

BASES

ADJUDICACIÓN SIMPLIFICADA N° 035-2021-COFIDE

TERCERA CONVOCATORIA

CONTRATACION DEL SERVICIO DE CONSULTORIA PARA LA ADECUACIÓN AL NUEVO REGLAMENTO DE LA GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN Y LA CIBERSEGURIDAD

DEBER DE COLABORACIÓN

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

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

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

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

SECCIÓN GENERAL

DISPOSICIONES COMUNES DEL PROCEDIMIENTO DE SELECCIÓN

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

CAPÍTULO I

ETAPAS DEL PROCEDIMIENTO DE SELECCIÓN

1.1. REFERENCIAS

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

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

1.2. CONVOCATORIA

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

1.3. REGISTRO DE PARTICIPANTES

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

Importante

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

1.4. FORMULACIÓN DE CONSULTAS Y OBSERVACIONES A LAS BASES

La formulación de consultas y observaciones a las bases se efectúa de conformidad con lo establecido en los numerales 72.1 y 72.2 del artículo 72 del Reglamento, así como el literal a) del artículo 89 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 el numeral 72.4 del artículo 72 y el literal a) del artículo 89 del Reglamento.

Importante

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

1.6. FORMA DE PRESENTACIÓN DE OFERTAS

Las ofertas se presentan conforme lo establecido en el artículo 59 y en el artículo 90 del Reglamento.

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

Importante

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

1.7. PRESENTACIÓN Y APERTURA DE OFERTAS

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

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

Importante

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

En la apertura electrónica de la oferta técnica, el órgano encargado de las contrataciones o el comité de selección, según corresponda, verifica la presentación de lo exigido en la sección específica de las bases de conformidad con el numeral 81.2 del artículo 81 del Reglamento y determina si las ofertas responden a las características y/o requisitos y condiciones de los Términos de Referencia, detallados en la sección específica de las bases. De no cumplir con lo requerido, la oferta se considera no admitida.

1.8. CALIFICACIÓN Y EVALUACIÓN DE LAS OFERTAS

La calificación y evaluación de los postores se realiza conforme los requisitos de calificación y factores de evaluación que se indican en la sección específica de las bases.

La evaluación técnica y económica se realiza sobre la base de:

Oferta técnica : 100 puntos
Oferta económica : 100 puntos

1.8.1 CALIFICACIÓN DE LAS OFERTAS TÉCNICAS

La calificación de las ofertas técnicas se realiza conforme a lo establecido en el numeral 82.1 del artículo 82 del Reglamento.

1.8.2 EVALUACIÓN DE LAS OFERTAS TÉCNICAS

La evaluación de las ofertas técnicas se realiza conforme a lo establecido en los numerales 82.2 y 82.3 del artículo 82 del Reglamento.

1.8.3 APERTURA Y EVALUACIÓN DE OFERTAS ECONÓMICAS

El órgano encargado de las contrataciones o el comité de selección, según corresponda, evalúa las ofertas económicas y determina el puntaje total de las ofertas de conformidad con el artículo 83 del Reglamento así como los coeficientes de ponderación previstos en la sección específica de las bases.

Importante

En el caso de contratación de consultorías que se presten fuera de la provincia de Lima y Callao, cuyo valor estimado no supere los doscientos mil Soles (S/ 200,000.00), a solicitud del postor se asigna una bonificación equivalente al diez por ciento (10%) sobre el puntaje total obtenido por los postores con domicilio en la provincia donde prestará el servicio, o en las provincias colindantes, sean o no pertenecientes al mismo departamento o región. El domicilio es el consignado en la constancia de inscripción ante el RNP¹. Lo mismo aplica en el caso de procedimientos de selección por relación de ítems, cuando algún ítem no supera el monto señalado anteriormente.

1.9. 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 La constancia de inscripción electrónica se visualizará en el portal web del Registro Nacional de Proveedores: www.rnp.gob.pe

1.10. OTORGAMIENTO DE LA BUENA PRO

La buena pro se otorga luego de la evaluación correspondiente según lo indicado en el numeral 1.8.3 de la presente sección.

Previo al otorgamiento de la buena pro, el órgano encargado de las contrataciones o el comité de selección, según corresponda, aplica lo dispuesto en los numerales 68.1, 68.2, 68.3 y 68.6 del artículo 68 del Reglamento, de ser el caso.

En el supuesto que dos (2) o más ofertas empaten, el otorgamiento de la buena pro se efectúa observando estrictamente el orden señalado en el numeral 91.2 del artículo 91 del Reglamento.

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

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

1.11. CONSENTIMIENTO DE LA BUENA PRO

Cuando se hayan presentado dos (2) o más ofertas, el consentimiento de la buena pro se produce a los cinco (5) días hábiles siguientes de la notificación de su otorgamiento, sin que los postores hayan ejercido el derecho de interponer el recurso de apelación.

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

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

Importante

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

CAPÍTULO II

SOLUCIÓN DE CONTROVERSIAS DURANTE EL PROCEDIMIENTO DE SELECCIÓN

2.1. RECURSO DE APELACIÓN

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

El recurso de apelación se presenta ante la Entidad convocante, y es conocido y resuelto por su Titular, cuando el valor estimado sea igual o menor a cincuenta (50) UIT. Cuando el valor estimado sea mayor a dicho monto, el recurso de apelación se presenta ante y es resuelto por el Tribunal de Contrataciones del Estado.

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

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

Importante

- *Una vez otorgada la buena pro, el órgano encargado de las contrataciones o el comité de selección, según corresponda, está en la obligación de permitir el acceso de los participantes y postores al expediente de contratación, salvo la información calificada como secreta, confidencial o reservada por la normativa de la materia, a más tardar dentro del día siguiente de haberse solicitado por escrito.*
- *A efectos de recoger la información de su interés, los postores pueden valerse de distintos medios, tales como: (i) la lectura y/o toma de apuntes, (ii) la captura y almacenamiento de imágenes, e incluso (iii) pueden solicitar copia de la documentación obrante en el expediente, siendo que, en este último caso, la Entidad deberá entregar dicha documentación en el menor tiempo posible, previo pago por tal concepto.*
- *El recurso de apelación se presenta ante la Mesa de Partes del Tribunal o ante las oficinas desconcentradas del OSCE o en la Unidad de Trámite Documentario de la Entidad, según corresponda.*

2.2. PLAZOS DE INTERPOSICIÓN DEL RECURSO DE APELACIÓN

La apelación contra el otorgamiento de la buena pro o contra los actos dictados con anterioridad a ella se interpone dentro de los cinco (5) días hábiles siguientes de haberse notificado el otorgamiento de la buena pro.

La apelación contra los actos dictados con posterioridad al otorgamiento de la buena pro, contra la declaración de nulidad, cancelación y declaratoria de desierto del procedimiento, se interpone dentro de los cinco (5) días hábiles siguientes de haberse tomado conocimiento del acto que se desea impugnar.

CAPÍTULO III DEL CONTRATO

3.1. PERFECCIONAMIENTO DEL CONTRATO

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

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

3.2. GARANTÍAS

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

3.2.1. GARANTÍA DE FIEL CUMPLIMIENTO

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

3.2.2. GARANTÍA DE FIEL CUMPLIMIENTO POR PRESTACIONES ACCESORIAS

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

Importante

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

3.2.3. GARANTÍA POR ADELANTO

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

3.3. REQUISITOS DE LAS GARANTÍAS

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

Importante

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

Advertencia

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

- 1. La clasificadora de riesgo que asigna la clasificación a la empresa que emite la garantía debe encontrarse listada en el portal web de la SBS (<http://www.sbs.gob.pe/sistema-financiero/clasificadoras-de-riesgo>).*
- 2. Se debe identificar en la página web de la clasificadora de riesgo respectiva, cuál es la clasificación vigente de la empresa que emite la garantía, considerando la vigencia a la fecha de emisión de la garantía.*
- 3. Para fines de lo establecido en el artículo 148 del Reglamento, la clasificación de riesgo B, incluye las clasificaciones B+ y B.*
- 4. Si la empresa que otorga la garantía cuenta con más de una clasificación de riesgo emitida por distintas empresas listadas en el portal web de la SBS, bastará que en una de ellas cumpla con la clasificación mínima establecida en el Reglamento.*

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

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

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

3.4. EJECUCIÓN DE GARANTÍAS

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

3.5. ADELANTOS

La Entidad puede entregar adelantos directos al contratista, los que en ningún caso exceden en

conjunto del treinta por ciento (30%) del monto del contrato original, siempre que ello haya sido previsto en la sección específica de las bases.

3.6. PENALIDADES

3.6.1. PENALIDAD POR MORA EN LA EJECUCIÓN DE LA PRESTACIÓN

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

3.6.2. OTRAS PENALIDADES

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

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

3.7. INCUMPLIMIENTO DEL CONTRATO

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

3.8. PAGOS

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

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

La conformidad se emite en un plazo máximo de 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 N° : 20100116392.
Domicilio legal : Augusto Tamayo N° 160 San Isidro.
Teléfono: : 615-4000.
Correo electrónico: : mreyes@cofide.com.pe.

1.2. OBJETO DE LA CONVOCATORIA

El presente procedimiento de selección tiene por objeto la contratación del servicio de consultoría para la adecuación al nuevo reglamento de la gestión de la seguridad de la información y la ciberseguridad.

1.3. EXPEDIENTE DE CONTRATACIÓN

El expediente de contratación fue aprobado mediante acta de aprobación del expediente N° 063A-2021-GGHA, el 21 de enero del 2022.

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. ALCANCES DEL REQUERIMIENTO

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

1.7. PLAZO DE PRESTACIÓN DEL SERVICIO DE CONSULTORÍA

Los servicios materia de la presente convocatoria se prestarán en el plazo de 110 días de acuerdo a lo indicado en los términos de referencia, en concordancia con lo establecido en el expediente de contratación.

1.8. 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.

1.9. 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 N° 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 N° 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 N° 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 N° 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.
- Decreto de Urgencia N° 063-2021, que establece medidas extraordinarias complementarias, durante el año fiscal 2021, para promover la dinamización de las inversiones en el marco de la reactivación económica y la ejecución del gasto público; así como asegurar la continuidad de los procesos de contratación en el marco del sistema nacional de abastecimiento y dicta otras disposiciones.

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 documentos², la siguiente documentación:

2.2.1. Documentación de presentación obligatoria

2.2.1.1. Documentación de presentación obligatoria

A. Documentos para la admisión de la oferta

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

a.2) Documento que acredite la representación de quien suscribe la oferta.

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

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

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

Advertencia

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

a.3) Declaración jurada de acuerdo con el literal b) del artículo 52 del

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

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

Reglamento (**Anexo N°2**).

- a.4) Declaración jurada de cumplimiento de los Términos de Referencia contenidos en el numeral 3.1 del Capítulo III de la presente sección. (Anexo N° 3).
- a.5) Declaración jurada de plazo de prestación del servicio de consultoría. (**Anexo N° 4**).
- a.6) Carta de compromiso del personal clave con firma legalizada, según lo previsto en el numeral 3.1 del Capítulo III de la presente sección. (**Anexo N° 5**).
- a.7) Promesa de consorcio con firmas legalizadas, de ser el caso, en la que se consigne los integrantes, el representante común, el domicilio común y las obligaciones a las que se compromete cada uno de los integrantes del consorcio así como el porcentaje equivalente a dichas obligaciones. (**Anexo N° 6**)

Importante

El órgano encargado de las contrataciones o el comité de selección, según corresponda, verifica la presentación de los documentos requeridos. De no cumplir con lo requerido, la oferta se considera no admitida.

B. 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.

2.2.1.2. Documentación de presentación facultativa:

- a) En el caso de microempresas y pequeñas empresas integradas por personas con discapacidad, o en el caso de consorcios conformados en su totalidad por estas empresas, deben presentar la constancia o certificado con el cual acredite su inscripción en el Registro de Empresas Promocionales para Personas con Discapacidad⁴.
- b) Incorporar en la oferta los documentos que acreditan los “**Factores de Evaluación**” establecidos en el Capítulo IV de la presente sección de las bases, a efectos de obtener el puntaje previsto en dicho Capítulo para cada factor.
- c) Solicitud de bonificación por tener la condición de micro y pequeña empresa. (**Anexo N° 13**)

Advertencia

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

⁴ Dicho documento se tendrá en consideración en caso de empate, conforme a lo previsto en el artículo 91 del Reglamento.

2.2.2. OFERTA ECONÓMICA

La oferta económica expresada en **Soles** debe registrarse directamente en el formulario electrónico del SEACE.

Adicionalmente, se debe adjuntar el **Anexo N° 7**, en el caso de procedimientos convocados a precios unitarios, tarifas u honorario fijo y la comisión de éxito.

En el caso de procedimientos convocados a suma alzada, únicamente se debe adjuntar el **Anexo N° 7** cuando corresponda indicar el monto de la oferta de la prestación accesoria o que el postor goza de alguna exoneración legal.

El monto total de la oferta económica y los subtotales que lo componen deben ser expresados con dos (2) decimales. Los precios unitarios o tarifas pueden ser expresados con más de dos (2) decimales.

Importante

La estructura de costos o análisis de precios, se presenta para el perfeccionamiento del contrato, de ser el caso.

2.3. DETERMINACIÓN DEL PUNTAJE TOTAL DE LAS OFERTAS

Una vez evaluadas las ofertas técnica y económica se procederá a determinar el puntaje total de las mismas.

El puntaje total de las ofertas es el promedio ponderado de ambas evaluaciones, obtenido de la aplicación de la siguiente fórmula:

$$PTP_i = c_1 PT_i + c_2 Pe_i$$

Donde:

PTP_i = Puntaje total del postor i
PT_i = Puntaje por evaluación técnica del postor i
Pe_i = Puntaje por evaluación económica del postor i
c₁ = Coeficiente de ponderación para la evaluación técnica.
c₂ = Coeficiente de ponderación para la evaluación económica.

Se aplicarán las siguientes ponderaciones:

c₁ = **0.80**

c₂ = **0.20**

Donde: c₁ + c₂ = 1.00

2.4. PRESENTACIÓN DEL RECURSO DE APELACIÓN

“El recurso de apelación se presenta ante la Unidad de Trámite Documentario de la Entidad.

En caso el participante o postor opte por presentar recurso de apelación y por otorgar la garantía mediante depósito en cuenta bancaria, se debe realizar el abono en:

N° de cuenta : Cta. Cte. N° 193-0245964-0-83
Banco : Banco de Crédito del Perú
N° CCI⁵ : 002 193 0002 4596 4083 11

⁵ En caso de transferencia interbancaria.

2.5. REQUISITOS PARA PERFECCIONAR EL CONTRATO

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

- Garantía de fiel cumplimiento del contrato.
- Contrato de consorcio con firmas legalizadas ante Notario de cada uno de los integrantes, de ser el caso.
- 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)	

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

Advertencia

De acuerdo con el artículo 4 del Decreto Legislativo N° 1246, las Entidades están prohibidas de exigir a los administrados o usuarios la información que puedan obtener directamente mediante la interoperabilidad a que se refieren los artículos 2 y 3 de dicho Decreto Legislativo. En esa medida, si la Entidad es usuaria de la Plataforma de Interoperabilidad del Estado – PIDE⁶ y siempre que el servicio web se encuentre activo en el Catálogo de Servicios de dicha plataforma, no corresponderá exigir los documentos previstos en los literales d) y e).

- Domicilio para efectos de la notificación durante la ejecución del contrato.
- Estructura de costos de la oferta económica⁷.
- Documentación que acredite la especialización del Jefe de proyecto y Consultor Senior.
- Declaración jurada solicitada por COFIDE (Anexo COFIDE 1).
- Declaración jurada del representante legal (Anexo COFIDE 2).

Importante

- En caso que el postor ganador de la buena pro sea un consorcio, las garantías que presente este para el perfeccionamiento del contrato, así como durante la ejecución contractual, de ser el caso, además de cumplir con las condiciones establecidas en el artículo 33 de la Ley y en el artículo 148 del Reglamento, deben consignar expresamente el nombre completo o la denominación o razón social de los integrantes del consorcio, en calidad de garantizados, de

⁶ 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/>

⁷ Incluir solo cuando resulte necesario para la ejecución contractual, identificar los costos de cada uno de los rubros que comprenden la oferta.

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

Importante

- Corresponde a la Entidad verificar que las garantías presentadas por el postor ganador de la buena pro cumplan con los requisitos y condiciones necesarios para su aceptación y eventual ejecución, sin perjuicio de la determinación de las responsabilidades funcionales que correspondan.*
- De conformidad con el Reglamento Consular del Perú aprobado mediante Decreto Supremo N° 076-2005-RE para que los documentos públicos y privados extendidos en el exterior tengan validez en el Perú, deben estar legalizados por los funcionarios consulares peruanos y refrendados por el Ministerio de Relaciones Exteriores del Perú, salvo que se trate de documentos públicos emitidos en países que formen parte del Convenio de la Apostilla, en cuyo caso bastará con que estos cuenten con la Apostilla de la Haya⁸.*
- La Entidad no puede exigir documentación o información adicional a la consignada en el presente numeral para el perfeccionamiento del contrato.*

2.6. 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 N° 160, San Isidro.

2.7. FORMA DE PAGO

La Entidad realizará el pago de la contraprestación pactada a favor del contratista en **2 cuotas equivalentes al 35% y 65% del monto contractual, según términos de referencia.**

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

- Acta de conformidad suscrita por el funcionario responsable.

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

- Entregables según términos de referencia.
- Comprobante de pago (deberá ser remitido al email facturaselectronicas@cofide.com.pe).

Dicha documentación se 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

Contratación del servicio de adecuación al nuevo Reglamento para la Gestión de la Seguridad de la Información y la Ciberseguridad.

2. FINALIDAD PÚBLICA

El servicio de consultoría permitirá cumplir adecuadamente con lo estipulado en la Resolución SBS 504-2021 – mediante el cual se aprueba el Reglamento para la Gestión de la Seguridad de la Información y la Ciberseguridad, la cual contribuirá a asegurar la sostenibilidad institucional de COFIDE.

3. NÚMERO MÁXIMO DE CONSORCIADOS

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

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

4. EQUIPO DE TRABAJO

La empresa deberá contar como mínimo con el siguiente personal, cabe mencionar que este detalle no limita a la empresa a colocar mayor cantidad o calidad de personal, de acuerdo a la eficiencia para el cumplimiento del servicio:

Cargo y Rol	Requerimiento mínimo
Jefe de Proyecto (Personal Clave)	<p>Años de Experiencia: Mínimo tres (3) años de experiencia como Oficial de Seguridad de Información o Jefe o Líder de proyectos de servicios similares al objeto de contratación, como Ciberseguridad, Seguridad de la Información, Seguridad Informática, Diseño e Implementación de Gobierno y Gestión de Tecnología o Seguridad en redes y nube; de los cuales por lo menos uno y medio (1.5) años deben ser en Seguridad de la Información y por lo menos seis (6) meses en Ciberseguridad o servicios relacionados con Ciberseguridad (Hacking Ético, Pentesting, Servicio de Centro de Operaciones de Seguridad, Análisis Forense), en ambos casos en Instituciones Financieras (empresas de operaciones múltiples, AFPs o empresas de seguros), en la calidad de Oficial de Seguridad de Información o Jefe o Líder de Proyecto.</p> <p>Carrera Profesional: Titulado en Ingeniería de Sistemas, Industrial, Electrónica, Computación e Informática o similares.</p> <p>Especialización: Diplomado en Gerencia de Proyectos o Certificación PMP.</p>
Consultor Senior	<p>Años de Experiencia: Mínimo tres (3) años de experiencia como Consultor en proyectos de servicios similares al objeto de contratación, como Ciberseguridad, Seguridad de la Información, Seguridad Informática o Seguridad en redes y nube; de los cuales por lo menos uno y medio (1.5) años deben</p>

(Personal Clave)	<p>ser en Seguridad de la Información y por lo menos seis (6) meses en Ciberseguridad o servicios relacionados con Ciberseguridad (Hacking Ético, Pentesting, Servicio de Centro de Operaciones de Seguridad, Análisis Forense), en ambos casos en Instituciones Financieras (empresas de operaciones múltiples, AFPs o empresas de seguros), en calidad de Consultor.</p> <p>Carrera Profesional: Titulado en Ingeniería de Sistemas, Electrónica, Computación e Informática o similares.</p> <p>Especialización: Contar con Certificación ISO 27032 Lead Cybersecurity Manager o Certificación ISO 27032 Senior Lead Cybersecurity Manager</p>
-------------------------	--

Para sustentar la carrera profesional y especialización del personal propuesto se deberá presentar copia simple de sus diplomas y/o títulos y/o constancia de estudios realizados.

Para sustentar los años de experiencia, se deberá presentar las certificaciones o constancias de trabajo o prestación de servicios, donde se indique claramente la vigencia del servicio, nombres y apellidos, y nombre del proyecto o actividades realizadas, y para qué empresa realizó el servicio (empresa cliente).

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

NOTA IMPORTANTE:

El personal propuesto solo podrá ser reemplazado por causas justificables aceptadas por la Corporación, y siempre que medie un aviso previo de siete (7) días calendario. El reemplazante deberá cumplir con igual o mejor perfil que el personal sustituido.

5. DESCRIPCIÓN DEL SERVICIO

COFIDE cuenta con un Sistema de Gestión de Seguridad Información (SGSI), conforme a lo establecido en la circular G-140-2009: Gestión de la Seguridad de la Información aprobado por la SBS; contando con una estructura organizativa como funcional definida para la gestión de riesgo de seguridad de la información y un marco de trabajo construido sobre la base de políticas, directivas, metodologías y procedimientos. Así mismo, cuenta con una infraestructura tecnológica que soporta los procesos y servicios (**Anexo 1**).

Mediante Resolución SBS N° 504-2021 se aprobó el Reglamento para la Gestión de Seguridad de Información y Ciberseguridad (SGSI-C), en adelante Reglamento SBS, siendo uno de los requerimientos que las empresas elaboren un Plan de Adecuación SBS a dicho Reglamento.

El servicio tiene por objetivo adecuar el Sistema de Gestión de Seguridad de la Información (SGSI) de COFIDE al Reglamento para la Gestión de la Seguridad de la Información y Ciberseguridad, así como al Reglamento Interno de CAVALI, relacionado a la Gestión de la Ciberseguridad, en adelante Reglamento CAVALI. Para ello se requiere que el Contratista realice un diagnóstico del SGSI que tiene actualmente COFIDE a fin de que identifique las brechas respecto a las normas antes mencionadas (Reglamento SBS y Reglamento CAVALI), considerando además el Plan de Adecuación SBS elaborado por COFIDE que fuera remitido a la SBS.

Sobre la base del diagnóstico, el Contratista, deberá establecer un *Plan de Trabajo de Implementación* que incluya los planes de acción para el cierre de brechas identificados en el Plan de Adecuación SBS que se especifican en la Etapa 4: Implementación, así como los planes de acción para la implementación del Reglamento CAVALI que también se especifican en la Etapa 4: Implementación.

Adicionalmente, el contratista deberá entregar propuestas de planes de acción para el cierre de brechas que haya identificado sobre el Reglamento SBS y sobre el Reglamento CAVALI y que no estén especificadas en la Etapa 4: Implementación.

Se deberá tomar en cuenta que, el plan de trabajo propuesto para la adecuación a la norma de la SBS, esté acorde con lo establecido en el Artículo 4 del Reglamento SBS, en el cual se indica que las disposiciones descritas en el Capítulo II, Subcapítulo V Régimen Simplificado del Reglamento SBS, es de aplicación obligatoria para COFIDE.

El servicio deberá considerar como mínimo las siguientes etapas:

Etapas 1: Inicio y planificación del servicio

El inicio del servicio tiene por finalidad tener un entendimiento de los canales de comunicación, entrega de información y puntos de contacto. El Contratista realizará las siguientes actividades:

- Reunión de lanzamiento (Kick-Off) con el personal de COFIDE.
- Presentar el Plan de Trabajo del Servicio, incluyendo el cronograma de actividades.

Etapas 2: Entendimiento de la Organización

Esta etapa tiene por finalidad entender a la organización, su naturaleza, cadena de valor, stakeholders y otros que se consideren relevantes para el desarrollo del servicio.

Se pondrá a disposición del Contratista del servicio, la información que consideren necesaria para el entendimiento de la organización.

El Contratista deberá indicar las entrevistas y reuniones con el personal de COFIDE que requiera, para el desarrollo de esta etapa.

Etapas 3: Diagnóstico, brechas y Planes de acción

Esta etapa tiene por finalidad realizar un diagnóstico de la situación actual del SGSI de COFIDE, identificar las brechas respecto a lo requerido en el Reglamento SBS y Reglamento CAVALI, y definir los planes de acción para el cierre de brechas.

Para el diagnóstico de la situación actual del SGSI de COFIDE se considerará:

- Revisar el marco para la gestión del sistema de seguridad de información
 - o Políticas de seguridad de información
 - o Directivas de seguridad de información
 - o Procedimientos
 - o Informe del Plan de Adecuación SBS elaborado por COFIDE.
- Roles y responsabilidades
 - o Roles y responsabilidades para la gestión de la seguridad de la información
 - o Manual de organización y funciones de las áreas con roles relevantes para la gestión de la seguridad de información
- Tecnología de información
 - o Infraestructura tecnológica y de comunicaciones
 - o Sistemas de información que soportan a los procesos críticos (Captaciones, Colocaciones, Inversiones y Fideicomisos)
 - o Servicio de ciberseguridad (SOC) contratado con un tercero. (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)
- Identificación de los principales actores para la adecuada gestión de la seguridad de información y ciberseguridad.

Para la identificación de brechas, se deberá tomar en cuenta la situación actual del SGSI de COFIDE respecto a lo solicitado en las normas relacionadas con el SGSI y Ciberseguridad emitidas por:

- SBS - Resolución N° 504-2021 aprobando el Reglamento para la Gestión de la Seguridad de la Información y la Ciberseguridad, en adelante Reglamento SBS (**Anexo 2**).
- SMV - Reglamento Interno de CAVALI, Capítulo II: De los Participantes, Anexo 2, Gestión de la Ciberseguridad (**Anexo 3**).

Como resultado del diagnóstico, identificación de brechas y planes de acción para el cierre de brechas, el Contratista deberá elaborar un Informe donde se incluya, el diagnóstico actual de COFIDE identificando: i) los requerimientos del Reglamento SBS y Reglamento CAVALI que COFIDE estaría cumpliendo con el sustento respectivo, ii) los requerimientos del Reglamento SBS y Reglamento CAVALI que no se estarían cumpliendo y representan una brecha con la explicación respectiva, iii) los planes de acción para cerrar cada una de las brechas identificadas, y iv) Plan de trabajo de Implementación que incluye el cronograma para la implementación de los planes de acción que cubren las brechas identificadas en el Plan de Adecuación SBS y los planes de acción respecto al Reglamento CAVALI, dentro del periodo del servicio contratado, indicando así mismo, las áreas de COFIDE que participarán en la implementación respectiva. Los planes de acción que serán implementados por el Contratista, son los que cubran las brechas identificadas en el Plan de Adecuación SBS de COFIDE y los planes de acción respecto al Reglamento CAVALI, detallados en la Etapa 4: Implementación.

El Contratista deberá solicitar la información adicional que consideren necesaria para realizar el diagnóstico de la situación actual e identificación de brechas respecto a lo requerido en el Reglamento SBS y el Reglamento CAVALI, así como para elaborar el Plan de Trabajo de Implementación.

El Contratista deberá indicar las entrevistas y reuniones con el personal de COFIDE que requiera, para el desarrollo de esta etapa.

Etapa 4: Implementación

Implementación de los planes de acción identificadas en la Etapa 3 que deben ser implementadas por el Contratista de acuerdo al Plan de Trabajo de Implementación.

Dentro de los planes de acción identificados en el Plan de Adecuación SBS de COFIDE se encuentran los siguientes:

- Desarrollar el Plan estratégico del SGSI-C, el mismo que se incorporará como componente en el Manual de Gestión de Seguridad de Información.
- Proponer el alcance de la función del Comité de Riesgos en relación a fomentar la cultura de riesgo y conciencia de la necesidad de medidas apropiadas para su prevención, para ser incluido en la Estructura Organizacional para la gestión de Seguridad de Información.
- Proponer el alcance de la función de Seguridad de Información y Ciberseguridad, de reportar a los entes gubernamentales cuando lo requieran, conforme a la normativa, para ser incluido en la Estructura Organizacional para la gestión de Seguridad de Información.
- Proponer las áreas y personal de COFIDE, definiendo roles, responsabilidades y procedimiento para la gestión de incidentes, que deben conformar el equipo de trabajo multidisciplinario de manejo de incidentes de ciberseguridad, el cual debe estar conformado por representantes de las áreas que permitan prever en ellos los aspectos legales, técnicos y organizacionales.
- Proponer un Programa de Ciberseguridad estableciendo los respectivos lineamientos para ser incluidos en las Políticas de Seguridad de la Información.
- Desarrollar un procedimiento para el análisis forense de incidentes cibernéticos significativos adversos y su reporte al regulador, estableciendo los respectivos lineamientos para ser incluidos en las Políticas de Seguridad de la Información.
- Proponer los criterios pertinentes para el intercambio de información relativa a ciberseguridad, así como el tratamiento de esta información, a fin de tomar acción oportuna frente a las amenazas y vulnerabilidades, desarrollando los respectivos procedimientos, así como los respectivos lineamientos para ser incluidos en las políticas de Seguridad de la Información; tomando como referencia los lineamientos que establezca la SBS para el intercambio de información de ciberseguridad, en caso estos hayan sido emitidos.
- Proponer los roles y responsabilidades que el proveedor asume contractualmente (Servicios provistos por terceros), sobre la seguridad de la información, para la atención de los requerimientos del Reglamento SBS.
- Proponer lineamientos de seguridad de información para el uso de la nube, los que serán adicionados en las políticas de Seguridad de Información, asimismo desarrollar procedimientos, considerando el marco de buenas prácticas internacionales para el uso de estos servicios, conforme al Reglamento SBS.
- Proponer lineamientos para la evaluación del uso de Servicios Significativos de Procesamiento de Datos, incluido los servicios en nube, a ser incorporado en el Proceso

para la Evaluación de Riesgo de nuevos productos o cambios importantes en ambiente de negocios, operativo e informático.

- Proponer lineamientos que se deben considerar para la solicitud de autorización al supervisor, para la contratación de Servicios Significativos de Procesamiento de Datos en el exterior, a ser incorporado en el Proceso para la Evaluación de Riesgo de nuevos productos o cambios importantes en ambiente de negocios, operativo e informático.
- Proponer procedimientos o lineamientos para la planificación y ejecución de las actividades a realizar para la gestión de seguridad de información y ciberseguridad con periodicidad anual, conforme al Régimen Simplificado del Reglamento SBS, considerando como mínimo:
 - o Identificar con las unidades de negocio y de apoyo, cuál es la información de mayor importancia, por las obligaciones normativas o contractuales existentes, y por la necesidad de operar.
 - o Identificar los dispositivos que se conectan a la red interna y todo software que se encuentre instalado en la infraestructura tecnológica, y asegurar que se encuentren acorde a una configuración segura previamente establecida.
 - o Identificar las cuentas de usuario con permisos de acceso habilitados y en particular las que poseen privilegios administrativos con posibilidad de adicionar software a la infraestructura, y mantener el principio de mínimos privilegios otorgados.
 - o Implementar y mantener una línea base de seguridad en sistemas operativos y aplicaciones utilizadas, incluidos los correspondientes a dispositivos móviles, estaciones de trabajo, servidores y dispositivos de comunicaciones. Identificar y evaluar la habilitación de las funciones de seguridad integradas en los sistemas operativos.
 - o Priorizar y gestionar las vulnerabilidades de seguridad identificadas, para cuya identificación oportuna debe contar con los servicios de información necesarios.
 - o Desarrollar una campaña de orientación para la adopción de prácticas seguras en seguridad de la información y ciberseguridad dirigida a los empleados, plana gerencial y de dirección.

Dentro de los planes de acción que se deben considerar para la adecuación al Reglamento CAVALI se encuentran los siguientes:

- Desarrollar una estrategia y marco de ciberseguridad para COFIDE, adaptados a los riesgos cibernéticos específicos, en línea con lo dispuesto por el marco normativo nacional e internacional vigente que resulte aplicable, tales como el marco de ciberseguridad de NIST, ISO 27002, Controles Críticos de Ciberseguridad del CIS, entre otros.
- Proponer lineamientos para el mantenimiento y revisión periódica de la estrategia y marco de ciberseguridad.
- Proponer los roles y responsabilidades para la gestión de la ciberseguridad, considerando recursos adecuados, la autoridad apropiada y acceso al órgano correspondiente dentro de COFIDE.
- Proponer lineamientos para la identificación, evaluación y mitigación (controles) de los riesgos cibernéticos a los que está expuesto COFIDE.
- Desarrollar procedimientos para la detección oportuna de incidentes cibernéticos y lineamientos para la evaluación periódica de la efectividad de controles, a través del monitoreo de la red, pruebas, auditorías y ejercicios.
- Desarrollar procedimientos para responder oportunamente ante los incidentes cibernéticos que considere las siguientes etapas: (a) evaluar la naturaleza, el alcance y el impacto de un incidente cibernético; (b) contener el incidente y mitigar su impacto; (c) notificar a las partes interesadas internas y externas (CAVALI, reguladores y otras autoridades, accionistas, proveedores y clientes, según corresponda); y (d) coordinación de las actividades de respuesta conjunta según sea necesario.
- Desarrollar procedimientos para reanudar las operaciones de manera responsable luego de la generación de un incidente cibernético que considere las siguientes etapas: (a) la eliminación de los restos dañinos del incidente; (b) la restauración de los sistemas y los datos a su estado normal; (c) la identificación y mitigación de todas las vulnerabilidades que fueron explotadas; (d) la remediación de las vulnerabilidades para prevenir incidentes similares; y (e) la comunicación apropiada, tanto interna como externa.
- Desarrollar procedimientos para compartir con CAVALI información de ciberseguridad referida a amenazas, vulnerabilidades, incidentes y respuestas tomadas por COFIDE, vinculada a los servicios a los que COFIDE accederá en su condición de Participante Directo, Indirecto o Indirecto Especial, según corresponda.

Adicionalmente, se deberá desarrollar una capacitación orientada a la adopción de prácticas seguras en seguridad de la información y ciberseguridad dirigida a los empleados, plana gerencial y de dirección. La capacitación se realizará vía la plataforma Teams dirigido a 2 grupos de 45 minutos cada uno: i) empleados y plana gerencial ii) Directores.

6. CONDICIONES DEL SERVICIO

6.1. Gestión del servicio y equipo de trabajo

El Contratista asume la gestión y ejecución de las tareas necesarias para la puesta en marcha del servicio que estén bajo su responsabilidad. COFIDE considera que dichas tareas deben incluir como mínimo las siguientes actividades:

6.1.1. Gestión del Servicio: Ejecución del servicio con base a una adecuada metodología de gestión de proyectos que incluya la planificación, ejecución, evaluación, recomendaciones y planes de acción sólidamente establecidos para alcanzar el cumplimiento mínimo indicado en el proyecto.

6.1.2. Administración y gestión de personal, de acuerdo a lo precisado en el numeral correspondiente a perfil de los consultores.

6.1.3. Entrega de documentos finales: La consultora deberá documentar, almacenar y brindar a COFIDE toda documentación funcional, técnica o de usuario recogida durante el servicio.

6.2. Confidencialidad

El Contratista deberá guardar reserva acerca de los asuntos y toda la información que le sea suministrada por COFIDE, quedando prohibida toda declaración ante cualquier medio de comunicación u otra empresa. Para tal efecto incluirá en el contrato del servicio una cláusula de confidencialidad respecto de la información que obtenga de la Corporación, ya sea de manera directa o indirecta.

6.3. Derechos de Propiedad

Todos los documentos, manuales, políticas, metodologías programas y cualquier otro producto que se obtenga, produzca o adquiera en el transcurso de los servicios prestados, sin importar el medio que los contenga ya sea óptico, magnético, electrónico o cualquier representación física, serán propiedad exclusiva de COFIDE.

En consecuencia, la consultora que realice el servicio se compromete a no divulgar, entregar o suministrar, total o parcialmente, el resultado del servicio sin el consentimiento escrito de COFIDE, aún después de haber finalizado la relación contractual.

6.4. Derecho a Auditar

COFIDE tiene el derecho a auditar las responsabilidades contractuales o puede contratar un tercero para realizar estas auditorías. Asimismo, la Corporación se reserva el derecho a monitorear las actividades que realice la consultora en las redes y equipo de COFIDE y como resultado de dicho monitoreo podrá revocar los privilegios de los usuarios que contravenga las disposiciones relacionadas con la seguridad de la información.

6.5. Transferencia de Conocimientos

La consultora que realice el servicio garantizará transferir al personal de la Corporación el conocimiento adquirido durante la prestación de los servicios a fin de evitar la dependencia y fuga de conocimientos.

6.6. Control de Acceso y Riesgos Informáticos

La consultora que realice el servicio se compromete a acatar las medidas de seguridad adoptadas por la Corporación para garantizar el acceso a las instalaciones y datos debiendo cumplir con al menos lo siguiente:

6.6.1. Usar de manera adecuada las contraseñas que se le proporcionarán para desarrollar su trabajo.

En caso de que se utilice algún equipo portátil o equipo que no sea propiedad de COFIDE, deberá incorporar los controles necesarios que garanticen protección contra programas maliciosos, lo cual requerirá efectuar una verificación por parte de la Corporación de sus equipos a fin de garantizar que cumple con lo requerido.

7. GESTIÓN DEL PERSONAL

EL CONTRATISTA deberá contar con el respaldo de especialistas de reemplazo ante cualquier eventualidad. El reemplazo puede ser solicitado por COFIDE o por el CONTRATISTA. En este último caso, se debe contar con la aprobación de COFIDE. Cabe indicar que los especialistas reemplazantes deberán contar como mínimo con las mismas calificaciones y competencias del especialista requeridas en los términos de referencia.

COFIDE se reserva el derecho, en todo momento, de solicitar el cambio de los especialistas encargados de la prestación de los servicios contratos, si a su criterio, no cumplen con los requisitos para las tareas encomendadas. Para el reemplazo, EL CONTRATISTA deberá presentar al candidato para su aprobación por parte de COFIDE, en un plazo no mayor a siete (7) días calendario. Este plazo podrá extenderse a consideración de COFIDE, siempre y cuando no sea mayor a cinco días laborables.

Aceptado el reemplazo del especialista, COFIDE no reconocerá doble cargo de horas hombre para ninguna etapa del proyecto y/o tarea, obligándose EL CONTRATISTA a cumplir con el cronograma y horas-hombre acordadas para el proyecto y/o tarea y los entregables en los que trabajará el nuevo especialista.

En caso de que, EL CONTRATISTA considere necesario contar con más especialistas de los originalmente propuestos, deberá comunicar tal hecho a COFIDE y presentar el (los) candidato(s), para su aprobación por parte de COFIDE, en un plazo no mayor a los tres (3) días calendario a partir de la comunicación referida. Este plazo podrá extenderse a consideración de COFIDE, siempre y cuando no sea mayor a cinco días laborables. La adición de más especialistas en ningún caso implica costos adicionales para el servicio brindado.

Ya sea en caso de reemplazos o nuevos ingresos los plazos que se tome EL CONTRATISTA para asignar a los nuevos especialistas, no deberán afectar los planes de trabajo de las tareas que forman parte del alcance del servicio, es decir, el reemplazo de especialistas no implicará la modificación de los cronogramas establecidos para los entregables que se encuentren en curso.

8. ENTREGABLES

Los siguientes entregables deberán ser entregados a través de mesa de partes a la cuenta mesadepartes@cofide.com.pe, y serán evaluados por la Gerencia de Riesgos, para otorgar la conformidad respectiva.

Entregable	Plazo de entrega	Forma de Pago
Al finalizar la etapa 1 y 2: Acta de inicio del servicio (Kick-off). Presentar el Plan de Trabajo del Servicio, incluyendo el cronograma de actividades.	Máximo a los cinco (5) días calendario contados desde el día siguiente de suscrito el contrato	—
Al finalizar la etapa 3: Informe de Diagnóstico, identificando: i) Los requerimientos del Reglamento SBS y Reglamento CAVALI que COFIDE estaría cumpliendo con el sustento respectivo. ii) Los requerimientos del Reglamento SBS y Reglamento CAVALI que no se estarían cumpliendo y representan una brecha con la explicación respectiva iii) Plan de Trabajo de Implementación que incluye los planes de acción que cubren las brechas identificadas en el Plan de Adecuación SBS y los planes de acción respecto al Reglamento CAVALI, que se especifica en la Etapa 4: Implementación, con el respectivo cronograma de implementación de los planes de acción, indicando así mismo, las áreas de COFIDE que participarán en la	Máximo a los cuarenta (40) días calendario contados desde el día siguiente de suscrito el contrato.	35%

Entregable	Plazo de entrega	Forma de Pago
implementación. iv) Propuestas de planes de acción para el cierre de brechas que haya identificado sobre el Reglamento SBS y sobre el Reglamento CAVALI y que no estén especificadas en la Etapa 4: Implementación.		
Al finalizar la etapa 4: Plan de adecuación SBS: <ol style="list-style-type: none"> 1. Plan estratégico del SGSI-C 2. Proponer el alcance de la función del Comité de Riesgos en relación a fomentar la cultura de riesgo y conciencia de la necesidad de medidas apropiadas para su prevención, para ser incluido en la Estructura Organizacional para la gestión de Seguridad de Información. 3. Proponer el alcance de la función de Seguridad de Información y Ciberseguridad, de reportar a los entes gubernamentales cuando lo requieran, conforme a la normativa, para ser incluido en la Estructura Organizacional para la gestión de Seguridad de Información 4. Propuesta de áreas, personal, roles, responsabilidades y procedimiento para la gestión de incidentes de ciberseguridad, que permitan prever en ellos los aspectos legales, técnicos y organizacionales del programa de ciberseguridad. 5. Programa de Ciberseguridad y los respectivos lineamientos para ser incluidos en las políticas de Seguridad de Información. 6. Procedimiento para el análisis forense de incidentes cibernéticos significativos adversos y su reporte al regulador, y los respectivos lineamientos para ser incluidos en las Políticas de Seguridad de la Información. 7. Criterios pertinentes para el intercambio de información relativa a ciberseguridad, así como el tratamiento de esta información, a fin de tomar acción oportuna frente a las amenazas y vulnerabilidades, y los respectivos procedimientos, así como los respectivos lineamientos para ser incluidos en las Políticas de Seguridad de la Información; tomando como referencia los lineamientos que establezca la SBS para el intercambio de información de ciberseguridad, en caso estos hayan sido emitidos. 8. Proponer los roles y responsabilidades que el proveedor asume contractualmente (Servicios provistos por terceros), sobre la seguridad de la información, para la atención de los requerimientos del Reglamento SBS. 9. Lineamientos de seguridad de información para el uso de la nube, para ser incluidos en las políticas de Seguridad de Información, así como la propuesta de los respectivos procedimientos, considerando el marco de buenas prácticas internacionales para el uso de estos servicios, conforme al Reglamento SBS. 10. Proponer lineamientos para la evaluación del uso de Servicios Significativos de Procesamiento de Datos, incluido los servicios en nube, a ser incorporado en el Proceso para la Evaluación de Riesgo de nuevos 	Se inicia al día siguiente hábil luego de otorgada la conformidad de la etapa 3. Máximo a los setenta (70) días calendario de otorgada la conformidad de la etapa 3.	65%

Entregable	Plazo de entrega	Forma de Pago
<p>productos o cambios importantes en ambiente de negocios, operativo e informático.</p> <p>11. Proponer lineamientos que se deben considerar para la solicitud de autorización al supervisor, para la contratación de Servicios Significativos de Procesamiento de Datos en el exterior, a ser incorporado en el Proceso para la Evaluación de Riesgo de nuevos productos o cambios importantes en ambiente de negocios, operativo e informático.</p> <p>12. Proponer procedimientos o lineamientos para la planificación y ejecución de las actividades a realizar para la gestión de seguridad de información y ciberseguridad con periodicidad anual, conforme al Régimen Simplificado del Reglamento SBS, considerando como mínimo:</p> <ul style="list-style-type: none"> a. Identificar con las unidades de negocio y de apoyo, cuál es la información de mayor importancia, por las obligaciones normativas o contractuales existentes, y por la necesidad de operar. b. Identificar los dispositivos que se conectan a la red interna y todo software que se encuentre instalado en la infraestructura tecnológica, y asegurar que se encuentren acorde a una configuración segura previamente establecida. c. Identificar las cuentas de usuario con permisos de acceso habilitados y en particular las que poseen privilegios administrativos con posibilidad de adicionar software a la infraestructura, y mantener el principio de mínimos privilegios otorgados. d. Implementar y mantener una línea base de seguridad en sistemas operativos y aplicaciones utilizadas, incluidos los correspondientes a dispositivos móviles, estaciones de trabajo, servidores y dispositivos de comunicaciones. Identificar y evaluar la habilitación de las funciones de seguridad integradas en los sistemas operativos. e. Priorizar y gestionar las vulnerabilidades de seguridad identificadas, para cuya identificación oportuna debe contar con los servicios de información necesarios. f. Desarrollar una campaña de orientación para la adopción de prácticas seguras en seguridad de la información y ciberseguridad dirigida a los empleados, plana gerencial y de dirección. <p>Planes de acción para la adecuación al Reglamento CAVALI</p> <p>13. Estrategia y marco de ciberseguridad para COFIDE, adaptados a los riesgos cibernéticos específicos, en línea con lo dispuesto por el marco normativo nacional e internacional vigente que resulte aplicable, tales como el marco de ciberseguridad de NIST, ISO 27002, Controles Críticos de Ciberseguridad del CIS,</p>		

Entregable	Plazo de entrega	Forma de Pago
<p>entre otros.</p> <ol style="list-style-type: none"> 14. Lineamientos para el mantenimiento y revisión periódica de la estrategia y marco de ciberseguridad. 15. Roles y responsabilidades para la gestión de la ciberseguridad, considerando recursos adecuados, la autoridad apropiada y acceso al órgano correspondiente dentro de COFIDE. 16. Lineamientos para la identificación, evaluación y mitigación (controles) de los riesgos cibernéticos a los que está expuesto COFIDE. 17. Procedimientos para la detección oportuna de incidentes cibernéticos y lineamientos para la evaluación periódica de la efectividad de controles, a través del monitoreo de la red, pruebas, auditorías y ejercicios. 18. Procedimientos para responder oportunamente ante los incidentes cibernéticos que considere las siguientes etapas: (a) evaluar la naturaleza, el alcance y el impacto de un incidente cibernético; (b) contener el incidente y mitigar su impacto; (c) notificar a las partes interesadas internas y externas (CAVALI, reguladores y otras autoridades, accionistas, proveedores y clientes, según corresponda); y (d) coordinación de las actividades de respuesta conjunta según sea necesario. 19. Procedimientos para reanudar las operaciones de manera responsable luego de la generación de un incidente cibernético que considere las siguientes etapas: (a) la eliminación de los restos dañinos del incidente; (b) la restauración de los sistemas y los datos a su estado normal; (c) la identificación y mitigación de todas las vulnerabilidades que fueron explotadas; (d) la remediación de las vulnerabilidades para prevenir incidentes similares; y (e) la comunicación apropiada, tanto interna como externa. 20. Procedimientos para compartir con CAVALI información de ciberseguridad referida a amenazas, vulnerabilidades, incidentes y respuestas tomadas por COFIDE, vinculada a los servicios a los que COFIDE accederá en su condición de Participante Directo, Indirecto o Indirecto Especial, según corresponda. <p>Adicionalmente:</p> <ol style="list-style-type: none"> 21. Material utilizado en la capacitación a los siguientes grupos: <ol style="list-style-type: none"> a. Colaboradores y Gerentes b. Directores 		

9. PLAZO DEL SERVICIO

ENTREGABLES	PLAZO DE ENTREGA
-------------	------------------

<p>Al finalizar la etapa 1 y 2: Acta de inicio del servicio (Kick-off). Presentar el Plan de Trabajo del Servicio, incluyendo el cronograma de actividades.</p>	<p>Máximo a los cinco (5) días calendario contados desde el día siguiente de suscrito el contrato</p>
<p>Al finalizar la etapa 3: Informe de Diagnóstico, identificando:</p> <ul style="list-style-type: none"> i) Los requerimientos del Reglamento SBS y Reglamento CAVALI que COFIDE estaría cumpliendo con el sustento respectivo. ii) Los requerimientos del Reglamento SBS y Reglamento CAVALI que no se estarían cumpliendo y representan una brecha con la explicación respectiva iii) Plan de Trabajo de Implementación que incluye los planes de acción que cubren las brechas identificadas en el Plan de Adecuación SBS y los planes de acción respecto al Reglamento CAVALI, que se especifica en la Etapa 4: Implementación, con el respectivo cronograma de implementación de los planes de acción, indicando así mismo, las áreas de COFIDE que participarán en la implementación. iv) Propuestas de planes de acción para el cierre de brechas que haya identificado sobre el Reglamento SBS y sobre el Reglamento CAVALI y que no estén especificadas en la Etapa 4: Implementación. 	<p>Máximo a los cuarenta (40) días calendario contados desde el día siguiente de suscrito el contrato.</p>
<p>Al finalizar la etapa 4:</p> <ul style="list-style-type: none"> 1. Plan estratégico del SGSI-C 2. Proponer el alcance de la función del Comité de Riesgos en relación a fomentar la cultura de riesgo y conciencia de la necesidad de medidas apropiadas para su prevención, para ser incluido en la Estructura Organizacional para la gestión de Seguridad de Información. 3. Proponer el alcance de la función de Seguridad de Información y Ciberseguridad, de reportar a los entes gubernamentales cuando lo requieran, conforme a la normativa, para ser incluido en la Estructura Organizacional para la gestión de Seguridad de Información 4. Propuesta de áreas, personal, roles, responsabilidades y procedimiento para la gestión de incidentes de ciberseguridad, que permitan prever en ellos los aspectos legales, técnicos y organizacionales del programa de ciberseguridad. 5. Programa de Ciberseguridad y los respectivos lineamientos para ser incluidos en las políticas de Seguridad de Información. 6. Procedimiento para el análisis forense de incidentes cibernéticos significativos adversos y su reporte al regulador, y los respectivos lineamientos para ser incluidos en las Políticas de Seguridad de la Información. 7. Criterios pertinentes para el intercambio de información relativa a ciberseguridad, así como el tratamiento de esta información, a fin de tomar acción oportuna frente a las amenazas y vulnerabilidades, y los respectivos procedimientos, así como los respectivos lineamientos para ser incluidos en las Políticas de Seguridad de la Información; tomando como referencia los lineamientos que establezca la SBS para el intercambio de información de ciberseguridad, en caso estos hayan sido emitidos. 	<p>Se inicia al día siguiente hábil luego de otorgada la conformidad de la etapa 3.</p> <p>Máximo a los setenta (70) días calendario de otorgada la conformidad de la etapa 3</p>

8. Proponer los roles y responsabilidades que el proveedor asume contractualmente (Servicios provistos por terceros), sobre la seguridad de la información, para la atención de los requerimientos del Reglamento SBS.
9. Lineamientos de seguridad de información para el uso de la nube, para ser incluidos en las políticas de Seguridad de Información, así como la propuesta de los respectivos procedimientos, considerando el marco de buenas prácticas internacionales para el uso de estos servicios, conforme al Reglamento SBS.
10. Proponer lineamientos para la evaluación del uso de Servicios Significativos de Procesamiento de Datos, incluido los servicios en nube, a ser incorporado en el Proceso para la Evaluación de Riesgo de nuevos productos o cambios importantes en ambiente de negocios, operativo e informático.
11. Proponer lineamientos que se deben considerar para la solicitud de autorización al supervisor, para la contratación de Servicios Significativos de Procesamiento de Datos en el exterior, a ser incorporado en el Proceso para la Evaluación de Riesgo de nuevos productos o cambios importantes en ambiente de negocios, operativo e informático.
12. Proponer procedimientos o lineamientos para la planificación y ejecución de las actividades a realizar para la gestión de seguridad de información y ciberseguridad con periodicidad anual, conforme al Régimen Simplificado del Reglamento SBS, considerando como mínimo:
 - a. Identificar con las unidades de negocio y de apoyo, cuál es la información de mayor importancia, por las obligaciones normativas o contractuales existentes, y por la necesidad de operar.
 - b. Identificar los dispositivos que se conectan a la red interna y todo software que se encuentre instalado en la infraestructura tecnológica, y asegurar que se encuentren acorde a una configuración segura previamente establecida.
 - c. Identificar las cuentas de usuario con permisos de acceso habilitados y en particular las que poseen privilegios administrativos con posibilidad de adicionar software a la infraestructura, y mantener el principio de mínimos privilegios otorgados.
 - d. Implementar y mantener una línea base de seguridad en sistemas operativos y aplicaciones utilizadas, incluidos los correspondientes a dispositivos móviles, estaciones de trabajo, servidores y dispositivos de comunicaciones. Identificar y evaluar la habilitación de las funciones de seguridad integradas en los sistemas operativos.
 - e. Priorizar y gestionar las vulnerabilidades de seguridad identificadas, para cuya identificación oportuna debe contar con los servicios de información necesarios.
 - f. Desarrollar una campaña de orientación para la adopción de prácticas seguras en seguridad de la información y ciberseguridad dirigida a los empleados, plana gerencial y de dirección

Planes de acción para la adecuación al Reglamento CAVALI

13. Estrategia y marco de ciberseguridad para COFIDE, adaptados a los riesgos cibernéticos específicos, en línea con lo dispuesto por el marco normativo nacional e internacional vigente que resulte aplicable, tales como el marco de ciberseguridad de NIST, ISO 27002, Controles Críticos de Ciberseguridad del CIS, entre otros.
14. Lineamientos para el mantenimiento y revisión periódica de la

<p>estrategia y marco de ciberseguridad.</p> <p>15. Roles y responsabilidades para la gestión de la ciberseguridad, considerando recursos adecuados, la autoridad apropiada y acceso al órgano correspondiente dentro de COFIDE.</p> <p>16. Lineamientos para la identificación, evaluación y mitigación (controles) de los riesgos cibernéticos a los que está expuesto COFIDE.</p> <p>17. Procedimientos para la detección oportuna de incidentes cibernéticos y lineamientos para la evaluación periódica de la efectividad de controles, a través del monitoreo de la red, pruebas, auditorías y ejercicios.</p> <p>18. Procedimientos para responder oportunamente ante los incidentes cibernéticos que considere las siguientes etapas: (a) evaluar la naturaleza, el alcance y el impacto de un incidente cibernético; (b) contener el incidente y mitigar su impacto; (c) notificar a las partes interesadas internas y externas (CAVALI, reguladores y otras autoridades, accionistas, proveedores y clientes, según corresponda); y (d) coordinación de las actividades de respuesta conjunta según sea necesario.</p> <p>19. Procedimientos para reanudar las operaciones de manera responsable luego de la generación de un incidente cibernético que considere las siguientes etapas: (a) la eliminación de los restos dañinos del incidente; (b) la restauración de los sistemas y los datos a su estado normal; (c) la identificación y mitigación de todas las vulnerabilidades que fueron explotadas; (d) la remediación de las vulnerabilidades para prevenir incidentes similares; y (e) la comunicación apropiada, tanto interna como externa.</p> <p>20. Procedimientos para compartir con CAVALI información de ciberseguridad referida a amenazas, vulnerabilidades, incidentes y respuestas tomadas por COFIDE, vinculada a los servicios a los que COFIDE accederá en su condición de Participante Directo, Indirecto o Indirecto Especial, según corresponda.</p> <p>Adicionalmente:</p> <p>21. Material utilizado en la capacitación a los siguientes grupos:</p> <ul style="list-style-type: none"> a. Colaboradores y Gerentes b. Directores 	
---	--

El plazo total es de hasta máximo ciento diez (110) días calendarios

22. FORMA DE PAGO

El pago se realizará al final de las siguientes etapas implementadas, con el visto bueno del área usuaria:

Etapa 3	35%
Etapa 4	65%

A los 7 días calendarios de otorgada la conformidad de servicio por parte del área usuaria, previa presentación de la factura respectiva.

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
- Conformidad de la Gerencia de Riesgos.
- Comprobante de pago, el cual deberá ser enviado a facturaselectronicas@cofide.com.pe

10. DEPENDENCIA ENCARGADA DE DAR LA CONFORMIDAD DEL SERVICIO

La conformidad del servicio será otorgada por la Gerencia de Riesgos.

11. ADECUACIÓN A PROTOCOLOS SANITARIOS

No Aplica

Anexo 1

Infraestructura Tecnológica

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.

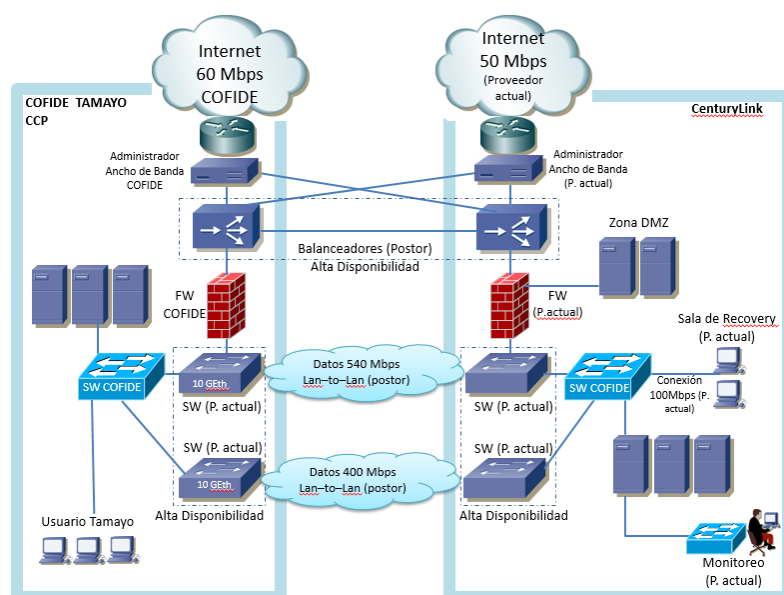


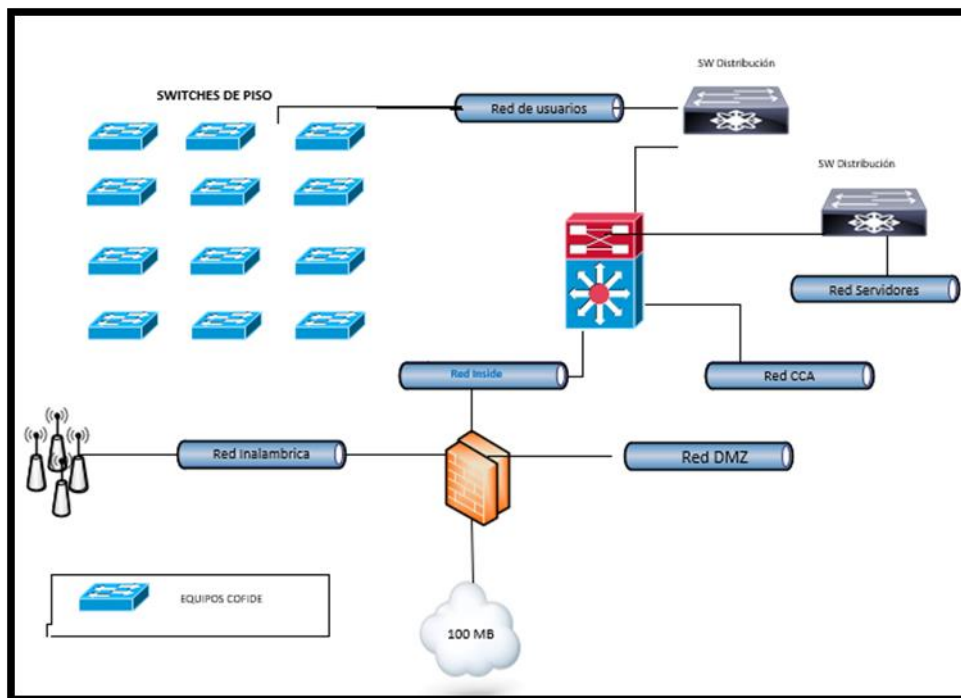
Diagrama General de Servicios actuales

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

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

Anexo 2**REGLAMENTO PARA LA GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN Y LA CIBERSEGURIDAD****CAPÍTULO I
DISPOSICIONES GENERALES****Artículo 1. Alcance**

- 1.1. El presente Reglamento es de aplicación a las empresas señaladas en los artículos 16 y 17 de la Ley General, así como a las Administradoras Privadas de Fondos de Pensiones (AFP), en adelante empresas, al igual que las referidas en los párrafos 1.2 y 1.3.
- 1.2. También es de aplicación al Banco de la Nación, al Banco Agropecuario, a la Corporación Financiera de Desarrollo (COFIDE), al Fondo MIVIVIENDA S.A., y a las Derramas y Cajas de Beneficios bajo control de la Superintendencia, en tanto no se contrapongan con las normativas específicas que regulen el accionar de dichas instituciones.
- 1.3. Es de aplicación a las empresas corredoras de seguros de acuerdo con lo dispuesto en la Cuarta Disposición Complementaria Final del presente Reglamento.

Artículo 2. Definiciones

Para efectos de la aplicación del presente Reglamento deben considerarse las siguientes definiciones:

- a) **Activo de información:** Información o soporte en que ella reside, que es gestionado de acuerdo con las necesidades de negocios y los requerimientos legales, de manera que puede ser entendida, compartida y usada. Es de valor para la empresa y tiene un ciclo de vida.
- b) **Amenaza:** Evento que puede afectar adversamente la operación de las empresas y sus activos de información, mediante el aprovechamiento de una vulnerabilidad.
- c) **Autenticación:** Para fines de esta norma, es el proceso que permite verificar que una entidad es quien dice ser, para lo cual hace uso de las credenciales que se le asignan. La autenticación puede usar uno, dos o más factores de autenticación independientes, de modo que el uso sin autorización de uno de ellos no compromete la fiabilidad o el acceso a los otros factores.
- d) **Canal digital:** Medio empleado por las empresas para proveer servicios cuyo almacenamiento, procesamiento y transmisión se realiza mediante la representación de datos en bits.
- e) **Ciberseguridad:** Protección de los activos de información mediante la prevención, detección, respuesta y recuperación ante incidentes que afecten su disponibilidad, confidencialidad o integridad en el ciberespacio; el que consiste a su vez en un sistema complejo que no tiene existencia física, en el que interactúan personas, dispositivos y sistemas informáticos.
- f) **Credencial:** Conjunto de datos que es generado y asignado a una entidad o un usuario para fines de autenticación.
- g) **Directorio:** Directorio u órgano equivalente.
- h) **Entidad:** Usuario, dispositivo o sistema informático que tiene una identidad en un sistema, lo cual la hace separada y distinta de cualquier otra en dicho sistema.
- i) **Evento:** Un suceso o serie de sucesos que puede ser interno o externo a la empresa, originado por la misma causa, que ocurre durante el mismo periodo de tiempo, según lo definido en el Reglamento de Gobierno Corporativo y Gestión Integral de Riesgos.
- j) **Factores de autenticación de usuario:** Aquellos factores empleados para verificar la identidad de un usuario, que pueden corresponder a las siguientes categorías:
 - Algo que solo el usuario conoce.
 - Algo que solo el usuario posee.
 - Algo que el usuario es, que incluye las características biométricas.
- k) **Identidad:** Una colección de atributos que definen de forma exclusiva a una entidad.
- l) **Incidente:** Evento que se ha determinado que tiene un impacto adverso sobre la organización y que requiere de acciones de respuesta y recuperación.
- m) **Información:** Datos que pueden ser procesados, distribuidos, almacenados y representados en cualquier medio electrónico, digital, óptico, magnético, impreso u otros, que son el elemento fundamental de los activos de información.
- n) **Interfaz de programación de aplicaciones:** Colección de métodos de invocación y parámetros asociados que puede utilizar un software para solicitar acciones de otro software, lo que define

los términos en que estos intercambian datos. También conocido como API, por sus siglas en inglés.

- o) Servicios en nube:** Servicio de procesamiento de datos provisto mediante una infraestructura tecnológica que permite el acceso de red a conveniencia y bajo demanda, a un conjunto compartido de recursos informáticos configurables que se pueden habilitar y suministrar rápidamente, con mínimo esfuerzo de gestión o interacción con los proveedores de servicios.
- p) Reglamento:** Reglamento para la Gestión de la Seguridad de la Información y la Ciberseguridad.
- q) Reglamento de Gobierno Corporativo y de la Gestión Integral de Riesgos:** Reglamento de Gobierno Corporativo y de la Gestión Integral de Riesgos, aprobado por la Resolución SBS N° 272-2017 y sus normas modificatorias.
- r) Reglamento para la Gestión de Riesgo Operacional:** Reglamento para la Gestión de Riesgo Operacional, aprobado por la Resolución SBS N° 2116-2009 y sus normas modificatorias.
- s) Superintendencia:** Superintendencia de Banca, Seguros y Administradoras Privadas de Fondos de Pensiones.
- t) Procesamiento de datos:** El conjunto de procesos que consiste en la recolección, registro, organización, estructuración, almacenamiento, adaptación, recuperación, consulta, uso, transferencia, difusión, borrado o destrucción de datos.
- u) Usuario:** persona natural o jurídica que utiliza o puede utilizar los productos ofrecidos por las empresas.
- v) Vulnerabilidad:** Debilidad que expone a los activos de información ante amenazas que pueden originar incidentes con afectación a los mismos activos de información, y a otros de los que forma parte o con los que interactúa.

Artículo 3. Sistema de gestión de seguridad de la información y Ciberseguridad (SGSI-C)

3.1. El sistema de gestión de seguridad de la información y ciberseguridad (SGSI-C) es el conjunto de políticas, procesos, procedimientos, roles y responsabilidades, diseñados para identificar y proteger los activos de información, detectar eventos de seguridad, así como prever la respuesta y recuperación ante incidentes de ciberseguridad.

3.2. El sistema de gestión de seguridad de la información y ciberseguridad (SGSI-C) implica, cuando menos, los siguientes objetivos:

- a) Confidencialidad: La información sólo es disponible para entidades o procesos autorizados, incluyendo las medidas para proteger la información personal y la información propietaria;
- b) Disponibilidad: Asegurar acceso y uso oportuno a la información; e,
- c) Integridad: Asegurar el no repudio de la información y su autenticidad, y evitar su modificación o destrucción indebida.

Artículo 4. Proporcionalidad del sistema de gestión de seguridad de la información y ciberseguridad (SGSI-C)

4.1. El sistema de gestión de seguridad de la información y ciberseguridad (SGSI-C) de la empresa debe ser proporcional al tamaño, la naturaleza y la complejidad de sus operaciones.

4.2. Las disposiciones descritas en el Capítulo II, Subcapítulos I, II, III y IV del presente Reglamento son de aplicación obligatoria a las siguientes empresas (Régimen General):

- a) Empresa Bancaria;
- b) Empresa Financiera;
- c) Caja Municipal de Ahorro y Crédito - CMAC;
- d) Caja Municipal de Crédito Popular - CMCP;
- e) Caja Rural de Ahorro y Crédito - CRAC;
- f) Empresa de Seguros y/o Reaseguros, conforme a lo dispuesto en el párrafo 4.4;
- g) Empresa de Transporte, Custodia y Administración de Numerario;
- h) Administradora Privada de Fondos de Pensiones;
- i) Empresa Emisora de Tarjetas de Crédito y/o de Débito;
- j) Empresa Emisora de Dinero Electrónico; y
- k) El Banco de la Nación.

4.3. Las disposiciones descritas en el Capítulo II, Subcapítulo V del presente Reglamento son de aplicación obligatoria a las siguientes empresas (Régimen Simplificado)⁹:

⁹ Párrafo modificado por la Resolución SBS N° 1515-2021 del 24/05/2021.

- a) Banco de Inversión;
- b) Empresa de Seguros y/o Reaseguros, no contempladas en el párrafo 4.4;
- c) Entidad de Desarrollo a la Pequeña y Micro Empresa – EDPYME;
- d) Empresa de Transferencia de Fondos;
- e) Derrama y Caja de Beneficios bajo control de la Superintendencia;
- f) La Corporación Financiera de Desarrollo –COFIDE;
- g) El Fondo MIVIVIENDA S.A.;
- h) Empresas afianzadoras y de garantías; y
- i) El Banco Agropecuario.

4.4. Las empresas de Seguros y/o Reaseguros cuyo volumen promedio de activos de los últimos tres (3) años sea mayor o igual a 450 millones de soles están comprendidas en el Régimen General del presente Reglamento.

4.5. Las empresas señaladas en el Artículo 1, no listadas en los párrafos 4.2 o 4.3 anteriores del presente Reglamento, podrán establecer un sistema de gestión de seguridad de la información y ciberseguridad (SGSI-C) conforme a las disposiciones de este Reglamento.

4.6. En caso las empresas del Sistema Financiero y las empresas emisoras de dinero electrónico listadas en el párrafo 4.2 encuentren limitaciones materiales para cumplir con el Régimen General pueden solicitar autorización para la aplicación del Régimen Simplificado del presente Reglamento, para lo cual deben presentar un informe que sustente la razonabilidad de la solicitud, en términos del tamaño, la naturaleza y la complejidad de sus operaciones, la cual será respondida por la Superintendencia en el plazo de sesenta (60) días hábiles¹⁰.

4.7. Las disposiciones descritas en el Capítulo II, Subcapítulo VI (Régimen Reforzado) del presente Reglamento son de aplicación obligatoria a las empresas sujetas a un requerimiento de patrimonio efectivo por riesgo de concentración de mercado, de acuerdo con lo señalado en el Reglamento para el requerimiento de patrimonio efectivo adicional, aprobado por la Resolución SBS N° 8425-2011 y sus normas modificatorias.

Artículo 5. Responsabilidades del directorio

El directorio es responsable de aprobar y facilitar las acciones requeridas para contar con un SGSI-C apropiado a las necesidades de la empresa y su perfil de riesgo, entre ellas:

- a) Aprobar políticas y lineamientos para la implementación del SGSI-C y su mejora continua.
- b) Asignar los recursos técnicos, de personal, financieros requeridos para su implementación y adecuado funcionamiento.
- c) Aprobar la organización, roles y responsabilidades para el SGSI-C, incluyendo los lineamientos de difusión y capacitación que contribuyan a un mejor conocimiento de los riesgos involucrados.

Artículo 6. Responsabilidades de la gerencia

6.1 La gerencia general es responsable de tomar las medidas necesarias para implementar el SGSI-C de acuerdo a las disposiciones del directorio y lo dispuesto en este Reglamento.

6.2 Los gerentes de las unidades de negocios y de apoyo son responsables de apoyar el buen funcionamiento del SGSI-C y gestionar los riesgos asociados a la seguridad de la información y Ciberseguridad en el marco de sus funciones.

Artículo 7. Funciones del comité de riesgos

7.1 Adicionalmente a las funciones que se han dispuesto que el Comité de Riesgos de las empresas asuman por parte de la normativa de la Superintendencia, se encuentran las siguientes vinculadas a la seguridad de la información y ciberseguridad:

- a) Aprobar el plan estratégico del SGSI-C y recomendar acciones a seguir.
- b) Aprobar el plan de capacitación a fin de garantizar que el personal, la plana gerencial y el directorio cuenten con competencias necesarias en seguridad de la información y Ciberseguridad.

¹⁰ Párrafo modificado por la Resolución SBS N° 1515-2021 del 24/05/2021.

- c) Fomentar la cultura de riesgo y conciencia de la necesidad de medidas apropiadas para su prevención.

7.2. Para el cumplimiento de las funciones indicadas en el párrafo 7.1, la empresa puede constituir un Comité Especializado en Seguridad de la Información y Ciberseguridad (CSIC). Para las empresas comprendidas en el régimen simplificado, que no cuenten con un Comité de Riesgos o un CSIC, las funciones antes indicadas son asignadas a la Gerencia General.

Artículo 8. Función de Seguridad de Información y Ciberseguridad

8.1. Son responsabilidades de la función de seguridad de la información y ciberseguridad:

- a) Proponer el Plan estratégico del SGSI-C y desarrollar los planes operativos.
- b) Implementar y manejar las operaciones diarias necesarias para el funcionamiento efectivo del SGSI-C.
- c) Implementar procesos de autenticación para controlar el acceso a la información y sistema que utilice la empresa, y a los servicios que provea.
- d) Informar al Comité de Riesgos periódicamente sobre los riesgos que enfrenta la empresa en materia de seguridad de información y ciberseguridad.
- e) Informar sobre los incidentes de seguridad de la información al Comité de Riesgos o CSIC, según los lineamientos que este establezca, y a las entidades gubernamentales que lo requieran de acuerdo con la normativa vigente.
- f) Evaluar las amenazas de seguridad en las estrategias de continuidad del negocio que la empresa defina y proponer medidas de mitigación de riesgos, así como informar al Comité de Riesgos o CSIC.
- g) En general realizar lo necesario para dar debido cumplimiento a lo dispuesto en el presente Reglamento.

8.2. Las empresas deben implementar la función de seguridad de la información y ciberseguridad. Además deben contar con un equipo de trabajo multidisciplinario de manejo de incidentes de ciberseguridad, el cual debe estar capacitado para implementar el plan y los procedimientos para gestionarlos, conformado por representantes de las áreas que permitan prever en ellos los aspectos legales, técnicos y organizacionales, de forma consistente con los requerimientos del programa de ciberseguridad establecidos en este Reglamento.

8.3. Las empresas comprendidas en el régimen simplificado, deben contar con una función de seguridad de la información y ciberseguridad, que cumpla por lo menos con los literales a), e), f) y g) del párrafo 8.1 del presente artículo.

Artículo 9. Información a la Superintendencia

Como parte de los informes periódicos sobre gestión del riesgo operacional requeridos por el Reglamento para la Gestión del Riesgo Operacional, las empresas deben incluir información sobre la gestión de la seguridad de la información y ciberseguridad.

CAPÍTULO II

SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN Y CIBERSEGURIDAD (SGSI-C)

SUBCAPÍTULO I

RÉGIMEN GENERAL DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN Y CIBERSEGURIDAD (SGSI-C)

Artículo 10. Objetivos y requerimientos del SGSI-C

Son objetivos del SGSI-C los siguientes:

1. Identificar los activos de información, analizar las amenazas y vulnerabilidades asociadas a estos, y formular programas y medidas que busquen reducir la posibilidad de incidentes en los siguientes aspectos:
 - a) El diseño e implementación de nuevos productos y procesos, proyectos y cambios operativos.
 - b) Las obligaciones de seguridad de la información que se derivan de disposiciones normativas, normas internas y de acuerdos contractuales.

- c) Las relaciones con terceros, en el sentido más amplio, incluyendo proveedores de servicios y empresas con las que se tiene relaciones de subcontratación.
 - d) Cualquier otra actividad que, a criterio de la empresa, exponga sus activos de información por causa interna o externa.
2. Revisar periódicamente el alcance y la efectividad de los controles mínimos indicados en el artículo 12 de este Reglamento y contar con capacidades de detección, respuesta y recuperación ante incidentes de seguridad de la información.
3. Establecer la relación existente con los planes de emergencia, crisis y de continuidad establecidos según lo previsto en la normativa correspondiente.

Artículo 11. Alcance del SGSI-C

El alcance del SGSI-C debe incluir las funciones y unidades organizacionales, las ubicaciones físicas existentes, la infraestructura tecnológica y de comunicaciones, así como el perímetro de control asociado a las relaciones con terceros, que estén bajo responsabilidad de la empresa, conforme a las disposiciones establecidas sobre subcontratación en el Reglamento de Gobierno Corporativo y Gestión Integral de Riesgos.

Artículo 12. Medidas mínimas de seguridad de la información a adoptar por las empresas

Las empresas deben adoptar las siguientes medidas mínimas de seguridad de información:

1. Seguridad de los recursos humanos:
 - a) Implementar protocolos de seguridad de la información aplicables en el reclutamiento e incorporación del personal, ante cambio de puesto y terminación del vínculo laboral.
 - b) Procesos disciplinarios en caso de incumplimiento de las políticas de seguridad de la información.
2. Controles de acceso físico y lógico:
 - a) Prevenir el acceso no autorizado a la información, así como a los sistemas, equipos e instalaciones mediante los cuales es procesada, transmitida o almacenada, sea de manera presencial o remota.
 - b) Implementar procedimientos de administración de accesos, lo que debe incluir a las cuentas de accesos con privilegios administrativos; asegurando una segregación de funciones para reducir el riesgo de error o fraude, siguiendo los principios de mínimo privilegio y necesidad de conocer.
 - c) Implementar procesos de autenticación para controlar el acceso a los activos de información; en particular, para el acceso a los servicios provistos a usuarios por canales digitales, los procesos de autenticación deben cumplir los requisitos establecidos en el Subcapítulo III del Capítulo II del presente Reglamento.
3. Seguridad en las operaciones:
 - a) Asegurar y prevenir el funcionamiento continuo de las instalaciones de procesamiento, almacenamiento y transmisión de información.
 - b) Mantener la operación de los sistemas informáticos acorde a procedimientos previamente establecidos.
 - c) Controlar los cambios en el ambiente operativo de sistemas, y mantener segregados los ambientes de desarrollo, pruebas y producción.
 - d) Implementar controles que aseguren la integridad de las transacciones que son ejecutadas en los servicios y sistemas informáticos.
 - e) Restringir la instalación de software en los sistemas operativos y prevenir la explotación de las vulnerabilidades de seguridad de la información.
 - f) Contar con protocolos de respuesta y recuperación ante incidentes de malware; generar y probar copias de respaldo de información, software y elementos que faciliten su restablecimiento.
 - g) Definir, implementar y mantener líneas base de configuración segura para el uso de dispositivos e implementación de sistemas informáticos.
 - h) Contar con una estrategia de copias de respaldo y procedimientos de restauración de información ante posibles incidentes, de origen interno o externo, que comprometa la

disponibilidad de la información para las operaciones y del ambiente productivo del centro de procesamiento de datos.

4. Seguridad en las comunicaciones:

- a) Implementar y mantener la seguridad de redes de comunicaciones acorde a la información que por ella se trasmite y las amenazas a las que se encuentra expuesta.
- b) Asegurar que las redes de comunicaciones y servicios de red son gestionados y controlados para proteger la información.
- c) Segregar los servicios de información disponibles, usuarios y sistemas en las redes de la empresa.
- d) Implementar protocolos seguros y controles de seguridad para la transferencia de información, dentro de la organización y con partes externas.
- e) Asegurar que el acceso remoto, el uso de equipos personales en la red de la empresa, dispositivos móviles y la interconexión entre redes propias y de terceros cuente con controles acorde a las amenazas de seguridad existentes.

5. Adquisición, desarrollo y mantenimiento de sistemas:

- a) Implementar y mantener la seguridad en los servicios y sistemas informáticos acorde a la información que se procese y amenazas a las que se encuentren expuestos.
- b) Asegurar que se incluyan prácticas de seguridad de la información en la planificación, desarrollo, implementación, operación, soporte y desactivación en las aplicaciones y sistemas informáticos.
- c) Limitar el acceso a la modificación de librerías de programas fuente y mantener un estricto control de cambios.
- d) Cuando la plataforma operativa sea cambiada, las aplicaciones críticas deben ser revisadas y probadas para evitar efectos adversos en la seguridad de estas.
- e) Asegurar que se efectúen pruebas técnicas, funcionales y de seguridad de la información en los sistemas informáticos antes del pase a producción.
- f) Implementar y verificar el cumplimiento de procedimientos que incluyan prácticas de desarrollo seguro de servicios y sistemas informáticos.

6. Gestión de incidentes de ciberseguridad:

- a) Implementar procedimientos para la gestión de incidentes de ciberseguridad, de acuerdo a lo señalado en el párrafo 8.2 del artículo 8 del presente Reglamento; así también, intercambiar información cuando corresponda, conforme al artículo 16 del presente Reglamento.
- b) Implementar una metodología para clasificar los incidentes de ciberseguridad y prever protocolos de respuesta y recuperación.
- c) Contar con un servicio de operaciones de seguridad de la información, que incluya capacidades para la detección y respuesta, el monitoreo de comunicaciones en la red interna y el grado de funcionamiento de la infraestructura tecnológica.
- d) Contar con acceso a la información de inteligencia de amenazas, vulnerabilidades e incidentes, así como también a bases de conocimiento de técnicas y tácticas utilizadas por los agentes de amenazas.
- e) Implementar mecanismos de reporte interno de incidentes de ciberseguridad, de acuerdo con lo señalado en el artículo 8 del presente Reglamento, y a la Superintendencia conforme al artículo 15 del presente Reglamento.
- f) Identificar las posibles mejoras para su incorporación a la gestión de incidentes de ciberseguridad, luego de la ocurrencia de estos.
- g) Preservar las evidencias que faciliten las investigaciones forenses luego de la ocurrencia de incidentes de seguridad de la información.

7. Seguridad física y ambiental

- a) Implementar controles para evitar el acceso físico no autorizado, daños o interferencias a la información o instalaciones de procesamiento de la empresa.
- b) Adoptar medidas para evitar pérdida, daño, robo o compromiso de los activos de información y la interrupción de las operaciones, mediante la protección del equipamiento y dispositivos tomando en cuenta el entorno donde son utilizados.

8. Criptografía

- a) Utilizar criptografía para asegurar la confidencialidad, autenticidad e integridad de la información, tanto cuando los datos asociados están en almacenamiento y en transmisión.

- b) Implementar los procedimientos necesarios para administrar el ciclo de vida de las llaves criptográficas a utilizar.
9. Gestión de activos de información
- a) Identificar los activos de información mediante un inventario, asignar su custodia, establecer lineamientos de uso aceptable de ellos y la devolución al término del acuerdo por el que se proporcionó.
 - b) Asegurar que el nivel de protección y tratamiento de la información se realice acorde a su clasificación en términos de los requisitos legales, valor, criticidad y sensibilidad a la divulgación o modificación no autorizada.
 - c) Establecer medidas para evitar la divulgación, modificación, eliminación o destrucción no autorizadas de información, en el uso de dispositivos removibles.

Artículo 13. Actividades planificadas

En el marco del Plan estratégico del SGSI-C, la empresa debe mantener planes operativos, por lo menos para los siguientes fines:

- a) Identificar los activos de información, clasificarlos, analizar las amenazas y vulnerabilidades asociadas a estos, y tomar medidas de tratamiento correspondientes.
- b) Someter el SGSI-C a evaluaciones, revisiones y pruebas periódicas para determinar su efectividad, mediante servicios internos y externos, y en función al nivel de complejidad y amenazas sobre los activos de información asociados. En función a los resultados que obtenga, debe incorporar las mejoras o adoptar los correctivos.
- c) Atender las necesidades de capacitación y difusión, según corresponda a los roles y funciones en la organización, en materia de seguridad de la información y ciberseguridad para asegurar la efectividad del SGSI-C.
- d) Desarrollar el programa de ciberseguridad, conforme al Subcapítulo II del Capítulo II del presente Reglamento.
- e) Revisar periódicamente, y actualizar cuando corresponda, las políticas de seguridad de la información que se establezcan para implementar los requerimientos establecidos en el artículo 12 del presente Reglamento.

SUBCAPÍTULO II CIBERSEGURIDAD

Artículo 14. Programa de ciberseguridad

14.1 Toda empresa que cuente con presencia en el ciberespacio debe mantener, con carácter permanente, un programa de ciberseguridad (PG-C) aplicable a las operaciones, procesos y otros activos de información asociados.

14.2 El PG-C debe prever un diagnóstico y un plan de mejora sobre sus capacidades de ciberseguridad, para lo cual debe seleccionar un marco de referencia internacional sobre la materia, que le permita cuando menos lo siguiente:

- a) Identificación de los activos de información.
- b) Protección frente a las amenazas a los activos de información.
- c) Detección de incidentes de ciberseguridad.
- d) Respuesta con medidas que reduzcan el impacto de los incidentes.
- e) Recuperación de las capacidades o servicios tecnológicos que pudieran ser afectados.

Artículo 15. Reporte de incidentes de ciberseguridad significativos

15.1 La empresa debe reportar a la Superintendencia, en cuanto advierta la ocurrencia de un incidente de ciberseguridad que presente un impacto adverso significativo verificado o presumible de:

- a) Pérdida o hurto de información de la empresa o de clientes.
- b) Fraude interno o externo.
- c) Impacto negativo en la imagen y reputación de la empresa.

d) Interrupción de operaciones.

15.2 La empresa debe efectuar un análisis forense para determinar las causas del incidente y tomar las medidas para su gestión. El informe resultante de dicho análisis debe estar a disposición de la Superintendencia, el que debe tener un contenido ejecutivo y también con el detalle técnico correspondiente.

15.3 La Superintendencia, mediante norma de carácter general, establece el contenido mínimo, formato y protocolos adicionales a utilizar en dicho reporte.

Artículo 16. Intercambio de información de ciberseguridad

16.1 La empresa debe hacer los arreglos necesarios para contar con información que le permita tomar acción oportuna frente a las amenazas de ciberseguridad y para el tratamiento de las vulnerabilidades.

16.2 Al intercambiar información relativa a ciberseguridad, la empresa puede suscribir acuerdos con otras empresas del sector o con terceros que resulten relevantes, de forma bipartita, colectiva o gremial, para lo cual definirán los criterios pertinentes.

16.3 Mediante norma de carácter general, la Superintendencia puede establecer requerimientos específicos para que se incorporen en el intercambio de información de ciberseguridad.

SUBCAPÍTULO III AUTENTICACIÓN

Artículo 17. Implementación de los procesos autenticación

17.1 La empresa debe implementar procesos de autenticación, conforme a la definición establecida en este Reglamento, para controlar el acceso a los servicios que provea a sus usuarios por canales digitales, previo a lo cual debe evaluar formalmente y tomar medidas sobre:

- a) El o los factores de autenticación que serán requeridos.
- b) Estándares criptográficos vigentes, basados en software o en hardware, y sus prestaciones de confidencialidad o integridad esperadas.
- c) Plazos y condiciones en las que será obligatorio requerir al usuario volver a autenticarse, lo que incluye y no se limita a casos por periodo de inactividad o sesiones de uso prolongado de sistemas.
- d) Línea base de controles de seguridad de la información requerida para prevenir las amenazas a que esté expuesto el proceso de autenticación, lo que incluye, y no se restringe, al número límite de intentos fallidos de autenticación, la prevención de ataques de interceptación y manipulación de mensajes.
- e) Lineamientos para la retención de registros de auditoría para la detección de amenazas conocidas y eventos de seguridad de la información.

17.2 Los procesos de autenticación deben ser reevaluados siempre que la tecnología utilizada para su implementación deje de contar con el soporte del fabricante, o tras el descubrimiento de nuevas vulnerabilidades que pueden exponerlos.

17.3 La empresa debe mantener y proteger los registros detallados de lo actuado en cada enrolamiento de usuario, intento de autenticación y cada operación que requiera de autenticación previa.

17.4 La empresa debe contar con herramientas y procedimientos para implementar el monitoreo de transacciones que permita tomar medidas de reducción de la posibilidad de operaciones fraudulentas, que incorpore los escenarios de fraude ya conocidos, y el robo o compromiso de los elementos utilizados para la autenticación.

Artículo 18. Enrolamiento del usuario en servicios provistos por canal digital

18.1 El enrolamiento de un usuario en un canal digital requiere por lo menos:

- a) Verificar la identidad del usuario y tomar las medidas necesarias para reducir la posibilidad de suplantación de identidad, lo que incluye el uso de dos factores independientes de categorías diferentes, según el literal j) del artículo 2 de este Reglamento.

- b) Generar las credenciales y asignarlas al usuario.

18.2 La empresa debe gestionar el ciclo de vida de las credenciales que genere y asigne a sus usuarios, para lo cual debe prever los procedimientos para su activación, suspensión, reemplazo, renovación y revocación; así también, cuando corresponda, asegurar su confidencialidad e integridad.

Artículo 19. Autenticación reforzada para operaciones por canal digital

Se requiere de autenticación reforzada para aquellas acciones que puedan originar operaciones fraudulentas u otro abuso del servicio en perjuicio del cliente, como las operaciones a través de un canal digital que impliquen pagos o transferencia de fondos a terceros, registro de un beneficiario de confianza, modificación en los productos de seguro ahorro/inversión contratados, la contratación de un producto o servicio, modificación de límites y condiciones, para lo cual se requiere:

- a) Utilizar una combinación de factores de autenticación, según el literal j) del artículo 2 del presente Reglamento que, por lo menos, correspondan a dos categorías distintas y que sean independientes uno del otro.
- b) Generar un código de autenticación mediante métodos criptográficos, a partir de los datos específicos de cada operación, el cual debe utilizarse por única vez.
- c) Cuando la operación sea exitosa, notificar los datos de la operación al usuario.

Artículo 20. Exenciones de autenticación reforzada para operaciones por canal digital

20.1 Están exentas del requisito de autenticación reforzada indicado en el artículo 19 del presente Reglamento, las siguientes operaciones realizadas por canal digital:

- a) Las operaciones de pago, pagos periódicos o transferencia hacia un beneficiario registrado previamente por el usuario como beneficiario de confianza, como destinatario usual de dichas operaciones.
- b) Las operaciones de pago, pagos periódicos o transferencias a cuentas en las que el cliente y el beneficiario sean la misma persona, sea natural o jurídica, y siempre que dichas cuentas se mantengan en la misma empresa.

20.2 Las operaciones de pago que presenten un nivel de riesgo de fraude bajo, como resultado de un análisis del riesgo en línea por operación, están exentas de la autenticación reforzada, siempre que la empresa cumpla con:

- i. Implementar alguno de los estándares de la industria de pagos, EMV 3DS y tokenización de pagos EMV, en sus versiones más recientes.
- ii. Definir el monto de umbral por operación por debajo del cual aplicará la exención por el citado análisis de riesgos.
- iii. Medir periódicamente la ratio de fraude de las operaciones de pago por canal y tipo de operación.
- iv. Actualizar periódicamente las reglas aplicables en el análisis de riesgo en función al indicador de riesgo de fraude.
- v. Utilizar los datos que estén disponibles por cada tipo de operación, que incluye, pero no se limita a, los asociados al comportamiento del usuario, al medio utilizado y los que de este se pueda obtener para fines del análisis de riesgo.

20.3 Las operaciones no reconocidas por los clientes que hayan sido efectuadas en aplicación de la exención señalada en el párrafo 20.2 del presente artículo, o que fueron realizadas luego de que el usuario reportara el robo o pérdida de sus credenciales, son responsabilidad de la empresa, para lo cual deben implementar mecanismos que ante el repudio de la operación por parte del usuario garanticen su aplicación inmediata.

Artículo 21. Uso de API para la provisión de servicios en línea

21.1 El uso de interfaces de programación de aplicaciones, para proveer servicios para realizar operaciones, a través de servicios de terceros, requiere que se implementen las siguientes medidas:

- a) Análisis de riesgos asociados e implementar las medidas de mitigación.
- b) La autenticación mutua de los sistemas y la de los usuarios.
- c) La autorización de las operaciones por parte de los usuarios.
- d) El cifrado de datos en almacenamiento o transmisión.

- e) Prácticas de desarrollo seguro de API y revisión de prácticas de codificación segura.
 - f) Análisis de vulnerabilidades y pruebas de penetración.
 - g) La seguridad de la infraestructura tecnológica que lo soporta.
 - h) Los mecanismos de tolerancia ante fallos y de contingencia.
 - i) Control de accesos en el entorno de datos, sistemas e infraestructura.
 - j) Monitoreo de eventos de seguridad de la información y gestión de estos cuando se constituyan en incidentes.
- 21.2 La empresa debe tomar como referencia estándares y marcos de referencia internacionales, y cuando sea factible adoptarlos en el marco de acuerdos gremiales o sectoriales, para la implementación del intercambio y encriptación de datos, así como la autenticación y la autorización de operaciones, sin que ello sea una lista restrictiva.
- 21.3 Las especificaciones técnicas de las API utilizadas deben encontrarse documentadas de forma que facilite su auditoría y la implementación necesaria para su uso.
- 21.4 Las empresas deben implementar las medidas necesarias para garantizar que el tercero autorizado por el usuario, acceda únicamente a la información indicada por este último.

SUBCAPÍTULO IV

PROVISIÓN DE SERVICIOS POR TERCEROS

Artículo 22. Servicios provistos por terceros

En el caso de servicios provistos por terceros en aspectos referidos a gestión de tecnología de la información, a gestión de seguridad de la información o a procesamiento de datos, la empresa, además de cumplir con los requerimientos establecidos en el Reglamento de Gobierno Corporativo y Gestión Integral de Riesgos y el Reglamento para la Gestión de Riesgo Operacional debe:

- a) Evaluar las amenazas y vulnerabilidades de seguridad de la información en la provisión de bienes y servicios e implementar medidas de tratamiento.
- b) Asegurar que el arreglo contractual con el proveedor y su implementación le permiten cumplir con las obligaciones establecidas en el presente Reglamento.
- c) Establecer los roles y responsabilidades que el proveedor asume contractualmente sobre la seguridad de la información y asegurar que la empresa efectúe las implementaciones complementarias correspondientes para la atención de los requerimientos del presente Reglamento.

Artículo 23. Uso de servicios en nube

Para hacer uso de los servicios en nube, la empresa debe implementar políticas y procedimientos de seguridad de la información que sean de aplicación específica, que tome en cuenta un marco de buenas prácticas internacionales para el uso de estos servicios, y que además de los requerimientos del artículo 22 del Reglamento, incluya los siguientes aspectos:

- a) Requerimientos de seguridad de la información que los servicios de nube deben cumplir y procedimientos para asegurar la implementación antes de su uso.
- b) Lineamientos para segregación de redes que permita el aislamiento de la información de la empresa respecto a la de terceros en el entorno compartido del servicio en nube.
- c) Evaluación de la disponibilidad de registro de eventos (log) que el proveedor de servicio en nube ofrece y atención de la necesidad de registros adicionales para el monitoreo de seguridad de la información.
- d) Previsión de plan de capacitación para los niveles gerenciales, administradores de estos servicios, personal a cargo de su implementación y quienes hacen uso de ellos, sobre aquello necesario para el manejo de la seguridad de la información en estos.

Artículo 24. Servicios significativos de procesamiento de datos

24.1 La contratación de un servicio significativo provisto por terceros para el procesamiento de datos, incluido los servicios en nube, debe ser considerado como un cambio importante en el ambiente informático, siendo aplicable la definición de servicio significativo establecida en el Reglamento de Gobierno Corporativo y Gestión Integral de Riesgos y la normativa vigente asociada a nuevos productos y cambios importantes.

24.2 La empresa debe cumplir los siguientes aspectos referidos a la contratación de un servicio significativo provisto por terceros para el procesamiento de datos, que incluye servicios en nube, de manera complementaria a lo establecido en los artículos 22 y 23 del presente Reglamento, según corresponda:

- a) Asegurar el acceso adecuado a la información, en tiempos razonables y a solo requerimiento, por parte de la Superintendencia, Auditoría Interna y la Sociedad de Auditoría Externa, en condiciones normales de operación y en regímenes especiales.
- b) Gestionar los incidentes de seguridad de la información, conforme al numeral 6 del artículo 12 y de desarrollar las actividades planificadas previstas en el artículo 13 del presente Reglamento, en lo aplicable al servicio significativo de procesamiento de datos del que se trate.
- c) Contar con una estrategia de salida de los servicios a cargo del proveedor que permita retomar operaciones por cuenta propia o mediante otro proveedor. Dicha estrategia debe prever, entre otros aspectos, las acciones necesarias para la migración de la información a los recursos de la empresa o de otro proveedor.¹¹
- d) Mantener un inventario de los servicios que el proveedor, a su vez, contrata con terceros (contratación en cadena) y que se encuentren relacionados a los servicios contratados por la empresa.
- e) Asegurar que la información de carácter confidencial en custodia del proveedor sea eliminada definitivamente ante la resolución del acuerdo contractual.
- f) Verificar anualmente que el proveedor de servicios de procesamiento de datos cuenta con controles de seguridad de la información, conforme a la normativa vigente sobre seguridad de la información, en lo aplicable al servicio provisto. Ello puede ser sustentado mediante informes independientes y reportes de auditoría que incluyen en su alcance la verificación de dichos controles.
- g) Cuando se trate de servicios en nube, para cumplir con lo requerido en el literal previo, la empresa debe evidenciar anualmente que el proveedor mantiene vigente las certificaciones ISO/IEC 27001, ISO/IEC 27017 e ISO/IEC 27018, y que cuenta con un reporte SOC 2 tipo 2 u otros equivalentes, relevantes al servicio provisto y a la zona o región desde donde se provee el servicio.

24.3 La empresa debe informar a esta Superintendencia sobre el servicio contratado, el proveedor involucrado, los niveles de servicio acordados, infraestructura tecnológica utilizada, así como los procedimientos y responsables para dar cumplimiento a los literales del a) al f), y según corresponda g) del párrafo anterior; como máximo treinta (30) días calendario después de iniciar la provisión del procesamiento de datos¹².

Artículo 25. Autorización para la contratación de servicio significativo de procesamiento de datos provisto por terceros desde el exterior¹³

25.1 La empresa debe solicitar autorización de la Superintendencia, previo a la contratación de un servicio significativo de procesamiento de datos provisto por terceros desde el exterior, en caso dicho servicio presente limitaciones para cumplir con los requerimientos establecidos en el párrafo 24.2 del artículo 24 del presente Reglamento, la cual será respondida por la Superintendencia en el plazo de sesenta (60) días hábiles. Para solicitar dicha autorización las empresas deben presentar junto con su solicitud, un informe con los sustentos legales de las limitaciones identificadas y una propuesta de plan de implementación de las medidas compensatorias.

25.2 La autorización que conceda esta Superintendencia es específica al proveedor del servicio y, al país y ciudad desde el que se recibe, así como a las condiciones generales que fueron objeto de la autorización, por lo que de existir modificaciones en ellas y, de mantenerse la limitación citada en el párrafo previo, se requiere de un nuevo procedimiento de autorización ante la Superintendencia.

SUBCAPÍTULO V RÉGIMEN SIMPLIFICADO DEL SGSI-C

Artículo 26. Sistema simplificado de gestión de seguridad de la información

26.1 El régimen simplificado de gestión de seguridad de la información requiere la planificación y ejecución de las siguientes actividades mínimas, cuya periodicidad por lo menos debe ser anual:

¹¹ Inciso modificado por la Resolución SBS N° 1515-2021 del 24/05/2021.

¹² Párrafo modificado por la Resolución SBS N° 1515-2021 del 24/05/2021.

¹³ Artículo vigente a partir del 24.02.2021

- a) Identificar con las unidades de negocio y de apoyo, cuál es la información de mayor importancia, por las obligaciones normativas o contractuales existentes, y por la necesidad de operar.
- b) Identificar los dispositivos que se conectan a la red interna y todo software que se encuentre instalado en la infraestructura tecnológica, y asegurar que se encuentren acorde a una configuración segura previamente establecida.
- c) Identificar las cuentas de usuario con permisos de acceso habilitados y en particular las que poseen privilegios administrativos con posibilidad de adicionar software a la infraestructura, y mantener el principio de mínimos privilegios otorgados.
- d) Implementar y mantener una línea base de seguridad en sistemas operativos y aplicaciones utilizadas, incluidos los correspondientes a dispositivos móviles, estaciones de trabajo, servidores y dispositivos de comunicaciones. Identificar y evaluar la habilitación de las funciones de seguridad integradas en los sistemas operativos.
- e) Priorizar y gestionar las vulnerabilidades de seguridad identificadas, para cuya identificación oportuna debe contar con los servicios de información necesarios.
- f) Desarrollar una campaña de orientación para la adopción de prácticas seguras dirigida a los empleados, plana gerencial y de dirección.

26.2 En caso la empresa provea alguna de las operaciones indicadas en el artículo 19 del presente Reglamento por canal digital, en lo que corresponda a su implementación, debe cumplir con las disposiciones establecidas en el Subcapítulo III del Capítulo II del presente Reglamento.

26.3 En caso utilice servicios significativos provistos por terceros, en lo que corresponda a su implementación, la empresa debe cumplir con las disposiciones establecidas en el Subcapítulo IV del Capítulo II del presente Reglamento.

26.4 La empresa debe mantener un programa de ciberseguridad, conforme al Subcapítulo II del Capítulo II del presente Reglamento, con un alcance que por lo menos incluya los servicios indicados en los párrafos 26.2 y 26.3 del artículo 26 del presente Reglamento.

SUBCAPÍTULO VI RÉGIMEN REFORZADO DEL SGSI-C

Artículo 27. Requerimientos adicionales para empresa con concentración de mercado

27.1 El directorio debe designar a un director como responsable de velar por la efectividad del sistema de gestión de seguridad de la información, lo que incluye el desarrollo del plan estratégico del SGSI-C.

27.2 La empresa debe someter periódicamente a una evaluación independiente del alcance y la efectividad del SGSI-C; dicha evaluación podrá ser realizada por la unidad de auditoría interna u otro equipo que cumpla el requisito de independencia, siempre que posea experiencia previa y certificaciones internacionales que demuestren la preparación técnica necesaria.

DISPOSICIONES COMPLEMENTARIAS FINALES

Primera.- La empresa puede contar con un marco para la gestión de los riesgos asociados a la seguridad de la información, que debe ser integrado en lo que corresponda en la gestión del riesgo operacional, conforme a los lineamientos establecidos en el artículo 22° del Reglamento de Gobierno Corporativo y de la Gestión Integral de Riesgos.

Segunda.- Los informes a los que se refieren los literales g) y h) del artículo 12°, y el artículo 27° del Reglamento de Gobierno Corporativo y de la Gestión Integral de Riesgos deben incluir la evaluación de los riesgos asociados a la seguridad de la información.

Tercera.- En caso de eventos que afecten la continuidad operativa y que tengan como causa probable un incidente de seguridad de la información, es aplicable lo señalado en el artículo 15 del Reglamento para la Gestión de la Continuidad del Negocio, aprobado por la Resolución SBS N° 877-2020, sobre reporte de eventos de interrupción significativa.

Cuarta.- La aplicación del presente Reglamento se extiende a las empresas corredoras de seguros del segmento 1, según segmentación establecida en el artículo 36 del Reglamento para la Supervisión y Control de los Corredores y Auxiliares de Seguros aprobado por la Resolución SBS N° 809-2019, a dichas empresas les es exigible el párrafo 26.1 del artículo 26, Subcapítulo V, Capítulo II, del presente Reglamento.

Artículo Segundo.- Modificar el Reglamento de Auditoría Interna, aprobado por la Resolución SBS N° 11699-2008 y sus modificatorias, conforme a lo siguiente:

En el Anexo “Actividades Programadas”, sustituir el numeral 3 de la Sección I, el numeral 1 de la Sección II, el numeral 1 de la Sección III, el numeral 2 de la Sección IV, el numeral 3 de la Sección V y el numeral 1 de la Sección VI, conforme a los siguientes textos:

“I. EMPRESAS SEÑALADAS EN LOS LITERALES A, B Y C DEL ARTÍCULO 16° DE LA LEY GENERAL (EXCEPTO LAS EMPRESAS AFIANZADORAS Y DE GARANTÍAS), BANCO DE LA NACIÓN, BANCO AGROPECUARIO, FONDO MIVIVIENDA Y CORPORACIÓN FINANCIERA DE DESARROLLO (COFIDE)

(...)

- 3) *Evaluación de la gestión del riesgo operacional y del cumplimiento de los procedimientos utilizados para la administración de los riesgos de operación; así como, de las disposiciones de la normativa vigente sobre gestión de continuidad del negocio y de seguridad de la información y ciberseguridad;*

(...)”

“II. EMPRESAS DE SEGUROS Y/O DE REASEGUROS:

- 1) *Evaluación de la gestión de los riesgos distintos a los riesgos técnicos de seguros, que incluyen riesgo operacional, de mercado, de crédito, entre otros, y de las disposiciones de la normativa vigente sobre gestión de continuidad del negocio y de seguridad de la información y ciberseguridad;*

(...)”

“III. EMPRESAS DE SERVICIOS COMPLEMENTARIOS Y CONEXOS

- 1) *Evaluación de la gestión del riesgo operacional y del cumplimiento de los procedimientos utilizados para la administración de los riesgos de operación; así como, de las disposiciones de la normativa vigente sobre gestión de continuidad del negocio y de seguridad de la información y ciberseguridad.*

(...)”

“IV. EMPRESAS AFIANZADORAS Y DE GARANTÍAS

(...)

- 2) *Evaluación de la gestión del riesgo operacional y del cumplimiento de los procedimientos utilizados para la administración de los riesgos de operación; así como, de las disposiciones de la normativa vigente sobre seguridad de la información y Ciberseguridad.*

(...)”

“V. DERRAMAS Y CAJAS DE PENSIONES

- 3) *Evaluación de la gestión del riesgo operacional y del cumplimiento de los procedimientos utilizados para la administración de los riesgos de operación; así como, de las disposiciones de la normativa vigente sobre gestión de continuidad del negocio y de seguridad de la información y Ciberseguridad;*

(...)”

“VI. ADMINISTRADORAS PRIVADAS DE FONDOS DE PENSIONES (AFP):

- 1) *Evaluación de la gestión del riesgo operacional y de las disposiciones de la normativa vigente sobre gestión de continuidad del negocio y de seguridad de la información;*

(...)”

Artículo Tercero.- Modificar el literal b) del segundo párrafo del artículo 20° Informe sobre el sistema de control interno del Reglamento de Auditoría Externa, aprobado por Resolución SBS N° 17026-2010 y sus modificatorias, de acuerdo a lo siguiente al siguiente texto:

“Artículo 20°.- Informe sobre el sistema de control interno

(...)

b) Evaluación de los sistemas de información de la empresa en el ámbito de la auditoría externa, que incluye, entre otros, el flujo de información en los niveles internos de la empresa para su adecuada gestión, y la revisión selectiva de la validez de los datos contenidos en la información complementaria a los estados financieros (anexos y reportes) que presentan las empresas a esta Superintendencia, según las normas vigentes sobre la materia; donde deben precisarse los sistemas que fueron parte del alcance de dicha evaluación; y,

(...)”

Artículo Cuarto.- Modificar el procedimiento N° 123 relativo a la “Autorización del Procesamiento Principal en el Exterior” por “Autorización para la contratación del servicio significativo de Procesamiento de Datos provisto por terceros desde el Exterior” e incorporar el procedimiento N°198 relativo a “Autorización para aplicar el Régimen Simplificado del Sistema de Gestión de la Seguridad de la Información y la Ciberseguridad” en el Texto Único de Procedimientos Administrativos de la Superintendencia de Banca, Seguros y Administradoras Privadas de Fondos de Pensiones, aprobado mediante Resolución N° 1678-2018, cuyo texto se anexa a la presente la presente resolución y se publica en el Portal Web institucional (www.sbs.gob.pe).

Artículo Quinto.- Modificar el Reglamento de Gobierno Corporativo y de la Gestión Integral de Riesgos, aprobado mediante Resolución SBS N° 272-2017 y sus modificatorias, de acuerdo a lo siguiente:

1. Incorporar en el Artículo 2 del Reglamento de Gobierno Corporativo y de la Gestión Integral de Riesgos, aprobado mediante Resolución SBS N° 272-2017 el siguiente texto:

“rr) Proveedor: tercero contratado para brindar bienes y/o servicios a una empresa, incluso bajo la modalidad de subcontratación. Las empresas que forman parte del mismo grupo económico que la empresa contratante también son consideradas como terceros.”

d) Modificar en el Artículo 2 Definiciones y/o referencias, el literal jj) Subcontratación, de acuerdo a lo siguiente:

“jj) Subcontratación: Modalidad mediante la cual una empresa contrata a un proveedor para que este entregue bienes y/o servicios que podrían ser desarrollados por ella.”

3. Sustituir el Capítulo IV, así como su referencia en el Índice de dicho Reglamento por “Bienes y/o Servicios Provistos por Terceros”, con el siguiente texto:

**“CAPÍTULO IV
BIENES Y/O SERVICIOS PROVISTOS POR TERCEROS**

Artículo 35.- Aspectos generales

35.1. Los bienes y/o servicios provistos por terceros son aquellos entregados a la empresa por parte de un proveedor.

35.2. En caso se trate de un bien y/o servicio que pudiera ser desarrollado por la empresa pero decide solicitarlo a través de un tercero, se configura la modalidad de subcontratación.

35.3. Los bienes y/o servicios significativos provistos por terceros son aquellos que, en caso de falla o suspensión, pueden poner en riesgo importante a la empresa al afectar sus ingresos, solvencia, continuidad operativa o reputación. En caso de que algún bien y/o servicio significativo sea provisto por un tercero bajo la modalidad de subcontratación, la subcontratación se considera significativa.

35.4. *Un proveedor es considerado significativo cuando provee servicios significativos, se encuentre o no, bajo la modalidad de subcontratación.*

Artículo 36.- Bienes y/o servicios provistos por terceros

36.1 *Los riesgos asociados a la entrega de bien y/o servicios provistos por terceros deben ser gestionados como parte del marco de gestión integral de riesgos de la empresa.*

36.2 *La empresa es responsable de los resultados de los bienes y/o servicios provistos por terceros bajo la modalidad de subcontratación.*

36.3 *La empresa debe realizar una evaluación de los riesgos asociados a los servicios significativos provistos por terceros, ya sea que se encuentren o no bajo la modalidad de subcontratación. Dicha evaluación debe ser presentada al directorio para su aprobación.*

36.4 *En el caso de subcontratación significativa se debe contar con cláusulas que faciliten una adecuada revisión de la respectiva prestación por parte de las empresas, de la unidad de auditoría interna, de la sociedad de auditoría externa, así como por parte de la Superintendencia o las personas que esta designe, en los contratos suscritos con los proveedores.*

36.5 *La subcontratación de las funciones de la gestión de riesgos es considerada como significativa para fines de este Reglamento.*

36.6 *Esta Superintendencia puede definir requisitos adicionales para algunos bienes y/o servicios específicos provistos por terceros.*

Artículo 37°.- Autorización para la contratación de bienes y/o servicios significativos provistos por terceros

La contratación de los siguientes bienes y/o servicios significativos requiere autorización previa de esta Superintendencia y debe sujetarse a lo establecido en las normas reglamentarias específicas:

- a) *La subcontratación significativa de auditoría interna, de acuerdo con lo establecido en el Reglamento de Auditoría Interna o norma que lo sustituya;*
- b) *Otros que indique la Superintendencia mediante norma general.”*

Artículo Sexto.- Modificar Reglamento de Riesgo Operacional, aprobado por Resolución SBS N° 2116-2009, según se indica a continuación:

1. Sustituir el literal i del artículo 2 y el artículo 14, de acuerdo con el siguiente texto:

“Artículo 2.- Definiciones

(...)

i. *Subcontratación: Modalidad mediante la cual una empresa contrata a un proveedor para que este entregue bienes y/o servicios que podrían ser desarrollados por ella.*

(...)

2. Sustituir el artículo 14 de acuerdo con el siguiente texto:

“Artículo 14.- Bienes y/o servicios provistos por terceros

La empresa debe contar con políticas y procedimientos apropiados para gestionar los riesgos asociados a los servicios provistos por terceros, y contar con un registro de estos.

La empresa debe implementar un procedimiento para la identificación de aquellos proveedores significativos precisando los casos en los que se encuentren bajo la modalidad de subcontratación.

En los casos de servicios significativos, se encuentren o no bajo la modalidad de subcontratación, y de servicios subcontratados la empresa debe considerar los siguientes aspectos:

- a) *Implementar un proceso de selección del proveedor del servicio.*
- b) *Contar con un contrato, el cual debe incluir acuerdos de niveles de servicio; establecer claramente las responsabilidades del proveedor y de la empresa; establecer la jurisdicción que prevalecerá en caso de conflicto entre las partes; e incorporar los niveles de seguridad de información requeridos.*
- c) *Gestionar y monitorear los riesgos asociados a estos servicios.*
- d) *Mantener un registro que debe contener como mínimo:*
 - i) *Nombre del proveedor*
 - ii) *Giro o actividad principal de negocio del proveedor*
 - iii) *Descripción o listado de los servicios provistos*
 - iv) *Países, regiones y/o zonas geográficas desde donde se provee el servicio a contratar*
 - v) *Niveles de servicio acordados para su provisión*
 - vi) *Si la subcontratación es o no considerada significativa por la empresa*
 - vii) *Fecha de inicio del servicio*
 - viii) *Fecha de última renovación, si corresponde*
 - ix) *Fecha de vencimiento del servicio o la próxima fecha de renovación del contrato, según corresponda*

Artículo Séptimo.- Modificar el Reglamento de Tarjetas de Crédito y Débito, aprobado por Resolución SBS N° 6523-2013 y sus normas modificatorias, según se indica a continuación:

1. Sustituir los artículos 6 y 12, de acuerdo con el siguiente texto:

“Artículo 6.- Información mínima, condiciones y vigencia aplicable a la tarjeta de crédito

Las tarjetas de crédito con soporte físico o digital se expiden con carácter de intransferible y deben incluir como mínimo la siguiente información:

1. *Denominación social de la empresa que emite la tarjeta de crédito.*
2. *Nombre comercial que la empresa asigne al producto.*
3. *Identificación del sistema de tarjeta de crédito (marca) al que pertenece, de ser el caso.*

En el caso de las tarjetas con soporte físico se debe incluir el nombre del usuario de la tarjeta de crédito; información de la que se puede prescindir siempre que la empresa cumpla con el Subcapítulo III del Capítulo II del Reglamento para la Gestión de la Seguridad de la Información y la Ciberseguridad, aprobado por Resolución SBS N°504-2021.

El plazo de vigencia de las tarjetas de crédito no puede exceder de cinco (5) años, pudiéndose acordar plazos de vencimiento menores.

Artículo 12.- Información mínima, condiciones y vigencia aplicable a las tarjetas de débito

Las tarjetas de débito con soporte físico o digital se expiden con carácter de intransferible y deben incluir como mínimo la siguiente información:

1. *Denominación social de la empresa que emite la tarjeta de débito.*
2. *Nombre comercial que la empresa asigne al producto.*
3. *Identificación del sistema de tarjeta de débito (marca) al que pertenece, de ser el caso.*

Para su uso, requieren adicionalmente la presencia de una clave secreta, firma, firma electrónica u otros mecanismos que permitan identificar al usuario, de acuerdo con lo pactado.

El plazo de vigencia de las tarjetas de débito no puede exceder de cinco (5) años, pudiéndose acordar plazos de vencimiento menores.”

Artículo Octavo.- Modificar el Reglamento de Operaciones con Dinero Electrónico aprobado por Resolución SBS N° 6283-2013 y sus normas modificatorias, según se indica a continuación:

1. Sustituir el artículo 4, de acuerdo con el siguiente texto:

“Artículo 4.- Soportes para uso de dinero electrónico

Los soportes mediante los cuales se puede hacer uso del dinero electrónico pueden ser los siguientes:

- a) Teléfonos móviles.*
- b) Tarjetas prepago.*
- c) Cualquier otro equipo o dispositivo electrónico, que cumpla los fines establecidos en la Ley.*

Estos dispositivos deben incluir como mínimo la siguiente información:

- 1. Denominación social de la empresa que emite el soporte mediante el cual se hace uso del dinero electrónico.*
- 2. Nombre comercial que la empresa asigne al producto.*
- 3. Identificación del sistema de tarjeta (marca) al que pertenece, de ser el caso.*

Dicha información debe ser mostrada en un espacio visible y de fácil acceso para el usuario.

Un mismo soporte puede ser utilizado y/o asociado para realizar transacciones con más de una cuenta de dinero electrónico.”

Artículo Noveno.- Plazos y Plan de adecuación

1. En un plazo que no debe exceder de sesenta (60) días calendario contados a partir del día siguiente de la publicación de la presente Resolución, las empresas deben presentar a la Superintendencia, un plan de adecuación al Reglamento para la Gestión de la Seguridad de la Información y la Ciberseguridad aprobado en el Artículo Primero de la presente Resolución, previamente aprobado por el directorio, en el cual incluya: a) un diagnóstico preliminar de la situación existente en la empresa; b) las acciones previstas para la total adecuación al Reglamento; c) los funcionarios responsables del cumplimiento de dicho plan; y, d) un cronograma de adecuación.

2. Las disposiciones señaladas en el Subcapítulo III del Capítulo II y la Tercera Disposición Complementaria Final del Reglamento para la Gestión de la Seguridad de la Información y la Ciberseguridad aprobado en el Artículo Primero de la presente Resolución tienen un plazo de adecuación hasta el 1 de julio de 2022.

3. En un plazo no mayor a treinta (30) días calendario contados a partir del día siguiente de la publicación de la presente Resolución, las empresas que cuenten con un servicio significativo de procesamiento de datos provisto por terceros desde el exterior, cuyo marco legal aplicable impida o limite el cumplimiento de las medidas definidas en el párrafo 24.2 del artículo 24 del Reglamento para la Gestión de la Seguridad de la Información y la Ciberseguridad, aprobado en el Artículo Primero de la presente Resolución, deben remitir un informe que contenga: i) las limitaciones presentadas, dicho informe debe contar con el sustento legal del impedimento de su aplicación y ii) las medidas compensatorias.

Artículo Décimo. - Vigencia

La presente Resolución entra en vigencia el 1 de julio de 2021, fecha en la que se deroga la Circular G 140-2009, con excepción de lo siguiente:

- a. Los párrafos 25.1 y 25.2 del artículo 25 del Reglamento para la Gestión de la Seguridad de la Información y la Ciberseguridad, aprobado por el Artículo Primero, que entran en vigencia al día siguiente de publicada la presente Resolución, fecha en la cual se deroga el artículo 7A de la Circular G 140-2009.
- b. El Artículo Segundo de la presente Resolución entra en vigencia a partir de la auditoría correspondiente al ejercicio 2022.

- c. Los Artículos Séptimo, Octavo y Noveno de la presente Resolución, entran en vigencia al día siguiente de la publicación de la presente Resolución, con excepción de lo indicado en el inciso d. del presente Artículo.
- d. El requerimiento asociado a la inclusión conjunta de la información sobre la denominación social de la empresa emisora y el nombre comercial que la empresa asigne al producto de tarjeta de crédito y/o débito, señalado en el Artículo Séptimo de la presente Resolución, así como el requerimiento asociado a la inclusión de la dicha información en los dispositivos de soporte al dinero electrónico, señalado en el artículo Octavo de la presente Resolución entran en vigencia el 1 de enero de 2022.

Regístrese, comuníquese y publíquese

SOCORRO HEYSEN ZEGARRA

Superintendente de Banca, Seguros y Administradoras
Privadas de Fondos de Pensiones

Anexo 3

(ii) Gestión de la Ciberseguridad:

- a) Establecer y mantener una estrategia y marco de ciberseguridad adaptados a los riesgos cibernéticos específicos, en línea con lo dispuesto por el marco normativo nacional e internacional vigente que resulte aplicable, tales como el marco de ciberseguridad de NIST, ISO 27002, Controles Críticos de Ciberseguridad del CIS, entre otros. (Nota: este requerimiento será exigible a partir del 01 de enero de 2022).
- b) Definir los roles y responsabilidades para la gestión de la ciberseguridad, proporcionar los recursos adecuados, la autoridad apropiada y el acceso al órgano correspondiente dentro de la empresa (por ejemplo: directorio, gerencia, etc).
- c) Tener identificados los riesgos cibernéticos a los que está expuesto el negocio del postulante, y tener implementados los controles para gestionar tales riesgos y proteger de los mismos al negocio. Asimismo, realizar una evaluación periódica de dichos riesgos.
- d) Implementar procesos de monitoreo sistemático para detectar oportunamente los incidentes cibernéticos y evaluar periódicamente la efectividad de los controles, a través del monitoreo de la red, pruebas, auditorías y ejercicios.
- e) Tener la capacidad de responder oportunamente ante los incidentes cibernéticos de la siguiente manera: (a) evaluar la naturaleza, el alcance y el impacto de un incidente cibernético; (b) contener el incidente y mitigar su impacto; (c) notificar a las partes interesadas internas y externas (CAVALI, reguladores y otras autoridades, accionistas, proveedores y clientes, según corresponda); y (d) coordinar las actividades de respuesta conjunta según sea necesario.
- f) Reanudar las operaciones de manera responsable luego de la generación de un incidente cibernético, permitiendo: (a) la eliminación de los restos dañinos del incidente; (b) la restauración de los sistemas y los datos a su estado normal; (c) la identificación y mitigación de todas las vulnerabilidades que fueron explotadas; (d) la remediación de las vulnerabilidades para prevenir incidentes similares; y (e) la comunicación apropiada, tanto interna como externa.
- g) Compartir con CAVALI información de ciberseguridad referida a amenazas, vulnerabilidades, incidentes y respuestas tomadas por la entidad, vinculada a los servicios a los que el postulante accederá en su condición de Participante Directo, Indirecto o Indirecto Especial, según corresponda.
- h) Implementar de forma periódica la revisión de la estrategia y el marco de ciberseguridad cuando los eventos lo justifiquen, incluidos los componentes de gobernanza, evaluación de riesgos y control, monitoreo, respuesta, recuperación e intercambio de información, para abordar los cambios en los riesgos cibernéticos, asignar recursos, identificar y remediar las brechas e incorporar lecciones aprendidas.

3.2. REQUISITOS DE CALIFICACIÓN

A	CAPACIDAD TÉCNICA Y PROFESIONAL
A.1	EXPERIENCIA DEL PERSONAL CLAVE
	<p><u>Requisitos:</u></p> <p><u>JEFE DE PROYECTO</u> Mínimo tres (3) años de experiencia como Oficial de Seguridad de Información o Jefe o Líder de proyectos de servicios similares al objeto de contratación, como Ciberseguridad, Seguridad de la Información, Seguridad Informática Diseño e Implementación de Gobierno y Gestión de Tecnología o Seguridad en redes y nube; de los cuales por lo menos uno y medio (1.5) años deben ser en Seguridad de la Información y por lo menos seis (6) meses en Ciberseguridad o servicios relacionados con Ciberseguridad (Hacking Ético, Pentesting, Servicio de Centro de Operaciones de Seguridad, Análisis Forense), en ambos casos en Instituciones Financieras (empresas de operaciones múltiples, AFPs o empresas de seguros) en la calidad de Oficial de Seguridad de Información o Jefe o Líder de Proyecto.</p> <p><u>CONSULTOR SENIOR</u> Mínimo tres (3) años de experiencia como Consultor en proyectos de servicios similares al objeto de contratación, como Ciberseguridad, Seguridad de la Información, Seguridad Informática o Seguridad en redes y nube; de los cuales por lo menos uno y medio (1.5) años deben ser en Seguridad de la Información y por lo menos seis (6) meses en Ciberseguridad o servicios relacionados con Ciberseguridad (Hacking Ético, Pentesting, Servicio de Centro de Operaciones de Seguridad, Análisis Forense), en ambos casos en Instituciones Financieras (empresas de operaciones múltiples, AFPs o empresas de seguros), en calidad de Consultor.</p> <p>De presentarse experiencia ejecutada paralelamente (traslape), para el cómputo del tiempo de dicha experiencia sólo se considerará una vez el periodo traslapado.</p> <p><u>Acreditación:</u></p> <p>La experiencia del personal 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 clave propuesto.</p> <p>Sin perjuicio de lo anterior, los postores deben llenar y presentar el Anexo N° 9 referido al personal clave propuesto para la ejecución del servicio de consultoría.</p> <div style="border: 1px solid black; padding: 5px; margin-top: 10px;"> <p>Importante</p> <ul style="list-style-type: none"> • <i>Los documentos que acreditan la experiencia deben incluir los nombres y apellidos del profesional, el cargo desempeñado, el plazo de la prestación indicando el día, mes y año de inicio y culminación, el nombre de la Entidad u organización que emite el documento, la fecha de emisión y nombres y apellidos de quien suscribe el documento.</i> • <i>En caso los documentos para acreditar la experiencia establezcan el plazo de la experiencia adquirida por el profesional en meses sin especificar los días se debe considerar el mes completo.</i> • <i>Se considerará aquella experiencia que no tenga una antigüedad mayor a veinticinco (25) años anteriores a la fecha de la presentación de ofertas.</i> • <i>Al calificar la experiencia de los profesionales, 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 profesional corresponden con la función propia del cargo o puesto requerido en las bases.</i> </div>
A.2	CALIFICACIONES DEL PERSONAL CLAVE
A.2.1	FORMACIÓN ACADÉMICA
	<p><u>Requisitos:</u></p>

	<p><u>JEFE DE PROYECTO</u> Titulado en Ingeniería de Sistemas, Industrial, Electrónica, Computación e Informática o similares.</p> <p><u>CONSULTOR SENIOR</u> Titulado en Ingeniería de Sistemas, Electrónica, Computación e Informática o similares.</p> <p><u>Acreditación:</u></p> <p>El Título Profesional requerido será verificado por el órgano encargado de las contrataciones o el comité de selección, según corresponda, 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/</p> <p>En caso el Título Profesional requerido no se encuentre inscrito en el referido registro, el postor debe presentar la copia del diploma respectivo a fin de acreditar la formación académica requerida.</p> <p>Sin perjuicio de lo anterior, los postores deben llenar y presentar el Anexo N° 9 referido al personal clave propuesto para la ejecución del servicio de consultoría.</p> <div style="border: 1px solid black; padding: 5px; margin-top: 10px;"> <p>Importante</p> <p><i>Se debe aceptar las diferentes denominaciones utilizadas para acreditar la carrera profesional requerida, aun cuando no coincida literalmente con aquella prevista en las bases (por ejemplo Ingeniería Ambiental, Ingeniería en Gestión Ambiental, Ingeniería y Gestión Ambiental u otras denominaciones).</i></p> </div>
B	<p>EXPERIENCIA DEL POSTOR EN LA ESPECIALIDAD</p> <p><u>Requisitos:</u> El postor debe acreditar un monto facturado acumulado equivalente a S/. 120,000.00 (Ciento Veinte Mil con 00/100 Soles), por la contratación de servicios iguales o similares al objeto de la convocatoria, durante los diez (10) años anteriores a la fecha de la presentación de ofertas que se computarán desde la fecha de la conformidad o emisión del comprobante de pago, según corresponda.</p> <p>Se consideran servicios de consultoría similares a los siguientes:</p> <ul style="list-style-type: none"> - Servicio de Ciberseguridad - Servicios en Sistemas de Gestión de Seguridad de la Información. - Implementación del Sistema de Gestión de Seguridad de la Información (SGSI) - Mantenimiento y Mejora Continua del Sistema de Gestión de Seguridad de la Información (SGSI) - Implementación de la NTP ISO/IEC 27001 Sistema de Gestión de Seguridad de la Información. <p><u>Acreditación:</u> 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 pago¹⁴.</p> <p>Los postores pueden presentar hasta un máximo de veinte (20) contrataciones para acreditar el requisito de calificación y el factor “Experiencia de Postor en la Especialidad”.</p> <p>En caso los postores presenten varios comprobantes de pago para acreditar una sola contratación, se</p>

¹⁴ Cabe precisar que, de acuerdo con la **Resolución N° 0065-2018-TCE-S1 del Tribunal de Contrataciones del Estado**:

“... el solo sello de cancelado en el comprobante, cuando ha sido colocado por el propio postor, no puede ser considerado como una acreditación que produzca fehaciencia en relación a que se encuentra cancelado. Admitir ello equivaldría a considerar como válida la sola declaración del postor afirmando que el comprobante de pago ha sido cancelado”

(...)

“Situación diferente se suscita ante el sello colocado por el cliente del postor [sea utilizando el término “cancelado” o “pagado”] supuesto en el cual sí se contaría con la declaración de un tercero que brinde certeza, ante la cual debiera reconocerse la validez de la experiencia”.

debe acreditar que corresponden a dicha contratación; de lo contrario, se asumirá que los comprobantes acreditan contrataciones independientes, en cuyo caso solo se considerará, las veinte (20) primeras contrataciones indicadas en el **Anexo N° 10** referido a la Experiencia del Postor en la Especialidad.

En el caso de servicios de ejecución periódica, solo se considera como experiencia la parte del contrato que haya sido ejecutada durante los diez (10) 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° 11**.

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 servicio o de cancelación del comprobante de pago, según corresponda.

Sin perjuicio de lo anterior, los postores deben llenar y presentar el **Anexo N° 10** referido a la Experiencia del Postor en la Especialidad.

Importante

- *El órgano encargado de las contrataciones o el comité de selección, según corresponda debe valorar de manera integral los documentos presentados por el postor para acreditar la 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, la calificación de la experiencia se realiza conforme a la Directiva "Participación de Proveedores en Consorcio en las Contrataciones del Estado".*

Importante

- *Si como resultado de una consulta u observación corresponde precisarse o ajustarse el requerimiento, se solicita la autorización del área usuaria y se pone de conocimiento de tal hecho a la dependencia que aprobó el expediente de contratación, de conformidad con el numeral 72.3 del artículo 72 del Reglamento.*
- *El cumplimiento de los Términos de Referencia se realiza mediante la presentación de una declaración jurada. De ser el caso, adicionalmente la Entidad puede solicitar documentación que acredite el cumplimiento del algún componente de estos. Para dicho efecto consignará de manera detallada los documentos que deben presentar los postores en el literal a.5) 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

EVALUACIÓN TÉCNICA (Puntaje: 100 Puntos)

FACTORES DE EVALUACIÓN		PUNTAJE / METODOLOGÍA PARA SU ASIGNACIÓN
A.	EXPERIENCIA DEL POSTOR EN LA ESPECIALIDAD	90 puntos
	<p><u>Evaluación:</u></p> <p>El postor debe acreditar un monto facturado acumulado equivalente a S/. 360,000.00 (Trescientos Sesenta Mil con 00/100 Soles), por la contratación de servicios de consultoría iguales o similares al objeto de la convocatoria, durante los diez (10) años anteriores a la fecha de la presentación de ofertas que se computarán desde la fecha de la conformidad o emisión del comprobante de pago, según corresponda.</p> <p><u>Acreditación:</u></p> <p>La experiencia 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 pago¹⁵.</p> <p>Las disposiciones sobre el requisito de calificación "Experiencia del postor en la especialidad" previstas en el literal C del numeral 3.2 del Capítulo III de la presente sección de las bases resultan aplicables para el presente factor.</p>	<p>M = Monto facturado acumulado por el postor por la prestación de servicios de consultoría en la especialidad</p> <p>M ≥ S/ 360,000.00 90 puntos</p> <p>M ≥ S/ 240,000.00 y < 360,000.00 80 puntos</p> <p>M > S/ 120,000.00 y < S/ 240,000.00 70 puntos</p>
B.	METODOLOGÍA PROPUESTA	10 puntos
	<p><u>Evaluación:</u></p> <p>Se evaluará la metodología propuesta por el postor para la ejecución de la consultoría, cuyo contenido mínimo es el siguiente:</p> <ul style="list-style-type: none"> - Alcance - Evaluación - Identificación - Análisis - Tratamiento - Seguimiento y revisión <p><u>Acreditación:</u></p> <p>Se acreditará mediante la presentación del documento que sustente la metodología propuesta.</p>	<p>Desarrolla la metodología que sustenta la oferta 10 puntos</p> <p>No desarrolla la metodología que sustente la oferta 0 puntos</p>

¹⁵ Cabe precisar que, de acuerdo con la **Resolución N° 0065-2018-TCE-S1 del Tribunal de Contrataciones del Estado**:

"... el solo sello de cancelado en el comprobante, cuando ha sido colocado por el propio postor, no puede ser considerado como una acreditación que produzca fehaciencia en relación a que se encuentra cancelado. Admitir ello equivaldría a considerar como válida la sola declaración del postor afirmando que el comprobante de pago ha sido cancelado"

(...)

"Situación diferente se suscita ante el sello colocado por el cliente del postor [sea utilizando el término "cancelado" o "pagado"] supuesto en el cual sí se contaría con la declaración de un tercero que brinde certeza, ante la cual debiera reconocerse la validez de la experiencia".

Para acceder a la etapa de evaluación económica, el postor debe obtener un **puntaje técnico mínimo de ochenta (80) puntos**.

Importante

- *Los factores de evaluación elaborados por el órgano encargado de las contrataciones o el comité de selección, según corresponda, 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.*
- *Las ofertas técnicas que no alcancen el puntaje mínimo especificado son descalificadas.*

EVALUACIÓN ECONÓMICA (Puntaje: 100 Puntos)

FACTOR DE EVALUACIÓN	PUNTAJE / METODOLOGÍA PARA SU ASIGNACIÓN
A. PRECIO	
<u>Evaluación:</u> Se evaluará considerando la oferta económica del postor. <u>Acreditación:</u> Se acreditará mediante el registro del monto de la oferta en el SEACE o documento que contiene la oferta económica (Anexo N° 7), según corresponda.	La evaluación consistirá en asignar un puntaje de cien (100) puntos a la oferta de precio más bajo y otorga a las demás ofertas puntajes inversamente proporcionales a sus respectivos precios, según la siguiente fórmula: $P_i = \frac{O_m \times PMP}{O_i}$ i= Oferta P _i = Puntaje de la oferta a evaluar O _i =Precio i O _m = Precio de la oferta más baja PMP=Puntaje máximo del precio 100 puntos
PUNTAJE TOTAL	100 puntos

CAPÍTULO V

PROFORMA DEL CONTRATO

Conste por el presente documento, la contratación del servicio de adecuación al nuevo reglamento para la gestión de la seguridad de la información y la ciberseguridad, que celebra de una parte la Corporación Financiera de Desarrollo S.A., en adelante COFIDE, con RUC N° 20100116392, con domicilio legal en [Calle Augusto Tamayo N° 160, San Isidro], representada por [.....], identificado con DNI N° [.....], y de otra parte [.....], con RUC N° [.....], con domicilio legal en [.....], inscrita en la Ficha N° [.....] Asiento N° [.....] del Registro de Personas Jurídicas de la ciudad de [.....], debidamente representado por su Representante Legal, [.....], con DNI N° [.....], según poder inscrito en la Ficha N° [.....], Asiento N° [.....] del Registro de Personas Jurídicas de la ciudad de [.....], a quien en adelante se le denominará EL CONTRATISTA en los términos y condiciones siguientes:

CLÁUSULA PRIMERA: ANTECEDENTES

Con fecha [.....], el órgano encargado de las contrataciones, adjudicó la buena pro de la **ADJUDICACIÓN SIMPLIFICADA N° 035-2021-COFIDE TERCERA CONVOCATORIA**, para la contratación del servicio de adecuación al nuevo reglamento para la gestión de la seguridad de la información y la ciberseguridad, a [INDICAR NOMBRE DEL GANADOR DE LA BUENA PRO], cuyos detalles e importe constan en los documentos integrantes del presente contrato.

CLÁUSULA SEGUNDA: OBJETO

El presente contrato tiene por objeto la contratación del servicio de adecuación al nuevo reglamento para la gestión de la seguridad de la información y la ciberseguridad.

CLÁUSULA TERCERA: MONTO CONTRACTUAL

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

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

CLÁUSULA CUARTA: DEL PAGO¹⁶

COFIDE se obliga a pagar la contraprestación a EL CONTRATISTA en S/., en 2 cuotas equivalentes al 35% y 65% del monto contractual, según términos de referencia, 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 quince (15) días, bajo responsabilidad de dicho funcionario.

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

En caso de retraso en el pago por parte de COFIDE, 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.

¹⁶ En cada caso concreto, dependiendo de la naturaleza del contrato, podrá adicionarse la información que resulte pertinente a efectos de generar el pago.

CLÁUSULA QUINTA: DEL PLAZO DE LA EJECUCIÓN DE LA PRESTACIÓN

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

CLÁUSULA SEXTA: PARTES INTEGRANTES DEL CONTRATO

El presente contrato está conformado por las bases integradas, la oferta ganadora¹⁷, 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 COFIDE, 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 los contratos de consultoría 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.”

CLÁUSULA OCTAVA: EJECUCIÓN DE GARANTÍAS POR FALTA DE RENOVACIÓN

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

CLÁUSULA NOVENA: 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.

¹⁷ La oferta ganadora comprende a la oferta técnica y oferta económica del postor ganador de la buena pro.

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 Auditoría 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 integradas 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 Riesgos.

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

Este procedimiento no resulta aplicable cuando la consultoría 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 COFIDE no enerva su derecho a reclamar posteriormente por defectos o vicios ocultos, conforme a lo dispuesto por los artículos 40 de la Ley de Contrataciones del Estado y 173 de su Reglamento.

El plazo máximo de responsabilidad del contratista es de un año contado a partir de la conformidad otorgada por COFIDE.

CLÁUSULA DÉCIMA QUINTA: PENALIDADES

Si EL CONTRATISTA incurre en retraso injustificado en la ejecución de las prestaciones objeto del contrato, COFIDE 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 COFIDE 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.

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, COFIDE 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, COFIDE 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.

EL CONTRATISTA tiene la obligación de proporcionar a COFIDE aquellos documentos que éste requiera y que sean necesarios a efectos de poder cumplir sus obligaciones aplicables a prevención de lavado de activos y financiamiento de terrorismo y de prevención de delitos en materia de corrupción, en su calidad de sujeto obligado.

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 DÉCIMA OCTAVA: SOLUCIÓN DE CONTROVERSIAS¹⁸

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 COFIDE, 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.

¹⁸ 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).

- (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 COFIDE. EL CONTRATISTA deberá cumplir estas obligaciones, sobretodo en relación a las personas, asociadas, agentes o subcontratistas que puedan ser utilizados en la ejecución de los servicios prestados a COFIDE.

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 COFIDE sea en su responsabilidad penal, civil o reputacional, deberá informar de inmediato de este hecho a COFIDE; sin perjuicio de tomar todas las medidas necesarias para evitar o mitigar estos efectos. Asimismo, EL CONTRATISTA se compromete a entregar a COFIDE 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 COFIDE 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 COFIDE requiera. En el evento en que no se cumpliera con la obligación consagrada en la presente cláusula, COFIDE solicitará a EL CONTRATISTA la subsanación del incumplimiento, bajo apercibimiento, en caso de no cumplir con dicha subsanación, de resolver el contrato.

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 COFIDE: [.....]

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].

"COFIDE"

"EL CONTRATISTA"

ANEXOS

ANEXO N° 1

DECLARACIÓN JURADA DE DATOS DEL POSTOR

Señores

DEPARTAMENTO DE COMPRAS
ADJUDICACIÓN SIMPLIFICADA N° 035-2021-COFIDE TERCERA CONVOCATORIA
Presente.-

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

Nombre, Denominación o Razón Social :					
Domicilio Legal :					
RUC :		Teléfono(s) :			
MYPE ¹⁹		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.

Asimismo, me comprometo a remitir la confirmación de recepción, en el plazo máximo de dos (2) días hábiles de recibida la comunicación.

[CONSIGNAR CIUDAD Y FECHA]

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

Importante

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

¹⁹ 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, según las condiciones previstas en el numeral 149.4 del artículo 149 y el numeral 151.2 del artículo 151 del Reglamento. Asimismo, dicha información se tendrá en cuenta en caso de empate, conforme a lo previsto en el artículo 91 del Reglamento.

Importante

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

ANEXO N° 1
DECLARACIÓN JURADA DE DATOS DEL POSTOR

Señores

DEPARTAMENTO DE COMPRAS
ADJUDICACIÓN SIMPLIFICADA N° 035-2021-COFIDE TERCERA CONVOCATORIA
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 ²⁰		Sí	No	
Correo electrónico :				

Datos del consorciado 2				
Nombre, Denominación o Razón Social :				
Domicilio Legal :				
RUC :	Teléfono(s) :			
MYPE ²¹		Sí	No	
Correo electrónico :				

Datos del consorciado ...				
Nombre, Denominación o Razón Social :				
Domicilio Legal :				
RUC :	Teléfono(s) :			
MYPE ²²		Sí	No	
Correo electrónico :				

Autorización de notificación por correo electrónico:

Correo electrónico del consorcio:

... [CONSIGNAR SÍ O NO] autorizo que se notifiquen al correo electrónico indicado las siguientes actuaciones:

²⁰ 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 original, en calidad de garantía de fiel cumplimiento, según las condiciones previstas en el numeral 149.4 del artículo 149 y el numeral 151.2 del artículo 151 del Reglamento. Asimismo, dicha información se tendrá en cuenta en caso de empate, conforme a lo previsto en el artículo 91 del Reglamento. Para dichos efectos, todos los integrantes del consorcio deben acreditar la condición de micro o pequeña empresa.

²¹ Ibidem.

²² Ibidem.

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.

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.

ANEXO N° 2

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

Señores

DEPARTAMENTO DE COMPRAS

ADJUDICACIÓN SIMPLIFICADA N° 035-2021-COFIDE TERCERA CONVOCATORIA

Presente.-

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

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

[CONSIGNAR CIUDAD Y FECHA]

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

Importante

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

ANEXO N° 3

DECLARACIÓN JURADA DE CUMPLIMIENTO DE LOS TÉRMINOS DE REFERENCIA

Señores

DEPARTAMENTO DE COMPRAS

ADJUDICACIÓN SIMPLIFICADA N° 035-2021-COFIDE TERCERA CONVOCATORIA

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 consultoría de adecuación al nuevo reglamento para la gestión de la seguridad de la información y la ciberseguridad, de conformidad con los Términos de Referencia que se indican en el numeral 3.1 del Capítulo III de la sección específica de las bases y los documentos del procedimiento.

[CONSIGNAR CIUDAD Y FECHA]

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

Importante

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

ANEXO N° 4

DECLARACIÓN JURADA DE PLAZO DE PRESTACIÓN DEL SERVICIO DE CONSULTORÍA

Señores

DEPARTAMENTO DE COMPRAS

ADJUDICACIÓN SIMPLIFICADA N° 035-2021-COFIDE TERCERA CONVOCATORIA

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 de consultoría objeto del presente procedimiento de selección en el plazo de **[CONSIGNAR EL PLAZO OFERTADO]**.

[CONSIGNAR CIUDAD Y FECHA]

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

ANEXO N° 5

Señores

DEPARTAMENTO DE COMPRAS

ADJUDICACIÓN SIMPLIFICADA N° 035-2021-COFIDE TERCERA CONVOCATORIA

Presente.-

Yo [CONSIGNAR NOMBRES Y APELLIDOS COMPLETOS] identificado con documento de identidad N° [CONSIGNAR NÚMERO DE DNI O DOCUMENTO DE IDENTIDAD ANÁLOGO], domiciliado en [CONSIGNAR EL DOMICILIO LEGAL], declaro bajo juramento:

Que, me comprometo a prestar mis servicios en el cargo de [CONSIGNAR EL CARGO A DESEMPEÑAR] para ejecutar [CONSIGNAR LA DENOMINACIÓN DE LA CONVOCATORIA] en caso que el postor [CONSIGNAR EL NOMBRE, DENOMINACIÓN O RAZÓN SOCIAL DEL POSTOR²³] resulte favorecido con la buena pro y suscriba el contrato correspondiente.

Para dicho efecto, declaro que mis calificaciones y experiencia son las siguientes:

A. Calificaciones

A.1 Formación académica:

Carrera profesional	
Universidad	
Título profesional o grado obtenido	
Fecha de expedición del grado o título	

A.2 Capacitación:

N°	Materia de la capacitación	Cantidad de horas lectivas	Institución educativa u organización	Fecha de expedición del documento
Total horas lectivas				

B. Experiencia

[CONSIGNAR LA EXPERIENCIA SEGÚN LO REQUERIDO EN EL CAPÍTULO III DE LA PRESENTE SECCIÓN DE LAS BASES].

N°	Cliente o Empleador	Objeto de la contratación	Fecha de inicio	Fecha de culminación	Tiempo
1					
2					
(...)					

La experiencia total acumulada es de: [CONSIGNAR LA EXPERIENCIA TOTAL ACUMULADA EN AÑOS, MESES Y DÍAS, SEGÚN CORRESPONDA].

Asimismo, manifiesto mi disposición de ejecutar las actividades que comprenden el desempeño del

²³ En el caso que el postor sea un consorcio se debe consignar el nombre del consorcio o de uno de sus integrantes.

referido cargo, durante el periodo de ejecución del contrato.

[CONSIGNAR CIUDAD Y FECHA]

.....
Firma, Nombres y Apellidos del personal

Importante

- *De conformidad con el literal d) del artículo 52 del Reglamento la carta de compromiso del personal clave, debe contar con la firma legalizada de este.*
- *De presentarse experiencia ejecutada paralelamente (trasape), para el cómputo del tiempo de dicha experiencia sólo se considerará una vez el periodo traslapado.*

ANEXO N° 6

PROMESA DE CONSORCIO

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

Señores

DEPARTAMENTO DE COMPRAS

ADJUDICACIÓN SIMPLIFICADA N° 035-2021-COFIDE TERCERA CONVOCATORIA

Presente.-

Los suscritos declaramos expresamente que hemos convenido en forma irrevocable, durante el lapso que dure el procedimiento de selección, para presentar una oferta conjunta a la **ADJUDICACIÓN SIMPLIFICADA N°** [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] [%]²⁴

[DESCRIBIR LAS OBLIGACIONES DEL CONSORCIADO 1]

2. OBLIGACIONES DE [NOMBRE, DENOMINACIÓN O RAZÓN SOCIAL DEL CONSORCIADO 2] [%]²⁵

[DESCRIBIR LAS OBLIGACIONES DEL CONSORCIADO 2]

TOTAL OBLIGACIONES

100%²⁶

²⁴ Consignar únicamente el porcentaje total de las obligaciones, el cual debe ser expresado en número entero, sin decimales.

²⁵ Consignar únicamente el porcentaje total de las obligaciones, el cual debe ser expresado en número entero, sin decimales.

²⁶ Este porcentaje corresponde a la sumatoria de los porcentajes de las obligaciones de cada uno de los integrantes del consorcio.

[CONSIGNAR CIUDAD Y FECHA]

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

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

Importante

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

ANEXO N° 7

OFERTA ECONÓMICA

Señores

DEPARTAMENTO DE COMPRAS

ADJUDICACIÓN SIMPLIFICADA N° 035-2021-COFIDE TERCERA CONVOCATORIA

Presente.-

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

CONCEPTO	OFERTA ECONÓMICA
TOTAL	

La oferta económica **S/.** 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 de consultoría a contratar; excepto la de aquellos postores que gocen de alguna exoneración legal, no incluirán en su oferta económica 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 monto total de la oferta económica, sin perjuicio, que de resultar favorecido con la buena pro, presente el detalle de precios unitarios y la estructura de costos para el perfeccionamiento del contrato.*
- El postor que goce de alguna exoneración legal, debe indicar que su oferta no incluye el tributo materia de la exoneración, debiendo incluir el siguiente texto:*

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

ANEXO N° 8

DECLARACIÓN JURADA DE CUMPLIMIENTO DE CONDICIONES PARA LA APLICACIÓN DE LA EXONERACIÓN DEL IGV

Señores

DEPARTAMENTO DE COMPRAS

ADJUDICACIÓN SIMPLIFICADA N° 035-2021-COFIDE TERCERA CONVOCATORIA

Presente.-

Mediante el presente el suscrito, postor y/o Representante Legal de [CONSIGNAR EN CASO DE SER PERSONA JURÍDICA], declaro bajo juramento que gozo del beneficio de la exoneración del IGV previsto en la Ley N° 27037, Ley de Promoción de la Inversión en la Amazonía, dado que cumplo con las condiciones siguientes:

- 1.- Que el domicilio fiscal de la empresa²⁷ se encuentra ubicada en la Amazonía y coincide con el lugar establecido como sede central (donde tiene su administración y lleva su contabilidad);
- 2.- Que la empresa se encuentra inscrita en las Oficinas Registrales de la Amazonía (exigible en caso de personas jurídicas);
- 3.- Que, al menos el setenta por ciento (70%) de los activos fijos de la empresa se encuentran en la Amazonía; y
- 4.- Que la empresa no presta servicios fuera de la Amazonía.

[CONSIGNAR CIUDAD Y FECHA]

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

Importante

Cuando se trate de consorcios, esta declaración jurada será presentada por cada uno de los integrantes del consorcio, salvo que se trate de consorcios con contabilidad independiente, en cuyo caso debe ser suscrita por el representante común, debiendo indicar su condición de consorcio con contabilidad independiente y el número de RUC del consorcio.

²⁷ En el artículo 1 del "Reglamento de las Disposiciones Tributarias contenidas en la Ley de Promoción de la Inversión en la Amazonía" se define como "empresa" a las "Personas naturales, sociedades conyugales, sucesiones indivisas y personas consideradas jurídicas por la Ley del Impuesto a la Renta, generadoras de rentas de tercera categoría, ubicadas en la Amazonía. Las sociedades conyugales son aquéllas que ejerzan la opción prevista en el Artículo 16 de la Ley del Impuesto a la Renta."

ANEXO N° 9**DECLARACIÓN JURADA DEL PERSONAL CLAVE PROPUESTO**

Señores

DEPARTAMENTO DE COMPRAS**ADJUDICACIÓN SIMPLIFICADA N° 035-2021-COFIDE TERCERA CONVOCATORIA**

Presente.-

Mediante el presente el suscrito, postor y/o Representante Legal de [CONSIGNAR EN CASO DE SER PERSONA JURÍDICA], declaro bajo juramento que la información del personal clave propuesto es el siguiente:

NOMBRES Y APELLIDOS	DOCUMENTO NACIONAL DE IDENTIDAD U OTRO ANÁLOGO	CARGO	CARRERA PROFESIONAL	N° DE FOLIO EN LA OFERTA	TIEMPO DE EXPERIENCIA ACREDITADA	N° DE FOLIO EN LA OFERTA

[CONSIGNAR CIUDAD Y FECHA]

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

Importante

El postor debe presentar dentro de su oferta la carta de compromiso del personal clave con firma legalizada, según Anexo N° 5.

ANEXO N° 10

EXPERIENCIA DEL POSTOR EN LA ESPECIALIDAD

Señores
DEPARTAMENTO DE COMPRAS
ADJUDICACIÓN SIMPLIFICADA N° 035-2021-COFIDE TERCERA CONVOCATORIA
Presente. -

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

N°	CLIENTE	OBJETO DEL CONTRATO	N° CONTRATO / O/S / COMPROBANTE DE PAGO	FECHA DEL CONTRATO O CP ²⁸	FECHA DE LA CONFORMIDAD DE SER EL CASO ²⁹	EXPERIENCIA PROVENIENTE ³⁰ DE:	MONEDA	IMPORTE ³¹	TIPO DE CAMBIO VENTA ³²	MONTO FACTURADO ACUMULADO ³³
1										
2										
3										
4										

²⁸ 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.

²⁹ Únicamente, cuando la fecha del perfeccionamiento del contrato, sea previa a los diez (10) 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.

³⁰ 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".

³¹ Se refiere al monto del contrato ejecutado incluido adicionales y reducciones, de ser el caso.

³² 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.

³³ 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 ²⁸	FECHA DE LA CONFORMIDAD DE SER EL CASO ²⁹	EXPERIENCIA PROVENIENTE ³⁰ DE:	MONEDA	IMPORTE ³¹	TIPO DE CAMBIO VENTA ³²	MONTO FACTURADO ACUMULADO ³³
5										
6										
7										
8										
9										
10										
...										
20										
TOTAL										

[CONSIGNAR CIUDAD Y FECHA]

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

ANEXO N° 11

**DECLARACIÓN JURADA
(NUMERAL 49.4 DEL ARTÍCULO 49 DEL REGLAMENTO)**

Señores

DEPARTAMENTO DE COMPRAS

ADJUDICACIÓN SIMPLIFICADA N° 035-2021-COFIDE TERCERA CONVOCATORIA

Presente. -

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

[CONSIGNAR CIUDAD Y FECHA]

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

Importante

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

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

ANEXO N° 12

**SOLICITUD DE BONIFICACIÓN DEL DIEZ POR CIENTO (10%) POR SERVICIOS PRESTADOS FUERA DE LA PROVINCIA DE LIMA Y CALLAO
(DE SER EL CASO, SOLO PRESENTAR ESTA SOLICITUD EN EL ÍTEM [CONSIGNAR EL N° DEL ÍTEM O ÍTEMS CUYO VALOR ESTIMADO NO SUPERA LOS DOSCIENTOS MIL SOLES (S/ 200,000.00)])**

Señores

DEPARTAMENTO DE COMPRAS

ADJUDICACIÓN SIMPLIFICADA N° 035-2021-COFIDE TERCERA CONVOCATORIA

Presente. -

Mediante el presente el suscrito, postor y/o Representante Legal de [CONSIGNAR EN CASO DE SER PERSONA JURÍDICA], solicito la asignación de la bonificación del diez por ciento (10%) sobre el puntaje total en [CONSIGNAR EL ÍTEM O ÍTEMS, SEGÚN CORRESPONDA, EN LOS QUE SE SOLICITA LA BONIFICACIÓN] debido a que el domicilio de mi representada se encuentra ubicado en la provincia o provincia colindante donde se ejecuta la prestación.

[CONSIGNAR CIUDAD Y FECHA]

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

Importante

- *Para asignar la bonificación, el órgano encargado de las contrataciones o comité de selección, según corresponda, verifica el domicilio consignado por el postor en el Registro Nacional de Proveedores (RNP).*
- *Para que el postor pueda acceder a la bonificación, debe cumplir con las condiciones establecidas en el literal f) del artículo 50 del Reglamento.*

Importante

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

ANEXO N° 12

SOLICITUD DE BONIFICACIÓN DEL DIEZ POR CIENTO (10%) POR SERVICIOS PRESTADOS FUERA DE LA PROVINCIA DE LIMA Y CALLAO (DE SER EL CASO, SOLO PRESENTAR ESTA SOLICITUD EN EL ÍTEM [INCLUIR EN CASO CORRESPONDA, EN PROCEDIMIENTOS POR RELACIÓN DE ÍTEMS, CONSIGNANDO EL N° DEL ÍTEM O ÍTEMS CUYO VALOR ESTIMADO NO SUPERA LOS DOSCIENTOS MIL SOLES (S/ 200,000.00)])

Señores
DEPARTAMENTO DE COMPRAS
ADJUDICACIÓN SIMPLIFICADA N° 035-2021-COFIDE TERCERA CONVOCATORIA
Presente. -

Mediante el presente el que se suscribe, [.....], representante común del consorcio [CONSIGNAR EL NOMBRE DEL CONSORCIO], solicito la asignación de la bonificación del diez por ciento (10%) sobre el puntaje total en [CONSIGNAR EL ÍTEM O ÍTEMS, SEGÚN CORRESPONDA, EN LOS QUE SE SOLICITA LA BONIFICACIÓN] debido a que los domicilios de todos los integrantes del consorcio se encuentran ubicados en la provincia o provincias colindantes donde se ejecuta la prestación.

[CONSIGNAR CIUDAD Y FECHA]

.....
**Firma, Nombres y Apellidos del representante
común del consorcio**

Importante

- *Para asignar la bonificación, el órgano encargado de las contrataciones o el comité de selección, verifica el domicilio consignado de los integrantes del consorcio, en el Registro Nacional de Proveedores (RNP).*
- *Para que un consorcio pueda acceder a la bonificación, cada uno de sus integrantes*



debe cumplir con las condiciones establecidas en el literal f) del artículo 50 del Reglamento.

ANEXO N° 13

SOLICITUD DE BONIFICACIÓN DEL CINCO POR CIENTO (5%) POR TENER LA CONDICIÓN DE MICRO Y PEQUEÑA EMPRESA

Señores

DEPARTAMENTO DE COMPRAS

ADJUDICACIÓN SIMPLIFICADA N° 035-2021-COFIDE TERCERA CONVOCATORIA

Presente. -

Mediante el presente el suscrito, postor y/o Representante legal de [CONSIGNAR EN CASO DE SER PERSONA JURÍDICA], solicito la asignación de la bonificación del cinco por ciento (5%) sobre el puntaje total obtenido, debido a que mi representada cuenta con la condición de micro y pequeña empresa.

[CONSIGNAR CIUDAD Y FECHA]

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

Importante

- *Para asignar la bonificación, el órgano encargado de las contrataciones o comité de selección, según corresponda, verifica 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/>.*
- *Para que un consorcio pueda acceder a la bonificación, cada uno de sus integrantes debe cumplir con la condición de micro y pequeña empresa.*

ANEXO COFIDE 1

Señores

DEPARTAMENTO DE COMPRAS

ADJUDICACIÓN SIMPLIFICADA N° 035-2021-COFIDE TERCERA CONVOCATORIA

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		
	<i>Añadir las filas que se necesiten</i>			
Nombres y Apellidos de Accionistas, Socios o Asociados con más de 25% de capital social, aporte o participación sea directa o indirectamente.		DNI		
	<i>Añadir las filas que se necesiten</i>			

(*) 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.

Importante

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

ANEXO COFIDE 2

Señores

DEPARTAMENTO DE COMPRAS

ADJUDICACIÓN SIMPLIFICADA N° 035-2021-COFIDE TERCERA CONVOCATORIA

Presente. –

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

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

DECLARO BAJO JURAMENTO: (marcar con un aspa):

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

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

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

Nombres y Apellidos completos:

Documento de Identidad / N°:

Cargo dentro de la empresa:

Fecha:

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

Importante

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

INVESTIGACIONES, ANTECEDENTES JUDICIALES, POLICIALES y/o PENALES

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