"DECENIO DE LA IGUALDAD DE OPORTUNIDADES PARA MUJERES Y HOMBRES"
"AÑO DE LA RECUPERACIÓN Y CONSOLIDACIÓN DE LA ECONOMÍA PERUANA"

BASES INTEGRADAS

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

CONCURSO PÚBLICO Nº CP 0009-2025-BCRPLIM

CONTRATACIÓN DEL SERVICIO DE UN SOC (SECURITY OPERATIONS CENTER) GESTIONADO PARA EL MONITOREO DE EVENTOS DE CIBERSEGURIDAD

Comité de Selección:

- Luis Miguel Venegas Vidaurre — Presidente
- Edgard Aguinaga Mogollón — Miembro
- Josue Asurza Caceres — Miembro Técnico

Firmado digitalmente por: VENEGAS VIDAURRE Luis Miguel Martin FAU 20122476309 soft
Motivo: En señal de conformidad
Fecha: 02/07/2025 11:22:44-0500

Lima, julio de 2025

Firmado digitalmente por: ASURZA CACERES Josue David FAU 20122476309 soft
Motivo: Especialista en Ciberdefensa
Fecha: 02/07/2025 15:55:29-0500

Firmado digitalmente por: AGUINAGA MOGOLLON Edgard Alexander FAU 20122476309 soft
Motivo: En señal de conformidad
Fecha: 02/07/2025 15:39:54-0500

DEBER DE COLABORACIÓN

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

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

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

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

SECCIÓN GENERAL

DISPOSICIONES COMUNES DEL PROCEDIMIENTO DE SELECCIÓN

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

CAPÍTULO I
ETAPAS DEL PROCEDIMIENTO DE SELECCIÓN

1.1. REFERENCIAS

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

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

1.2. CONVOCATORIA

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

1.3. REGISTRO DE PARTICIPANTES

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

Importante

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

1.4. FORMULACIÓN DE CONSULTAS Y OBSERVACIONES A LAS BASES

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

Importante

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

1.5. ABSOLUCIÓN DE CONSULTAS, OBSERVACIONES E INTEGRACIÓN DE BASES

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

Importante

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

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

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

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

Advertencia

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

Importante

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

1.7. FORMA DE PRESENTACIÓN DE OFERTAS

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

Las declaraciones juradas, formatos o formularios previstos en las bases que conforman la oferta deben estar debidamente firmados por el postor (firma manuscrita o digital, según la Ley Nº 27269, Ley de Firmas y Certificados Digitales[1]). Los demás documentos deben ser visados por el postor. En el caso de persona jurídica, por su representante legal, apoderado o mandatario designado para dicho fin y, en el caso de persona natural, por este o su apoderado. No se acepta el pegado de la imagen de una firma o visto. Las ofertas se presentan foliadas.

Importante

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

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

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

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

1.8. PRESENTACIÓN Y APERTURA DE OFERTAS

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

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

Importante

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

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

1.9. EVALUACIÓN DE LAS OFERTAS

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

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

1.10. CALIFICACIÓN DE OFERTAS

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

1.11. SUBSANACIÓN DE LAS OFERTAS

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

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

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

1.12. RECHAZO DE LAS OFERTAS

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

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

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

1.13. OTORGAMIENTO DE LA BUENA PRO

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

1.14. CONSENTIMIENTO DE LA BUENA PRO

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

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

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

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

CAPÍTULO II
SOLUCIÓN DE CONTROVERSIAS DURANTE EL PROCEDIMIENTO DE SELECCIÓN

2.1. RECURSO DE APELACIÓN

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

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

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

Importante

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

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

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

- *El recurso de apelación se presenta ante la Mesa de Partes del Tribunal o ante las oficinas desconcentradas del OSCE.*

2.2. PLAZOS DE INTERPOSICIÓN DEL RECURSO DE APELACIÓN

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

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

CAPÍTULO III
DEL CONTRATO

3.1. PERFECCIONAMIENTO DEL CONTRATO

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

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

3.2. GARANTÍAS

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

3.2.1. GARANTÍA DE FIEL CUMPLIMIENTO

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

3.2.2. GARANTÍA DE FIEL CUMPLIMIENTO POR PRESTACIONES ACCESORIAS

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

Importante

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

- *En los contratos periódicos de prestación de servicios en general que celebren las Entidades con las micro y pequeñas empresas, estas últimas pueden otorgar como garantía de fiel cumplimiento el diez por ciento (10%) del monto del contrato, porcentaje que es retenido por la Entidad durante la primera mitad del número total de pagos a realizarse, de forma prorrateada en cada pago, con cargo a ser devuelto a la finalización del mismo, conforme lo establecen los numerales 149.4 y 149.5 del artículo 149 del Reglamento y numeral 151.2 del artículo 151 del Reglamento.*

3.2.3. GARANTÍA POR ADELANTO

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

3.3. REQUISITOS DE LAS GARANTÍAS

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

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

Advertencia
Los funcionarios de las Entidades no deben aceptar garantías emitidas bajo condiciones distintas a las establecidas en el presente numeral, debiendo tener en cuenta lo siguiente: *1. La clasificadora de riesgo que asigna la clasificación a la empresa que emite la garantía debe encontrarse listada en el portal web de la SBS (http://www.sbs.gob.pe/sistema-financiero/clasificadoras-de-riesgo).* *2. Se debe identificar en la página web de la clasificadora de riesgo respectiva, cuál es la clasificación vigente de la empresa que emite la garantía, considerando la vigencia a la fecha de emisión de la garantía.* *3. Para fines de lo establecido en el artículo 148 del Reglamento, la clasificación de riesgo B, incluye las clasificaciones B+ y B.* *4. Si la empresa que otorga la garantía cuenta con más de una clasificación de riesgo emitida por distintas empresas listadas en el portal web de la SBS, bastará que en una de ellas cumpla con la clasificación mínima establecida en el Reglamento.* *En caso exista alguna duda sobre la clasificación de riesgo asignada a la empresa emisora de la garantía, se deberá consultar a la clasificadora de riesgos respectiva.* *De otro lado, además de cumplir con el requisito referido a la clasificación de riesgo, a efectos de verificar si la empresa emisora se encuentra autorizada por la SBS para emitir garantías, debe revisarse el portal web de dicha Entidad (http://www.sbs.gob.pe/sistema-financiero/relacion-de-empresas-que-se-encuentran-autorizadas-a-emitir-cartas-fianza).* *Los funcionarios competentes deben verificar la autenticidad de la garantía a través de los mecanismos establecidos (consulta web, teléfono u otros) por la empresa emisora.*

3.4. EJECUCIÓN DE GARANTÍAS

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

3.5. ADELANTOS

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

3.6. PENALIDADES

3.6.1. PENALIDAD POR MORA EN LA EJECUCIÓN DE LA PRESTACIÓN

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

3.6.2. OTRAS PENALIDADES

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

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

3.7. INCUMPLIMIENTO DEL CONTRATO

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

3.8. PAGOS

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

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

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

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

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

3.9. DISPOSICIONES FINALES

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

SECCIÓN ESPECÍFICA

CONDICIONES ESPECIALES DEL PROCEDIMIENTO DE SELECCIÓN

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

CAPÍTULO I
GENERALIDADES

1.1. ENTIDAD CONVOCANTE

Nombre	:	Banco Central de Reserva del Perú (BCRP)
RUC Nº	:	20122476309
Domicilio legal	:	Jirón Santa Rosa 441 – 445, Lima
Teléfono:	:	6132000
Correo electrónico:	:	compras@bcrp.gob.pe

1.2. OBJETO DE LA CONVOCATORIA

El presente procedimiento de selección tiene por objeto la CONTRATACIÓN DEL SERVICIO DE UN SOC (SECURITY OPERATIONS CENTER) GESTIONADO PARA EL MONITOREO DE EVENTOS DE CIBERSEGURIDAD

1.3. EXPEDIENTE DE CONTRATACIÓN

El expediente de contratación fue aprobado por la Gerencia de Compras y Servicios mediante Memorando N° 0111-2025-ADM000-N de fecha 21 de abril de 2025.

1.4. FUENTE DE FINANCIAMIENTO

Recursos propios.

1.5. SISTEMA DE CONTRATACIÓN

El presente procedimiento se rige por el sistema de Esquema Mixto de suma alzada y precios unitarios 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

Los servicios materia de la presente convocatoria se prestarán en los siguientes plazos en concordancia con lo establecido en el expediente de contratación:

Prestación principal

Descripción	Plazo
Implementación del servicio SOC Gestionado	Fase 1: Noventa (90) días calendarios contabilizados desde el día siguiente de la firma del contrato. Fase 2: Sesenta (60) días calendarios, comenzando a los 396 días calendarios (13 meses) de iniciada la ejecución de la Fase 1.

Descripción	Plazo
Ejecución del Servicio SOC Gestionado	Fase 1: El plazo de ejecución de esta fase será de 456 días calendarios (15 meses) contabilizados desde el día siguiente de terminada la implementación de la fase 1. Fase 2: El plazo de ejecución de esta fase será de 273 días calendarios (9 meses) contabilizados desde el día siguiente de terminada la implementación de la fase 2.

Prestación accesoria

Descripción	Plazo
Servicio de mantenimiento preventivo, mesa de ayuda y soporte técnico local 24x7x365	Fase 1: 456 días calendario (15 meses) contabilizados desde el día siguiente de terminada la implementación de la fase 1. Fase 2: 273 días calendarios (9 meses) contabilizados desde el día siguiente de terminada la implementación de la fase 2. Respecto al servicio de mantenimiento preventivo para ambas fases se programará con una periodicidad de por lo menos una (01) vez de forma semestral.

Descripción	Plazo
Ejecución de una Capacitación (de acuerdo con lo establecido en el numeral 3.17.	Noventa (90) días a partir del día siguiente del acta final de conformidad de implementación de la Fase 1.

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 s/ 5,00 (CINCO Y 00/100 soles) en el Departamento de Caja del Banco Central de Reserva del Perú. Las Bases serán entregadas en el Departamento de Trámite Documentario para lo cual deberán presentar el comprobante del pago efectuado.

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

1.9. BASE LEGAL

- Ley de Contrataciones del Estado y su Reglamento.
- Constitución Política del Perú
- Decreto Ley N° 26123, Ley Orgánica del BCRP.
- Estatuto del BCRP.
- Acuerdo de Directorio de fecha 19 de diciembre de 2024, que aprueba el uso de las Bases Estándar y Solicitud de Expresión de Interés Estándar.
- Ley N° 32185, Ley de Presupuesto del Sector Público para el Año Fiscal 2025, en lo que resulte aplicable para el BCRP.
- Ley N° 32186, Ley de Equilibrio Financiero del Presupuesto del Sector Público del año fiscal

2025, en lo que resulte aplicable para el BCRP.
- Ley N° 27444, Ley del Procedimiento Administrativo General.
- Ley Nº 27806, Ley de Transparencia y de Acceso a la Información Pública.
- Ley Nº 28015, Ley de Promoción y Formalización de la Pequeña y Microempresa.

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

CAPÍTULO II
DEL PROCEDIMIENTO DE SELECCIÓN

2.1. CALENDARIO DEL PROCEDIMIENTO DE SELECCIÓN

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

2.2. CONTENIDO DE LAS OFERTAS

NOTA IMPORTANTE:

De acuerdo con lo indicado en el numeral 1.7 de la Sección General de las presentes Bases, las declaraciones juradas, formatos o formularios previstos en las bases que conforman la oferta deben estar debidamente firmados por el postor (firma manuscrita o digital, según la Ley Nº 27269, Ley de Firmas y Certificados Digitales[2]). 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.

La oferta contendrá, además de un índice de documentos3, la siguiente documentación:

2.2.1. Documentación de presentación obligatoria

2.2.1.1. Documentos para la admisión de la oferta

a) Declaración jurada de datos del postor. (**Anexo Nº 1)**

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

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

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

En caso de postores no domiciliados se podrá presentar el documento equivalente en su país de origen.

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

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

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

Plataforma de Interoperabilidad del Estado – PIDE[4] y siempre que el servicio web se encuentre activo en el Catálogo de Servicios de dicha plataforma, no corresponderá exigir el certificado de vigencia de poder y/o documento nacional de identidad.

c) Declaración jurada de acuerdo con el literal b) del artículo 52 del Reglamento. **(Anexo Nº 2)**

d) Declaración jurada de cumplimiento de los Términos de Referencia contenidos en el numeral 3.1 del Capítulo III de la presente sección. (**Anexo Nº 3**)

e) Documentación técnica y/o carta del fabricante de la solución SIEM empleada que sustente el cumplimiento de las características mencionadas en los literales c, d, e, f del numeral 3.1.1 de los términos de referencia. Se aceptarán folletos, brochure, catálogo, documentación técnica, datasheet u otro documento de carácter técnico del fabricante. Dicha información técnica complementaria puede ser presentada en el idioma original o inglés o español.

f) Declaración jurada de plazo de prestación del servicio. **(Anexo Nº 4)**[5]

g) Promesa de consorcio con firmas legalizadas, de ser el caso, en la que se consigne los integrantes, el representante común, el domicilio común y las obligaciones a las que se compromete cada uno de los integrantes del consorcio así como el porcentaje equivalente a dichas obligaciones. (**Anexo Nº 5**)

h) El precio de la oferta en Soles. Adjuntar obligatoriamente el **Anexo Nº 6.**

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

Importante

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

2.2.1.2. Documentos para acreditar los requisitos de calificación

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

Advertencia

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

2.3. REQUISITOS PARA PERFECCIONAR EL CONTRATO

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

[4] 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/

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

a) Garantía de fiel cumplimiento del contrato.
b) Garantía de fiel cumplimiento por prestaciones accesorias.
c) Contrato de consorcio con firmas legalizadas ante Notario de cada uno de los integrantes de ser el caso.
d) Código de cuenta interbancaria (CCI) o, en el caso de proveedores no domiciliados, el número de su cuenta bancaria y la entidad bancaria en el exterior.
e) Copia de la vigencia del poder del representante legal de la empresa que acredite que cuenta con facultades para perfeccionar el contrato, cuando corresponda. En caso de postores no domiciliados se podrá presentar el documento equivalente en su país de origen.
f) Copia de DNI del postor en caso de persona natural, o de su representante legal en caso de persona jurídica. En caso de postores no domiciliados podrá presentar el pasaporte o documento de identidad de su país de origen. Se puede presentar también carné de extranjería.

Advertencia

De acuerdo con el artículo 4 del Decreto Legislativo N° 1246, las Entidades están prohibidas de exigir a los administrados o usuarios la información que puedan obtener directamente mediante la interoperabilidad a que se refieren los artículos 2 y 3 de dicho Decreto Legislativo. En esa medida, si la Entidad es usuaria de la Plataforma de Interoperabilidad del Estado – PIDE[6] y siempre que el servicio web se encuentre activo en el Catálogo de Servicios de dicha plataforma, no corresponderá exigir los documentos previstos en los literales e) y f).

g) Domicilio para efectos de la notificación durante la ejecución del contrato.
h) Autorización de notificación de la decisión de la Entidad sobre la solicitud de ampliación de plazo mediante medios electrónicos de comunicación [7] (**Anexo N° 9**).
i) Detalle de los precios unitarios del precio ofertado[8].
j) Copia simple de la certificación ISO 27001; ISO20000 y/o ISO9001; SIM3 2022 y/o SOC II tipo 2 emitida a nombre de la empresa, vigente y relacionada a algunas de las actividades o alcances señaladas en el numeral 3.8.3 de los términos de referencia.
k) Copia simple de las certificaciones requeridas para el personal clave según lo indicado en el numeral 3.11 de los términos de referencia.
l) Relación del personal clave. Esta relación deberá incluir como mínimo la siguiente información: nombres, apellidos, tipo y número de documento de identidad y el cargo que va a ocupar.
m) Copia de certificación internacional ISO 27001; ISO 20000 y/o ISO9001 del proveedor para el caso de plataformas ofertadas On-premise y/o en la nube del Security Service Provider ó certificaciones tales como SIM3 2022 o SOC II tipo 2 para el caso de soluciones SaaS, a fin de acreditar el requerimiento del numeral 3.1.3 de los términos de referencia.

Importante

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

- *En los contratos periódicos de prestación de servicios en general que celebren las Entidades con las micro y pequeñas empresas, estas últimas pueden otorgar como garantía de fiel cumplimiento el diez por ciento (10%) del monto del contrato, porcentaje que es retenido por la Entidad durante la primera mitad del número total de pagos a realizarse, de forma*

[6] Para mayor información de las Entidades usuarias de la Plataforma de Interoperabilidad del Estado – PIDE ingresar al siguiente enlace https://www.gobiernodigital.gob.pe/interoperabilidad/

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

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

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

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

Importante

- *Corresponde a la Entidad verificar que las garantías presentadas por el postor ganador de la buena pro cumplan con los requisitos y condiciones necesarios para su aceptación y eventual ejecución, sin perjuicio de la determinación de las responsabilidades funcionales que correspondan.*
- *De conformidad con el Reglamento Consular del Perú aprobado mediante Decreto Supremo N° 076-2005-RE para que los documentos públicos y privados extendidos en el exterior tengan validez en el Perú, deben estar legalizados por los funcionarios consulares peruanos y refrendados por el Ministerio de Relaciones Exteriores del Perú, salvo que se trate de documentos públicos emitidos en países que formen parte del Convenio de la Apostilla, en cuyo caso bastará con que estos cuenten con la Apostilla de la Haya[9].*
- *La Entidad no puede exigir documentación o información adicional a la consignada en el presente numeral para el perfeccionamiento del contrato.*

2.4. PERFECCIONAMIENTO DEL CONTRATO

El contrato se perfecciona con la suscripción del documento que lo contiene. Para dicho efecto el postor ganador de la buena pro, dentro del plazo previsto en el artículo 141 del Reglamento, debe presentar la documentación requerida en el Departamento de Compras del BCRP, primer piso de la Oficina Principal; jirón Santa Rosa 441 – 445, Lima.

Importante

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

2.5. FORMA DE PAGO

La Entidad realizará el pago de la contraprestación pactada a favor del contratista de acuerdo con el siguiente detalle:

Prestación principal

✓ Costos fijos
No incluyen las horas de respuesta a incidentes, adicionales a la bolsa de doce (12) horas mensuales.

Descripción	Fase	Forma de pago

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

Implementación del servicio	Fase 1	Único pago, equivalente al 4%, del monto total correspondiente a los costos fijos de la fase 1 de la prestación principal. NOTA: El pago será realizado una vez culminado la implementación.
	Fase 2	Único pago, equivalente al 4.06%, del monto total correspondiente a los costos fijos de la fase 2 de la prestación principal. NOTA: El pago será realizado una vez culminado la implementación.
Ejecución del servicio	Fase 1	En forma mensual, en 15 pagos equivalentes al 6.4% del monto total correspondiente a los costos fijos de la fase 1 de la prestación principal.
	Fase 2	En forma mensual, en 9 pagos equivalentes al 10.66% del monto total correspondiente a los costos fijos de la fase 2 de la prestación principal.

✓ Costo variable

	Descripción	**Forma de pago**
Fase 1	Horas de respuesta a incidentes, adicionales a la bolsa de doce (12) horas mensuales contratadas. Bolsa estimada de 12* horas. Nota: *No es un tope de consumo de horas y tampoco un consumo fijo, sino es una cantidad estimada adicional para toda la fase 1. Este excedente a las horas contratadas sirve para fines de cálculo para el monto total de la fase 1.	En forma mensual, según informe de sustento de incremento de horas aprobado por el BCRP.
	Incremento de EPS a los 5000 contratados, según consumo. Bolsa estimada de 1000* EPS adicionales. Nota: *No es un tope de consumo de EPS y tampoco un consumo fijo, sino es una cantidad estimada adicional para toda la fase 1, este excedente a los EPS contratados sirve para fines de cálculo para el monto total de la fase 1.	En forma mensual, según informe de sustento de incremento de EPS aprobado por el BCRP.
Fase 2	Horas de respuesta a incidentes, adicionales a la bolsa de doce (12) horas mensuales contratadas. Bolsa estimada de 12* horas. Nota: *No es un tope de consumo de horas y tampoco un consumo fijo, sino es una cantidad estimada adicional para toda la fase 2, este excedente a las horas contratadas sirve para fines de cálculo para el monto total de la fase 2.	En forma mensual, según informe de sustento de incremento de horas aprobado por el BCRP
	Incremento de EPS a los 10000 contratados, según consumo. Bolsa estimada de 1000* EPS adicionales. Nota: *No es un tope de consumo de EPS y tampoco un	En forma mensual, según informe de sustento de incremento de EPS aprobado por el BCRP.

	consumo fijo, sino es una cantidad estimada adicional para toda la fase 2, este excedente a los EPS contratados sirve para fines de cálculo para el monto total de la fase 2.	

NOTA: El informe de sustento se refiere al informe técnico mensual mencionado en el numeral 3.10 de los términos de referencia en el que se detallará el incremento de horas y EPS.

Prestación accesoria

Descripción	Fase	Forma de pago
Servicio de mantenimiento preventivo, mesa de ayuda y soporte técnico local 24 x 7 x 365	Fase 1	En forma mensual, en 15 pagos iguales correspondiente al monto de este servicio de la prestación accesoria de la fase 1.
	Fase 2	En forma mensual, en 9 pagos iguales correspondiente al concepto de este servicio de la prestación accesoria de la fase 2.
Capacitación	Fase 1	El 100% del monto correspondiente a este concepto a la conformidad de su realización.

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

- Informe del funcionario responsable del Departamento de Ciberdefensa emitiendo la conformidad de la prestación efectuada.
- Comprobante de pago.

Dicha documentación se debe presentar en formato pdf, xml y cdr, al correo electrónico recepcioncomprobanteselectronicos@bcrp.gob.pe. Los comprobantes deberán estar acompañados de la Guía de Remsión (pdf), de ser el caso, y deberán hacer referencia al número de contrato o, en su defecto acompañar la primera página del mismo en formato pdf.

CAPÍTULO III
REQUERIMIENTO

3.1. TERMINOS DE REFERENCIA

1. Objetivo

La contratación del servicio de un SOC (Security Operation Center) Gestionado para el monitoreo de eventos de Ciberseguridad para el Banco Central de Reserva del Perú. Dicho servicio brindará la monitorización, detección, alertas, y contención que permitan responder a los distintos tipos de amenazas, vectores de ataque e intrusiones a los que se encuentran expuestos los principales servicios y aplicaciones del BCRP, según los plazos indicados:

Prestación principal

Descripción	Plazo
Implementación del servicio SOC Gestionado	Fase 1: Noventa (90) días calendarios contabilizados desde el día siguiente de la firma del contrato. Fase 2: Sesenta (60) días calendarios, comenzando a los 396 días calendarios (13 meses) de iniciada la ejecución de la Fase 1.

Descripción	Plazo
Ejecución del Servicio SOC Gestionado	Fase 1: El plazo de ejecución de esta fase será de 456 días calendarios (15 meses) contabilizados desde el día siguiente de terminada la implementación de la fase 1. Fase 2: El plazo de ejecución de esta fase será de 273 días calendarios (9 meses) contabilizados desde el día siguiente de terminada la implementación de la fase 2.

- **Prestación accesoria**

Descripción	Plazo
Servicio de mantenimiento preventivo, mesa de ayuda y soporte técnico local 24x7x365	Fase 1: 456 días calendario (15 meses) contabilizados desde el día siguiente de terminada la implementación de la fase 1. Fase 2: 273 días calendarios (9 meses) contabilizados desde el día siguiente de terminada la implementación de la fase 2. Respecto al servicio de mantenimiento preventivo para ambas fases se programará con una periodicidad de por lo menos una (01) vez de forma semestral.

Descripción	Plazo
Ejecución de una Capacitación (de acuerdo con lo establecido en el numeral 3.17.	Noventa (90) días a partir del día siguiente del acta final de conformidad de implementación de la Fase 1.

2. Estructura del Servicio

La ejecución del servicio se estructura en 2 fases y abarca 5 Data Centers.

Nombre	Descripción	Dirección
Data Center 1	Ubicado en la OP del BCRP	Jr. Santa Rosa 441
Data Center 2	Ubicado en el local del Reserclub del BCRP	Cl. Diego de Medina 295, Pueblo Libre
Data Center 3	Ubicado en el local de la sucursal Piura	
Data Center 4	Ubicado en el local de Jr. Carabaya	Jr. Carabaya 698
Data Center 5	Ubicado en el local del Reserclub del BCRP	Cl. Diego de Medina 295, Pueblo Libre

Nota: Se precisa que para trabajos de implementación y atención de soporte a la infraestructura puesta para el servicio SOC en el Data Center 3 serán con conexión remota.

NOTA: Para el caso de la implementación de los colectores (in situ), estos serán instalados en los Data Centers 1, 2, 4 y 5; precisando que se instalará un (01) colector como mínimo.

Fases del Servicio:

Nombre	Descripción	Alcance EPS	Duración
Fase 1 (Ejecución)	Contempla el monitoreo de 60 Data Sources ubicados en el Datacenter Principal, CER Pueblo Libre y CER-Piura.	Hasta 5000 EPS	456 días calendarios (15 meses) contabilizados desde el día siguiente de terminada la implementación de la fase 1.
Fase 2 (Ejecución)	Contempla el monitoreo de 159 Data Sources, 60 ubicados en el Datacenter Principal, CER-Pueblo Libre y CER-Piura; y 99 Ubicados en los dos nuevos Datacenters que soportarán la nueva plataforma de pagos minoristas.	Hasta 10000 EPS	273 días calendarios (9 meses) contabilizados desde el día siguiente de terminada la implementación de la fase 2.

3. Condiciones generales

El BCRP requiere contratar el servicio de monitoreo, detección y respuesta ante amenazas de seguridad (SOC Gestionado) y ciber inteligencia de forma continua (24x7x365) para proteger los activos de la infraestructura tecnológica existente del BCRP.

A continuación, se detallan cada uno de los requerimientos mínimos, de capacidad operacional, de recursos tecnológicos y de personal.

3.1. Requerimientos del Servicio SOC Gestionado (Fases 1 y 2)

3.1.1. El servicio SOC hará uso de una solución SIEM, la misma que deberá contar con las siguientes características:

a. Deberá permitir ingesta de datos locales y nube.
b. Correlacionar actividades para priorización de incidentes.
c. Contar con múltiples modalidades de integración de Datasources (por ejemplo, Syslog, API, entre otras), permitiendo incluso desarrollar integraciones no nativas.
Se entiende por integración no nativa al caso en que el Datasource no cuenta con plantillas de integración ya incluidas en la propia solución SIEM.
d. Contar con funcionalidades User Behavior Analysis o User and Entity Behavior Analytics.
NOTA: Estas funcionalidades deberán estar activadas y operativas durante todo el periodo del servicio para capacidades como por ejemplo desarrollo, monitoreo y creación de casos de uso, detección de amenazas internas (Insider Threats), análisis contextual de eventos, reducción de falsos positivos, entre otras.
e. Emplear tecnologías de AI (Artificial Intelligence) y/o ML (Machine Learning) para procesos relacionados con la detección y modelamiento de amenazas.
f. Una Interface web con acceso a la plataforma que permita ejecutar tareas de Monitoreo, Detección, Investigación y Gestión de Incidentes proporcionando distintas capas de visibilidad y acceso a los eventos crudos, eventos o atributos base, eventos enriquecidos, anomalía y detecciones de manera detallada y con apoyos gráficos y drill-down de los detalles en el modelo de detección. Se precisa que el acceso será a través de una URL con https.

Nota:

Se deberá presentar documentación técnica y/o carta del fabricante de la solución SIEM empleada, que sustente el cumplimiento de cada una de las características mencionadas en los literales c, d, e, f. Dicho(s) documento(s) será(n) parte de la documentación de presentación obligatoria que los postores deberán incluir en sus ofertas.

Se aceptarán folletos, brochure, catálogo, documentación técnica, datasheet u otro documento de carácter técnico del fabricante. Dicha información técnica complementaria puede ser presentada en el idioma original o inglés o español.

3.1.2. Deberá tener implementada una plataforma gráfica en la nube y con acceso de MFA para interactuar en tiempo real con la información que es trabajada por el SIEM y por la capa de investigación. Esta plataforma debe incluir un número suficiente de dashboards que permita, como mínimo, disponer de las siguientes vistas:

- Top de IoC dando información como mínimo de IP, dominio y/o HASH maliciosos asociados al BCRP.
- Top de exploits asociados a activos que dispone el BCRP.

NOTA: Se precisa que los eventos de tipo Exploit Detection serán brindados por los data sources integrados al servicio SOC Gestionado.

Respecto a este dashboard, es sobre la infraestructura de seguridad informática, y de servicios y aplicaciones Web y puede ser mostrado en la plataforma SIEM que cumpla con los requisitos de este numeral.

- Detalle de hallazgos de alertas de phishing, smishing, vishing y/o pharming entre otras.
  NOTA: El detalle de hallazgos de alertas de phishing, smishing, vishing y/o pharming entre otras, dependerán si los casos de uso implementados en la plataforma en coordinación con el Banco cubren los tipos de casos de uso indicados.
- Estado de los Colectores y Data Sources.
- Tipos de alertas clasificadas.
- Estado de las investigaciones, permitiendo interactuar a través de un chat en la interfaz con un especialista para la resolución del mismo.

  NOTA: El término "chat" se referencia como un canal de registro en tiempo real, que permita documentar de forma inmediata y continua las interacciones entre el BCRP y el equipo de investigación del SOC, dentro del mismo entorno operativo, garantizando su trazabilidad, control y evidencia oportuna en las decisiones y acciones durante el ciclo de vida de una investigación.

Se precisa que para el estado de los colectores y datasources se espera visualizar que estos se encuentran correctamente conectados con la plataforma SIEM.

NOTA: Se precisa que, siempre que la solución SIEM ofertada permita cumplir de forma integral y nativa con todas las funcionalidades descritas en el numeral 3.1.2, la implementación de una plataforma gráfica adicional en la nube no será necesaria.

3.1.3. Deberá contar con acreditación de cumplimiento de:

- Manejo y almacenamiento de la información cumpliendo los principios de confidencialidad, disponibilidad, integridad y privacidad en el procesamiento, de forma que se garantice que los controles de seguridad empleados fueron diseñados apropiadamente, así como la efectividad operacional de dichos controles de seguridad.
- Normativas de gestión de seguridad de la información y de gestión de la continuidad del negocio en los procesos de investigación forense y/o ciber inteligencia y operación de SOC y/o monitoreo de seguridad.

Notas:

a. Este requerimiento debe ser acreditado mediante la certificación internacional ISO 27001 así como la certificación ISO 20000 o ISO9001 del proveedor, ya sea plataforma On-premise y/o en la nube. Para el caso de soluciones SaaS, adicionalmente deberá presentar certificaciones tales como SIM3 2022 o SOC II tipo 2.
   NOTA: Para el caso que el proveedor presente una arquitectura solo On-Premise, deberá presentar obligatoriamente dos (02) certificaciones: ISO 27001; ISO20000 y/o ISO9001.
b. En caso de que el servicio sea gestionado por un SSP (Security Service Provider), la acreditación de cumplimiento de las certificaciones SIM3 2022 o SOC II tipo 2 deberá realizarse sobre el servicio brindado por dicho SSP.

3.1.4. Contar con una capa de investigación, conformado por personal certificado en SIEM, que reciba y analice la información procesada por el motor de IA de la solución, y con base en patrones y playbooks correspondientes de amenazas avanzadas, se pueda determinar con precisión amenazas que constituyan un impacto a la organización.
NOTA: Se precisa que el termino playbooks indicado en este numeral son aquellos desarrollados por el propio personal del SOC y hacen referencia a un conjunto estructurado de procedimientos, guías técnicas operativas, que no corresponden a los playbooks automatizados de una plataforma SOAR.

3.1.5. Contar con un CSIRT (Computer Security Incident Response Team) que ejecute actividades de:

- Alertamiento Oportuno ante posibles incidentes de seguridad, que pudieran tener impacto negativo en la infraestructura tecnológica del BCRP.
- Generación de recomendaciones aplicables por el BCRP y asesoría de mitigación de incidentes puntuales o de gran escala.
- Respuesta avanzada a incidentes de seguridad que se hayan materializado, de acuerdo

con una bolsa de horas definida en el numeral 3.7.5, utilizando herramientas y playbooks alineados al estándar NIST SP 800-61.

NOTA: El CSIRT realizará la investigación con sus expertos acreditados, analizando los activos informáticos afectados con una diversidad de herramientas especializadas; y, planteará las acciones de mitigación, contención o remediación recomendadas correspondientes, precisando entre ellas la evaluación de riesgos, estrategias a seguir. Resultado de las recomendaciones del proveedor, están serán evaluadas conjuntamente con el Banco para su aplicación.

La respuesta avanzada a incidentes podrá ser activada en los siguientes casos:

- Por una ocurrencia en el site de BCRP
- A solicitud sustentada del equipo de ciberdefensa de BCRP
- Alerta preventiva en el sistema de correlación - BCRP
- Acciones de iniciativa propia del Contratista (ej..: durante el análisis de riesgo)

El CSIRT atenderá incidentes causados por ataques, comportamiento malicioso, malware o ransomware. Asimismo, realizará la investigación con sus expertos acreditados, analizando los activos informáticos afectados con una diversidad de herramientas especializadas; y, planteará las acciones de mitigación, contención o remediación recomendadas correspondientes.

3.1.6. El SOC deberá gestionarse según métricas como: tiempo de detección, tasa de respuesta de falsos positivos, número de incidentes detectados, cumplimiento de SLAs, análisis de tendencias, entre otras. debiendo especificar la clasificación de incidentes según criticidad.

3.1.7. El SOC deberá contar con infraestructura redundante que le permita brindar sus servicios con una disponibilidad mensual no menor al 99.95%.

Nota:

El numeral 3.8.2 de los términos de referencia brinda la posibilidad de que el proveedor haga uso de suscripciones, contratadas para el BCRP, a servicios brindados por un SSP (Security Service Provider). En dicho caso la disponibilidad mensual corresponde al servicio brindado por dicho SSP no debiendo ser menor al 99.95%.

3.1.8. En el caso de incluir soluciones de tipo SaaS dentro de los servicios brindados, se deberá cumplir con los lineamientos para uso de servicios en nube. La información deberá obligatoriamente ser almacenada (en reposo) y transmitida (en tránsito), en forma cifrada, garantizando la confidencialidad de la misma.

3.1.9. El servicio deberá brindarse en idioma español; permitiéndose que la información técnica incluida reportes e informes, sea brindada en idioma inglés.

3.1.10. Niveles de Acuerdo de Servicio:

Los niveles de acuerdo de servicio establecidos tienen por finalidad asegurar la calidad en la ejecución del servicio. Para tal efecto, se establecerá los tiempos medios de detección que el contratista deberá cumplir como parte del servicio. El SOC deberá brindar SLAs de atención de alertas y tickets de al menos 99,95%, de acuerdo con las siguientes especificaciones:

<u>Niveles de impacto</u>

Se consideran los niveles de impacto según la afectación en el negocio, ya sea en los objetivos, finanzas o reputación.

<u>Máximo Tiempo de Respuesta Inicial (MTRI)</u>

Es el máximo tiempo transcurrido en tiempo real entre la detección del evento anómalo, la notificación y la investigación de la alerta reportada.

Nivel	Impacto	Descripción	Peso	MTRI

1	Crítico	Impacto confirmado o inminente	4	30 minutos
2	Alto	Impacto altamente probable o significativo	3	1 hora
3	Medio	Impacto medianamente probable o de mediano alcance	2	6 horas
4	Bajo	Impacto bajamente probable o de reducido alcance	1	24 horas

NI =NI = Nivel de impacto

$$\text{SLA del NI} = \frac{(\text{Número de Incidentes del NI atendidos dentro del MTRI}) * 100\%}{\text{Total de incidentes del NI}}$$

$$\text{SLA mensual} = \sum (\text{SLA del NI}) * (\text{Peso del NI}) / \sum \text{Pesos}$$

Máximo Tiempo de Resolución de Requerimientos (MTRR)

Tiempo máximo permitido para completar un requerimiento o ticket de servicio desde que se registra hasta que se entrega al cliente.

Se precisa que se debe aplicar estos tiempos para la resolución de un requerimiento o aplicación de un workaround. De ser un caso excepcional el proveedor deberá presentar la solicitud de excepción con sustento para revisión y aprobación por el banco.

Nivel	**Prioridad**	**Descripción**	**Peso**	**MTRR**
1	Alto	Relevancia alta para el servicio. Por ejemplo: Falla de ingesta de logs, mal funcionamiento o caída de sensores, desincronización de feeds de inteligencia, entre otros.	3	4 horas
2	Medio	Relevancia media o de mediano alcance para el servicio. Por ejemplo: Creación u optimización de Casos de Uso, implementación de nuevas integraciones con fuentes de logs, revisión y mejora de informes, entre otros.	2	2 días hábiles
3	Bajo	Relevancia baja o de reducido alcance para el servicio. Por ejemplo: Depuración de casos de uso obsoletos, revisión y actualización de dashboards, configuraciones de la plataforma SOC, entre otros.	1	5 días hábiles

NP = Nivel de priorida

NP = Nivel de Prioridad

$$\text{SLA del NP} = \frac{(\text{Número de Incidentes del NP atendidos dentro del MTRR}) * 100\%}{\text{Total de incidentes del NP}}$$

$$\text{SLA mensual} = \sum (\text{SLA del NP}) * (\text{Peso del NP}) / \sum \text{Pesos}$$

Las atenciones de averías deberán estar disponibles sin límite de horas por intervención, ni cantidad de intervenciones mensuales, dándose por atendido una avería cuando es solucionado en su totalidad y a satisfacción del BCRP.

Para las remediaciones, de ser el caso, el BCRP proporcionará las facilidades necesarias para realizar los trabajos de manera presencial dentro de sus instalaciones o virtualmente inclusive fuera de horarios laborales.

Cada vez que ocurra un incidente de seguridad y/o una avería en la plataforma o servicio implementado, y finaliza la atención de esta a satisfacción del BCRP, el contratista deberá entregar un informe técnico detallado en documento físico o electrónico. El informe se entregará en un plazo no mayor de cinco (05) días calendario, luego de finalizada la atención de la avería. Dicho informe deberá contener como mínimo lo siguientes puntos:

- Causa Raíz
- Tratamiento
- Tiempos de resolución
- Oportunidades de mejora

NOTA: Se precisa que el CSIRT no dispone de un SLAs de tiempo de resolución especifico, debido a la naturaleza impredecible y compleja de los incidentes de ciberseguridad. Sin embargo, el proveedor debe cumplir en mantener un seguimiento continuo y priorización del incidente hasta su cierre, informando al Banco los avances al menos cada 2 horas para incidentes críticos y cada 4 horas para los de alta severidad, manteniendo trazabilidad de acciones en la plataforma del SOC Gestionado.

3.1.11. Deberá presentar mensualmente un informe Gerencial con información y métricas de los principales Eventos y Amenazas detectadas que incluya como mínimo el ranking de países atacantes, objetivos atacados, IPs atacantes, remitentes de correos maliciosos, destinatarios de correos maliciosos, y las acciones tomadas ante ellos. Adicionalmente el informe gerencial debe incluir información relevante de inteligencia de amenazas.
NOTA: El mismo puede ser entregado en formato digital con firma electrónica avanzada. La presentación del informe gerencial debe ser en modalidad presencial.

3.2. Monitoreo a través de Correlación de Eventos de Seguridad

Como parte del servicio de SOC, el proveedor deberá incluir una solución SIEM, a través de, como mínimo, un contenedor o Tenant exclusivo para uso del BCRP (no ser compartido con otros clientes).
NOTA: Se precisa que el termino contenedor hace referencia a una "instancia" aislada del SIEM y no hace referencia al colector o collector.
El proveedor deberá cubrir todos los gastos de licencias, suscripciones, cómputo, infraestructura y demás que se requiera para que el servicio se integre y recolecte los eventos de todos los orígenes que el BCRP decida integrar de la infraestructura preexistente.
Esta solución SIEM, que es parte del servicio SOC, deberá cumplir con los siguientes requisitos:

3.2.1. Deberá proveer una visibilidad integral sobre los eventos de seguridad informática en tiempo real que almacena y procesa, con la finalidad de facilitar la toma de decisiones que permitan asistir en la investigación y remediación oportuna de los incidentes de seguridad que se presenten.
3.2.2. Deberá proporcionar un Tenant dedicado otorgado al BCRP sin costo alguno.
3.2.3. Deberá haber obtenido la calificación como “Leaders” o “Visionaries” en el cuadrante de Gartner dentro de su escala de medición y/o haber obtenido la calificación “Leaders” o “Strong Performers” en ForresterWave en 2024.
3.2.4. Deberá unir eventos utilizando modelos de cadena de amenazas (Kill Chain) o MITRE ATT&CK para el análisis de eventos de mayor riesgo.
3.2.5. El proveedor en su servicio del SOC gestionado deberá incluir una solución SIEM licenciada.
3.2.6. Permitir la caza de amenazas de manera rápida mediante la búsqueda de un lenguaje estándar.
3.2.7. Deberá admitir cifrado de datos transparente (TDE) de extremo a extremo. Transparente significa que los usuarios finales no deben percibir los procesos de cifrado / descifrado, y de extremo a extremo que los datos se cifran tanto en reposo como en tránsito.
3.2.8. Deberá admitir control de acceso basado en roles granulares (RBAC) con soporte para administración delegada, tanto a las funcionalidades en la interfaz de usuario como a los

datos que pueden tener acceso.

3.2.9. Deberá contar con una interfaz de usuario que permita visualizar los eventos crudos, eventos base, enriquecidos y data histórica.

3.2.10. Deberá contar con conectores/parseadores preconfigurados listos para usar, pero que se puedan modificar según sea necesario. El parseo, normalización y categorización de los colectores deben ser personalizable desde la interfaz de usuario. Asimismo, deberá contar con una API RESTful de servicios web abiertos y disponible en internet para la integración bidireccional con otras tecnologías.

3.2.11. Deberá poder integrarse a las tecnologías de seguridad de la red local, infraestructura de comunicaciones y servidores, plataformas de seguridad multinube tipo Azure, Office365, y herramientas para gestión de otras herramientas de seguridad.

3.2.12. Deberá soportar la integración con más de 500 fuentes de terceros mediante los métodos syslog, formatos de registros estructurados, archivos, bases de datos, conexión API y registros no estructurados.

3.2.13. En la implementación de recolectores locales, el contratista deberá de cubrirlos sin perjuicio económico para el BCRP. La infraestructura de los colectores deberá cumplir con las siguientes características:

- Tenga la capacidad de gestionar el ancho de banda de la red interna, en la comunicación entre las fuentes y el colector, para la trasmisión de los datos entre la capa de recolección y la de análisis.

NOTA: Esta capacidad se refiere a como el colector gestiona la entrada y salida de datos del mismo de tal manera que permita recopilar la información localmente y enviarla en tiempo real hacia el servicio SOC para su procesamiento. Al ser el colector proporcionado por el contratista este determinará la cantidad de interfaces mapeada para el tráfico a correlacionar, ancho de banda usado en dichas interfaces y crecimiento para el consumo de EPS solicitado.

- Realizar caché local y/o almacenamiento en búfer en los puntos de recolección de los datos (colector) para garantizar que no se pierdan datos en tránsito en caso de un problema de red o un pico en el volumen de eventos.

3.2.14. Realizar la optimización continua del servicio del SOC, considerando Actualización de los reportes e informes entregados por el servicio.

3.3. Detección y Analítica de Eventos de Seguridad a través de la solución SIEM

El servicio de gestión de eventos (SIEM) deberá realizar la detección y analítica de eventos de seguridad a partir de estos requisitos:

3.3.1. Las fuentes de datos locales (Datasources) del BCRP enviarán información de sus eventos a la solución SIEM empleada por el servicio SOC, para ello los componentes de dicha solución (denominado colectores) será implementado en la red del BCRP, el mismo que se encargará de recopilar la información localmente y enviarla en tiempo real hacia el servicio SOC para su procesamiento. En el caso de fuentes de datos externos a la red del BCRP, se puede optar por canales alternativos de comunicación hacia la plataforma SIEM, tales como API connection, Cloud Storage Integration, streaming vía logs forwarders, entre otras.

3.3.2. El BCRP cuenta con dos datacenters (Principal y Contingencia) conectados mediante fibra oscura (LAN extendida), para propósito de alta disponibilidad se requiere que los componentes(s) colector(es) sean implementados como mínimo en dos (02) servidores físicos (que deben ser provistos durante el periodo de contrato), ubicados uno en cada datacenter, sólo uno de ellos a la vez se conectará al servicio SOC.

3.3.3. El proveedor es responsable de proporcionar la infraestructura, incluyendo la cantidad de colectores necesaria para la recolección de eventos de los Datasources del BCRP.

3.3.4. Cada uno de los servidores entregados por el proveedor (colector) deberá cumplir con las siguientes características:

- Ser montable en gabinetes de 19” (incluir los accesorios de rackeo necesarios).
- Contar con fuente de energía de 220 VAC redundante (incluir los power cords necesarios).

- Contar como mínimo con dos interfaces Ethernet 10/100/1000 Base-T RJ45 (según los requerimientos del BCRP).
- Contar con una interface Ethernet 10/100/1000 Base-T RJ45 para el acceso a la consola de gestión del servidor físico.
- Proporcionar el cableado de red categoría 6A desde las interfaces de los servidores a los equipos de comunicaciones del BCRP.

Notas:

a) Se precisa que el equipamiento deberá ser nuevo (de primer uso).

b) Se permite que el proveedor utilice appliances virtuales dentro de los servidores.

El BCRP es responsable de:

- Proporcionar la infraestructura de datacenter (gabinetes, conectividad, suministros de energía estabilizada y aire acondicionado) requeridos para la operación de los servidores que conforman el componente colector.
- Proporcionar el ancho de banda de acceso a Internet que pueda requerir el componente colector.

3.3.5. En caso de fallas de hardware en alguno de los servidores que conforman el componente colector, los elementos de reemplazo (partes o servidor completo) deberán ser suministrado como máximo al siguiente día útil, contabilizado a partir del momento en que se determina tal necesidad. El contratista es responsable de implementar las configuraciones que puedan ser requeridas para su incorporación al servicio.
NOTA: En caso el contratista no pueda suministrar los elementos de reemplazo al siguiente día útil, se podrá extender el tiempo de RMA a la disponibilidad de stock del fabricante siempre que el contratista proporcione otro equipo temporal para mitigar el riesgo de que se afecte la disponibilidad del servicio.

3.3.6. La transferencia de información desde los componentes colectores (en la red del BCRP) hacia el servicio SOC, se realizará mediante una conexión cifrada a través de Internet (los componentes colectores iniciarán las conexiones).

Nota

El servicio SOC deberá contar con su propia conexión a Internet para recibir la información enviada por el componente colector.

3.3.7. Deberá detectar amenazas internas y cibernéticas avanzadas mediante el uso de aprendizaje automático (machine learning y/o inteligencia artificial) para crear los casos de uso y otros análisis que sean parte del servicio.

3.3.8. En caso de una interrupción en la recepción de eventos desde cualquier Datasource, el proveedor en conjunto con el BCRP iniciará una investigación para determinar si la causa raíz se encuentra en su infraestructura o en la del BCRP. Una vez confirmado que la interrupción no se deberá a problemas en la red o configuración del BCRP, el proveedor deberá restaurar el flujo de datos en un plazo máximo de 4 horas según lo establecido en el Máximo Tiempo de Resolución de Requerimientos (MTRR) como prioridad Alta.

3.3.9. Deberá proporcionar contenido listo para usar, que incluya conectores, parsers, políticas y modelos de amenazas. Las políticas y los modelos de amenazas deben estar clasificados por funcionalidad, fuente de datos o clasificación dentro del modelo MITRE ATT&CK o Kill Chain.

3.3.10. Deberá contar con un empaquetado de casos de uso y modelos de amenazas listos para ser usado en los distintos casos como: amenazas cibernéticas, amenazas internas, análisis de seguridad en la nube, análisis de identidades y acceso, exfiltración de datos, command control, phishing, tampering, espionaje y movimientos laterales.

3.3.11. Deberá contar con diferentes técnicas de análisis como perfiles de comportamiento, análisis de pares y grupos, casos de uso específicos para el negocio y modelado de amenazas.

3.3.12. Deberá proporcionar capacidades integrales para modelar y ajustar la puntuación de riesgo según el perfil del usuario o entidad o el tipo de anomalía, la gravedad de la amenaza y la secuencia/combinación de eventos que ocurren durante un período de tiempo.

3.3.13. Deberá permitir el modelado de riesgos desde la interfaz de usuario según las prioridades de la organización.

3.3.14. Deberá contar con modelos de amenazas que permitan aplicarlo en la agrupación de eventos realizados por un usuario o entidad que abarque días, semanas, meses, etc. Estas actividades se deben mostrar en la UI en forma de Kill Chain y/o MITRE ATT&CK con cada evento categorizado en etapas predefinidas.

3.3.15. Deberá disponer de algoritmos de aprendizaje automático, con clasificadores específicos aplicables al tipo de datos y fuente que permitan modelar y detectar amenazas avanzadas de malware por ejemplo DGA, ataques de phishing / SPAM, etc.

3.3.16. Deberá disponer de técnicas de análisis de datos de ubicación geográfica para buscar patrones de inicio de sesión que indiquen el potencial intercambio/compromiso de la identidad del usuario. Por ejemplo, distintos inicios de sesión de un usuario desde diferentes países en un periodo de tiempo muy corto reportado con una alerta de Azure del BCRP.

3.3.17. Deberá poder realizar el análisis de alertas por parte de Azure (Microsoft 365) que cuenta el BCRP.

NOTA: Para el caso de los servicios de Azure (Microsoft 365) con que cuenta el BCRP, los servicios a considerar en caso de una integración para el análisis de alertas por parte de Azure (Microsoft 365) serán: Microsoft Entra ID, Microsoft Defender for Cloud Apps, Microsoft Defender for Cloud, entre otros que se considere durante la implementación y/o ejecución del servicio.

3.3.18. Deberá proporcionar la capacidad de definir políticas basadas en reglas para detectar amenazas conocidas. Estas amenazas conocidas deben utilizarse como potenciadores de riesgos y combinados con los análisis “sin firma” en los modelos de amenazas.

3.3.19. Deberá contar con modelamiento de amenazas que permita identificar amenazas compuestas, que si se observan de forma aislada pueden ser de bajo riesgo, sin embargo, cuando se combinan, son un indicio de un evento de alto riesgo. La visualización deberá entregarse en una línea de tiempo sin limitarse por licenciamiento al número de usuarios y/o entidades.

3.3.20. Deberá reducir el número de falsos positivos al aplicar capacidades avanzadas de aprendizaje automático (machine learning y/o inteligencia artificial) para aprender lo que es normal y no normal en el entorno añadiendo la actividad a un contexto amplio dentro del evento simple, la correlación y el encadenamiento de amenazas.

3.4. Detección y Alertas a través de la solución SIEM

El servicio de gestión de eventos (SIEM) deberá:

3.4.1. Permitirse el acceso al SIEM y/o plataforma de observabilidad, solo para monitoreo y consulta para el personal designado del BCRP.

3.4.2. Contar con un sistema de administración de casos nativo e incluir el riesgo asociado al usuario o entidad involucrada y el historial de la actividad maliciosa que hace parte de la cadena en la detección.

3.4.3. Utilizar técnicas de aprendizaje automático para notificar al personal interno del BCRP sobre riesgos emergentes, permitiendo buscar en múltiples dimensiones de visualización

las actividades anómalas de los usuarios y/o red para detectar amenazas avanzadas.

3.4.4. Tener la capacidad de presentación gráfica personalizable de la detección de un modelo de amenaza directamente en la línea del tiempo del usuario o del BCRP, con el objetivo de poder interpretar en un menor tiempo el origen del ataque, IP's, puertos, acciones tomadas, cantidad de eventos, etc. Se precisa que este numeral hace referencia a una plataforma de observabilidad que puede estar dentro del SIEM o externa.

3.4.5. Soportar la integración con soluciones de orquestación, automatización y respuesta de seguridad de terceros.

3.4.6. Soportar creación de políticas, reglas y cadenas a partir de una consulta desde la consola de investigación.

3.4.7. Incluir el acceso integrado al datalake donde se puedan consultar los eventos crudos, enriquecidos, filtrados por fecha, atributos específicos, anomalías, usuarios, entidades, activos, watchlist con la posibilidad de accionar filtros y consultas desde un atributo específico y así mismo generar análisis gráficos.

3.4.8. Establecer líneas base de eventos para cada fuente de datos y detectar anomalías en la generación de eventos.

3.4.9. Generar alertas en un tiempo máximo de 30 minutos cuando se detecte una disminución significativa en el número de eventos o la ausencia total de eventos de una fuente.

3.5. Ciberinteligencia

El servicio deberá contar con la integración de al menos cinco (05) fuentes de inteligencia de amenazas de diferentes proveedores tipo suscripción (no gratuitas) provistas por la misma plataforma y/o se integre de manera externa a esta sin costo adicional.

NOTA: Entre estas fuentes de inteligencia deberán estar aquellos feeds de inteligencia de amenazas donde se recopila información tales como foros y sitios web, datos de la dark web, y blogs.

Se aclara que, si múltiples tipos de datos son provistos por un mismo proveedor o fabricante, estos se contabilizarán como una única fuente de inteligencia.

Las características de estas fuentes son las siguientes:

3.5.1. Deberá estar licenciado y/o contratado para ser usados por el contratista para monitorear únicamente amenazas que tengan como objetivo al BCRP.
NOTA: Se precisa que las herramientas de inteligencia de amenazas provistas por el proveedor serán para uso del servicio SOC Gestionado y del Banco, permitiendo que, dentro del alcance de sus funciones, realice un filtrado de monitoreo de amenazas que tengan como objetivo al BCRP.

3.5.2. La fuente de información de ciber inteligencia deberán ser de empresas especializadas en el rubro con presencia internacional.

3.5.3. Deberá brindar información especializada en tiempo real, con la finalidad de obtener un informe global de nivel de amenazas en internet. El informe deberá describir detalladamente, las condiciones de las amenazas de seguridad en internet.

3.5.4. Identificación de posibles escenarios de explotación, alerta de potenciales APT y denegación de servicio que afecte al BCRP.

3.5.5. Identificación de IoC (Indicadores de Compromiso), que pueden poner en riesgo o estén relacionados al BCRP.
NOTA: Esta información debe ser entregada en boletines de información según lo indicado en el numeral 3.7.10.

3.5.6. Brindar informes detallados de los hallazgos por cada caso identificado.

3.5.7. Identifica indicadores de amenazas relacionados con el BCRP.

3.5.8. Cada fuente de información a ser utilizadas deberá pertenecer como mínimo a un (01) grupo de cooperación internacional de ciberseguridad, por ejemplo: APWG, FIRST, FS-ISAC, OIC-CERT u otro correspondiente a ciberseguridad.

NOTA: Se precisa que la pertenencia a un grupo de cooperación internacional de ciberseguridad podrá ser sobre el equipo de respuesta del contratista hacia alguno de los grupos mencionados y/o desde las fuentes de inteligencia que se deberán integrar al SIEM.

3.5.9. El servicio deberá proporcionar feeds personalizados de todos los tipos de URL de

phishing (para la detección de riesgos de correo electrónico empresarial) dedicados a la entidad de forma nativa en el portal.

3.6. Protección de Marca

El servicio deberá contar con las siguientes características:

3.6.1. Monitorear operaciones y/o tendencias que pueden poner en riesgo la reputación y la marca del BCRP, tanto en el Deep web como en la Dark web.
3.6.2. Monitoreo de otras posibles fuentes de amenazas en la Dark web y Deep web relacionadas con el BCRP.
3.6.3. Brindar información de cuentas de usuario (con dominio @BCRP.gob.pe) que han sido exfiltrados (Leaked Data).
3.6.4. Implementar un dashboard que incluya el Top 100 de credenciales exfiltradas de cuentas del BCRP
3.6.5. Mensualmente indicar mediante un reporte que detalle la información relacionada a los hallazgos, entre los que se deberá incluir al menos lo siguiente:
- Robo de credenciales y/o credenciales expuestas con dominio BCRP.gob.pe indicando la fuente exacta de donde previene la información. Se precisa que el dominio a monitorear es bcrp.gob.pe y los subdominios y demás assets serán entregados al postor ganador luego de la firma del contrato.
- Dominios sospechosos.
- Uso no autorizado de marca.
- Contenidos ofensivos en redes sociales al BCRP y/o a sus principales funcionarios.
- Hacktivismo/Activismo.
- Aplicaciones móviles sospechosas.
- Información del BCRP en Redes Sociales como Facebook, Telegram, TikTok, entre otras redes.
- Monitoreo avanzado de hasta 30 cuentas de funcionarios del BCRP, el cual debe enfocarse en una vigilancia proactiva para detectar y eliminar rápidamente cuentas falsas o ilegales, monitorear la web continuamente para suprimir copias no autorizadas de perfiles y datos, protegiendo así la presencia digital de los funcionarios contra uso indebido y suplantación de identidad.

3.6.6. El servicio deberá proporcionar detección y alerta sobre la mención del cliente en los repositorios de código (por ejemplo, Github).
3.6.7. El servicio deberá realizar la detección y eliminación de grupos y cuentas falsas de las plataformas más grandes, por ejemplo: Facebook, Instagram, LinkedIn y Twitter (X), entre otros.
3.6.8. El servicio deberá realizar la detección en grupos fraudulentos dentro de las redes sociales por ejemplo Telegram y WhatsApp (canales), entre otros.
3.6.9. El servicio deberá proporcionar información de páginas web que estén utilizando el logotipo, nombre y/o imagen de alguno de los funcionarios del Banco, o de la institución.
3.6.10. El servicio deberá de considerar hasta 25 takedowns anuales, por ejemplo: Eliminación de perfiles falsos de las cuentas de BCRP en redes sociales, sitios webs fraudulentos que utilizan nombre y logotipo del BCRP, entre otros.

NOTA: Se precisa que el Banco administra una cantidad total de 25 takedowns anuales.

3.6.11. El servicio deberá realizar la detección y eliminación de sitios de phishing que se hacen pasar por la entidad y roban credenciales.

3.7. Características específicas

3.7.1. Realizar la detección de posibles incidentes de ciberseguridad en tiempo real.
3.7.2. Realizar el triaje (análisis de los eventos) para la detección de posibles incidentes de seguridad, empleando para ello casos de uso (correlaciones), así como información de fuentes de ciber inteligencia y otras herramientas disponibles por el SOC (tales como análisis de comportamiento, análisis de anomalías, entre otras).

3.7.3. Realizar la detección proactiva de posibles amenazas (cacería de amenazas). Se precisa que dicha actividad deberá realizarse en una frecuencia determinada por las buenas prácticas propias del servicio SOC.

NOTA: Se precisa que la detección proactiva de posibles amenazas (cacería de amenazas) que es parte del servicio SOC Gestionado, deberá ser a través del monitoreo de eventos de seguridad que se muestra en la plataforma de gestión SIEM y coordinado con el BCRP, si se presentará alguna incidencia.

NOTA: El proveedor deberá realizar esta actividad al menos una (01) vez por mes, combinadas con hunting automatizado o reactivo en función de alertas, indicadores o campañas, por ejemplo, Basado en IOCs, Análisis de comportamiento, Análisis retrospectivo, alineándose con los marcos como MITRE CTI, SANS Threat Hunting Cycle y estándares de ciberseguridad como ISO/IEC 27001/27035 y el NIST CSF.

3.7.4. La información sobre la investigación de incidentes, así como las medidas de mitigación recomendadas, deberá ser proporcionada al BCRP, para el tratamiento correspondiente. El BCRP también contará con la posibilidad de solicitar que el tratamiento de incidentes sea efectuado por el servicio SOC (respuesta a incidentes), para lo cual el BCRP proporcionará los accesos que sean necesarios.

NOTA: Se precisa que toda posibilidad de solicitar que el tratamiento de incidentes sea efectuado por el servicio SOC (respuesta a incidentes), el Banco proporcionará los accesos que sean necesarios en sesión activa y bajo la supervisión del departamento de Ciberdefensa.

3.7.5. Se incluye dentro del servicio, una bolsa de doce (12) horas mensuales, no acumulables, para actividades de respuesta a incidentes e investigación forense.

3.7.6. Las horas de respuesta a incidentes adicionales a la bolsa de doce (12) horas mensuales que puedan ser solicitadas por el BCRP, serán facturadas en forma independiente, para lo cual el proveedor deberá especificar el costo unitario (por hora) en su propuesta económica.

3.7.7. Brindar acceso en línea a un portal web de investigación de incidentes, para al menos ocho (08) conexiones concurrentes del BCRP. Dicho portal deberá contar con las siguientes características:

- Permitir el acceso con autenticación de doble factor.
- Incluir una vista ejecutiva del estado actual del servicio a través de dashboards.
- Brindar información (durante un intervalo seleccionable) sobre el número de investigaciones por estado, criticidad, acciones realizadas, medidas de mitigación recomendadas y distribución de las tácticas del framework MITRE ATT & CK. Las acciones realizadas y las medidas de mitigación recomendadas podrán ser visualizadas cuando se ingrese al detalle de cada investigación.
- Los niveles de criticidad de las investigaciones son los definidos en el numeral 3.1.10 de los términos de referencia. (Cuatro niveles: Crítico, Alto, Medio y Bajo). Sin embargo, se aceptarán denominaciones equivalentes siempre y cuando se mantenga el número de niveles, pues ello está asociado al cumplimiento del SLA del servicio.
- Toda investigación deberá mostrar información sobre las tácticas empleadas de acuerdo con el framework MITRE ATT & CK.
- Brindar la siguiente información sobre cada investigación: Estado, tipo, analista asignado, fuente de datos que registra
- el incidente, resumen ejecutivo con el detalle de lo ocurrido, magnitud (usuarios, hosts, casillas de correo, IP origen/destino), conclusiones, información detallada sobre indicadores y archivos.

3.7.8. Entregar reportes periódicos de tipo técnico y tipo gerencial (un reporte cada mes), que incluyan entre los resultados: el monitoreo de eventos, el análisis de los incidentes detectados (triage, análisis profundo, cacería de amenazas), la optimización continua de la operación (cuando se hayan realizado acciones al respecto) y otros en coordinación con el BCRP. Asimismo, también se deben proporcionar reportes en demanda (a requerimiento del BCRP) en situaciones donde sean necesarios (por ejemplo, con motivo del uso de la respuesta a incidentes). Para más detalle referirse al numeral 3.10 de entregables.

3.7.9. Cuando se haga uso del servicio de respuesta a incidentes, el proveedor deberá emitir un informe técnico firmado por el jefe del SOC que incluya el detalle del caso tratado

considerando, entre otros aspectos la recopilación de evidencias, análisis, hallazgos, acciones realizadas y acciones recomendadas. Asimismo, se deberá incluir una sección de resumen ejecutivo.

3.7.10. Proporcionar al BCRP boletines de información en el rubro de Banca y Finanzas como principal fuente de información (incluyendo detalles de las amenazas, vulnerabilidades y los IOC correspondientes), tanto en forma semanal como en casos considerados críticos. El BCRP se encargará del tratamiento correspondiente a la información recibida.

3.7.11. El BCRP deberá tener acceso a:

- Los datos sin procesar (datos crudos) durante el periodo de doce (12) meses. El proveedor deberá almacenar esta información en su infraestructura, de ser en forma local (red del BCRP), será con recursos de almacenamiento provistos por el proveedor hasta dejarla totalmente operativa a conformidad del BCRP y brindará las facilidades para que se pueda realizar el respaldo de dicha información en coordinación con el Banco durante el periodo de servicio, en caso lo requiera.
- Los datos normalizados (datos procesados y almacenados por la solución SIEM) durante el periodo de tres (03) meses.
- La información de investigaciones en un dashboard durante el periodo de servicio SOC.

NOTA: Se precisa que, data cruda tiene correspondencia con data fría y data normalizada tiene correspondencia con data en línea que son los datos procesados y almacenados por la solución SIEM respectivamente.

3.7.12. El análisis de madurez del servicio consistirá en la evaluación del cumplimiento de los objetivos del mismo, considerando las métricas de operación, para el efecto se deberán emitir informes referentes a este aspecto, con una periodicidad mensual.

NOTA: La evaluación de cumplimiento de los objetivos del servicio será según las siguientes métricas:

1. NIST Cybersecurity Framework.
2. ISO 27001.
3. Proceso de mejora continua incluyendo Ciclo Plan–Do–Check–Act (PDCA), tareas correctivas documentadas y trazables, KPIs y métricas de mejora (MTTD, MTTR, tasa de falsos positivos, entre otros).

3.7.13. Durante la ejecución del servicio, el BCRP podrá solicitar cambios en el listado de Datasources implementados (adición, retiro, modificación), sin costo adicional, sin exceder del promedio diario de 5000 EPS. A partir de la Fase 2 este valor se verá incrementado a 10000 EPS.

3.7.14. Contar con una mesa de ayuda disponible las 24 horas del día, los 7 días de la semana, los 365 días del año ininterrumpidamente (24 x 7 x 365) y un procedimiento para el reporte de incidentes del servicio que incluya los niveles de escalamiento correspondientes y que contemple, entre otras cosas, la asignación, en un plazo no mayor a diez (10) minutos, de un número de atención (ticket) que facilite el seguimiento de los incidentes reportados. El reporte de estos incidentes podrá realizarse a través de la línea telefónica, correo electrónico, sistemas en línea, cuando se requiera.

3.7.15. Las notificaciones de alertas de seguridad proveniente del SOC Gestionado deberán ser reportadas en un plazo no mayor a quince (15) minutos de ocurrida la detección del incidente, debiendo ser este reporte a través de correo electrónico; en situación de horarios fuera de oficina del BCRP o cuando se requiera escalar por una respuesta inmediata, se podrá reportar también por llamada telefónica y/o sistemas en línea según matriz de disponibilidad de especialistas en coordinación con el Banco.

3.7.16. El proveedor deberá garantizar que brindará facilidades para que el servicio sea auditado a requerimiento del BCRP, en cualquier horario dentro de la prestación del servicio. En dicha oportunidad se firmará un acta de verificación del servicio.

NOTA: Para los diferentes casos de verificación, entre ellos: servicios brindados, CSIRT, infraestructura redundante, reportes, mesa de ayuda según lo indicado en el numeral 3 Condiciones Generales, serán realizados en cualquier horario dentro de la prestación del servicio comunicándose previamente con dos (02) días de anticipación al proveedor.

3.7.17. El proveedor deberá incluir entre otras actividades la gestión, generación de casos de uso

a demanda requeridos por el BCRP, para lo cual se iniciará el servicio con la creación de veinticuatro (24) CUS (casos de uso), posteriormente, el incremento será en coordinación con el BCRP durante el periodo de servicio.

3.7.18. El proveedor deberá analizar los correos sospechosos reportados por el BCRP con la finalidad de determinar si es phishing, spam, si contiene malware o si es correo benigno.

NOTA: Para los casos de los correos sospechosos, que ya pasaron el filtro de la plataforma antispam, estos serán reportados por el BCRP al proveedor para su análisis.

3.7.19. Realizar la recopilación, procesamiento y análisis de los eventos generados por las fuentes de datos del BCRP hacia múltiples destinos en tiempo real permitiendo su observabilidad.

NOTA: Se precisa que el termino múltiple destino hace referencia a una característica que debe estar soportada por la solución del proveedor para recopilación, procesamiento y análisis de eventos generados a más de un destino simultáneamente y en tiempo real.

3.7.20. Destinar capacidad operativa para realizar instalaciones o configuraciones en la integración de las soluciones de seguridad implementadas materias de este servicio, ello incluye cambios en la plataforma.

3.7.21. Como parte del servicio de SOC, el postor deberá ofertar la instalación, configuración, puesta en marcha y gestión de la plataforma NG-SIEM (Next Generation SIEM):

- Tecnología de Security Information and Event Management (SIEM), que se encuentre como “Leaders” o “Visionaries” en el cuadrante de Gartner dentro de su escala de medición y/o haber obtenido la calificación “Leaders” o “Strong Performers” en ForresterWave en 2024 exclusivamente para uso del BCRP (no compartido con otros clientes), con la finalidad de monitorizar y proteger cada uno de los activos digitales del Banco.

3.7.22. El BCRP cuenta con una infraestructura de seguridad informática, y de servicios y aplicaciones Web la misma que está basada en las siguientes tecnologías.

Lista de tecnologías de Seguridad:

TECNOLOGÍA	NÚMERO DE FUENTES
Firewall perimetral	10
Anti-Malware y EDR	1
Proxy Gateway de Internet	2
Web Application Firewall (On-Prem)	2
Web Application Firewall y Anti DDoS (SaaS)	1
Proxy Reverso	2
Controladores de Dominio y Directorio Activo	3
Servidores Windows	2
Antispam	1
Switches	12
VPN Gateway	2
Balanceadores de Enlace	2
Firewall de Base de Datos	2
Privileged Access Manager	2

NOTA: Los activos que se tienen actualmente en la nube son "Antispam" y "Web Application Firewall y Anti DDoS SaaS", los otros indicados en la lista de tecnologías de seguridad son On-Premise.

NOTA: En la fase 2 de implementación de data sources, estos corresponden nuevos equipos los cuales se describen a continuación:

TECNOLOGÍA	NÚMERO DE FUENTES
Firewall perimetral	4
HSM	7
Servidores	58
Balanceadores/Web Application Firewall	8
Storage	2
Switches	20

El detalle de esta información será proporcionado al inicio de la fase 2 según lo indicado en numeral 1 Plazos.

Información referida a las marcas de las tecnologías

MARCA
Palo Alto
Skyhigh
Radware
Microsoft Windows
Cisco
Citrix
IBM
Symantec

Esta infraestructura deberá ser monitorizada permanentemente para la identificación, análisis y alertas ante las distintas amenazas, vectores de ataque y cualquier incidente de seguridad informática al cual sea expuesto.

La(s) version(es) de firmware o SO de la infraestructura o servicio, será brindada al contratista al inicio de la ejecución del servicio.
Estas tecnologías podrían variar durante la ejecución del servicio y el contratista deberá a solicitud del BCRP, brindar sin costo el servicio de integración e implementación a la nueva tecnología mientras no supere la cantidad de EPS (eventos por segundo) contratada; de ser el caso que supere la cantidad de ingesta monitoreo y correlación a los EPS contratados, el proveedor deberá incluir en su propuesta económica, adicionalmente, el costo variable por 1000 EPS (o su equivalente en GB debidamente sustentado por el fabricante).

El proveedor, en el servicio SOC deberá permitir la observabilidad en tiempo real del consumo de EPS o tráfico per-Giga, el flujo de datos proveniente de los Data Sources y todos los componentes del servicio SOC para evaluar en conjunto con el BCRP si se requiere incrementar u optimizar la cantidad de los mismos.

En el caso de optar por un incremento de consumo de EPS o tráfico per-Giga, esta se verá reflejada en una factura aparte, previa coordinación y sustento con el BCRP.

La infraestructura tecnológica preexistente opera simultáneamente en centros de datos del BCRP ubicado en la oficina principal (OP), centro externo de respaldo (CER) en Lima, Centro de cómputo en Piura, así como a través de servicios en nube.

El contratista, deberá validar previamente que su plataforma Next Generation – Security Information and Event Management a ofertar e implementar, sea compatible con cada uno de los componentes de la infraestructura preexistente. La compatibilidad deberá permitir que las soluciones ofertadas por el contratista puedan almacenar, procesar

y correlacionar correctamente los eventos y registros (logs) enviados a dicha plataforma, por cada uno de los componentes.

3.8. Modalidad de Servicio

La modalidad del servicio hace referencia a un servicio SOC gestionado a cargo del contratista, el cual incluye actividades de monitoreo las 24 horas del día, los 365 días del año ininterrumpidamente, incluyendo domingos y feriados en línea (conexión permanente). El plazo del servicio será de veinticuatro (24) meses iniciándose a partir del día siguiente de la subscripción del Acta final de Conformidad de implementación del servicio SOC.

Para ello, el servicio deberá incorporar las capacidades de un SOC (personas, tecnología, procesos) que tiene por objetivo identificar las amenazas dentro de la infraestructura de una organización (detección) y responder a ellas de manera eficiente mediante las actividades de monitoreo, detección y alerta de eventos de seguridad informática.

3.8.1. El servicio de SOC se podrá brindar de manera remota, incluso desde el exterior del país. En el caso que se presente un inconveniente con el internet del BCRP o un evento crítico que tenga efecto en la operación del servicio SOC, el proveedor deberá tener la capacidad de brindar el servicio de respuesta a incidentes en forma local, a solicitud del BCRP. Se precisa que el plazo de inicio de las actividades presenciales será de dos (02) horas, contabilizadas a partir del momento en que el BCRP lo solicite.

NOTA: Se precisa que el servicio de respuesta a incidentes en forma local será solo para los Data Centers en Lima.

3.8.2. Las prestaciones podrán ser proporcionadas directamente por el proveedor, estando permitido que este pueda hacer uso de suscripciones, contratadas para el BCRP, a servicios brindados por un SSP (Security Service Provider), en cuyo caso tanto el proveedor como el SSP brindará la infraestructura y personal especializado (numeral 3.12) requeridos por el servicio SOC.

Nota:

En caso de que el proveedor haga uso de suscripciones a servicios brindados por un SSP, deberá acreditarlo mediante una carta de autorización del SSP para brindar los servicios empleados. Dicho documento será parte de la documentación de presentación obligatoria que los postores deberán incluir en sus ofertas.

3.8.3. El Centro de Operaciones de Seguridad (SOC/CyberSOC), deberá operar bajo estándares internaciones y buenas prácticas en ciberseguridad y seguridad de la información, y deberá contar con alta disponibilidad a nivel de infraestructura y a nivel de personal, desplegados en diferentes ubicaciones dentro o fuera de territorio nacional para asegurar la continuidad del servicio. Esto implica asegurar contingencias ante cualquier tipo de evento disruptivo incluyendo eventos catastróficos. Por lo que el proveedor debe considerar que el equipamiento que de soporte a la herramienta SIEM debe contar con contingencia en distintas ubicaciones físicas, y el equipo de personas encargados de la operación de SOC, incluida la capa de investigación, deben estar descentralizados en distintas ubicaciones.

Para acreditarlo, como requisito para la suscripción del contrato, el postor ganador de la buena pro deberá presentar copia simple de la certificación internacional ISO 27001, además la certificación ISO 20000 o ISO9001 del proveedor, ya sea plataforma On-premise y/o en la nube. Y para el caso de soluciones SaaS, adicionalmente deberá presentar certificaciones tales como SIM3 2022 o SOC II tipo 2.

Estas certificaciones deberán estar relacionadas a alguna de las siguientes actividades o alcances:

- Servicio de CYBERSOC.
- Servicio de monitoreo de eventos de seguridad (SOC).
- Servicios de Centro de Operaciones de Seguridad (SOC).
- Servicio de Inteligencia de Amenazas en la Red.
- Servicio de soporte a través de SOC (Security Operation Center), monitoreo y correlación de eventos para infraestructura de red y seguridad.
- Servicio de ciberseguridad.
- Servicio de detección y respuesta ante amenazas.
- Servicio de operación de la seguridad y servicio De CyberSOC.
- Servicio de gestión de eventos e incidentes de seguridad.
- Servicio de Monitoreo & Alerta Temprana (CyberSOC).
- Solución de análisis, detección y respuesta ante Amenazas de Seguridad Informática en la red interna.

3.9. Ejecución del Servicio

Como parte del servicio, el contratista deberá monitorear los eventos de seguridad que se muestra en la plataforma de gestión SIEM y deben coordinar con el equipo de Ciberdefensa del BCRP, si se presentara alguna incidencia.

Para ello, el contratista deberá contar con las capacidades de un SOC (personas, tecnología, procesos) que tiene por objetivo identificar las amenazas dentro de la infraestructura de una organización (detección y alertas), mediante las actividades de monitoreo, detección y alertas de eventos de seguridad informática.

El contratista, deberá crear una matriz de escalamiento en conjunto con el BCRP, en la cual se determine cuándo un incidente deberá ser escalado y quiénes son los roles autorizados del escalamiento de los tickets. La matriz deberá incluir tiempos de atención para el manejo de las alertas.

Los incidentes de seguridad solo podrán ser concluidos, previa conformidad del departamento de ciberdefensa del BCRP.

El contratista deberá proveer un único de punto de contacto (número telefónico) para comunicarse en formato 24x7x365. Este punto de contacto no deberá tener una atención típica de una central telefónica o contact center, por el contrario, deberá ser una línea directa que permita la atención inmediata y permanente, con la finalidad de atender el requerimiento y proveer información en tiempo real al BCRP sobre las amenazas que sean detectadas.

Mediante este canal directo, el BCRP podrá comunicarse con el servicio gestionado para notificar un incidente, una amenaza potencial o en curso. Como flujo de verificación, el servicio gestionado deberá validar la información a través de una cuenta de correo asignada por el BCRP, mediante el cual, el analista y el equipo del servicio gestionado deberán confirmar la recepción e incluir esta notificación como parte del registro del incidente.

3.10. Entregables del Contratista

Durante la Implementación del servicio se deberá entregar como mínimo la siguiente información al BCRP:

ETAPA	ENTREGABLE	Frecuencia
Implementación del Servicio Fase 1	Plan de implementación de la Fase 1 del servicio, contemplando todo lo señalado en el numeral 3.16	Según el numeral 1. Plazos.

Ejecución del Servicio Fase 1	Planificación del servicio y actividades para identificación, detección y alertas de incidentes en conjunto con el equipo del BCRP, el cual deberá incluir: - Matriz de Responsabilidades - SLAs - Flujo de Coordinaciones y matriz de escalamiento - Datos de Contacto	Al inicio de la Fase 1
	Informes Gerenciales	Mensual
	Informe de Incidente	5 días calendario al finalizar la atención
	Dashboards en línea y para ser exportados en Power BI	Según los numerales: 3.1.2, 3.6.4, 3.7.7, 3.7.11, 3.7.22, 3.16.4
	Informe Técnico Mensual (incluyendo como mínimo informe de Ciberinteligencia, madurez del servicio, consumo de EPS, incremento de bolsa de horas y/o EPS en el mes correspondiente, entre otros que considere el proveedor y en coordinación con BCRP).	Mensual
	Plan de Actividades para las labores de Capacitación.	Según el numeral 1. Plazos.
Implementación del Servicio Fase 2	Plan de implementación de la Fase 2 del servicio, contemplando todo lo señalado en el numeral 3.16	Según el numeral 1. Plazos.
Ejecución del Servicio Fase 2	Planificación del servicio y actividades para identificación, detección y alertas de incidentes en conjunto con el equipo del BCRP, el cual deberá incluir: - Matriz de Responsabilidades - SLAs - Flujo de Coordinaciones y matriz de escalamiento - Datos de Contacto	Al inicio de la Fase 2
	Informes Gerenciales	Mensual
	Informe de Incidente	5 días calendario al finalizar la atención
	Dashboards en línea y para ser exportados en Power BI	Según los numerales: 3.1.2, 3.6.4, 3.7.7, 3.7.11, 3.7.22, 3.16.4
	Informe Técnico Mensual (incluyendo como mínimo informe de Ciber inteligencia, madurez del servicio, consumo de EPS, incremento de bolsa de horas y/o EPS en el mes correspondiente, entre otros que considere el	

	proveedor y en coordinación con BCRP).	Mensual
	Plan de Actividades para las labores de Capacitación.	Según el numeral 1. Plazos.

Adicionalmente, respecto a la capacitación se deberá entregar lo siguiente:

ETAPA	ENTREGABLE
Capacitación	Certificados de capacitación a los participantes.

Cada uno de estos documentos deberán ser referidos en las actas correspondientes; asimismo deberá tener la conformidad previa del BCRP.

KPI – Indicador Clave de Rendimiento

El contratista deberá asegurar como mínimo los siguientes KPI's para el servicio:

ID INDICADOR	INDICADOR	FRECUENCIA	OBJETIVO	INFORMACIÓN A OBTENER
KPI I.1	% Reportes vulnerabilidad enviados	Mensual	Detectar las vulnerabilidades existentes	Número de vulnerabilidades por criticidad/Número de vulnerabilidades por tecnología
KPI I.2	% Ataques bloqueados	Mensual	Cantidad de Ataques a la BCRP	Número de ataques bloqueados válidos / Número total de eventos bloqueados
KPI I.3	% Eventos Falsos Positivos	Mensual	Reducir el número de falsos positivos bloqueados	Número de ataques bloqueados No validos/ Número total de eventos bloqueados
KPI I.4	% Casos de Uso	Trimestral	Garantizar la actualización de los C.U. en el NG-SIEM	Número total de casos nuevos y/o actualizados / Número total de casos de uso validos
KPI I.5	% Eventos alertados	Mensual	Cantidad de eventos a la BCRP	Número de eventos alertados / Número de eventos con tratamiento

Sobre el KPI I.1: No hace referencia a la ejecución directa de escaneos de vulnerabilidades mediante plataformas especializadas (scaners de vulnerabilidades per se), sino que se refiere a la capacidad del servicio SOC Gestionado de identificar vulnerabilidades a partir del análisis de eventos y registros provenientes de las fuentes de datos (data sources).

NOTA: Este KPI está alineado al resumen mensual consolidado de la información contenida en los boletines técnicos que deberán ser enviados semanalmente, según numeral 3.7.10.

Sobre el KPI I.2: No se encuentra limitado a las capacidades del SIEM ni a sus casos de uso, sino que contempla la integración y análisis de eventos generados por múltiples tecnologías de seguridad implementadas en la infraestructura del Banco, tales como firewalls, WAFs, XDR entre otras soluciones que sí poseen funciones de bloqueo nativas.

Adicionalmente, como parte de la ejecución del servicio se podrán solicitar la confección de 50 indicadores más, en caso sea necesario, que podrán ser implementados durante la ejecución del servicio, para ello el contratista deberá brindar una plataforma actualizada para lo cual brindará acceso como mínimo a ocho (08) usuarios del BCRP.

NOTA: Estos indicadores podrán incluir métricas orientadas a la mejora continua de la detección, análisis, respuesta y recuperación ante incidentes de ciberseguridad, así como al desempeño del servicio.

Su funcionalidad estará orientada a proporcionar visibilidad estratégica y operativa sobre la eficacia de los casos de uso implementados, cobertura de amenazas, tiempos de respuesta, calidad de las investigaciones, entre otros aspectos críticos.

3.11. Requerimientos del Personal Clave

El Contratista deberá asignar el siguiente personal clave:

- Jefe del proyecto SOC

  Es el responsable máximo del servicio por parte del proveedor, teniendo las siguientes responsabilidades:

  - Asegurar que la implementación y ejecución se haga de acuerdo a los requerimientos técnicos solicitados.
  - Brindar todos los entregables del servicio en los plazos establecidos.
  - Velar por el cumplimiento de los SLA.
  - Realizar el seguimiento de las actividades para garantizar la calidad del Servicio.
  - Supervisar de la respuesta a incidentes críticos y garantizar la correcta escalabilidad y comunicación entre equipos SOC y BCRP.
  - Preparar y presentar de informes gerenciales de estado del servicio para BCRP.
  - Asistir a reuniones de carácter gerencial, en coordinación con el BCRP.

  Este profesional debe contar con una experiencia mínima de tres (03) años en la gestión de servicios SOC.

  Así mismo, este profesional debe contar como mínimo con dos (02) de las siguientes certificaciones vigentes en:

  - CompTIA Security+
  - EC-Council Certified Incident Handler, of Cloud Security Knowledge (CCSK)
  - Certified Ethical Hacker – CEH
  - ISACA CSX Fundamentals Certificate
  - Certified Information Security Manager – CISM
  - Certified Information Systems Security Professional - CISSP
  - ISO 27001 Lead Implementer / Lead Auditor
  - Security Operations Center Capability Maturity Model - SOC-CMM
  - CSIRT Manager – CERT/CC (Carnegie Mellon)
  - SOC 2 Auditor / Implementador
  - CISA (Certified Information Systems Auditor) – ISACA

- Supervisor de Implementación SOC

Es el responsable de la correcta implementación del servicio SOC en sus 2 fases, teniendo las siguientes funciones:

- Realizar del plan de trabajo y reuniones de avance de la implementación de SOC en todas sus fases.
- Gestionar requerimientos para las integraciones de las fuentes de datos.
- Gestionar y coordinar con el equipo de especialistas de implementación SOC.
- Gestionar el alcance, cronograma, calidad, recursos humanos, comunicaciones, riesgos, e interesados de la implementación de la fase.

Este profesional debe contar con una experiencia mínima de tres (03) años en la gestión de proyectos de Tecnologías de Información y/o proyectos de seguridad informática.

Así mismo, este profesional debe contar con certificación o diplomado vigente de Project Management Professional – PMP y/o especialización en dirección y gestión de proyectos y/o ITIL.

- Dos Especialistas de implementación SOC (02)

Son los responsables que realizaran las actividades técnicas de implementación del servicio en sus dos (02) fases, como integración de Fuentes de datos, configuración de colectores, registro y configuración de plataforma, entre otros.

Estos profesionales deben contar con una experiencia mínima de cuatro (04) años en la implementación o ejecución de servicio SOC con al menos dos (02) tecnologías descritas en la lista de tecnologías de Seguridad (Numeral 3.7.22).

Así mismo, estos profesionales deben contar con al menos una (01) certificación en las tecnologías descritas en la lista de tecnologías de Seguridad (Numeral 3.7.22).

- Coordinador SOC

Es el responsable del seguimiento de la respuesta de los incidentes presentados y requerimientos al servicio SOC. Este personal deberá asistir a reuniones mensuales en coordinación con el BCRP para la explicación del proceso de gestión del SOC y puntos de mejoras.

Este profesional debe contar con una experiencia mínima de dos (02) años en la función de mesa de ayuda y/o en la coordinación de solución de incidentes de TI.

Este profesional debe contar con alguna de las certificaciones o diplomados siguientes: ISO/IEC 27032 Lead CyberSecurity Manager y/o ISO/IEC 27001 Lead Auditor y/o ISO/IEC 27001 Lead Implementer y/o CISM1 y/o CISSP y/o PMP y/o ITIL y/o Service Desk Leader y/o gestión de proyectos y/o gerencia de proyectos.

Como requisito para la firma del contrato, el postor ganador de la buena pro deberá presentar lo siguiente:

- Copia simple de las certificaciones requeridas para el personal clave.
- Relación del personal clave. Esta relación deberá incluir como mínimo la siguiente información: nombres, apellidos, tipo y número de documento de identidad y el cargo que va a ocupar.
- Documentos adicionales solicitados para el personal clave.

El contratista no podrá modificar el equipo de trabajo señalado en su oferta (Personal Clave). En caso de cambio de algún personal, el reemplazo deberá cumplir como mínimo con las calificaciones y experiencia solicitadas en los Términos de Referencia y Requisitos de Calificación, previa comunicación y autorización del BCRP, para lo cual deberá presentar el respectivo sustento, teniendo como plazo máximo para efectuar el reemplazo, 48 horas luego de la aceptación del BCRP al personal propuesto.

NOTA: Los casos de reemplazos temporales por motivos personales que determinen su ausencia por unos días, se tratarán con suplencia de funciones por el personal ya presentado como Personal Clave para el servicio que cumpla con las mismas competencias y se verificará que cumplan con los requisitos de su puesto según lo indicado en el numeral 3.11.

No es permitido que los roles del personal de Jefe del proyecto SOC y Supervisor de Implementación SOC sean realizados por personal que cumpla los roles de Especialistas de implementación SOC, Coordinador SOC, Analista SOC, Especialista CSIRT y viceversa.

3.12. Roles Adicionales para el Servicio SOC

- Analistas SOC

Son los responsables de realizar actividades de análisis de los posibles incidentes a mayor profundidad, como parte de la capa de investigación, coordinando con el personal del BCRP y Especialistas CSIRT, para determinar la naturaleza de las amenazas y el impacto que genera en la infraestructura del BCRP. El servicio debe contar con personal suficiente garantizar la continuidad permanente del servicio y cumplir con el esquema de disponibilidad 24 x 7 x 365.

Estos profesionales deben contar con una experiencia mínima de dos (02) años en análisis de incidentes de ciberseguridad.

Estos profesionales deben contar con la certificación en la solución SIEM ofertada del servicio SOC.

- Especialistas CSIRT

Son los responsables de realizar actividades de respuesta a los incidentes más complejos y analizar datos forenses y de telemetría, así como información de ciberinteligencia para encontrar amenazas que pueden no haber sido identificadas previamente. El servicio debe contar con personal suficiente garantizar la continuidad permanente del servicio y cumplir con el esquema de disponibilidad 24 x 7 x 365.

Estos profesionales deben contar con una experiencia mínima de dos (02) años en respuesta a incidentes de ciberseguridad.

Estos profesionales deben contar con la certificación en la solución SIEM ofertada del servicio SOC.

NOTA: El BCRP en cualquier momento durante la ejecución contractual puede solicitar evidencia de las calificaciones de algún miembro del grupo de analista SOC o Analista CSIRT.

3.13. Mantenimiento Preventivo

El servicio deberá incluir el mantenimiento preventivo de todos los componentes de la solución, con una periodicidad de por lo menos una (01) vez cada seis (06) meses y quince (15) días antes de finalizar el contrato, dentro del periodo de servicio,

NOTA: Todas las herramientas que se requieran para realizar el servicio de mantenimiento preventivo, mesa de ayuda y soporte técnico local 24x7x365, deberán ser consideradas por los postores en su oferta.

NOTA: Se precisa que el mantenimiento preventivo de los componentes de la solución podrá realizarse de manera remota, excepto para los componentes on-premise que requieran intervención física, en cuyos casos el mantenimiento preventivo debe ser presencial y de acuerdo a las mejores prácticas del fabricante.

Considerar los siguientes aspectos:

Inspección

Comprende la revisión de la configuración establecida, las versiones de software de los componentes empleados y el estado de operación de la solución.

NOTA: Cuando nos referimos a solución, comprende a toda la infraestructura, plataformas, herramientas y componentes que conforman la prestación del servicio SOC Gestionado, incluyendo aquellos inicialmente propuestos y cualquier variación, actualización o reemplazo que se efectúe durante el periodo de ejecución del contrato.

Entregables

a) Informe de inspección

El proveedor deberá presentar un informe en el cual deberá indicar el estado de operación de la solución, las actualizaciones de software (nuevas versiones y parches) requeridas y recomendaciones para la optimización de la configuración.

b) Plan de actualización y optimización

El proveedor presentará un plan de ejecución para la instalación de las actualizaciones de software (nuevas versiones y parches) requeridas y la aplicación de recomendaciones para la optimización de la configuración. Dicho plan deberá incluir el detalle de las tareas a realizar, su duración estimada, los responsables de las mismas (BCRP/Proveedor), así como los riesgos implicados y medidas de mitigación consideradas.

Ejecución

Comprende la ejecución del plan de actualización y optimización.

Entregables

c) Informe de actualización y optimización

El proveedor deberá presentar un informe con los resultados de las acciones realizadas.

Nota:

Los entregables estarán sujetos a la revisión y conformidad por parte del BCRP.

3.14. Actualizaciones de software e Infraestructura

3.14.1. El proveedor deberá proporcionar el acceso, autorizado por el fabricante, a las actualizaciones del software y firmware de la infraestructura provista, lo cual deberá incluir el suministro de nuevas versiones (releases) y reparaciones (denominadas comercialmente como parches, temporary fixes y updates) para la de implementada.

3.14.2. El proveedor deberá notificar al BCRP, mediante correo electrónico y/o boletines de la marca de ser el caso, respecto a las actualizaciones de software y firmware de la infraestructura que libere el fabricante y cuya aplicación sea recomendada o requerida.

3.14.3. El proveedor deberá ejecutar previa coordinación con el BCRP las actualizaciones de software y firmware de la infraestructura que libera el fabricante y cuya aplicación sean recomendada o requerida.

3.15. Vigencia Tecnológica

3.15.1. En caso de presentarse, en cualquier momento anterior a la entrega definitiva de la solución, versiones nuevas de cualquiera de los componentes de la misma, se deberán entregar tales elementos actualizados, sin costo adicional, contando con autorización previa del BCRP.

3.15.2. Si durante el periodo de servicio el fabricante realiza un cambio de denominación del licenciamiento, suscripciones y servicios que fueron implementados, deberán proporcionarse los componentes equivalentes necesarios para mantener el cumplimiento de las prestaciones contratadas y sin costo adicional para el BCRP.

3.16. Implementación del Servicio

3.16.1. Para la implementación de la Fase 1 se deberá considerar la siguiente información

referencial:

- Actualmente se cuenta con 44 fuentes de datos (Datasources). Entre los Datasources empleados tenemos: NGFW, AntiDDoS, WAF, Antispam, Antimalware, EDR, Web Proxy, Switches de Core, Wireless Controllers, VPN Gateway, Link Balancers, Microsoft Active Directory, entre otros que serán entregados al proveedor a la firma de contrato. La información detallada (incluyendo marca, modelo y versión del producto, así como la dirección IP que se utilizará para la conexión) se entregará dentro de los diez (10) días calendario posteriores a la firma del contrato.
- Se precisa que se cuenta con un aproximado de 1100 cuentas de usuario en Active Directory.
- Se tiene un promedio de 122 a 179 casos de investigación mensuales que requieren intervención manual.
- Se precisa que se cuenta con un aproximado de 2300 endpoints bajo el alcance de la solución EDR.

3.16.2. Para la implementación de la Fase 2 se deberá considerar la siguiente información referencial:

Nombre	Descripción	Alcance EPS
Fase 2	Contempla el monitoreo de 159 Data Sources, 60 ubicados en el Data Center 1, 2 y 3; 99 Ubicados en el Data Center 4 y 5.	Hasta 10000 EPS

3.16.3. Las configuraciones requeridas en los Datasources para su integración con los componentes colectores serán responsabilidad del proveedor y el BCRP.

3.16.4. Como parte de la implementación se deberán considerar las actividades siguientes:

I. Consideraciones para la gestión y soporte

a) Planificación del servicio para identificación, detección y alerta de incidentes en conjunto con el equipo del BCRP.

b) Diez (10) días calendario, luego de la entrega de la información detallada de los Datasources, según numeral 3.7.22, el proveedor presentara un plan de implementación, el mismo que estará sujeto a la revisión y ratificación por parte del BCRP, de tal modo que cubra todas las tareas a llevar a cabo para la implementación del servicio.

NOTA: Se precisa que el Banco responderá en un plazo de hasta 7 días calendarios para la aprobación u observación del plan de implementación presentado.

El plan de implementación para cada fase deberá incluir lo siguiente:

- ✓ La documentación descriptiva del servicio, indicando en forma detallada los componentes empleados por el mismo.
- ✓ Los plazos mínimos y máximos para cada una de las tareas a cumplir, debiéndose discriminar las que deberá cumplir el BCRP, el proveedor en forma exclusiva, y las que deben asumir en forma compartida.
- ✓ Requerimientos de conectividad (accesos de red, ancho de banda, entre otros), para la operación del componente colector de datos.
- ✓ Los requerimientos técnicos que deben cumplir las instalaciones físicas para el correcto montaje y funcionamiento de los servidores empleados por el componente colector.
- ✓ Los procedimientos de configuración en los Datasources del BCRP, requeridos para su integración con el componente colector.

c) La aceptación del plan de implementación será mediante la firma del acta de conformidad de implantación.

d) Implementación de un dashboard de KPIs (indicadores del servicio gestionado).

e) Realizar la implementación del servicio, incluyendo:

- ✓ Implementación de los componentes colectores, incluyendo su configuración para la integración de los Datasources del BCRP.
- ✓ En el caso de no contar con integración nativa con algún Datasource en particular, deberá desarrollarse dicha integración sin costo adicional.
- ✓ Configuración de casos de uso y alertas iniciales, que sean apropiadas según buenas prácticas y experiencia del servicio SOC en coordinación con BCRP.
- ✓ Configuración de reportes periódicos.

f) Al finalizar esta etapa el proveedor entregará, para ambas fases, al BCRP, en formato electrónico:

- ✓ El informe de implementación del servicio.
- ✓ La documentación de procesos, procedimientos y buenas prácticas a ser empleados en la operación del SOC. Entre los procesos a considerar tenemos: Clasificación de eventos y triaje, priorización y análisis, remediación y recuperación, así como evaluación y auditoría.
- ✓ Procedimiento de reporte de incidentes con el servicio brindado, incluyendo la Información de contacto y escalamiento.
- ✓ El acta final de conformidad de implementación del servicio SOC, será entregada a través de mesa de partes del BCRP (mesadepartesvirtual@bcrp.gob.pe) en atención al Departamento de Ciberdefensa.

II. Consideración para las operaciones con la solución SIEM

g) Habilitación de instancias e implementación de la solución SIEM.
h) Configuración e integración de los activos SIEM con los activos BCRP.
i) Migración de los casos de uso personalizados de la plataforma actual a la nueva plataforma, para lo cual el BCRP proporcionara la lógica de los actuales 24 casos de uso.

NOTA: Las actividades de migraciones comprenden la implementación completa, validación y puesta en operación de dichos casos de uso en la nueva solución SIEM que el contratista proponga e implemente como parte del servicio SOC Gestionado, a conformidad del Banco.

j) Creación de hasta diez (10) nuevos casos de uso, durante la Fase 1 del servicio.
k) Creación de hasta diez (10) nuevos casos de uso, durante la Fase 2 del servicio.
l) Para los 20 nuevos casos de uso, el proveedor deberá coordinarlos con el equipo de Ciberdefensa del BCRP.

NOTA: Según lo indicado en los literales i, j, k, l, el servicio iniciará en la Fase 1 con 24 casos de uso migrados del servicio SOC anterior, pudiendo aumentar durante la ejecución del servicio esta cantidad hasta 34 casos de uso considerando la adición de los 10 casos de uso personalizados de la Fase 1.
En la Fase 2 pudiendo aumentar durante la ejecución del servicio esta cantidad hasta 44 casos de uso considerando la adición de los 10 casos de uso personalizados de la Fase 2.
NOTA: Se han integrado hasta 10 Data Sources y se han generado doce (12) casos de uso en los últimos 6 meses.

m) Creación de dashboard de casos de uso para uso del BCRP.

Operaciones de alertamiento

n) Creación de alertas de casos de uso
o) Creación de procedimientos automáticos para alertar las anomalías.
p) Verificación de falsos positivos, de modo que se optimicen, las alertas al BCRP.

Entrega de credenciales

q) Entrega de credenciales al BCRP para acceder al dashboard del Servicio SOC.

3.17. Capacitación

3.17.1. <u>En la herramienta SIEM- Servicio SOC Gestionado</u>

Capacitación para seis (06) personas, como mínimo de dieciséis (16) horas, de la solución SIEM que utiliza el servicio SOC Gestionado basado en el material oficial; puede realizarse de manera presencial y/o virtual en coordinación con el BCRP en dos grupos.

Los puntos por cubrir en la capacitación son como mínimo:

- Administración y operaciones de la solución SIEM.
- Flujo de trabajo del servicio de Ciber inteligencia implementado.
- Flujo de trabajo de la respuesta ante incidentes de seguridad.
- Ciclo de vida de un incidente.

El contratista será responsable del contenido y material didáctico necesario y se deben incluir las constancias de participación correspondientes.

3.17.2. <u>En seguridad ofensiva y operaciones en un SOC</u>

Curso oficial de Security Operations and Defensive Analysis SOC-200 (OSDA) y constancia de participación del curso para seis (06) personas en modalidad asíncrono, con una duración de horas recomendada por la marca.

Las capacitaciones serán dictados de manera virtual y/o presencial, en idioma español o inglés. Para las capacitaciones virtuales, el contratista brindará el acceso mediante una plataforma virtual. En caso de que las capacitaciones sean presenciales, el contratista brindará el acceso sus oficinas para su realización. El horario será definido en coordinación con el Banco.

3.18. Lugar de Ejecución de la Prestación

La implementación del servicio se realizará en 2 fases y abarca 5 Data Centers.

Nombre	Descripción	Dirección
Data Center 1	Ubicado en la OP del BCRP	Jr. Santa Rosa 441
Data Center 2	Ubicado en el local del Reserclub del BCRP	Cl. Diego de Medina 295, Pueblo Libre
Data Center 3	Ubicado en el local de la sucursal Piura	
Data Center 4	Ubicado en el local de Jr. Carabaya	Jr. Carabaya 698
Data Center 5	Ubicado en el local del Reserclub del BCRP	Cl. Diego de Medina 295, Pueblo Libre

Nota: Se precisa que para trabajos de implementación y atención de soporte a la infraestructura puesta para el servicio SOC en el Data Center 3 serán con conexión remota.

3.19. Subcontratación

El contratista puede subcontratar, previa autorización del BCRP, la ejecución de determinadas prestaciones del contrato hasta el porcentaje que establezca el reglamento. El contratista no puede subcontratar las prestaciones principales y esenciales del contrato.

El contratista tiene la responsabilidad por la ejecución total del contrato materia del servicio del concurso frente al BCRP.

3.20. Confidencialidad

El contratista, subcontratistas (en caso aplique) y su personal clave firmarán acuerdos de confidencialidad (Anexos N° 10 y 11) a fin de mantener en reserva, y no revelar a terceros, sin autorización escrita del BCRP, la información que le sea suministrada por este último o a la cual tenga acceso, excepto en cuanto resultare estrictamente necesario para el cumplimiento del contrato, y que restringirá la revelación de dicha información sólo a sus empleados y subcontratistas, sobre la base de "necesidad de conocer".

Los acuerdos de confidencialidad se firmarán junto con la suscripción del contrato.

3.21. Forma de pago

El pago se efectuará de la siguiente forma:

Prestación principal

- ✓ Costos fijos

No incluyen las horas de respuesta a incidentes, adicionales a la bolsa de doce (12) horas mensuales.

Descripción	Fase	Forma de pago
Implementación del servicio	Fase 1	Único pago, equivalente al 4%, del monto total correspondiente a los costos fijos de la fase 1 de la prestación principal. NOTA: El pago será realizado una vez culminado la implementación.
	Fase 2	Único pago, equivalente al 4.06%, del monto total correspondiente a los costos fijos de la fase 2 de la prestación principal. NOTA: El pago será realizado una vez culminado la implementación.
Ejecución del servicio	Fase 1	En forma mensual, en 15 pagos equivalentes al 6.4% del monto total correspondiente a los costos fijos de la fase 1 de la prestación principal.
	Fase 2	En forma mensual, en 9 pagos equivalentes al 10.66% del monto total correspondiente a los costos fijos de la fase 2 de la prestación principal.

- ✓ Costo variable

	Descripción	Forma de pago
Fase 1	Horas de respuesta a incidentes, adicionales a la bolsa de doce (12) horas mensuales contratadas. Bolsa estimada de 12* horas. Nota: *No es un tope de consumo de horas y tampoco un consumo fijo, sino es una cantidad estimada adicional para toda la fase 1. Este excedente a las horas contratadas sirve para fines de cálculo para el monto total de la fase 1.	En forma mensual, según informe de sustento de incremento de horas aprobado por el BCRP.
	Incremento de EPS a los 5000 contratados, según consumo. Bolsa estimada de 1000* EPS adicionales. Nota:	En forma mensual, según informe de sustento de incremento de EPS aprobado por el BCRP.

	*No es un tope de consumo de EPS y tampoco un consumo fijo, sino es una cantidad estimada adicional para toda la fase 1, este excedente a los EPS contratados sirve para fines de cálculo para el monto total de la fase 1.	
Fase 2	Horas de respuesta a incidentes, adicionales a la bolsa de doce (12) horas mensuales contratadas. Bolsa estimada de 12* horas. Nota: *No es un tope de consumo de horas y tampoco un consumo fijo, sino es una cantidad estimada adicional para toda la fase 2, este excedente a las horas contratadas sirve para fines de cálculo para el monto total de la fase 2.	En forma mensual, según informe de sustento de incremento de horas aprobado por el BCRP
	Incremento de EPS a los 10000 contratados, según consumo. Bolsa estimada de 1000* EPS adicionales. Nota: *No es un tope de consumo de EPS y tampoco un consumo fijo, sino es una cantidad estimada adicional para toda la fase 2, este excedente a los EPS contratados sirve para fines de cálculo para el monto total de la fase 2.	En forma mensual, según informe de sustento de incremento de EPS aprobado por el BCRP.

NOTA: El informe de sustento se refiere al Informe Técnico Mensual mencionado en el numeral 3.10 de los términos de referencia en el que se detallará el incremento de horas y EPS.

Prestación accesoria

Descripción	Fase	Forma de pago
Servicio de mantenimiento preventivo, mesa de ayuda y soporte técnico local 24 x 7 x 365	Fase 1	En forma mensual, en 15 pagos iguales correspondiente al monto de este servicio de la prestación accesoria de la fase 1.
	Fase 2	En forma mensual, en 9 pagos iguales correspondiente al concepto de este servicio de la prestación accesoria de la fase 2.
Capacitación	Fase 1	El 100% del monto correspondiente a este concepto a la conformidad de su realización.

3.2. REQUISITOS DE CALIFICACIÓN

<table>
<tr><td>A</td><td>CAPACIDAD TÉCNICA Y PROFESIONAL</td></tr>
<tr><td>A.1</td><td>EXPERIENCIA DEL PERSONAL CLAVE</td></tr>
<tr><td></td><td>Requisitos:

- Jefe del proyecto SOC
Contar con una experiencia mínima de tres (03) años en la gestión de servicios SOC en el rubro financiero.

- Supervisor de Implementación SOC
Contar con una experiencia mínima de tres (03) años en la gestión de proyectos de Tecnologías de Información y/o proyectos de seguridad informática.

- Dos Especialistas de implementación SOC (02)
Contar con una experiencia mínima de cuatro (04) años en la implementación o ejecución de servicio SOC.

- Coordinador SOC
Contar con una experiencia mínima de dos (02) años en la función de mesa de ayuda y/o en la coordinación de solución de incidentes de TI.

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

Acreditación:

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

Importante

• Los documentos que acreditan la experiencia deben incluir los nombres y apellidos del personal clave, el cargo desempeñado, el plazo de la prestación indicando el día, mes y año de inicio y culminación, el nombre de la Entidad u organización que emite el documento, la fecha de emisión y nombres y apellidos de quien suscribe el documento.

• En caso los documentos para acreditar la experiencia establezcan el plazo de la experiencia adquirida por el personal clave en meses sin especificar los días se debe considerar el mes completo.

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

• Al calificar la experiencia del personal, se debe valorar de manera integral los documentos presentados por el postor para acreditar dicha experiencia. En tal sentido, aun cuando en los documentos presentados la denominación del cargo o puesto no coincida literalmente con aquella prevista en las bases, se deberá validar la experiencia si las actividades que realizó el personal corresponden con la función propia del cargo o puesto requerido en las bases.</td></tr>
<tr><td>B</td><td>EXPERIENCIA DEL POSTOR EN LA ESPECIALIDAD</td></tr>
</table>

	Requisitos: El postor debe acreditar un monto facturado acumulado equivalente a S/ 2 000 000 (Dos millones con 00/100 Soles) por la contratación de servicios iguales o similares al objeto de la convocatoria, durante los ocho (8) años anteriores a la fecha de la presentación de ofertas que se computarán desde la fecha de la conformidad o emisión del comprobante de pago, según corresponda. Se consideran servicios similares a los siguientes: - Servicio de CYBERSOC. - Servicio de monitoreo de eventos de seguridad (SOC). - Servicios de Centro de Operaciones de Seguridad (SOC). - Servicio de Inteligencia de Amenazas en la Red. - Servicio de soporte a través de SOC (Security Opera Center), monitoreo y correlación de eventos para infraestructura de red y seguridad. - Servicio de ciberseguridad. - Servicio de detección y respuesta ante amenazas. - Servicio de operación de la seguridad y servicio De CyberSOC. - Servicio de gestión de eventos e incidentes de seguridad. - Servicio de Monitoreo & Alerta Temprana (CyberSOC). - Solución de análisis, detección y respuesta ante Amenazas de Seguridad Informática en la red interna. Acreditación: La experiencia del postor en la especialidad se acreditará con copia simple de (i) contratos u órdenes de servicios, y su respectiva conformidad o constancia de prestación; o (ii) comprobantes de pago cuya cancelación se acredite documental y fehacientemente, con voucher de depósito, nota de abono, reporte de estado de cuenta, cualquier otro documento emitido por Entidad del sistema financiero que acredite el abono o mediante cancelación en el mismo comprobante de pago[10], correspondientes a un máximo de veinte (20) contrataciones. En caso los postores presenten varios comprobantes de pago para acreditar una sola contratación, se debe acreditar que corresponden a dicha contratación; de lo contrario, se asumirá que los comprobantes acreditan contrataciones independientes, en cuyo caso solo se considerará, para la evaluación, las veinte (20) primeras contrataciones indicadas en el **Anexo Nº 7** referido a la Experiencia del Postor en la Especialidad. En el caso de servicios de ejecución periódica o continuada, solo se considera como experiencia la parte del contrato que haya sido ejecutada durante los ocho (8) años anteriores a la fecha de presentación de ofertas, debiendo adjuntarse copia de las conformidades correspondientes a tal parte o los respectivos comprobantes de pago cancelados. En los casos que se acredite experiencia adquirida en consorcio, debe presentarse la promesa de consorcio o el contrato de consorcio del cual se desprenda fehacientemente el porcentaje de las obligaciones que se asumió en el contrato presentado; de lo contrario, no se computará la experiencia proveniente de dicho contrato. Asimismo, cuando se presenten contratos derivados de procesos de selección convocados antes del 20.09.2012, la calificación se ceñirá al método descrito en la Directiva "Participación de Proveedores en Consorcio en las Contrataciones del Estado", debiendo presumirse que el porcentaje de las obligaciones equivale al porcentaje de participación de la promesa de consorcio o del contrato de consorcio. En caso que en dichos documentos no se consigne el porcentaje de participación se presumirá que las obligaciones se ejecutaron en partes iguales. Si el titular de la experiencia no es el postor, consignar si dicha experiencia corresponde a la matriz en caso que el postor sea sucursal, o fue transmitida por reorganización societaria, debiendo acompañar la documentación sustentatoria correspondiente.

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

> *"… el solo sello de cancelado en el comprobante, cuando ha sido colocado por el propio postor, no puede ser considerado como una acreditación que produzca fehaciencia en relación a que se encuentra cancelado. Admitir ello equivaldría a considerar como válida la sola declaración del postor afirmando que el comprobante de pago ha sido cancelado"*
> *(…)*
> *"Situación diferente se suscita ante el sello colocado por el cliente del postor [sea utilizando el término "cancelado" o "pagado"] supuesto en el cual sí se contaría con la declaración de un tercero que brinde certeza, ante la cual debiera reconocerse la validez de la experiencia".*

	Si el postor acredita experiencia de otra persona jurídica como consecuencia de una reorganización societaria, debe presentar adicionalmente el **Anexo N° 8.** Cuando en los contratos, órdenes de servicios o comprobantes de pago el monto facturado se encuentre expresado en moneda extranjera, debe indicarse el tipo de cambio venta publicado por la Superintendencia de Banca, Seguros y AFP correspondiente a la fecha de suscripción del contrato, de emisión de la orden de servicios o de cancelación del comprobante de pago, según corresponda. Sin perjuicio de lo anterior, los postores deben llenar y presentar el **Anexo Nº 7** referido a la Experiencia del Postor en la Especialidad. **Importante** • *Al calificar la experiencia del postor, se debe valorar de manera integral los documentos presentados por el postor para acreditar dicha experiencia. En tal sentido, aun cuando en los documentos presentados la denominación del objeto contractual no coincida literalmente con el previsto en las bases, se deberá validar la experiencia si las actividades que ejecutó el postor corresponden a la experiencia requerida.* • *En el caso de consorcios, solo se considera la experiencia de aquellos integrantes que se hayan comprometido, según la promesa de consorcio, a ejecutar el objeto materia de la convocatoria, conforme a la Directiva "Participación de Proveedores en Consorcio en las Contrataciones del Estado".*

Importante

- *Si como resultado de una consulta u observación corresponde precisarse o ajustarse el requerimiento, se solicita la autorización del área usuaria y se pone de conocimiento de tal hecho a la dependencia que aprobó el expediente de contratación, de conformidad con el numeral 72.3 del artículo 72 del Reglamento.*

- *El cumplimiento de los Términos de Referencia se realiza mediante la presentación de una declaración jurada. De ser el caso, adicionalmente la Entidad puede solicitar documentación que acredite el cumplimiento del algún componente de estos. Para dicho efecto, consignará de manera detallada los documentos que deben presentar los postores en el literal e) del numeral 2.2.1.1 de esta sección de las bases.*

- *Los requisitos de calificación determinan si los postores cuentan con las capacidades necesarias para ejecutar el contrato, lo que debe ser acreditado documentalmente, y no mediante declaración jurada.*

CAPÍTULO IV
FACTORES DE EVALUACIÓN

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

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

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

Importante

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

CAPÍTULO V
PROFORMA DEL CONTRATO

Conste por el presente documento, la CONTRATACIÓN DEL SERVICIO DE UN SOC (SECURITY OPERATIONS CENTER) GESTIONADO PARA EL MONITOREO DE EVENTOS DE CIBERSEGURIDAD, que celebra de una parte el Banco Central de Reserva del Perù, en adelante LA ENTIDAD, con RUC Nº 20122476309, con domicilio legal en jiròn Santa Rosa 441 -445, Lima, representada por [……..…], identificado con DNI Nº [……], y de otra parte […….....], con RUC Nº [.....], con domicilio legal en […….....], inscrita en la Ficha N° […….....] Asiento N° […….....] del Registro de Personas Jurídicas de la ciudad de [……], debidamente representado por su Representante Legal, […….....], con DNI N° [……..], según poder inscrito en la Ficha N° [……..], Asiento N° [……] del Registro de Personas Jurídicas de la ciudad de [……], a quien en adelante se le denominará EL CONTRATISTA en los términos y condiciones siguientes:

CLÁUSULA PRIMERA: ANTECEDENTES

Con fecha [……..], el comité de selección adjudicó la buena pro del **CONCURSO PÚBLICO Nº CP 0009-2025-BCRPLIM** para la CONTRATACIÓN DEL SERVICIO DE UN SOC (SECURITY OPERATIONS CENTER) GESTIONADO PARA EL MONITOREO DE EVENTOS DE 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 UN SOC (SECURITY OPERATIONS CENTER) GESTIONADO PARA EL MONITOREO DE EVENTOS DE 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 PAGO[11]

LA ENTIDAD se obliga a pagar la contraprestación a EL CONTRATISTA en [INDICAR MONEDA] en pagos parciales**,** 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, de acuerdo con el siguiente detalle:

Prestación principal

- ✓ Costos fijos
  No incluyen las horas de respuesta a incidentes, adicionales a la bolsa de doce (12) horas mensuales.

Descripción	Fase	Forma de pago
Implementación del servicio	Fase 1	Único pago, equivalente al 4%, del monto total correspondiente a los costos fijos de la fase 1 de la prestación principal.
	Fase 2	Único pago, equivalente al 4%, del monto total correspondiente a los costos fijos de la fase 2 de la prestación principal.

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

Ejecución del servicio	Fase 1	En forma mensual, en 15 pagos equivalentes al 6.4% del monto total correspondiente a los costos fijos de la fase 1 de la prestación principal.
	Fase 2	En forma mensual, en 9 pagos equivalentes al 10.66% del monto total correspondiente a los costos fijos de la fase 2 de la prestación principal.

✓ Costo variable

	Descripción	**Forma de pago**
Fase 1	Horas de respuesta a incidentes, adicionales a la bolsa de doce (12) horas mensuales contratadas. Bolsa estimada de 12* horas. Nota: *No es un tope de consumo de horas y tampoco un consumo fijo, sino es una cantidad estimada adicional para toda la fase 1. Este excedente a las horas contratadas sirve para fines de cálculo para el monto total de la fase 1.	En forma mensual, según informe de sustento de incremento de horas aprobado por el BCRP.
	Incremento de EPS a los 5000 contratados, según consumo. Bolsa estimada de 1000* EPS adicionales. Nota: *No es un tope de consumo de EPS y tampoco un consumo fijo, sino es una cantidad estimada adicional para toda la fase 1, este excedente a los EPS contratados sirve para fines de cálculo para el monto total de la fase 1.	En forma mensual, según informe de sustento de incremento de EPS aprobado por el BCRP.
Fase 2	Horas de respuesta a incidentes, adicionales a la bolsa de doce (12) horas mensuales contratadas. Bolsa estimada de 12* horas. Nota: *No es un tope de consumo de horas y tampoco un consumo fijo, sino es una cantidad estimada adicional para toda la fase 2, este excedente a las horas contratadas sirve para fines de cálculo para el monto total de la fase 2.	En forma mensual, según informe de sustento de incremento de horas aprobado por el BCRP
	Incremento de EPS a los 10000 contratados, según consumo. Bolsa estimada de 1000* EPS adicionales. Nota: *No es un tope de consumo de EPS y tampoco un consumo fijo, sino es una cantidad estimada adicional para toda la fase 2, este excedente a los EPS contratados sirve para fines de cálculo para el monto total de la fase 2.	En forma mensual, según informe de sustento de incremento de EPS aprobado por el BCRP.

Prestación accesoria

Descripción	**Fase**	**Forma de pago**

Servicio de mantenimiento preventivo, mesa de ayuda y soporte técnico local 24 x 7 x 365	Fase 1	En forma mensual, en 15 pagos iguales correspondiente al monto de este servicio de la prestación accesoria de la fase 1.
	Fase 2	En forma mensual, en 9 pagos iguales correspondiente al concepto de este servicio de la prestación accesoria de la fase 2.
Capacitación	Fase 1	El 100% del monto correspondiente a este concepto a la conformidad de su realización.

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

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

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

CLÁUSULA QUINTA: DEL PLAZO DE LA EJECUCIÓN DE LA PRESTACIÓN

El plazo de ejecución del presente contrato es de [……..], 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 ULTIMO CASO].

CLÁUSULA SEXTA: PRESTACIONES ACCESORIAS[12]

"Las prestaciones accesorias tienen por objeto [CONSIGNAR EL OBJETO DE LAS PRESTACIONES ACCESORIAS].

El monto de las prestaciones accesorias asciende a [CONSIGNAR MONEDA Y MONTO], que incluye todos los impuestos de Ley.

El plazo de ejecución de las prestaciones accesorias es de [……..], el mismo que se computa desde [CONSIGNAR SI ES DEL DÍA SIGUIENTE DEL CUMPLIMIENTO DE LAS PRESTACIONES PRINCIPALES, 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 DE LAS PRESTACIONES ACCESORIAS, DEBIENDO INDICAR LAS MISMAS EN ESTE ULTIMO CASO].

[DE SER EL CASO, INCLUIR OTROS ASPECTOS RELACIONADOS A LA EJECUCIÓN DE LAS PRESTACIONES ACCESORIAS]."

CLÁUSULA SÉTIMA: PARTES INTEGRANTES DEL CONTRATO

[12] De conformidad con la Directiva sobre prestaciones accesorias, los contratos relativos al cumplimiento de la(s) prestación(es) principal(es) y de la(s) prestación(es) accesoria(s), pueden estar contenidos en uno o dos documentos. En el supuesto que ambas prestaciones estén contenidas en un mismo documento, estas deben estar claramente diferenciadas, debiendo indicarse entre otros aspectos, el precio y plazo de cada prestación.

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

CLÁUSULA OCTAVA: GARANTÍAS

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

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

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

En el caso que corresponda, consignar lo siguiente:

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

Importante
Al amparo de lo dispuesto en el numeral 151.2 del artículo 151 del Reglamento de la Ley de Contrataciones del Estado, si el postor ganador de la buena pro solicita la retención del diez por ciento (10%) del monto del contrato de la prestación accesoria como garantía de fiel cumplimiento de prestaciones accesorias, debe consignarse lo siguiente: • *"De fiel cumplimiento por prestaciones accesorias:* [CONSIGNAR EL MONTO]*, a través de la retención que debe efectuar LA ENTIDAD, durante la primera mitad del número total de pagos a realizarse, de forma prorrateada, con cargo a ser devuelto a la finalización del mismo."*

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

CLÁUSULA NOVENA: EJECUCIÓN DE GARANTÍAS POR FALTA DE RENOVACIÓN

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

CLÁUSULA DÉCIMA: CONFORMIDAD DE LA PRESTACIÓN DEL SERVICIO

La conformidad de la prestación del servicio se regula por lo dispuesto en el artículo 168 del Reglamento de la Ley de Contrataciones del Estado. La conformidad será otorgada por el Departamento de Ciberseguridad en el plazo máximo de siete (7) días de producida la recepción.

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

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

CLÁUSULA UNDÉCIMA: DECLARACIÓN JURADA DEL CONTRATISTA

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

CLÁUSULA DUODÉCIMA: RESPONSABILIDAD POR VICIOS OCULTOS

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

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

CLÁUSULA DÉCIMA TERCERA: PENALIDADES

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

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

Donde:

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

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

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

Esta penalidad se deduce 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.

Este tipo de penalidad pueden alcanzar cada una un monto máximo equivalente al diez por ciento (10%) del monto del contrato vigente.

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

CLÁUSULA DÉCIMA CUARTA: RESOLUCIÓN DEL CONTRATO

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

CLÁUSULA DÉCIMA QUINTA: RESPONSABILIDAD DE LAS PARTES

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

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

CLÁUSULA DÉCIMA SEXTA: ANTICORRUPCIÓN

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

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

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

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

CLÁUSULA DÉCIMA SÉTIMA: MARCO LEGAL DEL CONTRATO

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

CLÁUSULA DÉCIMA OCTAVA: SOLUCIÓN DE CONTROVERSIAS[13]

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

[13] 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).

acuerdo entre ambas partes o se llegue a un acuerdo parcial. Las controversias sobre nulidad del contrato solo pueden ser sometidas a arbitraje.

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

CLÁUSULA DÉCIMA NOVENA: FACULTAD DE ELEVAR A ESCRITURA PÚBLICA
Cualquiera de las partes puede elevar el presente contrato a Escritura Pública corriendo con todos los gastos que demande esta formalidad.

CLÁUSULA VIGÉSIMA: DOMICILIO PARA EFECTOS DE LA EJECUCIÓN CONTRACTUAL
Las partes declaran el siguiente domicilio para efecto de las notificaciones que se realicen durante la ejecución del presente contrato:

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

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

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

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

"LA ENTIDAD" "EL CONTRATISTA"

Importante

Este documento puede firmarse digitalmente si ambas partes cuentan con firma digital, según la Ley Nº 27269, Ley de Firmas y Certificados Digitales[14].

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

ANEXOS

ANEXO Nº 1

DECLARACIÓN JURADA DE DATOS DEL POSTOR

Señores
COMITÉ DE SELECCIÓN
CONCURSO PÚBLICO Nº CP 0009-2025-BCRPLIM
Presente.-

El que se suscribe, [……..], postor y/o Representante Legal de [CONSIGNAR EN CASO DE SER PERSONA JURÍDICA], identificado con [CONSIGNAR TIPO DE DOCUMENTO DE IDENTIDAD] N° [CONSIGNAR NÚMERO DE DOCUMENTO DE IDENTIDAD], con poder inscrito en la localidad de [CONSIGNAR EN CASO DE SER PERSONA JURÍDICA] en la Ficha Nº [CONSIGNAR EN CASO DE SER PERSONA JURÍDICA] Asiento Nº [CONSIGNAR EN CASO DE SER PERSONA JURÍDICA], **DECLARO BAJO JURAMENTO** que la siguiente información se sujeta a la verdad:

Nombre, Denominación o Razón Social :					
Domicilio Legal :					
RUC :	Teléfono(s) :				
MYPE[15]		Sí		No	
Correo electrónico :					

Autorización de notificación por correo electrónico:

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

1. Solicitud de la descripción a detalle de todos los elementos constitutivos de la oferta.
2. Solicitud de reducción de la oferta económica.
3. Solicitud de subsanación de los requisitos para perfeccionar el contrato.
4. Solicitud para presentar los documentos para perfeccionar el contrato, según orden de prelación, de conformidad con lo previsto en el artículo 141 del Reglamento.
5. Respuesta a la solicitud de acceso al expediente de contratación.
6. Notificación de la orden de servicios[16]

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.

[15] Esta información será verificada por la Entidad en la página web del Ministerio de Trabajo y Promoción del Empleo en la sección consulta de empresas acreditadas en el REMYPE en el link http://www2.trabajo.gob.pe/servicios-en-linea-2-2/ y se tendrá en consideración, en caso el postor ganador de la buena pro solicite la retención del diez por ciento (10%) del monto del contrato, en calidad de garantía de fiel cumplimiento, en los contratos periódicos de prestación de servicios, según lo señalado en el numeral 149.4 del artículo 149 y numeral 151.2 del artículo 151 del Reglamento.

[16] Consignar en el caso de procedimientos de selección por relación de ítems, cuando el monto del valor estimado del ítem no supere los doscientos mil Soles (S/ 200 000.00), cuando se haya optado por perfeccionar el contrato con una orden de servicios.

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

ANEXO Nº 1

DECLARACIÓN JURADA DE DATOS DEL POSTOR

Señores
COMITÉ DE SELECCIÓN
CONCURSO PÚBLICO Nº CP 0009-2025-BCRPLIM
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[17]		Sí		No	
Correo electrónico :					

Datos del consorciado 2					
Nombre, Denominación o Razón Social :					
Domicilio Legal :					
RUC :	Teléfono(s) :				
MYPE[18]		Sí		No	
Correo electrónico :					

Datos del consorciado …					
Nombre, Denominación o Razón Social :					
Domicilio Legal :					
RUC :	Teléfono(s) :				
MYPE[19]		Sí		No	
Correo electrónico :					

Autorización de notificación por correo electrónico:

Correo electrónico del consorcio:

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

1. Solicitud de la descripción a detalle de todos los elementos constitutivos de la oferta.
2. Solicitud de reducción de la oferta económica.
3. Solicitud de subsanación de los requisitos para perfeccionar el contrato.

[17] En los contratos periódicos de prestación de servicios, esta información será verificada por la Entidad en la página web del Ministerio de Trabajo y Promoción del Empleo en la sección consulta de empresas acreditadas en el REMYPE en el link http://www2.trabajo.gob.pe/servicios-en-linea-2-2/ y se tendrá en consideración, en caso el consorcio ganador de la buena pro solicite la retención del diez por ciento (10%) del monto del contrato, en calidad de garantía de fiel cumplimiento, según lo señalado en el numeral 149.4 del artículo 149 y numeral 151.2 del artículo 151 del Reglamento. Para dicho efecto, todos los integrantes del consorcio deben acreditar la condición de micro o pequeña empresa.

[18] Ibídem.

[19] Ibídem.

4. Solicitud para presentar los documentos para perfeccionar el contrato, según orden de prelación, de conformidad con lo previsto en el artículo 141 del Reglamento.
5. Respuesta a la solicitud de acceso al expediente de contratación.
6. Notificación de la orden de servicios[20]

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.

[20] Consignar en el caso de procedimientos de selección por relación de ítems, cuando el monto del valor estimado del ítem no supere los doscientos mil Soles (S/ 200 000.00), cuando se haya optado por perfeccionar el contrato con una orden de servicios.

ANEXO Nº 2

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

Señores
COMITÉ DE SELECCIÓN
CONCURSO PÚBLICO Nº CP 0009-2025-BCRPLIM
Presente.-

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

i. No haber incurrido y me obligo a no incurrir en actos de corrupción, así como a respetar el principio de integridad.

ii. No tener impedimento para postular en el procedimiento de selección ni para contratar con el Estado, conforme al artículo 11 de la Ley de Contrataciones del Estado.

iii. Conocer las sanciones contenidas en la Ley de Contrataciones del Estado y su Reglamento, así como las disposiciones aplicables de la Ley N° 27444, Ley del Procedimiento Administrativo General.

iv. Participar en el presente proceso de contratación en forma independiente sin mediar consulta, comunicación, acuerdo, arreglo o convenio con ningún proveedor; y, conocer las disposiciones del Decreto Legislativo Nº 1034, Decreto Legislativo que aprueba la Ley de Represión de Conductas Anticompetitivas.

v. Conocer, aceptar y someterme a las bases, condiciones y reglas del procedimiento de selección.

vi. Ser responsable de la veracidad de los documentos e información que presento en el presente procedimiento de selección.

vii. Comprometerme a mantener la oferta presentada durante el procedimiento de selección y a perfeccionar el contrato, en caso de resultar favorecido con la buena pro.

[CONSIGNAR CIUDAD Y FECHA]

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

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

ANEXO Nº 3

DECLARACIÓN JURADA DE CUMPLIMIENTO DE LOS TÉRMINOS DE REFERENCIA

Señores
COMITÉ DE SELECCIÓN
CONCURSO PÚBLICO Nº CP 0009-2025-BCRPLIM
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 UN SOC (SECURITY OPERATIONS CENTER) GESTIONADO PARA EL MONITOREO DE EVENTOS DE 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 Nº 4

DECLARACIÓN JURADA DE PLAZO DE PRESTACIÓN DEL SERVICIO

Señores
COMITÉ DE SELECCIÓN
CONCURSO PÚBLICO Nº CP 0009-2025-BCRPLIM
Presente.-

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

Prestación principal

Descripción	Plazo
Implementación del servicio SOC Gestionado	Fase 1: Noventa (90) días calendarios contabilizados desde el día siguiente de la firma del contrato. Fase 2: Sesenta (60) días calendarios, comenzando a los 396 días calendarios (13 meses) de iniciada la ejecución de la Fase 1.

Descripción	Plazo
Ejecución del Servicio SOC Gestionado	Fase 1: El plazo de ejecución de esta fase será de 456 días calendarios (15 meses) contabilizados desde el día siguiente de terminada la implementación de la fase 1. Fase 2: El plazo de ejecución de esta fase será de 273 días calendarios (9 meses) contabilizados desde el día siguiente de terminada la implementación de la fase 2.

Prestación accesoria

Descripción	Plazo
Servicio de mantenimiento preventivo, mesa de ayuda y soporte técnico local 24x7x365	Fase 1: 456 días calendario (15 meses) contabilizados desde el día siguiente de terminada la implementación de la fase 1. Fase 2: 273 días calendarios (9 meses) contabilizados desde el día siguiente de terminada la implementación de la fase 2. Respecto al servicio de mantenimiento preventivo para ambas fases se programará con una periodicidad de por lo menos una (01) vez de forma semestral.

Descripción	Plazo
Ejecución de una Capacitación (de acuerdo con lo establecido en el numeral 3.17.	Noventa (90) días a partir del día siguiente del acta final de conformidad de implementación de la Fase 1.

[CONSIGNAR CIUDAD Y FECHA]

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

ANEXO Nº 5

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

Señores
COMITÉ DE SELECCIÓN
CONCURSO PÚBLICO Nº CP 0009-2025-BCRPLIM
Presente.-

Los suscritos declaramos expresamente que hemos convenido en forma irrevocable, durante el lapso que dure el procedimiento de selección, para presentar una oferta conjunta al **CONCURSO PÚBLICO Nº CP 0009-2025-BCRPLIM.**

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]	[%][21]
	[DESCRIBIR LAS OBLIGACIONES DEL CONSORCIADO 1]	
2.	OBLIGACIONES DE [NOMBRE, DENOMINACIÓN O RAZÓN SOCIAL DEL CONSORCIADO 2]	[%][22]
	[DESCRIBIR LAS OBLIGACIONES DEL CONSORCIADO 2]	
	TOTAL OBLIGACIONES	100%[23]

[CONSIGNAR CIUDAD Y FECHA]

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

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

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

.....	.....
Consorciado 1	**Consorciado 2**
Nombres, apellidos y firma del Consorciado 1	**Nombres, apellidos y firma del Consorciado 2**
o de su Representante Legal	**o de su Representante Legal**
Tipo y N° de Documento de Identidad	**Tipo y N° de Documento de Identidad**

Importante

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

ANEXO Nº 6

PRECIO DE LA OFERTA

Señores
COMITÉ DE SELECCIÓN
CONCURSO PÚBLICO Nº CP 0009-2025-BCRPLIM
Presente.-

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

Prestación principal

✓ Suma alzada

Concepto	Fase	Monto S/
Implementación del servicio	Fase 1	
	Fase 2	
Ejecución del servicio	Fase 1	
	Fase 2	

✓ Precios Unitarios

	Concepto	Cantidad	Precio Unitario	Monto S/
Fase 1	Bolsa estimada de 12 horas de respuesta a incidentes	12 horas		
	Bolsa estimada de 1000 EPS adicionales.	1000 EPS		
Fase 2	Bolsa estimada de 12 horas de respuesta a incidentes	12 horas		
	Bolsa estimada de 1000 EPS adicionales.	1000 EPS		

TOTAL PRESTACIÓN PRINCIPAL S/	

Prestación accesoria

Concepto	Fase	Monto S/
Servicio de mantenimiento preventivo, mesa de ayuda y soporte técnico local 24 x 7 x 365	Fase 1	
	Fase 2	
Capacitación	Fase 1	
TOTAL PRESTACIÓN ACCESORIA S/		

MONTO TOTAL S/ (PRINCIPAL + ACCESORIA)	

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

[CONSIGNAR CIUDAD Y FECHA]

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

Importante

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

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

ANEXO Nº 7

EXPERIENCIA DEL POSTOR EN LA ESPECIALIDAD

Señores
COMITÉ DE SELECCIÓN
CONCURSO PÚBLICO Nº CP 0009-2025-BCRPLIM
Presente.-

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

Nº	CLIENTE	OBJETO DEL CONTRATO	N° CONTRATO / O/S / COMPROBANTE DE PAGO	FECHA DEL CONTRATO O CP [24]	FECHA DE LA CONFORMIDAD DE SER EL CASO[25]	EXPERIENCIA PROVENIENTE[26] DE:	MONEDA	IMPORTE[27]	TIPO DE CAMBIO VENTA[28]	MONTO FACTURADO ACUMULADO [29]
1										
2										
3										
4										

[24] 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.

[25] Únicamente, cuando la fecha del perfeccionamiento del contrato, sea previa a los ocho (8) años anteriores a la fecha de presentación de ofertas, caso en el cual el postor debe acreditar que la conformidad se emitió dentro de dicho periodo.

[26] 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"*.

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

[28] 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.

[29] 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 [24]	FECHA DE LA CONFORMIDAD DE SER EL CASO[25]	EXPERIENCIA PROVENIENTE[26] DE:	MONEDA	IMPORTE[27]	TIPO DE CAMBIO VENTA[28]	MONTO FACTURADO ACUMULADO [29]
5										
6										
7										
8										
9										
10										
	…									
20										
TOTAL										

[CONSIGNAR CIUDAD Y FECHA]

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

ANEXO Nº 8

DECLARACIÓN JURADA
(NUMERAL 49.4 DEL ARTÍCULO 49 DEL REGLAMENTO)

Señores
COMITÉ DE SELECCIÓN
CONCURSO PÚBLICO Nº CP 0009-2025-BCRPLIM
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° 9

AUTORIZACIÓN DE NOTIFICACIÓN DE LA DECISIÓN DE LA ENTIDAD SOBRE LA SOLICITUD DE AMPLIACIÓN DE PLAZO MEDIANTE MEDIOS ELECTRÓNICOS DE COMUNICACIÓN

(DOCUMENTO A PRESENTAR EN EL PERFECCIONAMIENTO DEL CONTRATO)

Señores
COMITÉ DE SELECCIÓN
CONCURSO PÚBLICO Nº CP 0009-2025-BCRPLIM
Presente.-

El que se suscribe, [……..], postor adjudicado y/o Representante Legal de [CONSIGNAR EN CASO DE SER PERSONA JURÍDICA], identificado con [CONSIGNAR TIPO DE DOCUMENTO DE IDENTIDAD] N° [CONSIGNAR NÚMERO DE DOCUMENTO DE IDENTIDAD], autorizo que durante la ejecución del contrato se me notifique al correo electrónico [INDICAR EL CORREO ELECTRÓNICO] lo siguiente:

✓ Notificación de la decisión de la Entidad respecto a la solicitud de ampliación de plazo.

[CONSIGNAR CIUDAD Y FECHA]

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

Importante
La notificación de la decisión de la Entidad respecto a la solicitud de ampliación de plazo se efectúa por medios electrónicos de comunicación, siempre que se cuente con la autorización correspondiente y sea posible obtener un acuse de recibo a través del mecanismo utilizado.

ANEXO N° 10

ACUERDO DE CONFIDENCIALIDAD Y CAUTELA DE LA PROPIEDAD INTELECTUAL DEL BANCO CENTRAL DE RESERVA DEL PERÚ

Conste por el presente documento el Acuerdo de Confidencialidad y Cautela de la Propiedad Intelectual del Banco Central de Reserva del Perú, que suscriben por una parte el Banco Central de Reserva del Perú, en adelante **"EL BANCO"**, con Registro Único de Contribuyentes No. 20122476309, debidamente representado por el Subgerente de Logística, señor ....., con Documento Nacional de Identidad No .....; y por el Subgerente de Servicios de Tecnologías de Información, el señor ……., con Documento Nacional de Identidad N° ……, con domicilio en el Jr. Santa Rosa No. 441 - 445, Cercado de Lima, y de la otra parte, la empresa ……., en adelante La Empresa, con Registro Único del Contribuyente No. ……., representado por el señor ……., con Documento Nacional de Identidad No. ……., con domicilio en ..... según poder inscrito en la Partida N° ..... de los Registros Públicos de Lima, a quien en adelante se le denominará **"EL CONTRATISTA",** en los términos y condiciones siguientes:

1. **"EL CONTRATISTA"** brindará a **"EL BANCO"** la **"CONTRATACIÓN DE SUSCRIPCIONES DE UN SIEM (SISTEMA DE GESTION DE CORRELACION DE EVENTOS PARA LA DETECCION, INVESTIGACION Y RESPUESTA FRENTE A AMENAZAS AVANZADAS)"** según Contrato / Orden de compra N°…….

   Con ese fin, **"EL BANCO"** revelará y entregará a **"EL CONTRATISTA",** información confidencial relacionada a los procesos del BCRP.

   Para el presente documento la palabra **"información"** significa toda información escrita, gráfica, oral, electromagnética y de cualquier otra índole, incluyendo materiales, documentos, planes, estrategias, proyectos, cuestionarios, procesamiento, informes, análisis y cualquier otra información que sea proporcionada por **"EL BANCO"** a la otra parte como consecuencia de este Convenio.

   Se exceptúa de este concepto y las partes acuerdan que la obligación de mantener la confidencialidad no es exigible respecto de la información:

   (i) que sea del dominio público (excepto en caso llegue a ser de dominio público por haber sido revelada por **"EL CONTRATISTA",** transgrediendo este Convenio);

   (ii) que estuviera disponible de manera no confidencial;

   (iii) que su divulgación haya sido autorizada por **"EL BANCO";** y,

   (iv) que su divulgación haya sido requerida por mandato judicial;

2. Son de aplicación los términos de este Convenio de Confidencialidad, a toda la información de propiedad de **"EL BANCO"** que hubiera sido o pudiera ser entregada a **"EL CONTRATISTA"** u obtenida para el desarrollo de las propuestas a que se refiere el numeral anterior, y, en consecuencia, se compromete a no copiarla, ni trasmitirla a terceros, ni divulgarla, por tratarse de secretos comerciales; obligándose a que tal información sea usada únicamente con los propósitos establecidos en el presente Convenio.

Se considera como violación de secretos y por tanto conducta desleal, la divulgación o explotación sin autorización de **"EL BANCO"**, de la información a la que tendrá acceso legítimamente, pero con deber de reserva **"EL CONTRATISTA".**

La utilización de la información para desarrollar propuestas similares a las que **"EL CONTRATISTA"** presente a **"EL BANCO"**, sea directamente o asociada con terceros se considerará incumplimiento de este Convenio.

3. **"EL CONTRATISTA"** reconoce que la información confidencial que se le entregue o facilite se considera un activo de **"EL BANCO"**; por consiguiente, se compromete a que por un período indefinido:

(a) mantendrá confidencial dicha información, sin divulgarla, ni entregarla, directa o indirectamente a terceros, sean personas naturales o jurídicas;

(b) no usará la información recibida en beneficio propio o de terceros, excepto para cumplir a cabalidad con los fines del negocio propuesto y siempre que cuente con la conformidad previa y escrita de **"EL BANCO"**; y,

(c) no revelará total ni parcialmente la información obtenida como consecuencia directa o indirecta de este Convenio a terceros, sin el consentimiento escrito previo de **"EL BANCO"**, aun cuando el tercero se encuentre obligado con **"EL CONTRATISTA"** por un Convenio de Confidencialidad similar.

4. **"EL CONTRATISTA"** se compromete a utilizar cuando menos el mismo grado de cuidado para proteger la confidencialidad de toda la información que reciba de **"EL BANCO"**, al que normalmente usa para proteger su información confidencial y de propiedad exclusiva que no desea publicarla, ni que sea de conocimiento de terceros.

5. En la eventualidad de que **"EL CONTRATISTA"** fuera requerida a revelar información obtenida como consecuencia directa o indirecta de la ejecución de este Convenio, se compromete a notificar a **"EL BANCO"** con prontitud y a prestarle ayuda razonable para la obtención de una orden judicial que expresamente señale que la información que requiere ser revelada, será únicamente para el propósito solicitado o para los propósitos señalados por ley.

6. **"EL CONTRATISTA"** reconoce que revelar, informar, usar, entregar, reproducir o transmitir la información o permitir que terceros la utilicen, constituye trasgresión de este Convenio, y conlleva serias consecuencias para **"EL BANCO"**, por lo tanto, acepta que en caso de incumplimiento indemnizará a **"EL BANCO"**, por los daños y perjuicios que le cause. En el supuesto mencionado, **"EL BANCO"** podrá asimismo iniciar las acciones administrativas que le faculta la ley.

7. Toda la información obtenida por **"EL CONTRATISTA"** como consecuencia de este Convenio, es y permanecerá en propiedad de **"EL BANCO"**, de manera que **"EL CONTRATISTA"** se compromete a devolver o destruir con prontitud a solicitud de **"EL BANCO"**, toda la información obtenida como consecuencia directa o indirecta

de este Convenio. Asimismo, **"EL CONTRATISTA"** deberá asegurarse, que las personas que de conformidad con el numeral siguiente hayan tenido acceso a la información la devuelvan o destruyan, según corresponda.

8. **"EL CONTRATISTA"** garantiza a **"EL BANCO"** que la información recibida estará disponible sólo para un número restringido de personas, a las que deberá informar de su obligación de confidencialidad según este Convenio, por lo tanto, su trabajo deberán desempeñarlo con total discreción, confidencialidad y lealtad, ya que cualquier revelación de información, accidental o intencional a terceros, perjudicará a **"EL BANCO"**.

De solicitarlo **"EL BANCO"**, **"EL CONTRATISTA"** informará el nombre de las personas designadas para tener acceso a la información, quienes sólo tienen autorización para discutir esta información reservada por razones de trabajo y dentro de la propia empresa.

En caso de incumplimiento de la presente cláusula, **"EL CONTRATISTA"** tendrá que indemnizar a **"EL BANCO"** por los daños y perjuicios que le irrogue; sin perjuicio de ello el BCRP podrá denunciar a las personas directamente responsables por el delito de violación del secreto profesional tipificado en el art. 165 del Código Penal o cualquier otro que corresponda.

9. Este Convenio refleja el total entendimiento de **"EL BANCO"** y **"EL CONTRATISTA"** respecto a la materia de qué trata, pudiendo ser modificado únicamente por acuerdo escrito entre las partes.

10. Este Convenio se rige por las leyes del Perú.

11. Toda controversia o discrepancia respecto de la ejecución o interpretación del presente Convenio, que no pueda ser resuelta dentro de un plazo de 30 días de producida la discrepancia entre las partes mediante una negociación de buena fe, será resuelta por los jueces y tribunales de Lima.

Se firma el presente documento, en Lima a los _____ días del mes de _____ de 2025.

_____	_____
"EL BANCO"	**"EL CONTRATISTA"**

ANEXO Nº 11

ACUERDO DE CONFIDENCIALIDAD Y CAUTELA DE LA PROPIEDAD INTELECTUAL DEL BANCO CENTRAL DE RESERVA DEL PERÚ

Conste por el presente documento un Acuerdo de Confidencialidad que celebran de una parte **BANCO CENTRAL DE RESERVA DEL PERÚ** con R.U.C. N° 20122476309, con Jr. Santa Rosa Nro. 441-445, Cercado de Lima, representado por el _____, señor _____, identificado con _____y por el , señor _____, identificado con _____, a quien en adelante se le denominará **"EL BANCO",** y de la otra parte, el señor _____, con domicilio en _____, _____, distrito _____, provincia de _____y departamento de ____, al que se denominará "**El INTEGRANTE"**, identificado con ____, bajo los términos y condiciones siguientes:

Antecedentes

"**El INTEGRANTE"** declara estar vinculado contractualmente con la empresa _____ _____ para brindar los servicios requeridos dentro de la **"CONTRATACIÓN DE SUSCRIPCIONES DE UN SIEM (SISTEMA DE GESTION DE CORRELACION DE EVENTOS PARA LA DETECCION, INVESTIGACION Y RESPUESTA FRENTE A AMENAZAS AVANZADAS)",** según Contrato / Orden de compra N° _____.

Primero: Confidencialidad

1.1 "**El INTEGRANTE"** acepta y reconoce que en virtud de las funciones inherentes al servicio que se contrata tiene acceso a información confidencial. A efectos de este contrato y sin que ello constituya una declaración taxativa sino meramente enunciativa, por "información confidencial" se entenderá, a toda la información escrita, gráfica, oral, electromagnética y de cualquier otra índole, incluyendo materiales, documentos, planes, estrategias, proyectos de comercialización, avisaje, estudios de mercado, cuestionarios, procesamiento, informes, análisis, presentaciones, costos, ventas y cualquier otra información que sea proporcionada por **"EL BANCO"** a la otra parte como consecuencia de este Convenio.

1.2 "**El INTEGRANTE"** se compromete a no usar para sus propios fines o de terceros, ni publicar, revelar, citar o de cualquier otra forma transmitir a terceros la información confidencial indicada en la cláusula anterior a la que haya tenido acceso o conocimiento con motivo de la ejecución del servicio contratado.

1.3 "**El INTEGRANTE"** se compromete a no obtener copia no autorizada por **"EL BANCO"** de cualquier documento, informe o material que reciba para la ejecución del presente trabajo, en cualquiera de sus formas (por ejemplo: versión escrita, electrónica, audio o video).

1.4 "**El INTEGRANTE"** se compromete a devolver **"EL BANCO"** toda la documentación que este le haya entregado tan pronto como termine la ejecución del servicio mencionado en los antecedentes de este acuerdo.

1.5 Las obligaciones asumidas por "**El INTEGRANTE"** en el presente documento serán a perpetuidad y en caso que se incumpla con el deber de confidencialidad y reserva previsto, **"EL BANCO"** se reserva los derechos de promover en contra de "**El INTEGRANTE"** la acción civil por daños y perjuicios y la penal que corresponda.

Segundo: Propiedad Intelectual

"**El INTEGRANTE"** se obliga a no utilizar, total o parcialmente, las técnicas, normativas, métodos, herramientas o prácticas de **"EL BANCO"** que se deriven de la gestión de sus activos de información, sin la autorización expresa de éste.

Se firma el presente documento, en Lima a los _____días del mes de _____ de 2025.

_____	_____
Nombre y firma del Integrante	Nombre y firma funcionario BCRP

_____
Nombre y firma funcionario BCRP

Firmado digitalmente por: ASURZA CACERES Josue David FAU 20122476309 soft
Motivo: Especialista en Ciberdefensa
Fecha: 02/07/2025 15:55:57-0500

Firmado digitalmente por: VENEGAS VIDAURRE Luis Miguel Martin FAU 20122476309 soft
Motivo: En señal de conformidad
Fecha: 02/07/2025 11:23:18-0500

Firmado digitalmente por: AGUINAGA MOGOLLON Edgard Alexander FAU 20122476309 soft
Motivo: En señal de conformidad
Fecha: 02/07/2025 15:40:35-0500