros de Cómputo. En la actualidad, el CCA contratado se encuentra ubicado en Av. Manuel Olguin 395, Surco, de la empresa CenturyLink Perú.

A continuación, se muestra una gráfica y descripción de las plataformas tecnológicas que se encuentran habilitadas actualmente en ambos sites.

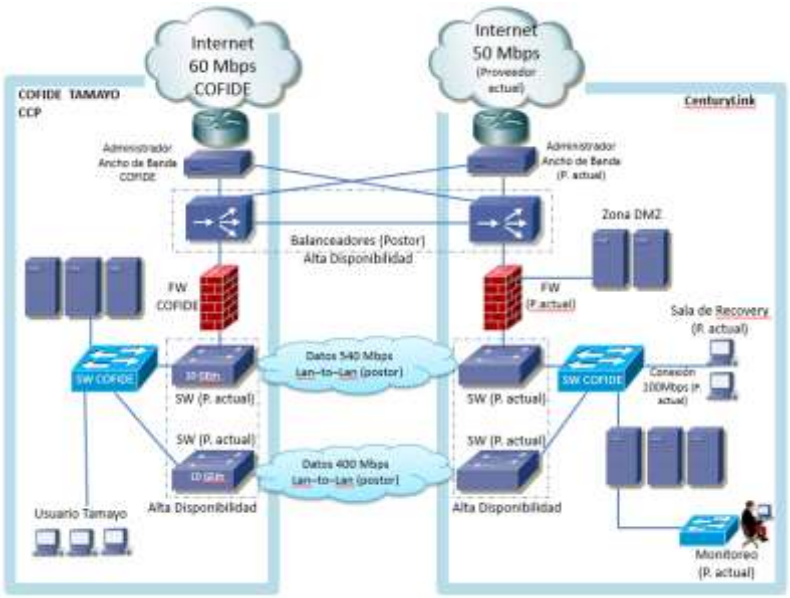


Diagrama General de Servicios actuales

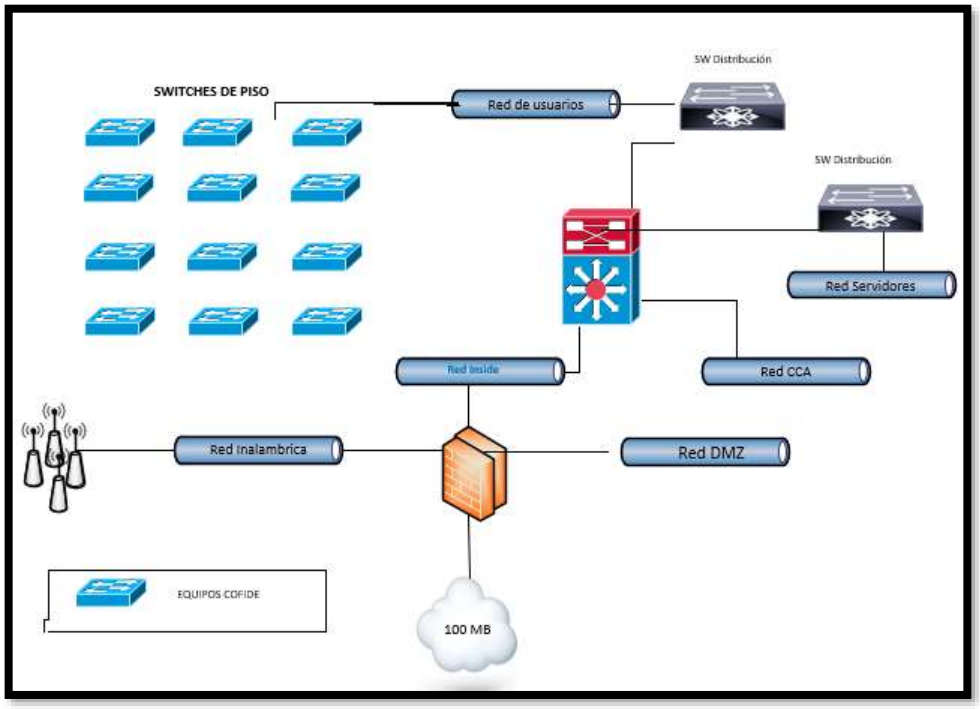
La comunicación entre el site principal (CCP) y el site alterno CCA se encuentra basada en una red LAN extendida, conectadas entre sí mediante switches en stack (redundantes) de propiedad del actual proveedor del servicio, el medio de comunicación es fibra óptica, formando un anillo de comunicación entre el CCP y CCA.

Infraestructura de redes, comunicaciones y seguridad

a. **Infraestructura de Redes**

La Plataforma computacional principal de COFIDE es soportada por una red Giga Ethernet, cuya conexión tiene un ancho de banda en promedio de 1 Gbps. Las estaciones de trabajo están distribuidas en un edificio principal de doce (12) pisos con aproximadamente 250 usuarios.

La red de COFIDE tiene como Core Switch de Datos una solución redundante, interconectada con una capa de distribución y una capa de acceso. Las conexiones de COFIDE usan el protocolo TCP/IP y emplean 4 segmentos de IPs (VLANS).



Red interna sede Tamayo

5.3 Detalle del Servicio

1. S1 - Servicio de evaluación de Seguridad TI

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

El servicio S1 se ejecuta al inicio durante los dos (02) primeros meses y 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, análisis de la configuración), la misma que deberá ser presentada en la fase de transición del servicio, arrojando como resultado una hoja de ruta para la mejora de los activos TI en términos de seguridad, lo cual puede incluir:

- 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 DE
COFIDE	08

Cantidad de Activos del servicio S1

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

(1) Políticas del Servicio.

Este servicio considera las siguientes políticas:

a. Trabajar con el total de los activos TI proporcionados por COFIDE.
b. El postor puede aplicar la metodología que considere conveniente basado en cumplir con el objetivo del servicio y los SLAs.
c. Los tiempos de las actividades serán coordinadas en la etapa de planificación y en ella se definirán las ventanas de recopilación de información
d. 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 a satisfacción de COFIDE.
e. 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.

(2) Actividades

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

a. **Preparación e inicio.** Se presentará el plan de trabajo y los requerimientos necesarios para la ejecución del servicio. Esta fase contempla lo siguiente:

1. Presentación del equipo de trabajo.
2. Establecimiento de los mecanismos de comunicación y seguimiento.

Resultados
1. Cronograma con el detalle de actividades para ejecutar el servicio.
2. Agenda de entrevistas con el personal de COFIDE.
3. 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:

1. Levantamiento de Información de los activos que forman parte del alcance.(ver Línea Base S1)
2. 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.
3. 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:

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

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

d. **Elaboración de los planes de acción y mejora.** El Contratista deberá presentar los siguientes entregables:
1. Informe técnico con los resultados de la evaluación de riesgos, el cual debe indicar los riesgos identificados, planes de acción y recomendaciones de mejora.
2. Inventario de los activos evaluados durante la ejecución del servicio.
3. Informe ejecutivo con el detalle de las fases ejecutadas.

(3) 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:

Activo	Cantidad	Marca	Modelo
Firewall (FORTIGATE 500D) Consola de gestión Fortimanager	2	FORTINET	FORTIGATE 500D
IPS (MCAFEE NS7300) Consola de gestión McAfee NSM	1	MCAFEE	NS7300
Filtro Web (WEBSENSE V5000 G3) Consola de gestión TRITON	1	FORCEPOINT	V5000 G3
Antispam (Proofpoint Email Protección SaaS)	1	PROOFPOINT	SAAS

Antivirus (KARSPERSKY 11) Consola de gestión KSC	1	KARSPERSKY	v11
EDR (KARSPERSKY Advanced EDR with Sandbox)	1	KARSPERSKY	ADVANCED EDR CON SANDBOX
WAF (SaaS	1	Fortinet	Forticloud

Línea base del servicio S1

Consideraciones

a. El Contratista deberá contar con personal calificado, con experiencia y conocimiento para realizar la evaluación de riesgos de seguridad de los activos TI.

b. De requerir recursos tecnológicos (hardware o software) para ejecutar el servicio, el Contratista deberá proporcionarlo a su equipo de trabajo asignado.

(4) Facilidades Mínimas

Los recursos mínimos requeridos para este servicio son:

a. Procesos o Metodologías

1. Metodología para la apreciación de riesgos de activos TI.

b. Personal

El Contratista deberá contar como mínimo con el siguiente equipo:

Ítem	Roles	Fase
1	Gestor de riesgos sobre activos TI.	Gestión y Operación
2	Analistas de riesgos TI.	Gestión y Operación

Personal para el Servicio S1

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

(5) Tecnologías

1. Correo electrónico corporativo del Contratista para coordinaciones.
2. Sistemas de videoconferencia para realizar las coordinaciones.
3. Estaciones de trabajo para los recursos humanos proporcionado por el Contratista.
4. 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) 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 evaluación de riesgos de los activos TI.
b. Planificar las etapas de evaluación de riesgos de los activos TI y sus limitaciones respecto de su ciclo de vida.
c. Garantizar que el servicio se realizará considerando la evaluación de una muestra de activos por tipología.
d. Agendar con la debida anticipación las entrevistas con el personal de COFIDE en la etapa de levantamiento de información de los activos TI.
e. 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.

(7) Responsabilidades de COFIDE

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

a. Durante la implementación o transición del servicio:
  1. Remitir información adecuada y correcta de los inventarios actualizados de los activos TI y su contexto.
  2. Designar el personal de contacto autorizado para el servicio.

b. Durante el servicio:
  1. Designar a las personas con responsabilidad suficiente, que serán autorizadas para servir como coordinadores del servicio.

(8) Entregables del servicio

El contratista debe presentar los siguientes entregables por única vez al finalizar el servicio:

a. Informe técnico con los resultados de la evaluación de riesgos, el cual debe indicar los riesgos identificados, planes de acción y recomendaciones de mejora.
b. Inventario de los activos evaluados durante la ejecución del servicio.
c. Informe ejecutivo con el detalle de las fases ejecutadas.

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)

2. 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 la configuración de los firewalls, IPS, IDS, entre otros equipos de seguridad perimetral y soluciones de seguridad.

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 y en el primer mes la sugerencia de arrendar equipos o soluciones que se integren al modelo del servicio. Este servicio se cotiza por la cantidad de activos TI a operar. A continuación, presentamos las la cantidad de activos a considerar para este servicio:

EMPRESA	CANTIDAD DE ACTIVOS
COFIDE	04

Cantidad de Activos del servicio S2

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

(9) 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.
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.

(10) Actividades

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

a. Gestión de la infraestructura de Seguridad

1. Supervisión.
2. Soporte especializado para los equipos y las soluciones de seguridad indicadas.
3. Administración delegada la cual tiene como funcionalidades la atención de requerimientos y atención de incidentes.

b. Monitorización de Seguridad

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

c. Planes de mejora

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

(11) 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:

Activo crítico	Cantidad	Marca	Modelo	Características habilitadas	Cantidad de puertos activos	Cantidad de usuarios asociados al activo
Firewall (FORTIGATE 500D)	2	FORTINET	FORTIGATE 500D	Firewall	4	
Filtro Web (WEBSENSE V5000 G3)	1	FORCEPOINT	V5000 G3	Web filter		350
Antivirus (KARSPERSKY 11)	1	KARSPERSKY	11	Karspersky Security Center y Karspersky Endpoint Security		500

Línea base del servicio S2

(12) Facilidades Mínimas

Los recursos mínimos requeridos por este servicio son:

a. Procesos o Metodologías

1. Metodología para la atención de requerimientos de operación del servicio

b. Personal

El Contratista deberá contar como mínimo con el siguiente equipo:

Ítem	Roles	Fase
1	Analistas de operación de equipos y soluciones de seguridad.	Gestión y Operación

Personal para el Servicio S2

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

(13) Tecnologias

1. Estaciones de trabajo para los recursos humanos proporcionado por el Contratista.
2. Conectividad para acceso hacia los equipos y soluciones de seguridad.

Nota: El contratista debe demostrar que posee derecho de uso sobre el hardware y software a utilizar para la conexión remota para las tareas relacionadas a la gestión de los dispositivos o activos, lo cual debe ser acreditado con la factura de la compra del hardware y la licencia del software o mediante una Declaración Jurada si el software ha sido desarrollado por el contratista. En el caso de utilizar servicios arrendados deberá demostrar que posee acceso al servicio y la forma de acreditarlo será con la factura del arrendamiento del servicio. La documentación señalada deberá ser presentada a la suscripción del contrato.

(14) 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. Realizar la supervisión, mantenimiento (Correctivo/Preventivo) y soporte especializado para los activos entregados en administración. Para los mantenimiento correctivos (RMA) y escalamiento de casos con el fabricante estos serán derivados con el proveedor de cada una de las tecnologías.
d. 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.
e. Realizar la vigilancia constante del perímetro y las operaciones internas, para identificar y hacer tratamiento a las brechas de seguridad.

f. Garantizar la atención proactiva de incidentes 7x24 con calidad de servicio especializada.
g. Realizar el servicio cada vez que COFIDE realice un requerimiento y reportar los resultados con una frecuencia mensual durante el período del contrato.
h. 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.

(15) 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.

(16) Entregables del servicio

El contratista debe presentar los siguientes entregables de forma mensual:

a. 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 en los casos que aplique.

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) y en medio físico (mesa de partes).

3. S3 - Servicios de Detección Avanzada

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. El servicio debe ser proporcionado con la experiencia de búsqueda de amenazas de un Centro de Operaciones de Seguridad (En adelante “SOC”).

Este servicio se realiza de manera continua y perenne (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:

- 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.

- 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.

- Una de las principales tareas del servicio de SOC es clasificar las alertas conforme se van recibiendo.

- 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.
- 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.
- 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 y la estimación de la cantidad de Eventos por Segundo (En adelante "EPS") que pueden generar, así como los casos de uso configurados, la cantidad de servidores y las licencias de soluciones Security Information and Event Management (En adelante "SIEM")). A continuación, presentamos la cantidad de activos y la cantidad de EPS:

EMPRESA	CANTIDAD DE ACTIVOS	CANTIDAD DE EPS ESTIMADOS
COFIDE	09	1300

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 proporcionara 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:

(17) **Políticas del Servicio.**

Este servicio considera las siguientes políticas:

a. De no llegar a cubrir los EPS incluidos en la línea base COFIDE podrá agregar equipos al servicio sin costo adicional, hasta cubrir la brecha presentada en coordinación y revisión entre COFIDE y el POSTOR.

b. Realizar la recolección de los logs de los diversos activos que han sido seleccionados para ser monitoreados.
c. Realizar la normalización de los logs recolectados.
d. Almacenar hasta un (01) año de información histórica.
e. 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.
f. Realizar correlación de eventos de seguridad mediante el uso de una solución tecnológica.
g. El servicio debe ser prestado en la modalidad 24x7 de manera continua.
h. La información obtenida y procesada por este servicio, debe estar almacenada en los centros de datos de COFIDE.
i. El Contratista accederá a la información obtenida y procesada resultante del monitoreo de activos a través de una conexión VPN SSL.
j. Toda la información generada y procesada por la infraestructura utilizada es propiedad de COFIDE, siendo además confidencial.
k. El Contratista deberá implementar los mecanismos físicos y lógicos de seguridad para garantizar que la información que produzca este servicio se mantenga confidencial, integra y disponible.
l. 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.
m. El Contratista debe preferir la instalación de componentes que generen ahorros de costo en la prestación del servicio sin perder las funcionalidades requeridas.
n. En caso El Contratista proponga infraestructura basada en máquinas virtuales, deberá establecer la configuración de los recursos de cada máquina virtual requerida.
o. En caso El Contratista proponga infraestructura basada en hardware deberá establecer la cantidad de unidades raqueables y consumo de energía requeridos.
p. Comunicar a COFIDE los eventos de seguridad, y de ser el caso lo incidentes de seguridad que se hayan identificado.
q. Asesorar a COFIDE en la remediación de los eventos de seguridad identificadas.
r. 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.
s. Los resultados de la prestación de este servicio serán almacenados en un portal al cual tendrá acceso COFIDE.
t. Analizar la criticidad de los incidentes de seguridad.
u. Elaborar y actualizar el plan de respuesta a incidentes.
v. Ejecutar medidas de contención de incidentes y mitigación de los impactos.
w. Considerar soluciones cuyas marcas de los últimos tres años, al menos dos hayan estado en el cuadrante líder de Gartner (Adjuntar el informe de Gartner de los tres últimos años).

(18) **Características 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 S4 para que realice un análisis, contención, erradicación, recuperación y seguimiento del incidente identificado. Esta solución debe contar con las siguientes características:

a. 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.
b. Reportar de manera inmediata cuando no pueda recolectar los logs desde los activos.
c. Hacer el correcto análisis de datos y eventos de seguridad.
d. El POSTOR propondrá la creación de 10 casos de uso basados en la experiencia del postor y las tecnologías que se van a correlacionar. Estos podrán ser actualizados, de ser el aplicable, durante la ejecución del servicio a solicitud de COFIDE o si el POSTOR considera mejorarlos.
e. Contar con inteligencia de correlación par tener un mejor análisis de eventos de seguridad contrastando bitácoras de dos o más dispositivos en ambientes seguros.
f. El equipo del SOC debe garantizar un monitoreo 24x7 para la atención a cualquier problema.
g. 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 estos cuando estos se materializan.
h. Analizar de manera oportuna las anomalías de tráfico observando patrones en bitácoras o flujos de datos.
i. Capacidad para realizar análisis de malware de día cero.

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:

1. **En el nivel 0**: Mesa de ayuda.

2. **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.

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 servicio S4 y pueden ser activados por el S3.

(19) 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:

Empresa	Requerimiento	1er parámetro		2do parámetro	
		Unidad de Medida	Cantidad	Unidad de Medida	Cantidad
COFIDE	Detección avanzada a través de una solución SIEM	Activo	09	EPS	1300

El detalle de los activos es el siguiente:

Activo crítico	Cantidad	Marca	Modelo
Firewall (FORTIGATE 500D)	2	FORTINET	FORTIGATE 500D
IPS (MCAFEE NS7300)	1	MACAFEE	NS7300
Filtro Web (WEBSENSE V5000 G3)	1	WEBSENSE	V5000 G3
Database Firewall (Imperva SecureSphere X2500)	1	IMPERVA	SECURESPHERE X2500
Antispam (Proofpoint Email Protecion SaaS)	1	PROOFPOINT	SAAS
Antivirus (KARSPERSKY 11)	1	KARSPERSKY	11
EDR (KARSPERSKY Advanced EDR with Sandbox)	1	KARSPERSKY	ADVANCED EDR CON SANDBOX
WAF	1	FORTINET	FORTICLOUD

Línea base del servicio S3

(20) Facilidades Mínimas

Los recursos mínimos requeridos por este servicio son:

a. Procesos o Metodologías

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

b. Personal

El Contratista deberá contar como mínimo con el siguiente equipo:

Ítem	Roles	Fase
1	Arquitecto de seguridad.	Transición de entrada

Ítem	Roles	Fase
2	Analistas de seguridad con experiencia en identificación, clasificación, análisis y eventual asesoría para la solución de eventos de seguridad.	Gestión y Operación

Personal para el Servicio S3

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

(21) Tecnologías

1. 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).
2. Consola de administración: Hardware ubicado en el SOC del Contratista que almacena los logs.
3. Conectividad para acceso al software y/o hardware de monitoreo.
4. Estaciones de trabajo para los recursos humanos proporcionado por el Contratista.
5. Correo electrónico corporativo del Contratista para coordinaciones.
6. 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.

(22) 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.

(23) 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.
2. 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.

(24) Entregables del servicio

El contratista debe presentar los siguientes entregables de forma mensual por empresa:

a. Informe que considera los aspectos de Monitoreo, Detección, Análisis e Interpretación de los resultados a partir del cual se podrán tomar decisiones.

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) y en medio físico (mesa de partes).

4. S4 – Servicio de 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.
- El Contratista debe ofertar el servicio de respuesta ante incidentes y emergencia de seguridad informática, con el objetivo de coadyuvar a COFIDE en la mitigación, contención y solución de las incidencias, así como en la preparación de la respuesta ante dichas emergencias.
- Diseñar todos los mecanismos necesarios de contención, análisis, respuesta, erradicación y recuperación como parte de la gestión de incidentes de seguridad.
- 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.
- 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:

EMPRESA	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:

(25) Políticas del Servicio.

Este servicio debe basarse en las siguientes políticas:

a. Realizar el registro, clasificación y atención de los incidentes de seguridad.
b. Asesora en la evaluación de los daños ocasionados por los incidentes de seguridad.
c. Asesorar 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, integra 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 antes incidentes del contratista debe estar registrado como miembro del FIRST (Forum of Incident Response and Security Teams). El contratista, para el inicio efectivo del servicio, debe presentar documentación que evidencie que es miembro del FIRST.

(26) Fase del Servicio S4

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:

1. Conocimiento de la infraestructura y de la red de COFIDE.
2. Clasificación y jerarquía de los activos de acuerdo con el valor del negocio.
3. 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 EN LAS ENTIDADES PÚBLICAS para la propuesta de la organización del servicio.
4. 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.
5. 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. Apoyo en la contención y mitigación del incidente. El Contratista deberá hacer las sugerencias y recomendaciones de las actividades que se deben realizar como parte de la respuesta de la atención del incidente reportado siguiendo estos pasos:

1. Realizar una evaluación inicial.
2. Generar recomendaciones para contener el daño y minimizar el riesgo.
3. Identificar el tipo y la gravedad del ataque.
4. Generar recomendaciones para proteger las pruebas en caso de requerir un análisis forense.
5. Notificar a los organismos externos cuando corresponda.
6. Generar recomendaciones para recuperar los sistemas.

7. Apoyar en la compilación y organización de la documentación del incidente.
8. Apoyar en la valoración de los daños del incidente.
9. Revisar las directivas de respuesta y actualización.

Dado que el servicio S3 tiene los niveles 0 y 1 del SOC, el servicio S4 considera los niveles 2 y 3 que pueden ser activados por el S3. 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:

1. **En el nivel 2**: Los analistas determinan si los datos o el sistema se han visto afectados y, de ser así, recomendarán una respuesta.

2. **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.

(27) Línea Base

El servicio contempla como línea base el siguiente alcance:

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

Línea base del servicio S4

Nota:

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

(28) Facilidades Mínimas

Los recursos mínimos requeridos para este servicio son:

a. Procesos o Metodologías

1. 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

Un Equipo de CSIRT, compuesto por lo menos por:

Ítem	Roles	Fase
1	Especialista en gestión de incidentes.	Gestión y Operación
2	Analista(s) de respuesta a incidentes en las plataformas utilizadas.	Gestión y Operación

Personal para el Servicio S4

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.

(29) Tecnologías

1. Software especializado, según requiera cada incidente (por ejemplo, software de volcado de memoria, de recuperación de datos, etc.).
2. Estaciones de trabajo para los recursos humanos proporcionado por el Contratista.
3. Correo electrónico corporativo del Contratista para coordinaciones.
4. 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.

(30) 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 y experiencia para la ejecución del servicio de respuesta a incidentes.
b. 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.

(31) Responsabilidades de COFIDE

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

a. Durante la implementación o transición del servicio:
1. Designar personal de contacto autorizado para el servicio.
2. Entregar la información requerida.

b. Durante el servicio:
1. 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.
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.

(32) Entregables del servicio

El contratista debe presentar los siguientes entregables de forma mensual por empresa:

a. Evaluación y Revisión del PROCEDIMIENTO DE GESTIÓN DE INCIDENTES DE SEGURIDAD DIGITAL EN LAS ENTIDADES PÚBLICAS
b. 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,
c. Informe de análisis forense del incidente significativo adverso que identifique las causas y las medidas para su gestión si este fuera necesario.

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) y en medio físico (mesa de partes).

6 ACUERDO DE NIVELES DE SERVICIO

a) Horario de Atención

HORARIO DE DISPONIBILIDAD DEL SERVICIO				
	S1	S2	S3	S4
Días de Disponibilidad	L-V	L-D	L-D	L-D
Hora Inicio	9 a.m.	24x7	24x7	24x7
Hora Fin	6 p.m.			
Periodo de vigencia	2 meses	36 meses		
Número de atenciones contratadas	Ilimitadas			

b) Métricas y Mediciones

El Factor Crítico de Éxito (CSF, por sus siglas en inglés) definido para el servicio es mejorar la Calidad de Servicios TI.
En este sentido, se han generado los siguiente Indicadores:

CSF	KPI
Mejorar la Calidad de los Servicios de Ciberseguridad	- Identificar los Riesgos de Ciberseguridad de los activos TI - Garantizar que los equipos y soluciones de seguridad están correctamente configurados - Minimizar los tiempos de parada de los servicios TI - Responder a las necesidades del negocio

Factores críticos de éxito

Los ANS definidos considerando las métricas para la evaluación del servicio son los siguientes:

ANS	KPI	Servicios	Métrica	Valor Objetivo	Periodo de Medición
ANS01	Identificar los Riesgos de Ciberseguridad de los activos TI	S1-Evaluación de Seguridad TI	Activos TI evaluados	100%	Por única vez
ANS02	Garantizar que los equipos y soluciones de seguridad están correctamente configurados	S2-Gestión de los equipos o soluciones de seguridad	Requerimientos atendidos de manera oportuna	95.00%	Mensual
ANS03	Minimizar los tiempos de parada de los servicios TI	S3-Detección Avanzada	Disponibilidad del servicio	99.00%	Mensual
ANS04	Minimizar los tiempos de parada de los servicios TI	S4-Respuesta a incidentes como servicio	Tiempo de Respuesta de Incidentes de Seguridad de	95.00%	Mensual

ANS	KPI	Servicios	Métrica	Valor Objetivo	Periodo de Medición
			manera oportuna		
ANS05	Responder a las necesidades del negocio	Gestión de Requerimientos (RQ) de los equipos y soluciones de seguridad	Tiempo Promedio de Respuesta inicial por email o asistencia remota (Prioridad del 4 al 1)	0.5 horas	Mensual
ANS06				01 horas	Mensual
ANS07				02 horas	Mensual
ANS08				04 horas	Mensual
ANS09			Tiempo Promedio de Respuesta presencial (Prioridad del 4 al 1)	04 horas	Mensual
ANS10				08 horas	Mensual
ANS11				24 horas	Mensual
ANS12				36 horas	Mensual
ANS13			Tiempo Promedio de Resolución por asistencia remota o presencial (Prioridad del 4 al 1)	01 horas	Mensual
ANS14				02 horas	Mensual
ANS15				04 horas	Mensual
ANS16				06 horas	Mensual
ANS17		Gestión de Incidentes	Tiempo Promedio de Respuesta inicial por email o asistencia remota	0.5 horas	Mensual
ANS18				01 horas	Mensual
ANS19				02 horas	Mensual

ANS	KPI	Servicios	Métrica	Valor Objetivo	Periodo de Medición
ANS20			(Prioridad del 4 al 1)	05 horas	Mensual
ANS21			Tiempo Promedio de Resolución por (Prioridad del 4 al 1)	01 horas	Mensual
ANS22				02 horas	Mensual
ANS23				04 horas	Mensual
ANS24				08 horas	Mensual

c) Penalidades

ANS	KPI	Servicios	Métrica	Porcentaje de Facturación Mensual
ANS01	Identificar los Riesgos de Ciberseguridad de los activos TI	S1-Evaluación de Seguridad TI	Activos TI evaluados	5%
ANS02	Garantizar que los equipos y soluciones de seguridad están correctamente configurados	S2-Gestión de los equipos o soluciones de seguridad	Requerimientos atendidos de manera oportuna	3%
ANS03	Minimizar los tiempos de parada de los servicios TI	S3-Detección Avanzada	Disponibilidad del servicio	5%
ANS04	Minimizar los tiempos de parada de los servicios TI	S4-Respuesta a incidentes como servicio	Incidentes atendidos de manera oportuna	8%

ANS	KPI	Servicios	Métrica	Porcentaje de Facturación Mensual
ANS05	Responder a las necesidades del negocio	Gestión de Requerimientos (RQ) de los equipos y soluciones de seguridad	Tiempo Promedio de Respuesta inicial por email o asistencia remota (Prioridad del 4 al 1)	3%
ANS06				3%
ANS07				1%
ANS08				1%
ANS09			Tiempo Promedio de Respuesta presencial (Prioridad del 4 al 1)	3%
ANS10				3%
ANS11				1%
ANS12				1%
ANS13			Tiempo Promedio de Resolución por asistencia remota o presencial (Prioridad del 4 al 1)	3%
ANS14				3%
ANS15				1%
ANS16				1%
ANS17		Gestión de Incidentes	Tiempo Promedio de Respuesta inicial por email o asistencia remota (Prioridad del 4 al 1)	3%
ANS18				3%
ANS19				1%
ANS20				1%
ANS21			Tiempo Promedio de Resolución por (Prioridad del 4 al 1)	3%
ANS22				3%
ANS23				1%
ANS24				1%

Cada mes se podrá aplicar una penalidad máxima del 10% de la facturación mensual.

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.

d) Informes Mensuales

Son informes tácticos que incluyen:

1. Cumplimiento de indicadores corporativos (SLA's)
2. Cuadro de control de semáforo.
3. Gráficos de rendimiento y tendencias.
4. Planes de acción correctivo con fecha de compromiso dentro de los plazos del contrato.
5. Consumos efectivos de capacidades contra la Línea Base.

7 ETAPAS DEL SERVICIO

El PROVEEDOR del servicio debe considerar las siguientes etapas del servicio:

FASES	MESES DE LOS SERVICIOS													
	(UN MES)	(UN MES)	(UN MES)	MES 1	MES 2	MES 3	MES 4	…	MES 8	…	MES 33	MES 34	MES 35	MES 36
Planificación	Plan.													
Transición de entrada		Transición de Entrada												
Ejecución / operación				Fase de Gestión y Operación del Servicio (36 meses)										
Transición de salida												Transición de Salida (03 meses)		

7.1 Etapa Planificación:

Esta etapa se inicia al día útil siguiente de la firma del contrato, en esta etapa el PROVEEDOR realizará la planificación del proyecto. Específicamente, el PROVEEDOR deberá preparar los siguientes entregables:

Entregables Generales

a. Plan de proyecto:

1. Plan de Proyecto, EDT, cronograma y matriz RACI.

b. **Plan de comunicaciones:** que debe incluir

1. Procedimiento de gestión de incidentes y problemas del proyecto.
2. Identificación de objetivos comunicacionales del proyecto y por servicio.
3. Determinación de estrategias de comunicación del proyecto y por servicio.
4. Identificación de partes interesadas o agentes relacionados del proyecto y del servicio.

c. Plan de riesgos:

1. Matriz de Riesgos del Proyecto (identificación, control y mitigación).

d. Plan de pruebas:

1. Protocolo de inspección y pruebas de recepción (incluye formatos).

e. **Plan de cierre de planeamiento del proyecto:** que debe incluir como mínimo:

1. Procedimiento de control de cambios
2. Procedimiento de gestión de la propiedad intelectual de la información:
3. Determinación del inventario de activos de información a evaluar durante el servicio.
4. Determinación de cuál de las partes es la responsable de su creación o generación.

Entregables de Planificación por servicio:

Servicio¨	Entregable de la planificación
S1 - Evaluación de Seguridad TI	● Plan para desarrollar procedimientos y formatos necesarios para la evaluación de seguridad de los activos TI. ● Plan de comunicaciones para el desarrollo del servicio.
S2 - Gestión de los equipos o soluciones de seguridad	● Plan para desarrollar procedimientos y formatos necesarios para realizar la gestión y operación de los equipos o soluciones de seguridad. ● Plan de comunicaciones para este servicio.
S3 - Detección Avanzada	● 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. ● Plan de comunicaciones para el desarrollo del servicio.

Servicio¨	Entregable de la planificación
S4 -Respuesta a incidentes como servicio	● Plan para desarrollar procedimientos y formatos necesarios para realizar la respuesta a incidentes como servicio. ● Plan de comunicaciones para el desarrollo del servicio.
Todos los servicios	● Manuales para el uso del portal de información. ● Manuales para el uso del portal de atención de requerimientos e incidentes del proyecto. ● Ficha técnica de los equipos y soluciones que presentarán en los servicios (deben ir como anexos dentro de la propuesta técnica) ● Procedimientos y formatos para solicitud de incremento/decremento 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. **Nota:** Los manuales deben estar en idioma español

Entregables por Servicio

La presentación de los entregables será como máximo hasta (07) días antes del fin de la fase de planificación. Se suscribirá un Acta de Conformidad de la Fase de Planeamiento.

7.2 Etapa de Transición de Entrada

Esta etapa se inicia al día siguiente de la firma del Acta de Conformidad de la Fase de Planeamiento. Se debe desarrollar la transición de los servicios las siguientes políticas y estrategias generales:

a. 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.
b. En la fase de planeamiento del Servicio El Contratista deberá desarrollar un Plan de Transición por cada servicio a detalle con COFIDE.
c. 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).
d. Para aquellos servicios que requieran la instalación, despliegue y configuración de componentes (Hardware, software y/o servicios) sobre la infraestructura de

COFIDE a implementarse durante en esta fase de la transición de entrada, El Contratista realizará dichas instalaciones y configuraciones en una ventana de tiempo coordinada entre El Contratista y COFIDE a fin de minimizar el impacto en el negocio.

e. El Contratista 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.

f. El personal del Contratista debe seguir los protocolos de seguridad de acuerdo con los planes de vigilancia contra el COVID-19 establecidos por COFIDE.

Plan de despliegue de Servicios

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

a. Preparación: Ejecutar las actividades de la planificación, coordinación y alistar los recursos necesarios (metodologías, personas, tecnología e infraestructura) para los servicios.

b. 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 deben estar desplegados e instalados en seis (60) días.

c. Pruebas de Recepción: Es la etapa de verificación del correcto despliegue de los servicios de Ciberseguridad.

Para el despliegue de los servicios se seguirá la siguiente referencia:

Ítem	Servicios	Entregable
1	S1	- Agenda de entrevistas con el personal de COFIDE. - Inventario de activos con detalles técnicos por cada empresa. - Metodología para la apreciación de riesgos de activos TI. - Estructura de los documentos base para ejecutar el servicio.
2	S2	- Metodología para la atención de requerimientos de operación. - Configuración de la conectividad mediante VPN para acceso hacia los equipos y soluciones de seguridad. - Acta de recepción definitiva del servicio.
3	S3	- Metodología para la evaluación de eventos de seguridad. - Metodología para analizar los resultados de la correlación. - Metodología para configurar los casos de uso nuevos.

Ítem	Servicios	Entregable
		- 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. - Acta de recepción definitiva del servicio. - Procedimiento para realizar la integración del SIEM en los equipos y soluciones que son gestionados por los proveedores de COFIDE.
4	S4	- Metodología para la gestión de incidentes, en sus diferentes etapas, lo que debe incluir como mínimo la identificación, clasificación, análisis, análisis forense para determinar las causas si se requiere., elaboración de planes de respuesta, planes de contención, planes de erradicación y planes de restauración.
5	Todos los servicios	- Configuración del Portal de atención de requerimientos e incidentes del proyecto. - Configuración del Portal de información. - Herramienta de Gestión de Servicios

Guía para la implementación de servicios

Responsabilidades de El Contratista

a. Realizar las coordinaciones con COFIDE para realizar el despliegue e instalación de la infraestructura en los equipos y soluciones que son gestionados por terceros.
b. 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.
c. 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.
d. Ser responsable por el mantenimiento, salvaguarda y respaldo de las configuraciones (Hardware, software y/o servicios) utilizadas para la ejecución de los servicios.

e. 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.

Responsabilidades de COFIDE

a. Entregar toda la información solicitada por El Contratista.
b. Brindar información acerca de las redes y componentes TI.
c. 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.
d. 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

Al finalizar esta etapa, se suscribirá un Acta de Inicio de la Etapa Operativa como conformidad de la correcta transición de los servicios a conformidad de COFIDE.

7.3 Etapa de Gestión y Operación del Servicio

Esta etapa se inicia al día siguiente de la firma del Acta de Inicio de la Etapa Operativa. 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:

a. 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*.
b. Los servicios de operación deben estar basados en buenas prácticas o estándares internacionales de seguridad y calidad como ISO 27001, ISO 9000 o ISO 20000. Se recomienda que el proveedor tenga al menos dos certificaciones, siendo obligatoria la ISO 27001.
c. 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.
d. Monitoreo de la Disponibilidad del Servicio: eventos que informan sobre la interrupción o indisponibilidad por conectividad para el servicio S8. Se deberá proveer un *Portal de Información*, donde COFIDE 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 gestión y monitoreo de los servicios en un formato ITIL (Eventos, Incidentes, Capacidad, etc.)
e. Monitoreo del tiempo de respuesta de los servicios S5 y S12, midiendo periódicamente los tiempos de respuesta de estos, de acuerdo con lo establecido en el *acuerdo de nivel de servicio*.
f. 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.

g. 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.

h. Administración de Cambios: Registro, seguimiento, colección de las aprobaciones y actualización hasta la atención de los Cambios Operacionales.

i. 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.

j. 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 2011/4 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:

1. Nivel de adherencia a los procedimientos e instructivos definidos.

2. 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.

Adicionalmente, durante esta fase, COFIDE podrá solicitar a El Contratista, la inclusión de capacidades adicionales para soportar nuevos activos y/o usuarios. Las condiciones para que estas nuevas capacidades sean aceptadas serán similares a las descritas en la fase de Transición de Entrada.

(a) Políticas del Servicio

a. Mantener la confidencialidad de la información de configuración, accesos, información recopilada y derivada durante la prestación del servicio

b. 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 cinco (05) políticas base, que constituirán las reglas básicas para su atención.

(1) Política de Monitoreo de Servicios

a. El Contratista debe poseer umbrales de capacidad y desempeño que garanticen la continuidad de los servicios de Ciberseguridad, por ejemplo:

1. Disco: Alerta Menor al 90% de capacidad, Alerta Critica al 95% de capacidad, Alerta Fatal al 98% de capacidad.

2. Almacenamiento: Alerta Menor al 90% de capacidad, Alerta Critica 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 garanticen los niveles de servicio necesarios.

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

(2) Política de Cambios

a. 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, de acuerdo con la siguiente matriz de Riesgos de los Cambios.

Riesgo	Características
4 – Extremo	Tiene el más alto factor de riesgo, así como el potencial de un impacto crítico sobre los objetivos de nivel de servicio. Estos cambios normalmente requieren planeamiento extensivo, programación, actividad de coordinación entre los múltiples grupos de soporte, y en ocasiones extensiones a la ventana de mantenimiento normal.
	Adicionalmente, este riesgo de cambio es típicamente implementado de a pasos sobre un periodo de tiempo extendido.
3 – Alto	Los cambios mayores típicamente tienen un mayor factor de riesgo y un potencial impacto significativo sobre los objetivos de nivel de servicio.
	Estos cambios también requieren planeamiento extensivo, programación, y coordinación de actividades entre los múltiples grupos de soporte.
	Adicionalmente, este riesgo de cambio puede implementarse en pasos sobre un periodo de tiempo extendido cuando sea posible.
2 - Medio	Los cambios medios tienen un factor de riesgo medio y un potencial de impacto mínimo a los objetivos de nivel de servicio.
	Estos cambios requieren un planeamiento cuidadoso, programación y coordinación de actividades entre los grupos de soporte.
1 - Bajo	Los cambios menores implican un factor de riesgo menor, y no tienen un potencial de impactar sobre los objetivos de nivel de servicio.

Riesgo	Características
	Planeamiento, programación, y coordinación de actividades toman lugar dentro de un solo grupo.

Matriz de riesgos de cambios.

Nota:

1. Cualquier otra situación que no genere riesgos será aceptada como un caso usual de negocio (BAU- Business as usual).

b. La gestión de accesos a los portales debe ser brindada como parte de un modelo restringido de "auto servicio", él mismo que deberá ser automatizado por El Contratista.

c. Los planes de vuelta atrás o 'rollback' deberán ser considerados en cualquier cambio cuyo impacto pueda afectar los niveles de servicio.

(3) Política de Requerimientos

Las políticas de requerimientos y su respectiva administración deberán ser descritas por El Contratista en su propuesta y deberán incluir, como mínimo, lo siguiente:

1. Registro de requerimientos de servicio
2. Reapertura de requerimientos
3. Categorización de los requerimientos de servicio
4. Manejo de requerimientos de servicios duplicados
5. Política de Asignación y reasignación
6. Propiedad
7. Aceptar o rechazar requerimientos colocados
8. Cierre de los requerimientos

El Contratista debe asegurarse que, al registrar cada requerimiento, la prioridad sea la adecuada, debido que esto determinará cómo será manejado el requerimiento, tanto por las herramientas como por el Propietario del Requerimiento.

La asignación de prioridades se determinará teniendo en cuenta tanto la urgencia de los hechos como el nivel de impacto en el negocio. El personal autorizado de COFIDE tendrá la potestad de establecer la prioridad de un requerimiento en un determinado momento, si así lo considera pertinente.

El impacto de los requerimientos será definido durante la fase de Planeamiento, pero deberá utilizarse como criterio inicial, una matriz de prioridad, que se determina en función de la urgencia y el impacto. En esta matriz existen cuatro niveles de prioridad, siendo la prioridad 4, la más crítica del negocio.

Prioridad de un requerimiento		IMPACTO			
		Extremo	Alto	Medio	Bajo
URGENCIA	Extremo	4	4	3	2

Prioridad de un requerimiento		IMPACTO			
		Extremo	Alto	Medio	Bajo
	Alto	4	3	3	2
	Medio	3	3	2	1
	Bajo	2	2	1	1

Matriz de Prioridad, Impacto y Urgencia

a. **Impacto:** Indica el efecto en el negocio de un requerimiento sin atender. El Contratista deberá utilizar la siguiente tabla para evaluar el impacto de un requerimiento, el cual puede ser extremo, alto, medio o bajo.

Impacto	Características
4 - Extremo	Gran parte de la infraestructura crítica de COFIDE quede expuesto a riesgos.
3 - Alto	Parte de la infraestructura crítica quede expuesta
2 - Medio	Algunos componentes de la infraestructura queden expuestas
1 - Bajo	No quedan expuestos componentes de la infraestructura de COFIDE o los que quedan expuestos no son críticos.

Escala de impacto de la atención de requerimientos

b. **Urgencia:** Se relaciona con la disponibilidad, y mide cuánto tiempo podría pasar antes de que el requerimiento tenga un impacto significativo en el negocio, es decir, cuánto tiempo se puede tolerar el requerimiento sin ser atendido. El Contratista deberá utilizar la siguiente tabla para evaluar la urgencia de un requerimiento, la cual puede ser extremo, alto, medio o bajo.

Urgencia	Características
4 - Extremo	Afecta al 100% de la funcionalidad. Afecta a la totalidad de los usuarios.
3 - Alto	Afecta al 80% de la funcionalidad. Afecta a gran parte de los usuarios.
2 - Medio	Afecta una funcionalidad particular. Afecta a un grupo de usuarios.
1 - Bajo	Funcionalidad degradada o respuesta lenta.

Escala de Urgencia de la atención de requerimientos

c. Prioridad: Se utiliza para determinar el orden en que los requerimientos deberán ser atendidos. A continuación, se encuentra un cuadro que indica, en general, la descripción de cada una de las prioridades:

Prioridad	Descripción
4 – Extremo	Cuando la falta de atención del requerimiento afecta los Ingresos del cliente o entrega del servicio.
3 – Alto	Cuando la falta de atención del requerimiento afecta algún componente clave o aplicación crítica que pueda producir degradación del servicio o interrumpir la entrega de los servicios.
2 – Medio	Cuando la falta de atención del requerimiento afecta un componente, aplicación, software o equipo con impacto menor.
1 – Bajo	Cuando la falta de atención del requerimiento afecta un componente, aplicación, software o equipo con impacto mínimo.

Escala de Prioridad de la atención de requerimientos

Nota: Cuando un requerimiento se trata de un trabajo planificado para ser ejecutado en una fecha determinada y coordinada con el solicitante o se trata de una solicitud de información que demanda cierto tiempo de obtener, éste será considerado un requerimiento planificado.

En caso de que múltiples requerimientos tengan la misma prioridad, El Contratista deberá considerar, en primera instancia la urgencia y luego el impacto, para identificar la secuencia de trabajo a realizar.

(4) Política de Incidentes y Problemas

1. **Incidente:** Interrupción no planificada en los Servicios de 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.

2. **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.

3. 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.

La gestión de incidentes y problemas de los servicios de Ciberseguridad de Gestión y Operación de Ciberseguridad Corporativa deberá aplicar las siguientes políticas:

a. Todo incidente y/o problema, deberá ser registrado en la herramienta de gestión de servicios, incluyendo la descripción, categorización y severidad:

1. **Descripción:** Características que definen el error, lentitud o indisponibilidad del incidente.

2. **Categorización:** Identificación acerca de la naturaleza del incidente. La categorización podrá contar con múltiples niveles de detalle, jerarquizado de tal manera que facilite la identificación del incidente en el sistema de gestión y los informes de ser necesario.

3. **Severidad:** Se define según los criterios de nivel de impacto en el negocio y la urgencia, es decir, la rapidez con que se requiere de una solución:

3.1 Impacto: Se refiere al efecto que puede haber en el negocio (por ejemplo: Daño financiero u operativo) o sus procesos, debido a la no atención de un incidente. El impacto está basado en cómo los niveles de servicio se pueden ver afectados y puede ser Alto, Medio o Bajo. A continuación, se muestran algunos criterios de evaluación para definir el impacto de un incidente:

IMPACTO	CARACTERÍSTICAS
EXTREMO	Infraestructura crítica para el negocio de COFIDE (aplicación, procesamiento o infraestructura) con indisponibilidad **TOTAL**. Por ejemplo: Entornos **PRODUCTIVOS**, o servicios masivos (Desarrollos In House críticos de negocio, ERP). Compromisos críticos del negocio no se pueden cumplir (ej.: se encuentra comprometida atención a clientes).
ALTO	Infraestructura crítica para el negocio COFIDE (aplicación, procesamiento o infraestructura) con indisponibilidad **PARCIAL**. Compromisos críticos del negocio se pueden cumplir parcialmente. Gran parte de la Infraestructura crítica del negocio queda expuesta debido a la falta de disponibilidad de los Servicios de Ciberseguridad
MEDIO	Una parte de la Infraestructura crítica del negocio queda expuesta debido a la falta de disponibilidad de los Servicios de Ciberseguridad

IMPACTO	CARACTERÍSTICAS
	Infraestructura no crítica para el negocio, queda con indisponibilidad **TOTAL.**
BAJO	Infraestructura no crítica del negocio queda expuesta debido a la falta de disponibilidad de los Servicios de Ciberseguridad. Infraestructura no crítica para el negocio, queda con indisponibilidad **PARCIAL.**

Escala de impacto de la severidad de incidentes

3.2 Urgencia: Celeridad con la cual se tiene que dar solución al incidente antes de que tenga un impacto significativo en el negocio. La urgencia de un incidente podrá ser Extremo, Alto, Medio o Bajo y puede variar en el tiempo para un mismo tipo de incidente (por ejemplo: un mismo incidente puede ser más urgente en cierre de mes que en cualquier otro día), lo cual será definido por COFIDE. A continuación, se muestran algunos criterios de evaluación para determinar la urgencia.

URGENCIA	CARACTERÍSTICAS
EXTREMO	Incidente que debe atenderse con celeridad desde que el incidente es reportado, debido a que uno o varios servicios de Ciberseguridad no están funcionando y esto genera indisponibilidad de la infraestructura crítica del negocio.
ALTO	Incidente que debe atenderse con moderada celeridad desde que el incidente es reportado, debido a que un servicio de Ciberseguridad no está funcionando y esto genera exposición a amenazas en la infraestructura crítica del negocio.
MEDIO	Incidente que debe atenderse con cierta celeridad desde que el incidente es reportado, debido a que un servicio de Ciberseguridad no está funcionando y esto genera indisponibilidad de la infraestructura no crítica del negocio.
BAJO	Incidente que debe atenderse con cierta celeridad desde que el incidente es reportado, debido a que un servicio de Ciberseguridad no está funcionando y esto genera exposición a amenazas en la infraestructura no crítica del negocio.

Escala de urgencia de la severidad de incidentes

La combinación del impacto y la urgencia, y la resultante severidad, se resume en el siguiente cuadro y permite calcular la severidad de un incidente o problema, siendo la Severidad 4 la más crítica del negocio:

Urgencia/Impacto	Extremo	Alto	Medio	Bajo
Extremo	4	4	3	2
Alto	4	3	3	2
Medio	3	3	2	1
Bajo	2	2	1	1

Matriz de Severidad de Incidentes

A continuación, se encuentra un cuadro que indica, en general, la descripción de cada una de las severidades:

Severidad	Descripción
4 – Extremo	Todo incidente que afecta la disponibilidad de la infraestructura crítica de COFIDE.
3 – Alto	Todo incidente que expone a amenazas la infraestructura crítica de COFIDE.
2 – Medio	Todo incidente que afecta la disponibilidad de la infraestructura no crítica de COFIDE.
1 – Bajo	Todo incidente que expone a amenazas la infraestructura no crítica de COFIDE.

Descripción de Severidades para Incidentes

El contacto hacia COFIDE para incidentes de Severidad 4 se debe realizar a través del Service Manager.

b. 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.

c. Para todos los incidentes de severidad 4 que hayan superado los niveles de servicio descritos la sección de “Niveles de servicio”, se requiere documentar la evidencia del Análisis Causa Raíz. Este análisis deberá incluir el detalle del incidente y las acciones tomadas, así como la causa del incidente y las acciones a seguir para que el mismo no se repita. El Contratista contará con siete (07) días útiles para entregar el informe de análisis causa raíz.

La siguiente tabla muestra los criterios de prioridad de los problemas. En la tabla hay cuatro niveles de prioridad, la prioridad 4 es la más crítica del negocio.

Prioridad	Características
4 - Impacto Total en el Negocio	Todo problema que afecta la disponibilidad de la infraestructura crítica de COFIDE.

Prioridad	Características
3 - Impacto Mayor al Negocio	Todo problema que expone a amenazas la infraestructura crítica de COFIDE.
2 - Impacto Menor al Negocio	Todo problema que afecta la disponibilidad de la infraestructura no crítica de COFIDE.
1 - Impacto Mínimo o Sin Impacto al Negocio	Todo problema que expone a amenazas la infraestructura no crítica de COFIDE.

Descripción de Prioridades para Problemas

d. 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

e. Se acordarán reuniones periódicas para la revisión de los Incidentes y Problemas acontecidos.

(5) Centro de Monitoreo y Herramientas

1. 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.
2. 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.
3. Diferenciación de los eventos por tipo color para un manejo simple pero eficiente, considerando hasta cuatro (04) tipos de eventos.
4. Debe permitir acceder a la consola de monitoreo, en modo de sólo lectura, para hasta tres (03) personas de COFIDE. 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.

(6) 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:

1. 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.

2. Web: Incidentes y requerimientos.
   - Correo: Coordinaciones y consultas. Contingencia del Portal de atención de requerimientos e incidentes del proyecto para generación de requerimientos.

3. 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.

4. 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.

5. 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.

6. 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.

7. La herramienta de gestión de Incidentes, Problemas, Cambios y Requerimientos debe permitir registrar la prioridad basada en el impacto y urgencia.

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).

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

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.

Reportes

a. Cantidad de llamadas concurrentes mensual (promedio y máximo).
b. Cantidad de problemas, incidentes y requerimientos recibidos por teléfono, mail, Portal de atención de requerimientos e incidentes del proyecto.
c. Cantidad de llamadas perdidas (promedio y máximo).
d. Tiempo de espera (promedio y máximo).

7.4 Etapa de Cierre

La duración de la fase de transición de salida será como mínimo de tres (03) 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:

Política y Estrategia de Migración

1. 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.
2. 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.
3. Se han definido dos (02) etapas para la transición de salida, estas son:

a. Etapa 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:

1. Reuniones de coordinación entre COFIDE, el Contratista y el futuro Contratista.
2. Programa de actividades de migración para el traslado de los servicios.
3. 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. Etapa 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:

1. Migración del Servicio de Gestión de los Equipos o Soluciones de Seguridad.
2. Migración del Servicio de Detección Avanzada.
3. 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.

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.

e. 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 por empresa 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.

8 CONDICIONES DEL SERVICIO

a. El servicio S1 se realizará una única vez, al inicio de la fase de operación del servicio.

b. Los servicios S2, S3 y S4 se realizan de manera mensual.

c. El servicio S2 se realiza en la modalidad 24x7, a demanda.

d. El servicio S3 se realizan de manera mensual, en la modalidad de 24x7 y de manera continua.

e. El servicio S4 se realiza según sea requerido durante toda la operación del servicio, en la modalidad 24x7, a demanda.

f. El horario de atención para la recepción de los requerimientos de operación y atención de incidentes es 24x7.

g. El horario para realizar el análisis y categorización de requerimientos de operación del servicio S2 será de lunes a viernes en el horario de 8:00am a 6:00pm, en días hábiles. Cualquier trabajo programado mediante un requerimiento deberá ser coordinado dentro del horario especificado, a menos que este sea crítico o urgente, cuya atención será de manera continua hasta la implementación de la configuración solicitada.

h. Para la suscripción del contrato, El Contratista deberá presentar los precios unitarios para adiciones y reducciones de (activos y horas) de los diferentes servicios que componen el Servicio de Ciberseguridad, con excepción del servicio S1.

i. El Postor deberá indicar en su propuesta técnica, las herramientas, equipos y/o productos que utilizará durante la ejecución de todos los servicios.

j. Los informes y recomendaciones entregados a COFIDE deben ser completamente en español, a excepción de los reportes técnicos emitidos directamente por las herramientas utilizadas, las cuales servirán como anexos a los informes finales presentados.

k. El contratista deberá considerar las redundancias en los servicios e infraestructura de SOC más idóneas que garanticen el cumplimiento de los SLAs.

Responsabilidades de El Contratista

Para todos los servicios, las siguientes actividades son de exclusiva responsabilidad de El Contratista:

a. Realizar mantenimiento periódico físico por lo menos una vez al año a los equipos (hardware y software) que soportan el servicio, alojados tanto en El Contratista como en los centros de datos de las empresas que forman parte del servicio.
b. Todo el software que El Contratista suministre o utilice debe contar con contrato de soporte con el fabricante respectivo, durante todo el periodo del contrato del presente servicio con el fin de escalar incidentes y problemas propios del servicio.
c. Realizar pruebas antes de aplicar actualizaciones a los componentes del servicio ya sean hardware y/o software. La aplicación de parches y actualizaciones debe contar con el conocimiento y autorización de COFIDE. Para lo cual El Contratista debe contar con equipamiento para los ambientes de pruebas, este equipamiento no necesariamente debe ser nuevo, ni será de uso exclusivo para COFIDE. Las pruebas están referidas a actualizaciones a los equipos y software provistos por El Contratista.
d. Mantener actualizados todo el hardware que soporta los servicios con las últimas versiones de BIOS y/o Firmware. La aplicación de actualizaciones debe ser resultado de un proceso de mantenimiento preventivo programado, con excepción de las que el fabricante recomiende aplicar inmediatamente.
e. Mantener actualizados todo el software que soporta los servicios con las últimas versiones, hotfix, support packages, service pack, patch, *security/advisory updates,* y cualquier otro medio de actualización utilizado para actualizar el software, para garantizar la disponibilidad y estabilidad del servicio. La aplicación de actualizaciones debe ser resultado de un proceso de mantenimiento preventivo programado, con excepción de las que el fabricante recomiende aplicar inmediatamente. El costo por las actualizaciones es asumido por El Contratista.
f. Realizar las copias de seguridad necesarias para garantizar la disponibilidad del servicio ante cualquier contingencia, cada vez que se realice cambios de configuración en los equipos o software suministrador por El Contratista.
g. Monitorear los componentes de cada servicio (hardware y software) de todos los servicios, las 24x7.
h. Almacenar los logs de los equipos y componentes que conforman los diferentes servicios, y proporcionarlos a las empresas en caso sean requeridos, por ejemplo, en caso de incidentes o problemas, o cuando COFIDE lo considere pertinente.
i. Monitorear permanentemente la atención a incidentes y requerimientos.
j. Garantizar la disponibilidad y tiempo de respuesta de acuerdo con los niveles de servicios establecidos en los SLAs.
k. Garantizar el soporte de los servicios ante un crecimiento bajo demanda.
l. Brindar los parámetros y configuraciones necesarias para acceder a la consola de administración de los servicios desde los locales de COFIDE.
m. El CONTRATISTA será responsable de instalar los certificados digitales SSL en los servicios de información que lo requieran. Estos certificados digitales serán provistos por El CONTRATISTA.
n. Realizar el mantenimiento preventivo de los componentes entregados por El Contratista, y que se instalen en los locales de COFIDE. Las actividades que este servicio incluirá son:
    1. Verificación de las condiciones de operación de los equipos, de acuerdo con las recomendaciones del fabricante: espacio, temperatura, ventilación, y seguridad física.
    2. Recolección de registros de errores (Error Logs) y análisis de los errores reportados.
    3. Recomendación de acciones correctivas necesarias antes de que se produzca una falla que impida el normal funcionamiento de sus equipos y por ende del ser servicio.
    4. Actualización (*upgrades* y *updates*) de Firmware.

o. Mantener vigente de manera continua el certificado de su SGSI durante el tiempo que el contrato sea vigente (planificación, transición de entrada, ejecución y transición de salida).

p. Garantizar las facilidades mínimas necesarias que incluyen hardware, software, metodologías y personas para la prestación de cada servicio

q. Garantizar que la ejecución del servicio no debe causar daño alguno en el funcionamiento de los activos o en el desempeño de la red de datos de COFIDE. Así mismo en ninguna circunstancia y momento se generará algún tipo de cambio sobre los activos a los que se logre acceso (salvo que sean generados por los registros de acceso y actividades de los activos), con excepción del servicio **S5**.

Las actividades de mantenimiento preventivo se realizarán una vez al año, de manera presencial, y se coordinará con COFIDE las fechas de su ejecución.

Reportes

Para todos los reportes se debe utilizar gráficos de tendencias de los últimos 12 meses, y gráficos con información diaria del mes. Dentro la especificación de cada servicio se encuentra listados los parámetros a reportar, esto no limita que durante el desarrollo del servicio COFIDE determine la conveniencia de incluir parámetros que deban ser informados mediante gráficos de tendencias, pudiendo sustituir unos por otros, siempre y cuando sea factible su medición.
Nota: Para el servicio S2 los reportes se colocarán en Portal de Información por única vez al finalizar la ejecución de estos servicios.

Comités del Servicio

Con el propósito de asegurar la correcta prestación de los Servicios materia del Contrato y el cumplimiento de los compromisos pactados, así como de facilitar la oportuna toma de decisiones al respecto, se requiere de la participación y coordinación permanente de ambas partes: COFIDE y El Contratista, para lo cual, se llevará a cabo un comité Ejecutivo del Servicio, cuyas funciones y composición se describen a continuación:

Comité Ejecutivo del Servicio:

Este comité es responsable del seguimiento, supervisión y coordinación de todas las actividades involucradas en el servicio y, por lo tanto, de la prestación satisfactoria de los Servicios.

Este comité está compuesto por:

- El Subgerente del Departamento de Tecnología de Información de COFIDE
- Ejecutivo de Infraestructura y Proyectos Especiales de COFIDE.
- Oficial de Seguridad de la Información de COFIDE.
- El Service Manager del Contratista.
- El Director del Proyecto del Contratista.
- Especialistas de ambas partes según sea necesario.

Debido a que el presente servicio puede tener dependencia y/o relación con otros servicios de TI que COFIDE terceriza, podrán participar en estas reuniones el(los) Gerente(s) de(los) Servicio(s) correspondiente(s) y sus coordinadores directos, en caso de que COFIDE lo considere necesario.

Las reuniones del Comité Ejecutivo se realizarán en las oficinas de COFIDE o de manera virtual, este comité se reunirá mensualmente y actuará como secretario el Service Manager del Contratista quien registrará en actas los acuerdos expresados por ambas Partes.

Son funciones de este Comité:

- Velar por el cumplimiento del alcance del presente servicio.
- Revisar los resultados de los ANS y definir los planes de mejora propuestos por el Contratista.
- Revisar la facturación mensual.
- Hacer seguimiento a los tickets pendientes.
- Definir acciones de mejora continua para el servicio
- Cualquier inquietud o necesidad de alguna de las Partes.

Es responsabilidad del Contratista ante el Comité Ejecutivo:

- Asegurar la correcta prestación de los servicios y el cumplimiento de los compromisos acordados.
- Comprometer fechas de cierre para los tickets pendientes.
- Proponer planes de acción ante la pérdida de algún ANS.
- Presentar acciones de mejora continua.

Es responsabilidad del Service Manager designado por el Contratista:

- Representar al Servicio en todos los aspectos referidos al contrato.
- Representar al Servicio en las reuniones del Comité Ejecutivo.
- Informar periódicamente al Comité Ejecutivo sobre el avance y desviaciones de los Acuerdos de Niveles de Servicio.
- Tomar acción sobre las decisiones que resulten de las reuniones de Comité Ejecutivo que competan al personal del Contratista.
- Velar por que todo incidente, cambio o requerimiento solicitado al centro de atención sea registrado en la herramienta y cuente con un número de ticket correspondiente.

Portal de Información

Se debe incorporar dentro del servicio de gestión y operación, un portal de información el cuál brindará información en línea acerca del comportamiento operativo del proyecto y de los servicios. Basado en la integración de diferentes fuentes de datos, dicho portal estará en condiciones de mostrar tableros de control, reportes e indicadores, brindando mayor visibilidad y mejor control de la operación de los servicios de Ciberseguridad.

El portal de información contendrá las siguientes funcionalidades:

1. Dashboards:
   - Un (01) Tablero de control, por perfil de usuario definido por servicio.
2. Indicadores de desempeño:
   - Indicadores relacionados a los servicios de Ciberseguridad contratados.
3. Reportes:
   - Información en diferentes formatos, reutilizando los diferentes repositorios de información que se integren a la plataforma.
4. Seguridad:
   - Control de acceso con autenticación de doble factor.

(a) Diseño del Servicio:

El portal de información estará en un ambiente acorde a las necesidades requeridas para que los usuarios accedan en línea a los tableros de control, reportes e indicadores.
La provisión de este portal de información contemplará la integración con las herramientas de:

a. Gestión de requerimientos, incidentes, problemas, cambios y configuraciones.
b. Monitoreo.

La integración de las herramientas antes mencionadas, así como la inclusión de otros repositorios, proveerán la información necesaria para construir los tableros de control, indicadores y reportes para los diferentes roles. Cualquier otra integración adicional, deberá ser acordada durante la fase de Planeamiento de este servicio.
El portal de información definirá los mecanismos necesarios para que los usuarios tengan los medios para consultar información acerca de:

1. Cantidad de requerimientos consumidos por servicio
2. Cantidad de incidentes por cada servicio.
3. Disponibilidad estimada de los servicios de Ciberseguridad.
4. Cantidad de cambios por servicio.
5. Tendencia de incidentes, requerimientos y problemas en la prestación de los servicios
6. Cantidad de tickets por estado (SLA), por servicio.

Durante la fase de Planeamiento, ambas partes definirán los indicadores finales a mostrar en el portal de información, y las fechas en las cuales irán integrándose y mostrándose los indicadores y reportes.
Este portal deberá estar operativo en el primer mes de la fase de Operación del Servicio.
Se proveerán dos (02) perfiles de acceso al portal de información:

c. Gestor: Perfil de consulta de reportes, indicadores y tablero de control. No tiene control sobre las modificaciones del portal.

d. Administrador de Cuenta: Perfil de consulta de reportes, indicadores y tablero de control, pudiendo modificar los indicadores y gráficos a ser mostrados dentro de la vista asociada a su perfil, de acuerdo con los reportes disponibles en el repositorio del Portal de Servicios.

Con la finalidad de simplificar la gestión del servicio y con el objetivo de un plan de mejora continua, se requiere que El Contratista no duplique información, es decir, debe evitar redundar la información presentada en el portal y en el Informe de Gestión Mensual.

(b) Responsabilidades de El Contratista

a. Instalación, configuración, integración y posterior mantenimiento y gestión de las herramientas necesarias a fin de proveer en calidad de uso, el Portal de Servicios.
b. Definición de los indicadores asociados a los perfiles de usuario, que conformarán los tableros de control, en conjunto con COFIDE.
c. Capacitación en el uso del portal. Las características de la capacitación se definirán en la fase de Planeamiento.

(c) Responsabilidades de COFIDE

a. Definición de la información (indicadores) que cada perfil de usuario definido podrá visualizar en los tableros de control, en conjunto con El Contratista.
b. Brindar las condiciones necesarias para llevar a cabo la capacitación realizada por El Contratista.

(d) Licenciamiento

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

Software	COFIDE	El Contratista
Sistema Operativo requerido para la provisión en uso del portal		**X**
Monitoreo de los componentes del portal		**X**
Cualquier otro software necesario para la operación y gestión del portal		**X**

Responsabilidad de provisión de las licencias

9 ENTREGABLES

Etapa del Servicio	Entregables	Plazo Máximo
Etapa de Planificación	**Entregables Generales** - Plan de proyecto - Plan de comunicaciones - Plan de riesgos - Plan de pruebas - Plan de cierre de planeamiento del proyecto **Entregables por servicio:** - S1 - Servicio de evaluación de Seguridad TI • Plan para desarrollar procedimientos y formatos necesarios para la evaluación de seguridad de los activos TI. • Plan de comunicaciones para el desarrollo del servicio.	30 días calendario después de la firma del contrato

	- S2 - Servicio de Gestión de los Equipos o Soluciones de Seguridad • Plan para desarrollar procedimientos y formatos necesarios para realizar la gestión y operación de los equipos o soluciones de seguridad. • Plan de comunicaciones para este servicio. - S3 - Servicios de Detección Avanzada • 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. • Plan de comunicaciones para el desarrollo del servicio. - S4 - Servicios Respuesta a Incidentes como Servicio • Plan para desarrollar procedimientos y formatos necesarios para realizar la respuesta a incidentes como servicio. • Plan de comunicaciones para el desarrollo del servicio. - Todos los servicios: • Manuales para el uso del portal de información. • Manuales para el uso del portal de atención de requerimientos e incidentes del proyecto. • Ficha técnica de los equipos y soluciones que presentarán en los servicios (deben ir como anexos dentro de la propuesta técnica) • Procedimientos y formatos para solicitud de incremento/decremento 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.	

Transición de Entrada	- S1 - Servicio de evaluación de Seguridad TI • Actas de entrevistas con el personal de COFIDE. • Inventario de activos con detalles técnicos por cada empresa. • 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 • Metodología para la atención de requerimientos de operación. • Configuración de la conectividad mediante VPN para acceso hacia los equipos y soluciones de seguridad. • Acta de recepción definitiva del servicio. - S3 - Servicios de Detección Avanzada • 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. • Acta de recepción definitiva del servicio. • Procedimiento para realizar la integración del SIEM en los equipos y soluciones que son gestionados por los proveedores de COFIDE. - S4 - Servicios Respuesta a Incidentes como Servicio	60 días calendario después del Acta de Conformidad de la Fase de Planeamiento

	• 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. - Informe mensual de gestión del Servicio: • Configuración del Portal de atención de requerimientos e incidentes del proyecto. • Configuración del Portal de información. • Herramienta de Gestión de Servicios	
Etapa Operativa	- S1 - Servicio de evaluación de Seguridad TI • 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. - S2 - Servicio de Gestión de los Equipos o Soluciones de Seguridad • 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. - S3 - Servicios de Detección Avanzada • Informe que considera los aspectos de Monitoreo, Detección, Análisis e Interpretación de los resultados a partir del cual se podrán tomar decisiones - S4 - Servicios Respuesta a Incidentes como Servicio • Informe de la gestión realizada por cada incidente que se produzca que incluya: las	Mensual a partir el mes siguiente a la firma del Acta de Inicio de la Etapa Operativa

	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 mensual de gestión del Servicio: • 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. • Consumos efectivos de capacidades contra la Línea Base. • Cantidad de llamadas concurrentes mensual (promedio y máximo). • Cantidad de problemas, incidentes y requerimientos recibidos por teléfono, mail, Portal de atención de requerimientos e incidentes del proyecto. • Cantidad de llamadas perdidas (promedio y máximo). • Tiempo de espera (promedio y máximo).	
Etapa de Cierre	• Plan de transición de salida para cada uno de los servicios	3 meses antes del fin del Contrato

Para la entrega formal de los entregables del servicio considerar el envío a los siguientes buzones de correo:

- mesadepartes@cofide.com.pe
- entregablesti@cofide.com.pe

10 PLAZO DEL SERVICIO

El plazo del servicio comprende 36 meses, contados a partir de la firma del Acta de Inicio de la Etapa Operativa. Asimismo, son 30 días para la etapa de planificación y 60 días para la etapa de Transición de entrada.

11 FORMA DE PAGO

El presente servicio se pagará en 36 cuotas mensuales iguales que iniciarán desde el mes siguiente a la firma del Acta de Inicio de la Etapa Operativa y previa entrega de la documentación exigida en la sección Entregables.

La forma de pago será a los 15 días calendarios de otorgada la conformidad de los entregables de la etapa, previa presentación de la factura e informe correspondiente.

El responsable de dar conformidad al servicio es el Subgerente de Tecnologías de Información de la Gerencia de Gestión Humana y Administración de COFIDE.

El pago se realizará, previa conformidad del servicio, de acuerdo con el artículo 168° del Reglamento de la Ley de Contrataciones del Estado, para efectos del pago de las contraprestaciones ejecutadas por el contratista, la Entidad deberá contar con la siguiente documentación:

- Entregables según términos de referencia.
- Informe de supervisión del servicio sobre sobre el cumplimiento de las condiciones del contrato elaborado por el Departamento de TI.
- Acta de conformidad de la Gerencia Usuaria.
- Comprobante de pago

12 GARANTÍA

No aplica.

13 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.

14 REQUISITO DEL PROVEEDOR

El Postor deberá contar con las siguientes certificaciones vigentes (Presentar para la firma de contrato):

a) Certificado en ISO/IEC 27001:2013 Sistema de Gestión de Seguridad de la Información.
b) Pertenecer a una comunidad de Ciberseguridad:
   1. Cumplir los requisitos del Anexo A.
   2. El postor DEBE pertenecer a la comunicad FIRST.

Acreditación:
Documentos vigentes en los cuales se pueda validar la entidad a la cual pertenecen, la fecha de emisión del documento y la fecha desde la cual pertenece a dicha comunidad.
Los postores deberán indicar un medio de verificación de estos documentos, por ejemplo, correos electrónicos, números telefónicos de la persona de contacto en la entidad emisora de los documentos o portales de verificación de los documentos de la empresa emisora. La acreditación de ser miembro de FIRST debe estar asociada al SOC que presente el postor como parte de su propuesta.

Presentación del documento emitido por FIRST que acredite la membresía vigente del postor.

La certificación puede ser en por lo menos uno de los procesos del SOC o en su defecto de alcance general para una sede o todas las sedes de las compañías del Postor que presenta su oferta.

Ser una empresa legalmente constituida en el Perú, dedicada a proveer e integrar servicios y soluciones de Seguridad Informática, Seguridad de la Información, Centro de Operaciones de Seguridad (SOC), Centros de Ciber Defensa (CCD) y/o Ciberseguridad.

Para aquellos postores cuya ubicación de su SOC se encuentre fuera del país, deberá contar por lo menos con un Centro de Respuesta Cibernética (CRC) con analistas de nivel 2 y 3 en Lima Perú, este CRC los perfiles de los analistas de nivel 2 y 3 se precisan en el presente TDR.

Los postores deben demostrar que cuentan con las capacidades necesarias para cumplir el contrato, descritas en los requisitos de los presentes Términos de Referencia, las cuales deben ser acreditadas documentalmente.

15 ADECUACIÓN A PROTOCOLOS SANITARIOS

El PROVEEDOR es responsable del cumplimiento de los siguientes puntos:

Documentos obligatorios:

- Presentar el “Plan para la vigilancia, prevención y control de COVID-19 en el trabajo” de acuerdo con lo establecido a la R.M. N° 239-2020-MINSA (y sus posteriores adecuaciones).

Descripción del servicio:

- El personal destacado a COFIDE deberá cumplir con el Plan y los protocolos instaurados por COFIDE para la prevención y control de COVID-19 en el trabajo.
- El contratista deberá implementar en coordinación con COFIDE el trabajo remoto o teletrabajo en aquellos puestos que no precisen de asistir a la sede central de COFIDE; así como para los trabajadores con factores de riesgo para COVID-19, a quienes además el contratista realizará un seguimiento clínico a distancia.
- Al identificar un caso con fiebre o sintomatología COVID-19, que lleve a la categorización de caso sospechoso, el contratista tendrá la obligación de cumplir con lo normado por el MINSA y el Gobierno Central e informar de inmediatamente a COFIDE.
- El contratista deberá asegurar que el personal que ingresará a la sede central de COFIDE cuente con los EPP de bioseguridad o cualquier otro requisito que sea determinado por el MINSA o el Gobierno Central.

A la firma del contrato:

- Facilitar el nombre y apellido, número de celular y correo electrónico del responsable de seguridad y salud en el trabajo del contratista.

Al inicio del servicio:

- Presentar fichas sintomatología COVID19 para regreso al trabajo u otro documento que sea determinado por el MINSA o el Gobierno Central.

16 ANEXO A

Catálogo de membresías de comunidades de Ciberseguridad

Ítem	Comunidad	Obligatorio / Opcional
1	FIRST	Obligatorio
2	ICSPA	Opcional

Ítem	Comunidad	Obligatorio / Opcional
3	CIC	Opcional
4	TELCO SECURITY ALLIANCE	Opcional

Comunidades de Ciberseguridad

17 ANEXO B

Facilidades mínimas requeridas por servicio

Servicio	Facilidades Tecnológicas Mínimas	Acreditación
S1	- 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.	El Postor debe demostrar que posee derecho de uso sobre el hardware y software a utilizar, lo cual debe ser acreditado mediante una Declaración Jurada. En el caso de utilizar servicios arrendados deberá demostrar que posee acceso al servicio y la forma de acreditarlo será con copia algún documento emitido por el proveedor del servicio o declaración jurada. La documentación señalada deberá ser presentada a la suscripción del contrato.
S2	- Estaciones de trabajo para los recursos humanos proporcionado por el Contratista. - Conectividad para acceso hacia los equipos y soluciones de seguridad.	
S3	- 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	- 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.	

Facilidades Tecnológicas

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

A	**CAPACIDAD TÉCNICA Y PROFESIONAL**
A.1	**CALIFICACIONES DEL PERSONAL CLAVE**
A.1.1	**FORMACIÓN ACADÉMICA**
	Requisitos: Director del Proyecto: • Titulado en las carreras de Ingeniería electrónica, o Ingeniería de Sistemas, o Ingeniería de Telecomunicaciones y Redes, Ingeniero Informático o Ingeniero Industrial. Gestor de Seguridad: • Titulado y/o Bachiller en carreras como Ingeniería Informática o Ingeniería Industrial o Ingeniería Electrónica o ingeniería de sistemas o Ingeniería Sistemas e Informática. Acreditación: El Grado o Título será verificado por el comité de selección en el Registro Nacional de Grados Académicos y Títulos Profesionales en el portal web de la Superintendencia Nacional de Educación Superior Universitaria - SUNEDU a través del siguiente link: https://enlinea.sunedu.gob.pe/ // o en el Registro Nacional de Certificados, Grados y Títulos a cargo del Ministerio de Educación a través del siguiente link : http://www.titulosinstitutos.pe/, según corresponda. En caso el Grado o Título no se encuentre inscrito en el referido registro, el postor debe presentar la copia del diploma respectivo a fin de acreditar la formación académica requerida.
A.1.2	**CAPACITACIÓN**
	Requisitos: **Director del Proyecto:** Diplomado en Gerencia de Proyectos o Diplomado en Seguridad Informática, o Curso en seguridad de la información o curso de Ciberseguridad de por lo menos 40 horas lectivas. **Gestor de Seguridad:** 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 de por lo menos 40 horas lectivas. Acreditación: Se acreditará con copia simple de CONSIGNAR CONSTANCIAS, CERTIFICADOS, U OTROS DOCUMENTOS, SEGÚN CORRESPONDA. **Importante** *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.*
A.2	**EXPERIENCIA DEL PERSONAL CLAVE**

Requisitos:

Director del Proyecto:

- Mínimo 3 años en proyectos de Ciberseguridad de TI, Seguridad de la Información, Seguridad Informática, Configuración de seguridad en redes y nube.

Gestor de Seguridad:

- Mínimo 3 años en Identificación, clasificación, análisis de eventos de seguridad, Identificación y gestión de incidentes de seguridad, Gestión y operación de soluciones SIEM

De presentarse experiencia ejecutada paralelamente (traslape), para el cómputo del tiempo de dicha experiencia sólo se considerará una vez el periodo traslapado.

Acreditación:

La experiencia del personal clave se acreditará con cualquiera de los siguientes documentos: (i) copia simple de contratos y su respectiva conformidad o (ii) constancias o (iii) certificados o (iv) cualquier otra documentación que de manera fehaciente demuestre la experiencia del personal propuesto.

Importante

- *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.*
- *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.*
- *Se considerará aquella experiencia que no tenga una antigüedad mayor a veinticinco (25) años anteriores a la fecha de la presentación de ofertas.*
- *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.*

B	**EXPERIENCIA DEL POSTOR EN LA ESPECIALIDAD**

Requisitos:

El postor debe acreditar un monto facturado acumulado equivalente a S/ 5,280,000.00 (Cinco millones doscientos ochenta 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:

- Servicios de CyberSOC / SOC y/o Administración y/o Monitoreo y/o soporte de Plataformas de Seguridad y Correlación.
- 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

Acreditación:

La experiencia del postor en la especialidad se acreditará con copia simple de (i) contratos u órdenes de servicios y su respectiva conformidad o constancia de prestación; o (ii) comprobantes de pago cuya cancelación se acredite documental y fehacientemente, con voucher de depósito, nota de abono, reporte de estado de cuenta, cualquier otro documento emitido por Entidad del sistema financiero que acredite el abono o mediante cancelación en el mismo comprobante de pago[7], correspondientes a un máximo de veinte (20) contrataciones.

[7] Cabe precisar que, de acuerdo con la **Resolución N° 0065-2018-TCE-S1 del Tribunal de Contrataciones del Estado**:

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 Nº 7** referido a la Experiencia del Postor en la Especialidad.

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

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

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

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

Si el postor acredita experiencia de otra persona jurídica como consecuencia de una reorganización societaria, debe presentar adicionalmente el **Anexo N° 8.**

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 Nº 7** 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

"… 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 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**	
	Evaluación: Se evaluará considerando el precio ofertado por el postor. Acreditación: Se acreditará mediante registro en el SEACE o el documento que contiene el precio de la oferta **(Anexo N° 6)**, según corresponda.	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: $$Pi = \frac{Om \times PMP}{Oi}$$ **i** = Oferta **Pi** = Puntaje de la oferta a evaluar **Oi** = Precio i **Om** = Precio de la oferta más baja **PMP** = Puntaje máximo del precio 100 **puntos**

Importante

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

CAPÍTULO V
PROFORMA DEL CONTRATO

Importante

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

Conste por el presente documento, la contratación del servicio de Ciberseguridad en los sistemas de COFIDE, que celebra de una parte COFIDE, en adelante LA ENTIDAD, con RUC Nº 20100116392, con domicilio legal en [Calle Augusto Tamayo Nº 160, San Isidro, representada por [……..…], identificado con DNI Nº [……], y de otra parte […….....], con RUC Nº [.....], con domicilio legal en […….....], inscrita en la Ficha N° […….....] Asiento N° [……....] del Registro de Personas Jurídicas de la ciudad de [……], debidamente representado por su Representante Legal, […….....], con DNI N° [……..], según poder inscrito en la Ficha N° [……..], Asiento N° [……] del Registro de Personas Jurídicas de la ciudad de [……], a quien en adelante se le denominará EL CONTRATISTA en los términos y condiciones siguientes:

CLÁUSULA PRIMERA: ANTECEDENTES

Con fecha [……..], el comité de selección adjudicó la buena pro del **CONCURSO PÚBLICO Nº** 04-2021-COFIDE para la contratación de Servicio de Ciberseguridad en los sistemas de COFIDE, 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 Ciberseguridad en los sistemas de COFIDE.

CLÁUSULA TERCERA: MONTO CONTRACTUAL

El monto total del presente contrato asciende a [CONSIGNAR MONEDA Y MONTO], que incluye todos los impuestos de Ley.

Este monto comprende el costo del servicio, todos los tributos, seguros, transporte, inspecciones, pruebas y, de ser el caso, los costos laborales conforme a la legislación vigente, así como cualquier otro concepto que pueda tener incidencia sobre la ejecución del servicio materia del presente contrato.

CLÁUSULA CUARTA: DEL PAGO[8]

LA ENTIDAD se obliga a pagar la contraprestación a EL CONTRATISTA en [INDICAR MONEDA], en 36 cuotas mensuales, después del inicio de la etapa operativa**,** 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.

[8] 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 36 meses, contados a partir de la firma del Acta de Inicio de la Etapa Operativa.

El plazo para la etapa de planificación es de 30 días calendario, el mismo que se computa desde el día siguiente a la firma del contrato.

El plazo para la etapa de Transferencia de entrada es de 60 días calendario, el mismo que se computa desde el día siguiente de finalizada la etapa de planificación.

CLÁUSULA SEXTA: PARTES INTEGRANTES DEL CONTRATO

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

CLÁUSULA SÉTIMA: GARANTÍAS

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

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

Importante
Al amparo de lo dispuesto en el numeral 149.4 del artículo 149 del Reglamento de la Ley de Contrataciones del Estado, en el caso de contratos periódicos de prestación de servicios en general, si el postor ganador de la buena pro solicita la retención del diez por ciento (10%) del monto del contrato original como garantía de fiel cumplimiento de contrato, debe consignarse lo siguiente: *"De fiel cumplimiento del contrato:* [CONSIGNAR EL MONTO]*, a través de la retención que debe efectuar LA ENTIDAD, durante la primera mitad del número total de pagos a realizarse, de forma prorrateada, con cargo a ser devuelto a la finalización del mismo."*

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

CLÁUSULA OCTAVA: EJECUCIÓN DE GARANTÍAS POR FALTA DE RENOVACIÓN

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

CLÁUSULA NOVENA: ACUERDO DE CONFIDENCIALIDAD

Las partes acuerdan que, como condición inherente a la prestación del servicio materia del presente contrato, toda la información a la cual tenga acceso EL CONTRATISTA, durante el plazo de

vigencia del mismo, será considerada como confidencial, debiendo EL CONTRATISTA instruir a su personal y asesores en relación a la obligación de mantener el deber de confidencialidad respecto de la información a la cual tengan acceso, cualquiera sea la fuente de la cual provenga.

El deber de confidencialidad implica, además, para EL CONTRATISTA y su personal, una obligación de no hacer, mediante la cual se comprometen a no hacer uso, en beneficio propio y/o de terceros, de los datos e información respecto de la cual tengan acceso directo o indirecto.
Toda la información, incluyendo la contenida en documentos impresos e incluso aquellos contenidos en medios digitales a los cuales acceda EL CONTRATISTA, su personal y asesores, deberán ser devueltos a COFIDE una vez que su utilidad no resulte relevante para la prestación del servicio materia del presente contrato.

Las obligaciones pactadas en la presente cláusula se mantendrán vigentes aun cuando haya culminado la prestación efectiva del servicio por parte de EL CONTRATISTA y se extenderán a todo su personal y asesores, aun cuando estos hayan dejado de laborar o prestar servicios para él.

En caso de incumplimiento de lo dispuesto en la presente cláusula, COFIDE se reserva el derecho de interponer ante EL CONTRATISTA y/o cualquier persona que resulte responsable del mismo, las acciones legales correspondientes.

CLÁUSULA DÉCIMA: SUPERVISIÓN DEL SERVICIO

EL CONTRATISTA se obliga a facilitar la revisión de todas las prestaciones a su cargo en virtud del presente contrato, tanto a la Gerencia de Asesoría Jurídica, a la Unidad de Auditoria Interna, al Órgano de Control Institucional, a la sociedad de auditoría externa que preste servicios a COFIDE, así como a la Superintendencia de Banca y Seguros o la persona que ésta designe.

CLÁUSULA DÉCIMA PRIMERA: CONTINUIDAD DEL SERVICIO

EL CONTRATISTA deberá cumplir con la prestación del servicio de manera continua e ininterrumpida, tomando en consideración los términos de referencia previstos en el Capítulo III de las Bases y en su oferta que forman parte integrante de EL CONTRATO.

CLÁUSULA DÉCIMA SEGUNDA: CONFORMIDAD DE LA PRESTACIÓN DEL SERVICIO

La conformidad de la prestación del servicio se regula por lo dispuesto en el artículo 168 del Reglamento de la Ley de Contrataciones del Estado. La conformidad será otorgada por La 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, en el plazo máximo de 07 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 cumpliese 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 TERCERA: 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 DÉCIMA CUARTA: 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 01 año(s) contado a partir de la

conformidad otorgada por LA ENTIDAD.

CLÁUSULA DÉCIMA QUINTA: PENALIDADES

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

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

Donde:

F = 0.25 para plazos mayores a sesenta (60) días o;
F = 0.40 para plazos menores o iguales a sesenta (60) días.

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

Importante

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

OTRAS PENALIDADES

ANS	KPI	Servicios	Métrica	Porcentaje de Facturación Mensual
ANS01	Identificar los Riesgos de Ciberseguridad de los activos TI	S1-Evaluación de Seguridad TI	Activos TI evaluados	5%
ANS02	Garantizar que los equipos y soluciones de seguridad están correctamente configurados	S2-Gestión de los equipos o soluciones de seguridad	Requerimientos atendidos de manera oportuna	3%
ANS03	Minimizar los tiempos de parada de los servicios TI	S3-Detección Avanzada	Disponibilidad del servicio	5%

ANS	KPI	Servicios	Métrica	Porcentaje de Facturación Mensual
ANS04	Minimizar los tiempos de parada de los servicios TI	S4-Respuesta a incidentes como servicio	Incidentes atendidos de manera oportuna	8%
ANS05	Responder a las necesidades del negocio	Gestión de Requerimientos (RQ) de los equipos y soluciones de seguridad	Tiempo Promedio de Respuesta inicial por email o asistencia remota (Prioridad del 4 al 1)	3%
ANS06				3%
ANS07				1%
ANS08				1%
ANS09			Tiempo Promedio de Respuesta presencial (Prioridad del 4 al 1)	3%
ANS10				3%
ANS11				1%
ANS12				1%
ANS13			Tiempo Promedio de Resolución por asistencia remota o presencial (Prioridad del 4 al 1)	3%
ANS14				3%
ANS15				1%
ANS16				1%
ANS17		Gestión de Incidentes	Tiempo Promedio de Respuesta inicial por email o asistencia remota (Prioridad del 4 al 1)	3%
ANS18				3%
ANS19				1%
ANS20				1%
ANS21			Tiempo Promedio de Resolución por (Prioridad del	3%
ANS22				3%
ANS23				1%

ANS	KPI	Servicios	Métrica	Porcentaje de Facturación Mensual
ANS24			4 al 1)	1%

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 SEXTA: 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 SÉTIMA: 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 OCTAVA: 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.

CLÁUSULA DÉCIMA NOVENA: 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 VIGÉSIMA: SOLUCIÓN DE CONTROVERSIAS[9]

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

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

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

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

CLÁUSULA VIGÉSIMA PRIMERA: PREVENCIÓN DE DELITOS, LAVADO DE ACTIVOS Y FINANCIAMIENTO DEL TERRORISMO.

En relación con los servicios prestados y el cumplimiento de las obligaciones derivadas del presente Contrato o de las operaciones realizadas por cuenta y en nombre de LA ENTIDAD, EL CONTRATISTA, declara estar de acuerdo y garantiza que:

(i) No ha violado ni violará directa o indirectamente las leyes vigentes relacionadas a la Responsabilidad Administrativa de las Personas Jurídicas (Ley N° 30424 y sus modificatorias), Lavado de Activos y Financiamiento del Terrorismo, (entre las que se encuentra el Decreto Legislativo N° 1106 o norma que la sustituya, modifique o complemente, entre otras); incluyendo, de ser el caso y sin limitación, la Ley de Prácticas Corruptas en el Extranjero de los Estados Unidos de Norteamérica, (colectivamente, "Normativa de Prevención de Delitos y LAFT").

(ii) Pondrá en práctica las medidas exigidas por la Normativa de Prevención de Delitos y LAFT vigente, y operará bajo los más estrictos principios éticos y con la observancia plena de las leyes y normas reglamentarias relacionadas con la prevención del lavado de activos y financiamiento del terrorismo.

(iii) Deberá procurar el cumplimiento de las obligaciones señaladas en los numerales (i) y (ii) de la presente cláusula, por parte de sus accionistas, directores, gerentes, representantes legales, funcionarios, apoderados, integrantes de los órganos de administración, empleados, asesores, consultores, agentes, contratistas y/o subcontratistas, y los de las personas naturales o jurídicas con las que EL CONTRATISTA tenga relación directa o indirecta de propiedad, vinculación o control (conforme al Reglamento de Propiedad Indirecta, Vinculación y Grupos Económicos, aprobado por Resolución SMV N° 019-2015-SMV/01 de la Superintendencia del Mercado de Valores, o cualquier norma posterior que la modifique o sustituya o complemente).

(iv) Deberá procurar el cumplimiento de las obligaciones señaladas en los numerales (i) y (ii) de la presente cláusula, por parte de sus propios asociados, agentes o subcontratistas que puedan ser utilizados por EL CONTRATISTA para el cumplimiento de las obligaciones en virtud del presente contrato.

(v) En caso de ser sujeto obligado a informar a la UIF, EL CONTRATISTA deberá contar con políticas y procedimientos diseñados para prevenir la comisión de delitos de lavado de activos, financiamiento del terrorismo, cohecho (en sus distintas formas) y/o corrupción, en la prestación de servicios a LA ENTIDAD. EL CONTRATISTA deberá cumplir estas obligaciones, sobre todo en relación a las personas, asociadas, agentes o subcontratistas que puedan ser utilizados en la ejecución de los servicios prestados a LA ENTIDAD.

[9] 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).

Adicionalmente y para todos los efectos del presente contrato y los servicios objeto del mismo, EL CONTRATISTA informa que cuenta con los medios idóneos para la prevención del lavado de activos y de la financiación del terrorismo y realizará las gestiones pertinentes para efectuar las verificaciones a que haya lugar con el fin de evitar el ingreso y egreso de recursos que provengan de actividades relacionadas a dichos delitos.

En caso que EL CONTRATISTA tuviera noticia de la ocurrencia de alguno de estos hechos que actual o potencialmente pudieran impactar de cualquier forma a LA ENTIDAD sea en su responsabilidad penal, civil o reputacional, deberá informar de inmediato de este hecho a LA ENTIDAD; sin perjuicio de tomar todas las medidas necesarias para evitar o mitigar estos efectos. Asimismo, EL CONTRATISTA se compromete a entregar a LA ENTIDAD toda la información que ésta le requiera en el marco de las investigaciones internas, sean éstas de carácter meramente preventivo o cuándo se indague sobre hechos constitutivos de delito, como también cuando las investigaciones tengan carácter sistemático o aleatorio.

Asimismo, EL CONTRATISTA se obliga expresamente a entregar a LA ENTIDAD la información veraz y verificable que éste le exija para el cumplimiento de la normativa relacionada, y a actualizar sus datos por lo menos anualmente, suministrando la totalidad de la información que LA ENTIDAD requiera. En el evento en que no se cumpliese con la obligación consagrada en la presente cláusula, LA ENTIDAD solicitará a EL CONTRATISTA la subsanación del incumplimiento, bajo apercibimiento, en caso de no cumplir con dicha subsanación, de resolver el contrato.

Considerando que el presente servicio comprende un periodo mayor o igual a dos años, de conformidad a lo detallado en el Artículo 36° de la Res. 2660-2015, Reglamento de Gestión de Riesgos de Lavado de Activos y del Financiamiento del Terrorismo, EL CONTRATISTA se compromete a actualizar la información de forma periódica; el plazo de actualización no puede ser mayor a los dos (2) años. En caso no se haya modificado la información, deberá dejarse constancia de ello

CLÁUSULA VIGÉSIMA SEGUNDA: 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 TERCERA: 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"

ANEXOS

ANEXO Nº 1

DECLARACIÓN JURADA DE DATOS DEL POSTOR

Señores
COMITÉ DE SELECCIÓN
CONCURSO PÚBLICO Nº 04-2021-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 Nº [CONSIGNAR EN CASO DE SER PERSONA JURÍDICA] Asiento Nº [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[10]		Sí		No	
Correo electrónico :					

Autorización de notificación por correo electrónico:

… [CONSIGNAR SÍ O NO] 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 subsanación de los requisitos para perfeccionar el contrato.
3. Solicitud al postor que ocupó el segundo lugar en el orden de prelación para presentar los documentos para perfeccionar el contrato.
4. Respuesta a la solicitud de acceso al expediente de contratación.
5. Notificación de la orden de servicios[11]

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

[10] 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.

[11] 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.

La notificación dirigida a la dirección de correo electrónico consignada se entenderá válidamente efectuada cuando la Entidad reciba acuse de recepción.

Importante

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

ANEXO Nº 1

DECLARACIÓN JURADA DE DATOS DEL POSTOR

Señores
COMITÉ DE SELECCIÓN
CONCURSO PÚBLICO Nº 04-2021-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[12]		Sí		No	
Correo electrónico :					

Datos del consorciado 2					
Nombre, Denominación o Razón Social :					
Domicilio Legal :					
RUC :	Teléfono(s) :				
MYPE[13]		Sí		No	
Correo electrónico :					

Datos del consorciado …					
Nombre, Denominación o Razón Social :					
Domicilio Legal :					
RUC :	Teléfono(s) :				
MYPE[14]		Sí		No	
Correo electrónico :					

Autorización de notificación por correo electrónico:

Correo electrónico del consorcio:

[12] 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.

[13] Ibídem.

[14] Ibídem.

… [CONSIGNAR SÍ O NO] 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 subsanación de los requisitos para perfeccionar el contrato.
3. Solicitud al postor que ocupó el segundo lugar en el orden de prelación para presentar los documentos para perfeccionar el contrato.
4. Respuesta a la solicitud de acceso al expediente de contratación.
5. Notificación de la orden de servicios[15]

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.

[15] 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 Nº 2

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

Señores
COMITÉ DE SELECCIÓN
CONCURSO PÚBLICO Nº 04-2021-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 Nº 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 Nº 3

DECLARACIÓN JURADA DE CUMPLIMIENTO DE LOS TÉRMINOS DE REFERENCIA

Señores
COMITÉ DE SELECCIÓN
CONCURSO PÚBLICO Nº 04-2021-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 Nº 4

DECLARACIÓN JURADA DE PLAZO DE PRESTACIÓN DEL SERVICIO

Señores
COMITÉ DE SELECCIÓN
CONCURSO PÚBLICO Nº 04-2021-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 Nº 5

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

Señores
COMITÉ DE SELECCIÓN
CONCURSO PÚBLICO Nº 04-2021-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 Nº** [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]	[%] [16]
	[DESCRIBIR LAS OBLIGACIONES DEL CONSORCIADO 1]	
2.	OBLIGACIONES DE [NOMBRE, DENOMINACIÓN O RAZÓN SOCIAL DEL CONSORCIADO 2]	[%] [17]
	[DESCRIBIR LAS OBLIGACIONES DEL CONSORCIADO 2]	
	TOTAL OBLIGACIONES	100%[18]

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

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

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

[CONSIGNAR CIUDAD Y FECHA]

.....	.....
Consorciado 1	**Consorciado 2**
Nombres, apellidos y firma del Consorciado 1	**Nombres, apellidos y firma del Consorciado 2**
o de su Representante Legal	**o de su Representante Legal**
Tipo y N° de Documento de Identidad	**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 Nº 6

PRECIO DE LA OFERTA

Señores
COMITÉ DE SELECCIÓN
CONCURSO PÚBLICO Nº 04-2021-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 Nº 7

EXPERIENCIA DEL POSTOR EN LA ESPECIALIDAD

Señores
COMITÉ DE SELECCIÓN
CONCURSO PÚBLICO Nº 04-2021-COFIDE
Presente.-

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

Nº	CLIENTE	OBJETO DEL CONTRATO	N° CONTRATO / O/S / COMPROBANTE DE PAGO	FECHA DEL CONTRATO O CP [19]	FECHA DE LA CONFORMIDAD DE SER EL CASO[20]	EXPERIENCIA PROVENIENTE[21] DE:	MONEDA	IMPORTE[22]	TIPO DE CAMBIO VENTA[23]	MONTO FACTURADO ACUMULADO [24]
1										
2										
3										
4										

[19] 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.

[20] 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.

[21] 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"*.

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

[23] 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.

[24] 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 [19]	FECHA DE LA CONFORMIDAD DE SER EL CASO[20]	EXPERIENCIA PROVENIENTE[21] DE:	MONEDA	IMPORTE[22]	TIPO DE CAMBIO VENTA[23]	MONTO FACTURADO ACUMULADO [24]
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 Nº 8

DECLARACIÓN JURADA
(NUMERAL 49.4 DEL ARTÍCULO 49 DEL REGLAMENTO)

Señores
COMITÉ DE SELECCIÓN
CONCURSO PÚBLICO Nº 04-2021-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/rnp/content/relación-de-proveedores-sancionados. *También le asiste dicha facultad al órgano encargado de las contrataciones o al órgano de la Entidad al que se le haya asignado la función de verificación de la oferta presentada por el postor ganador de la buena pro.*

ANEXO COFIDE 1

Señores
DEPARTAMENTO DE COMPRAS
ADJUDICACIÓN SIMPLIFICADA Nº 023-2021-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 Directores de la empresa		DNI		
	Añadir las filas que se necesiten			
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)

(*) para mayor información www.osce.gob.pe, link Legislación y documentos Osce, Ley de Contrataciones del Estado y Reglamento.

ANEXO COFIDE 2

Señores
DEPARTAMENTO DE COMPRAS
ADJUDICACIÓN SIMPLIFICADA Nº 023-2021-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.	☐	☐
Tener antecedentes judiciales.	☐	☐
Tener procesos judiciales abiertos y/o investigaciones judiciales a la fecha de la firma de la presente declaración.	☐	☐
Tener antecedentes Policiales.	☐	☐
Tener procesos Policiales abiertos y/o investigaciones policiales a la fecha de la firma de la presente declaración.	☐	☐
Tener antecedentes Penales.	☐	☐
Tener procesos Penales abiertos y/o investigaciones penales a la fecha de la firma de la presente declaración.	☐	☐

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 respetivo.

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:

_____
_____
_____
_____
_____
_____
_____
_____
_____
_____
_____
_____
_____
_____
_____
_____

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

Código de Ética
y Conducta para Proveedores de Cofide

1. Objetivo.-

El presente lineamiento tiene como objetivo que los proveedores que intervienen activamente en la cadena de valor de COFIDE, 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 son fundamentales 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.

3. Compromisos de los proveedores.-

Las pautas éticas que deben de 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 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 Promover a la interna el rechazo el trabajo forzoso u obligatorio y el trabajo infantil.
3.5 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.
3.6 No ofrecer presentes, invitaciones o atenciones que, directa o indirectamente, puedan llevar a establecer vínculos o compromisos que empañen la transparencia de los negocios, salvo las excepciones contenidas en el Código de Ética y Conducta de Cofide.
3.7 Cumplir con la normativa de Seguridad y Salud ocupacional en sus instalaciones con su personal, y al prestar un servicio a Cofide.
3.8 Cumplir con las políticas de Cofide relativas a la prevención de delitos, lavado de activos, soborno y extorsión, así como con las normas de conducta ética y moral, respetando las leyes aplicables sobre esta materia y asegurándose de que establecen los procedimientos adecuados que sean exigidos.
3.9 Actuar de manera honesta e integra, 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.

3.10 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.

3.11 Reportar de manera inmediata cuando noten cualquier incumplimiento comprobado o potencia a los presentes lineamientos y código de ética y conducta de Cofide.

3.12 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.

4. Compromisos de Cofide hacia los proveedores.-

De acuerdo al Código de Ética y Conducto 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 – Línea Ética.-

Cofide pone a disposición una línea ética, que es administrada por un tercero independiente y accesible a través de:

6.1 Intranet web: www.bdolineaetica.com/cofide

6.2 Línea Telefónica 0800-00-626 ó (01) 622-3103

6.3 Correo electrónico lineaetica@bdo.com.pe

6.4 Buzón de correspondencia: enviar una carta indicando como referencia Línea Ética BDO, a las oficinas de BDO Consulting: Av. Antonio Miroquesada N° 425 piso 10, Magdalena del Mar.

6.5 Entrevista personal, solicitarla vía correo electrónico o por teléfono, se le recibirá con total discreción en la dirección precisada en el numeral precedente.

Aprobado por: Gerencia de Gestión Humana y Administración
Fecha: 17.11.2020
Versión 2.0