BASES INTEGRADAS

Concurso de Méritos Nº 0007-2023-BN

Servicio de Solución para la Protección Avanzada en Endpoints y la Red del Banco de la Nación

2023

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 generales del derecho público que resulten aplicables al presente proceso de contratación.

En este contexto, se encuentran obligados a prestar su colaboración 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 de 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 a la Secretaría Técnica de la Comisión de Defensa de la Libre Competencia del INDECOPI el acceso a la información que sea requerida, prestar testimonio o absolución de posiciones que se requieran, entre otras formas de colaboración.

CAPÍTULO I

1. DISPOSICIONES GENERALES Y BIENES A ADQUIRIR

1.1 OBJETO DEL PROCESO DE CONCURSO DE MERITOS

El Banco de la Nación, convoca a un concurso de méritos para contratar una empresa legalmente autorizada, que cuente con soluciones que le permitan prevenir, detectar y mitigar en tiempo real amenazas en sus equipos (endpoints) y en la red interna a través de una solución que le permita correlacionar eventos de seguridad de las soluciones de seguridad existentes.

Asimismo, la finalidad publica de la presente contratación es lograr la contratación del servicio de solución para la protección avanzada en endpoints y la red interna, el Banco de la Nación (en adelante BN) que logrará fortalecer y optimizar sus procesos de gestión de incidentes de seguridad, en cumplimiento del Reglamento para la Gestión de la Seguridad de la Información y la Ciberseguridad (Resolución SBS 504-2021), en el cual se indica que toda empresa que cuenta con presencia en el ciberespacio debe mantener con carácter permanente un Programa de Ciberseguridad, el cual contempla: protección frente a las amenazas a los activos, detección y respuesta de incidentes de ciberseguridad.

Asimismo, este servicio permitirá al BN alinearse a las normas de seguridad de datos para la industria de tarjetas de pago, impartidas por PCI DSS (Payment Card Industry Data Security Standard) y por consiguiente al artículo 18 del Reglamento de las Tarjetas de Crédito y Débito Resolución SBS 6523-2013 y sus modificatorias, en lo que respecta a protección contra malware y actualización de los programas o software antivirus en endpoint.

1.2 ALCANCES DEL REQUERIMIENTO

El alcance de la prestación está definido en el **Anexo N° 1** – Términos de Referencia para la Contratación de Servicios, de las presentes bases.

1.3 CONDICIONES DE LA CONTRATACION

1.3.1 VALOR REFERENCIAL

El valor referencial del presente Concurso de Méritos es de S/. 10,997,800.00 (Diez Millones Novecientos Noventa y Siete Mil Ochocientos con 00/100 Soles), el cual incluye todos los impuestos de ley; así como, cualquier otro concepto que pueda tener incidencia sobre el costo del servicio a contratar.

1.3.2 SISTEMA DE CONTRATACIÓN

El sistema de contratación es A Suma Alzada.

1.3.3 LUGAR Y PLAZO DE EJECUCION DE LA PRESTACION

Lugar

EL CONTRATISTA suministrará los equipos (hardware/software, licenciamiento y accesorios) en la cantidad y especificaciones técnicas referidas en el presente documento.

EL CONTRATISTA implementará el servicio, en los lugares que se muestran a continuación:

NODO	DEPENDENCIA	DIRECCION
1	Centro de Datos Principal BN (CDP)	Av. Javier Prado Este 2499 – San Borja – Lima
2	Centro de Datos de Respaldo BN (CDR)	Av. Arequipa 2720 San Isidro – Lima

Plazo de Instalación e Implementación del Servicio

El proceso de instalación de los equipos e implementación de las soluciones adquiridas incluirá el uso de sus recursos humanos, herramientas, útiles y materiales de trabajo, por lo que el servicio deberá ser presupuestado a todo costo, y por lo tanto al BN no le debe significar ningún costo adicional.

EL CONTRATISTA deberá realizar todas las configuraciones necesarias para lograr el objetivo descrito en el alcance, así como realizará otras configuraciones involucradas y que no están mencionadas en el presente documento con el fin de dejar todo el sistema de red operativo, y sin perder la continuidad del servicio que se brinda actualmente. Dado que los equipos solicitados están íntimamente relacionados a la continuidad operativa del Banco de la Nación.

EL ganador de la buena pro debe asegurar que durante la instalación e implementación de los equipos de la solución tendrá acompañamiento por al menos un especialista del área de servicios profesionales del fabricante de la solución ofertada (debe ser refrendado con una carta del fabricante) durante al menos las dos primeras semanas de instalación, a fin de asegurar la adecuada integración de las soluciones adquiridas con los endpoints y la red del banco.

El Plazo de Entrega máximo del servicio será de noventa (90) días calendario (contados a partir del día siguiente de la fecha de suscripción del Contrato)

Para la implementación del servicio el contratista deberá cumplir con lo siguiente:

- ✓ Designar un Jefe de Proyectos el cual tendrá la responsabilidad de gestionar el proceso de implementación con el BN.

- ✓ El Jefe de Proyectos deberá seguir las mejores prácticas según la metodología PMP.
- ✓ EL CONTRATISTA, dentro de los cinco (05) días calendario posteriores de firmado el contrato deberá organizar una reunión kick off en coordinación con el BN, donde serán presentados los contactos de las diferentes áreas y otros proveedores quienes estarán involucrados en la ejecución del proyecto.
- ✓ En dicha reunión (Kick off), el jefe de proyecto deberá presentar un Plan/Cronograma de implementación, mismo que será ratificado por el BN dentro de los 05 días calendario siguientes. Este Plan/Cronograma de implementación debe cubrir todas las tareas a llevarse a cabo desde la firma del contrato hasta la entrega del Acta de Conformidad de Aceptación. El plan de trabajo, debe establecer plazos mínimos y máximos para cada una de las tareas a cumplir, diferenciándose claramente las que debe cumplir el BN, EL CONTRATISTA en forma exclusiva, y las que deben asumir en forma compartida.
- ✓ El Jefe de Proyectos tendrá que reportar semanalmente los avances del proyecto, así como sus riesgos, al personal encargado de administrar el servicio en el BN, este reporte será en físico y lógico.
- ✓ El CONTRATISTA debe gestionar el servicio con un enfoque de proyecto bajo el estándar PMI y estará obligado a presentar los siguientes entregables de gestión además de los relacionados al producto o servicio propiamente dicho:

  - **Fase de Iniciación:**
    - Project Chárter del Proyecto
    - Identificación de todos los involucrados
  - **Fase de Planificación:**
    - WBS (Estructura de desglose del trabajo)
    - Cronograma en detalle
    - Plan de Gestión del Proyecto
  - **Fase de Ejecución:**
    - Actividades de detalle orientadas a la puesta en servicio como objetivo del proyecto.
    - Manejo de las expectativas de los involucrados.
  - **Fase de Seguimiento y Control:**
    - Actas de Reuniones
    - Peticiones o Solicitudes de Cambios aprobadas.
    - Informes de avances periódicos según el cronograma.
  - **Fase de Cierre:**
    - Lecciones aprendidas
    - Acta de Conformidad de implementación del Servicio.

Para el Acta de Conformidad de implementación del Servicio el Contratista debe entregar el informe el cual debe incluir:

- ✓ Diseño descriptivo de las soluciones implementadas.
- ✓ Diagrama Esquemático implementada en los Centros de Datos (CDP, CDR).
- ✓ Diagrama unifilar de interconexión de los equipos instalados en los Centros de Datos (CDP, CDR).
- ✓ Documentación Técnica y/o Manual de la instalación, configuración y administración de los equipos y soluciones adquiridas.
- ✓ Inventario de Equipos.

1.3.4 FORMA DE PAGO

1.3.4.1 SERVICIO

El pago del servicio será de manera mensual.

Previo al pago del servicio, el CONTRATISTA deberá entregar un informe y este informe formará parte de la documentación necesaria para expedir el acta de conformidad del servicio, el informe debe contener lo siguiente:

- ➢ Informe mensual de tipo gerencial que relacione como mínimo los eventos detectados, correlacionados y notificados, los hallazgos más relevantes del periodo, el estado de salud/capacidad de la plataforma gestionada y las acciones de mejora sugeridas.
- ➢ Reporte mensual de estado de salud del servicio y de las soluciones implementadas.

Para tal efecto la Oficina de Seguridad Informática de la Gerencia de Tecnologías de Información del BN emitirá el acta de conformidad del servicio previo informe técnico emitido por la Oficina de Seguridad Informática y visado por la subgerencia de Producción en un plazo que no excederá de los diez (10) días calendario de ser recibida la documentación correspondiente del Contratista.

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

a. Comprobante de pago.
b. Acta de Conformidad emitida por la Oficina de Seguridad Informática de la Gerencia de Tecnologías de Información.
c. Informe Técnico del funcionario de la Oficina de Seguridad Informática de la Gerencia de Tecnologías de Información.

1.3.4.2 PRESTACIÓN ACCESORIA

Previo al pago de la prestación accesoria, el CONTRATISTA deberá entregar un informe donde se indique todas las actividades

ejecutadas, este informe formará parte de la documentación necesaria para expedir el acta de conformidad de la Prestación Accesoria.

La prestación Accesoria se pagará en un solo pago, en soles.

- ✓ El Entrenamiento en el semestre en que se realizó la misma.

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

a) Comprobante de pago.
b) Acta de Conformidad emitida por la Oficina de Seguridad Informática.
c) Informe del funcionario responsable de Oficina de Seguridad Informática, emitiendo la conformidad de la prestación efectuada.

1.3.5 SUBCONTRATACIÓN

El contratista está impedido de subcontratar alguna de las actividades y condiciones técnicas establecidas en los Términos del Referencia del Servicio (Anexo N° 1), no pudiendo transferir esa responsabilidad ni subcontratar las actividades a su cargo a otras entidades ni terceros en general.

1.3.6 CONTRATACIONES CONSIDERADAS COMO SIGNIFICATIVAS

El Contratista procederá obligatoriamente acorde a lo señalado en el numeral 14. del Anexo N° 01 de las Bases.

1.3.7 DEL CODIGO DE ETICA DEL BANCO DE LA NACION

El proveedor del servicio declara bajo juramento conocer que el Banco cuenta con un código de Ética, cuyo objetivo está orientado a establecer valores instituciones, principios, derechos, deberes y prohibiciones éticas. Por lo tanto, el proveedor del servicio se compromete a tomar conocimiento del contenido de este, a través del enlace www.bn.com.pe/nosotros/archivos/CodigoEticaBN.pdf.

1.3.8 ANTICORRUPCION

EL PROVEEDOR 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 con el contrato/orden de servicio.

Asimismo, EL PROVEEDOR 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 PROVEEDOR 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.

1.3.9 INTEGRIDAD

En caso de falsedad de cualquiera de las declaraciones efectuadas por el Proveedor, el Banco podrá declarar la nulidad del presente contrato/orden de servicio por infracción del principio de presunción de veracidad.

1.3.10 RESPONSABILIDAD DEL PROVEEDOR 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 de responsabilidad del contratista es de treinta y seis (36) meses, contado a partir de la conformidad otorgada por LA ENTIDAD.

1.3.11 SEGUROS

El personal del contratista que realizará los servicios a contratar deberá contar con el Seguro Complementario de Trabajo de Riesgo Pensión y Salud vigente durante la ejecución del contrato.

1.3.12 GARANTÍA COMERCIAL

Para los equipos en alquiler se deberán considerar lo siguiente:

- En el caso que el equipo dañado no pueda ser reparado, éste será reemplazado por un equipo nuevo teniendo en consideración lo siguiente:
- El equipo deberá ser del mismo modelo o superior, del mismo fabricante y compatible con la plataforma de seguridad con que cuenta el Banco.
- En caso se requiera un cambio o nueva configuración, ésta se realizará previo a un reporte elaborado por EL CONTRATISTA y aprobado por el BN, manejando un control de cambios.
- Deberá contar con garantía del fabricante.

1.3.13 CONFIDENCIALIDAD DE LA INFORMACION

- Como parte del servicio el CONTRATISTA tomará conocimiento de la información del Banco. Esta información es confidencial, por lo tanto, el CONTRATISTA y todo su personal mantendrá la confidencialidad de la misma. El compromiso de confidencialidad se prolonga indefinidamente aún después de terminado el servicio, y se hace extensivo al personal que el CONTRATISTA subcontrate aun cuando hayan dejado de tener vínculo laboral con el CONTRATISTA.

- El CONTRATISTA se compromete a mantener toda información suministrada por el Banco en estricta reserva y absoluta confidencialidad, así como de adoptar las medidas que resulten necesarias para impedir que la Información Confidencial sea conocida o revelada a terceros o que sea utilizada para fines distintos para los cuales fue entregada.

- Se entiende que la obligación asumida está referida no sólo a documentos e informaciones señalados por la otra parte como "confidenciales" sino a todos los documentos e informaciones que, en razón del referido intercambio, pueda ser conocida por cualquier medio, incluyendo, sin limitarse a ella, a programas de cómputo, nombres de clientes, estrategias financieras o comerciales, etc.

- El CONTRATISTA se obliga a tomar todas las medidas y precauciones razonables para que sus trabajadores y en general cualquier persona con la que tenga relación, no divulgue a ningún tercero los documentos o información a los que tengan acceso, haciéndose responsables por la divulgación que se pueda producir y asumiendo el pago de la indemnización por daños y perjuicios. Estas medidas incluyen, aunque no se limitan a: (i) poner en disposición la información confidencial sólo a un número restringido de personas; (ii) permitir que sus trabajadores, agentes o terceros, accedan a la información confidencial sólo hasta donde sea necesario para la prestación de los servicios; (iii) exigir a su personal o trabajadores como condición previa al acceso a la información confidencial que se obliguen por escrito a respetar esta cláusula de confidencialidad. El compromiso de confidencialidad se prolonga por 10 años después de terminado el servicio, y se hace extensivo al personal que el proveedor subcontrate aun cuando hayan dejado de tener vínculo laboral con el CONTRATISTA.

- El CONTRATISTA reconoce que la información que se le entregue, procese, facilite o genere en razón a su desempeño y/o ejecución del presente contrato, se considera un activo del Banco, por consiguiente, el CONTRATISTA se obliga a:

  1. Mantener en confidencial dicha información, sin divulgarla, ni entregarla, directa o indirectamente a terceros, sean personas naturales o jurídicas.

2. No usarla para cualquier otro fin que no sea en relación con la prestación de los servicios; ni obtener un beneficio propio o de terceros de ella.
3. No entregarla o revelarla, de manera total o parcial, pública o privada, a ninguna persona sea en el Perú como en el extranjero, sin el consentimiento escrito previo del Banco, aun cuando se encuentre obligado con alguna de las partes por un acuerdo de confidencialidad similar; salvo a los empleados de cada una de ellas o de cualquier otra persona que se encuentre en una relación contractual o de confianza con el proveedor y que requiera dicha información para utilizarla para asuntos relacionados con los servicios.
4. El CONTRATISTA debe asegurar de que toda la Información Confidencial sea usada para el exclusivo beneficio de los servicios que se prestan en virtud del contrato. Por tal razón, la violación de cualquiera de las disposiciones establecidas en esta cláusula obligará al proveedor a indemnizar todos los perjuicios directos que cause con motivo de ello y, de caso ser necesario, a resolver de manera automática el contrato.

- Se considera como violación de la confidencialidad y, por tanto, una conducta desleal, la divulgación o explotación sin autorización de la otra parte, de la información a la que tendrá acceso legítimamente, pero con deber de reserva.

- Se entiende que la obligación asumida está referida no sólo a documentos e informaciones señalados por la otra parte como "confidenciales" sino a todos los documentos e informaciones que, en razón del referido intercambio, pueda ser conocida por cualquier medio, incluyendo sin limitarse a ella, características técnicas, sistemas, programación de instalación, ubicación física, información de las Oficina, etc.

- El CONTRATISTA se obliga a mantener y guardar en estricta reserva y absoluta confidencialidad todos los documentos e informaciones que reciban del Banco, durante las negociaciones y ejecución del servicio.

- Para la prestación del servicio el proveedor se compromete a firmar un acuerdo de confidencialidad de la información.

- Para la prestación del servicio el CONTRATISTA se compromete a firmar un acuerdo de confidencialidad.

1.3.14 CONFORMIDAD DEL SERVICIO

La conformidad del servicio será otorgada por la Oficina de Seguridad Informática de la Gerencia de Tecnologías de Información, en su calidad de área usuaria y técnica, quienes deberán verificar el cumplimiento de las condiciones contractuales.

1.3.15 GARANTIAS

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.

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.

1.3.16 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.

Esta penalidad puede alcanzar hasta 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 o el monto máximo para otras penalidades, de ser el caso, LA ENTIDAD puede resolver el contrato por incumplimiento.

1.3.17 OTRAS PENALIDADES

El Contratista adicionalmente deberá considerar obligatoriamente la aplicación de Otras Penalidades, acorde a lo señalado en el numeral 6 de los Términos de Referencia del Anexo N° 01 de las Bases, detalladas en el Anexo "A" del mismo anexo.

1.4 EL COMITÉ DE CONCURSO DE MERITOS

El presente Concurso de Méritos, se desarrollará de acuerdo con lo establecido en las presentes Bases, y será conducido por el Comité de Concurso de Méritos designado, quienes actúan en forma colegiada cuentan con autonomía para interpretar y adoptar las decisiones que sean pertinentes, las cuales no requieren ratificación de algún funcionario del Banco de la Nación.

Ante la ausencia de un miembro titular en el Comité, este será reemplazado por el suplente designado, siempre y cuando se respete la conformación aprobada por la Gerencia de Administración y Logística del Banco de la Nación. El suplente solo reemplazará al titular en las sesiones del Comité en las que este último se encuentre ausente.

En caso de ausencia de un titular y su suplente, la Gerencia que los designó, deberá designar con carácter de urgente a un miembro adicional, en reemplazo de ambos por las sesiones que cualquiera de ellos no pueda asistir.

Para sesionar y adoptar acuerdos válidos, el Comité del Concurso de Méritos deberán tener un quórum igual a la totalidad de sus miembros titulares o suplentes y los acuerdos serán adoptados por mayoría y consignados en Actas.

CAPÍTULO II

BASE NORMATIVA

- Ley N° 31638 - Ley de Presupuesto Sector Público Año Fiscal 2023.
- Ley N° 30353, Ley que crea el Registro de Deudores de Reparaciones Civiles (REDERECI), y su Reglamento probado por Decreto Supremo Nº 022-2017-JUS.
- Ley Nº 27815, Ley del Código Ética de la Función Pública.
- Decreto Supremo Nº 004-2019-JUS, que aprueba el Texto Único Ordenado de la Ley Nº 27444, Ley del Procedimiento Administrativo General.
- Artículo 4° literal a) del TUO de la Ley N° 30225, Ley de Contrataciones del Estado, aprobado por Decreto Supremo N° 082-2019-EF y sus modificatorias.
- Primera Disposición Complementaria Final de la Ley N° 30225, Ley de Contrataciones del Estado.
- Ley N° 26702, Ley General del Sistema Financiero y del Sistema de Seguros y Orgánica de la Superintendencia de Banca y Seguros.
- Acuerdo de Promoción Comercial Perú - Estados Unidos aprobado por el Congreso de la República mediante Resolución Legislativa N° 28766 y ratificado mediante Decreto Supremo N° 030-2006-RE.
- Manual de Organización y Funciones de las Gerencias del Banco que están relacionadas o involucradas en el Concurso de Méritos convocado.
- Opiniones emitidas por la Dirección Técnico Normativa del Organismo Supervisor de las Contrataciones del Estado (OSCE) y pronunciamientos de la Superintendencia de Banca, Seguros y AFP (SBS) a solicitud del Banco.
- Directiva BN-DIR-2600-152-01 Rev. 8, Contratación de Servicios Financieros
- Reglamento de Gestión de Riesgos de Lavado de Activos y del Financiamiento al Terrorismo, aprobado por Resolución SBS N° 2660-2015 y modificatorias.
- Manual BN-MAN-1200-001-07 Rev. 3, Manual de Prevención y Gestión de los Riesgos de Lavado de Activos y del Financiamiento del Terrorismo del Banco de la Nación.
- Manual BN-MAN-2100-010-05 Rev. 7, Manual para el Tratamiento de Contrataciones / Subcontrataciones Significativas en el Banco de la Nación.
- Circular BN-CIR-2100-216-05 Rev. Genérica, Gestión de Riesgos de nuevos Productos o Cambios importantes en el Ambiente de Negocios, Operativo o Informático del Banco.
- Las demás que disposiciones que resulten aplicables.

CAPÍTULO III

PROCESO DE SELECCIÓN

3.1 REQUISITOS DE LOS POSTORES

Los postores deben cumplir con los siguientes requisitos generales para presentar oferta en el presente proceso de concurso de méritos:

- No haber incurrido en actos de corrupción.
- No tener impedimento para postular en el proceso de concurso de méritos ni para contratar con el Estado.
- No encontrarse inscrito en el Registro de Deudores de Reparaciones Civiles (REDERECI).
- Conocer que el Banco de la Nación es una Entidad Financiera sujeta al cumplimiento del Reglamento de Gestión de Riesgos de Lavado de Activos y del Financiamiento del Terrorismo, aprobado por resolución SBS N° 2660-2015 y que se obliga a proporcionar información necesaria a fin de dar cumplimiento a lo dispuesto en los artículos 36° y 37° del mencionado Reglamento, así como cualquier otra norma legal sobre esta materia, desde su entrada en vigencia.
- Conocer las disposiciones aplicables del Texto Único Ordenado de la Ley N° 27444, Ley del Procedimiento Administrativo General.
- 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.
- Conocer, aceptar y someterme a las bases, condiciones y reglas del proceso de concurso de méritos.
- Ser responsable de la veracidad de los documentos e información que presento en el presente proceso de concurso de méritos.
- Comprometerme a mantener la oferta presentada durante el proceso de concurso de méritos y a perfeccionar el contrato **(Anexo N° 3)**, en caso de resultar favorecido con la buena pro.

3.2 ETAPAS DEL CONCURSO DE MERITOS

El Concurso de Méritos se desarrolla conforme a las disposiciones del cronograma establecido en las presentes Bases **(Anexo N° 2)**.

Las etapas del Concurso de Méritos son las siguientes:

3.2.1 Convocatoria

Se efectuará a través de invitaciones (cartas o correo electrónico), a las empresas que ofrecen el servicio requerido, adjuntando copia de las Bases del Concurso de Méritos aprobadas.

3.2.2 Formulación de Consultas

Las consultas que formulen los participantes deben estar referido al alcance o contenido de cualquier aspecto de las Bases, deberán ser enviadas a los correos electrónicos: avalenzuela@bn.com.pe, mpachasl@bn.com.pe y msalazar@bn.com.pe, respetando el plazo de presentación establecido en el Cronograma, las consultas o solicitud de aclaración o pregunta específica que presenten fuera del plazo establecido en el Cronograma se considerarán como no presentadas y no serán tomados en cuenta por el Comité que conduce el proceso de selección.

3.2.3 Absolución de Consultas

El Comité del Concurso de Méritos absolverá las consultas presentadas por los participantes, la Absolución de Consultas será comunicada a todos los participantes a través de los correos electrónicos que hayan designado, dentro de los plazos establecidos en el Cronograma del proceso de selección.

3.2.4 Integración de Bases

Las Bases integradas constituyen las reglas definitivas del Concurso de Méritos, las que contendrán las correcciones, precisiones y/o modificaciones producidas como consecuencia de la Absolución de las Consultas.

3.2.5 Presentación de Propuestas

La presentación de propuestas se realiza en acto público, en la fecha y hora señaladas en el cronograma del proceso, en el Piso 8° de la Sede Principal del BN, sito en Av. Javier Prado Este N° 2499 - San Borja, con la participación de Notario Público.

El acto se inicia cuando el Comité empieza a llamar a los participantes para que entreguen sus propuestas. Si al momento de ser llamado el participante no se encuentra presente, se le tendrá por desistido.

Las propuestas se presentarán en dos (2) sobres cerrados, de los cuales el primero contendrá la propuesta técnica y el segundo la propuesta económica, las que deben estar foliadas correlativamente empezando por el número uno y deben llevar el sello y la rúbrica del postor o de su representante legal o mandatario designado para dicho fin.

Después de recibidas las propuestas, el Comité procederá a abrir los sobres que contienen la propuesta técnica de cada postor, a fin de verificar que se encuentren los documentos presentados por cada postor sean los solicitados en las Bases.

Todos los documentos que contengan información referida a los requisitos para la admisión de propuestas y factores de evaluación se presentarán en idioma castellano o, en su defecto, acompañados de la respectiva traducción por traductor público juramentado o traductor colegiado

certificado, salvo el caso de la información técnica complementaria contenida en folletos, instructivos, catálogos o similares, que podrá ser presentada en el idioma original. El postor será responsable de la exactitud y veracidad de dichos documentos.

En el caso que de la revisión de la propuesta se adviertan defectos de forma, tales como errores u omisiones subsanables en los documentos presentados que no modifiquen el alcance de la propuesta técnica, se puede otorgar plazo para subsanar la propuesta técnica.

Después de abierto cada sobre que contiene la propuesta técnica y verificado que contengan los requeridos como documentación de presentación obligatoria, se procederá a la apertura de los sobres que contiene las propuestas económicas, el Notario procederá a sellar y firmar cada hoja de los documentos de la propuesta técnica y económica.

Al terminar el acto público, se levantará un acta, la cual será suscrita por el Notario y por todos los miembros del Comité del Concurso de Méritos.

✓ **Sobre N° 1 - Propuesta Técnica**

Se presentará en un original con el siguiente rotulado:

Señores Banco de la Nación Av. Javier Prado Este N° 2499 - San Borja **Att.: Comité del Concurso de Méritos** **CONCURSO DE MERITOS N° 0007-2023-BN** **"Servicio de solución para la Protección Avanzada en Enpoints y la Red del Banco de la Nación".** SOBRE N° 1: PROPUESTA TÉCNICA [NOMBRE / RAZÓN SOCIAL DEL POSTOR]

El Sobre Nº 1 contendrá, además de un índice de documentos, la siguiente documentación:

Documentación de Presentación Obligatoria:

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

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

Copia del certificado de vigencia de poder del representante legal, apoderado o mandatario designado para tal efecto.

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.

c) Declaración jurada de cumplir con los requisitos para ser postor

en el presente proceso de selección. **(Formato N° 2).**

d) Declaración jurada de cumplimiento de los Términos de Referencia contenidos en el Anexo N° 1 de la presente Bases. **(Formato N° 3).**

e) Declaración jurada de plazo de la prestación. **(Formato N° 4).**

f) Promesa de consorcio con firmas legalizadas, de ser el caso, en la que se consigne los integrantes, el representante común, el domicilio común y las obligaciones a las que se compromete cada uno de los integrantes del consorcio, así como el porcentaje equivalente a dichas obligaciones. **(Formato N° 5).**

g) Detalle de la Experiencia del Postor en la Especialidad **(Formato N° 7).**

h) De ser el caso, Declaración Jurada de Reorganización Societaria **(Formato N° 8).**

Documentos para Acreditar los Requisitos de Calificación:

Copia simple y legible de los documentos que acreditan los "Requisitos de Calificación" que se detallan:

A EXPERIENCIA DEL POSTOR EN LA ESPECIALIDAD

Requisitos:

El postor debe acreditar un monto facturado acumulado equivalente a S./10´000,000.00 (diez Millones y 00/00 Soles), por la contratación de servicios iguales o similares al objeto de la convocatoria, durante los ocho (08) años anteriores a la fecha de la presentación de ofertas que se computarán desde la fecha de la conformidad o emisión del comprobante de pago, según corresponda.

Se consideran servicios similares a los siguientes: Servicio de Licencias o Servicio de CYBERSOC o Administración y Monitoreo de Plataformas de Seguridad y Correlación Inteligente de Eventos de Seguridad o Servicio de soporte de mantenimiento o Servicio de monitoreo y administración de plataformas de seguridad TI o Servicio de monitoreo de eventos de seguridad (SOC) o Servicio de CyberSOC, Servicio de Red Team o Servicio de monitoreo de equipamiento de seguridad o Servicio de seguridad Gestionada o Servicio de Solución Integral Tecnológica de Ciberseguridad – SIEM o Servicio de soporte de plataforma de seguridad y correlación o Servicio de Ciberseguridad o Servicios Gestionados de seguridad o Soporte Local o Ethical Hacking o Servicio de Seguridad de la Red Interna y Perimetral o Servicio de Detección y Respuesta ante Amenazas o Servicio de Operación de la Seguridad y Servicio de CyberSOC o Servicios de Ciberseguridad y ciberdefensa

Acreditación:

La experiencia del postor en la especialidad se acreditará con copia simple de (i) contratos u órdenes de compra, 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, correspondientes a un máximo de treinta (30) 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 según las contrataciones indicadas en el **Formato N° 7** referido a la Experiencia del Postor en la Especialidad.

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.

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

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

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

Sin perjuicio de lo anterior, los postores deben llenar y presentar el **Formato N° 7** referido a la Experiencia del Postor en la Especialidad.

B CAPACIDAD TÉCNICA Y PROFESIONAL

B.1 EXPERIENCIA DEL PERSONAL CLAVE

Requisitos:

- Un (01) especialista con experiencia mínima dos (02) años en implementación de soluciones de XDR y EDR.
- Un (01) especialista con experiencia mínima dos (02) años en implementación de solución de NDR.
- Un (01) Jefe de Proyecto con experiencia mínima de dos (02) años de experiencia en la gestión de proyectos de TIC.

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.

B.2 FORMACIÓN ACADÉMICA DEL PERSONAL CLAVE

Requisitos:

- Un (01) especialista con Formación académica: Técnico Titulado o Bachiller o Profesional Titulado en la especialidad de ingeniería en Sistemas o Telecomunicaciones o Informática o Electrónica o Ingeniería de Seguridad y Auditoria Informática o Ingeniería de Sistemas y Computo o Ingeniería de Computación o Ingeniería Informática o Ingeniería de Sistemas Empresariales o Ingeniería de Sistemas y Computación o Ingeniería de redes y comunicación o Ingeniería de software.
- Un (01) especialista con Formación académica: Técnico Titulado o Bachiller o Profesional Titulado en la especialidad de ingeniería en Sistemas o Telecomunicaciones o Informática o Electrónica o Ingeniería de Sistemas y Computo o Ingeniería de Computación o Ingeniería Informática o Ingeniería de Sistemas Empresariales o Ingeniería de Sistemas y Computación o Ingeniería de redes y comunicación o Ingeniería de software.

- Un (01) Jefe de Proyecto con Formación académica: Titulado en Ingeniería de la especialidad de Sistemas o Telecomunicaciones o Informática o Electrónica o Ingeniero Informático y de Sistemas o Ingeniería de Sistemas y Computo o Ingeniería de Computación o Ingeniería Informática o Ingeniería de Sistemas Empresariales o Ingeniería de Sistemas y Computación o Ingeniería de Seguridad o Auditoria Informática o Ingeniería Industrial.

Acreditación:
Se acreditará con copia simple de Título de Técnico o grado de Bachiller o Título Profesional.

B.3 CAPACITACIÓN DEL PERSONAL CLAVE

Requisitos:

- Un (01) especialista con e Certificación Oficial vigente en la solución XDR y/o EDR ofertada expedida por el fabricante (Nivel técnico vigente).
- Un (01) especialista con Certificación Oficial de fabricante de la solución NDR propuesta (Nivel técnico vigente).
- Un (01) Jefe de Proyecto con Certificación PMP (Project Management Profesional) vigente o diplomado de especialización en dirección y gestión de proyectos bajo el enfoque PMI con un mínimo de 360 horas de duración o diplomado de especialización en dirección y gestión de proyectos bajo el enfoque PMI con un mínimo 24 créditos académicos.

Acreditación:
Se acreditará con copia simple de constancia, certificado u otro documento, según corresponda.

✓ **Sobre N° 2 - Propuesta Económica**

Se presentará en un original, con el siguiente rotulado:

Señores Banco de la Nación Av. Javier Prado Este N° 2499 - San Borja **Att.: Comité del Concurso de Méritos** **CONCURSO DE MERITOS N° 0007-2023-BN** **"Servicio de solución para la Protección Avanzada en Enpoints y la Red del Banco de la Nación".** SOBRE N° 2: PROPUESTA ECONOMICA [NOMBRE / RAZÓN SOCIAL DEL POSTOR]

La propuesta económica, será formulada en Soles S/., deberá incluir el precio conforme a los establecido en el **Formato N° 6** de las presentes Bases; asimismo, la propuesta económica debe incluir todos los tributos, seguros, 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 de los bienes a adquirirse.

El monto total de la propuesta económica deberá ser expresada con dos decimales. Los precios unitarios podrán ser expresados con más de dos decimales.

En el documento que contiene el precio ofertado u oferta económica puede subsanarse la rúbrica y la foliación.

En caso de divergencia entre el precio cotizado en números y letras, prevalece este último. Cuando se advierta errores aritméticos, corresponde su corrección al Comité, debiendo constar dicha rectificación en el acta respectiva; en este último caso, dicha corrección no implica la variación del precio unitario ofertado.

3.2.6 Evaluación de Propuestas

La evaluación de propuestas se realizará en dos (2) etapas: La evaluación técnica y la evaluación económica.

La información contenida en la oferta debe ser objetiva, clara, precisa y congruente entre sí y debe encontrarse conforme con lo requerido en las bases, a fin de que el Comité del Concurso de Méritos encargado de la Contratación, puedan apreciar el real alcance de la misma y su idoneidad para satisfacer el requerimiento de la Entidad, lo contrario, por los riesgos que implica, determinará que la Oferta sea desestimada.

No es función del Comité del Concurso de Méritos, interpretar el alcance de una oferta, esclarecer ambigüedades, o precisar contradicciones o imprecisiones, sino evaluar las ofertas en virtud a las bases, realizando un análisis integral que permita generar convicción de lo realmente ofertado, sin posibilidad de inferir o interpretar hecho alguno.

3.2.6.1 Evaluación Técnica

Se verificará que la propuesta técnica cumpla con los requerimientos técnicos mínimos contenidos en las presentes Bases. Las propuestas que no cumplan dichos requerimientos no serán admitidas.

Sólo aquellas propuestas admitidas y aquellas a las que el Comité hubiese otorgado plazo de subsanación pasarán a la evaluación técnica.

En aquellos casos en los que se hubiese otorgado plazo para la subsanación de la propuesta, el Comité deberá determinar si se cumplió o no con la subsanación solicitada. Si luego de vencido el plazo otorgado, no se cumple con la subsanación, el Comité tendrá la propuesta por no admitida.

Una vez cumplida la subsanación de la propuesta o vencido el plazo otorgado para dicho efecto, se continuará con la evaluación de las propuestas técnicas admitidas, verificando que cumplan con los requisitos de calificación. La oferta que no cumpla con los requisitos de calificación es descalificada.

3.2.6.2 Evaluación Económica

Solo se evaluarán las ofertas que cumplan con los requisitos de calificación; si, las propuestas económicas incorporan costos no considerados en **Formato N° 6** - Precio de la Oferta, serán devueltas por el Comité y se tendrán por no presentadas.

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

1. **Puntaje Total:** 100 puntos

2. **Evaluación del Costo de la contratación del Servicio de Solución para la Protección Avanzada en Endpoints y la Red del Banco de la Nación**

   Para determinar la oferta con el mejor puntaje, consistirá en asignar el puntaje máximo establecido a la propuesta económica de menor monto. Al resto de propuestas se les asignará un puntaje inversamente proporcional, según la siguiente fórmula:

$$Pi = \frac{Om \times PMPE}{Oi}$$

   Donde:

   I = Propuesta

Pi	=	Puntaje de la propuesta económica i
Oi	=	Propuesta Económica i
Om	=	Propuesta Económica de monto o precio más bajo
PMPE	=	Puntaje Máximo de la Propuesta Económica

3.2.7 Otorgamiento de la Buena Pro

Una vez evaluadas las propuestas económicas el Comité procederá a otorgar la Buena Pro a la propuesta ganadora, de acuerdo con el cuadro comparativo en el que se consignará el orden de prelación en que han quedado calificados.

En el supuesto que dos (2) o más ofertas empaten, la determinación del orden de prelación de las ofertas empatadas se realiza a través de sorteo efectuado por un Notario Público.

3.2.8 Comunicación de Resultados

El presidente del Comité comunicará los resultados del Concurso de Méritos, mediante carta o correo electrónico dirigido a todos los postores del concurso de méritos.

3.3 Procedimiento para la Atención de Solicitudes o Reclamos Presentados por Postores

En el supuesto que algún postor presente una solicitud, o presente un reclamo, en formato de recurso de revisión, apelación u otro similar, respecto a cualquier acto que haya realizado el Comité del Concurso de Méritos en el ejercicio de sus funciones, se deberá seguir el procedimiento que se detalla a continuación (no se incluyen en este procedimiento, las consultas y/o observaciones que se efectúen dentro del Concurso de Méritos, cuando correspondan estos a la etapa del Concurso):

a) El Postor deberá presentar su reclamo o solicitud en un plazo máximo de 3 días hábiles a partir del día siguiente de otorgada la Buena Pro, en la Sección Trámite Documentario sito en la Calle Arqueología N° 120 - San Borja en el horario de 08:30 a 16:30 Horas, quien deberá remitirlo a la Gerencia de Administración y Logística. Dicha Gerencia, de manera inmediata, enviará el documento a los miembros del Comité de Concurso de Méritos para su revisión, quienes emitirán de manera colegiada, el informe técnico respectivo, dando respuesta a cada una de las solicitudes, reclamos y/o pedidos formulados por el postor.

b) El informe deberá ser emitido dentro de los 3 días hábiles siguientes desde la fecha de recepción del documento, por parte del comité, bajo responsabilidad. En caso se requiera de mayor tiempo para emitir el informe, por complejidad del asunto a contestar o por necesitar información y/o documentación de otras áreas del Banco, se puede ampliar el plazo por 3 días hábiles adicionales por una sola vez.

c) Dicho informe será remitido a la Subgerencia de Compras de la Gerencia de Administración y Logística juntamente con el Expediente de Contratación para su revisión y análisis; y elaboración del proyecto de carta de respuesta, previa consulta con la Gerencia Legal.

d) La Gerencia Central de Administración y Logística en un plazo máximo de tres días hábiles suscribirá la carta de respuesta previa visación de la Gerencia Legal, para su envío al postor por parte de la Gerencia de Administración y Logística.

3.4 Del Perfeccionamiento del Contrato

Dentro del plazo de ocho (8) días hábiles siguientes al otorgamiento de la Buena Pro, el postor ganador debe presentar la totalidad de la siguiente documentación:

a) Contrato de consorcio con firmas legalizadas ante Notario de cada uno de los integrantes, de ser el caso.

b) 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.

c) Copia de la vigencia del poder del representante legal de la empresa que acredite que cuenta con facultades para perfeccionar el contrato.

d) Copia de DNI del representante legal.

e) Declaración Jurada que cumple las disposiciones establecidas en la Ley N° 29783 - Ley de Seguridad y Salud en el Trabajo y su Reglamento, acompañado de copia de la Póliza del Seguro Complementario de Trabajo de Riesgo, Pensión y Salud que comprenda al personal del contratista que realizará el internamiento de bienes a adquirirse.

f) Domicilio para efectos de la notificación durante la ejecución del contrato.

g) Autorización de notificaciones por el Banco de la Nación, durante la ejecución contractual mediante medios electrónicos de comunicación **(Formato N° 9).**

h) En atención a la Resolución SBS N° 2660-2015 - Reglamento de Gestión de Riesgos de Lavado de Activos y del Financiamiento del Terrorismo, a la suscripción del contrato, el ganador de la buena pro deberá presentar el **(Formato N° 10)** debidamente completado.

i) Sustentación del Perfil del Personal No Clave denominado Residente de Seguridad, adjuntando los documentos que acrediten su Formación Académica, Capacitación y Experiencia, de acuerdo con lo solicitado en el numeral 3.3 literal d) de los Términos de Referencia del Anexo N° 1 de las Bases.

j) Sustentación de las exigencias requeridas sobre Seguridad y Salud en el Trabajo, adjuntando los documentos que acrediten su cumplimiento, de acuerdo con lo solicitado en el numeral 15. de los Términos de Referencia del Anexo N° 1 de las Bases.

k) Sustentación de las exigencias requeridas sobre Prevención del Lavado de Activos y del Financiamiento del Terrorismo, adjuntando los documentos que acrediten su cumplimiento, de acuerdo con lo solicitado en el numeral 16. de los Términos de Referencia del Anexo N° 1 de las Bases

l) Declaración Jurada de no encontrarse inscrito en el Registro de Deudores de Reparaciones Civiles (REDERECI), acorde a lo solicitado en el numeral 17. de los Términos de Referencia del Anexo N° 1 de las Bases
m) Carta fianza como Garantía de Fiel Cumplimiento del Contrato, por una suma equivalente al 10% del monto del contrato original.

En un plazo que no puede exceder de los dos (2) días hábiles siguientes de presentados los documentos, de existir observaciones el BN solicitará la subsanación de los requisitos, en un plazo adicional de cuatro (04) días contados desde el día siguiente de la notificación al postor. De no existir observaciones, el BN solicitará al postor que en un plazo no mayor de dos (02) días hábiles comunique sobre sus observaciones al Proyecto de Contrato contenido en las Bases, luego de lo cual, las partes tendrán un plazo de cuatro (04) días hábiles para realizar los ajustes que resulten necesarios dentro de los alcances del servicio contratado y suscribir el contrato. Dicho plazo podrá ser ampliado por acuerdo de las partes.

Cuando no se perfeccione el contrato, por causa imputable al postor, éste pierde automáticamente la buena pro; en tal supuesto, la Subgerencia de Compras como órgano encargado de las contrataciones (OEC) del BN, en un plazo máximo de tres (3) días hábiles, requiere al postor que ocupó el segundo lugar que presente los documentos para perfeccionar el contrato en los mismos plazos previstos. Si el postor no perfecciona el contrato, el órgano encargado de las contrataciones del BN declara desierto el proceso de concurso de méritos.

3.5 DISPOSICIONES FINALES

El Comité del Concurso de Méritos culminará sus funciones con la entrega del expediente correspondiente a la Subgerencia de Compras de la Gerencia de Administración y Logística, lo que se producirá luego de la notificación en acto público del otorgamiento de la buena pro del Concurso de Méritos, de conformidad con lo estipulado en la Directiva BN-DIR-5500-152-01 Rev. 8.

Anexos

Anexo N° 1

INDICE

Contenido

GERENCIA DE TECNOLOGÍAS DE INFORMACIÓN	SERVICIO DE SOLUCIÓN PARA LA PROTECCIÓN AVANZADA EN ENDPOINTS Y LA RED DEL BANCO DE LA NACION	

1. GENERALIDADES

1.1. DENOMINACIÓN DE LA CONTRATACIÓN

SERVICIO DE SOLUCIÓN PARA LA PROTECCIÓN AVANZADA EN ENDPOINTS Y LA RED DEL BANCO DE LA NACION.

1.2. ANTECEDENTES

En el año 2022 el Banco de la Nación Gestionó el Proyecto para la implementación de un Cybersecurity Operation Center de acuerdo a lo requerido en el Reglamento para la Gestión de la Seguridad de la Información y la Ciberseguridad (Resolución SBS 504-2021), para lograr este objetivo se ha visto por conveniente desplegarlo en 3 fases, siendo la primera obtener una solución para la protección avanzada de endpoints y en la red interna del Banco de la Nación.

1.3. SITUACIÓN ACTUAL

A la fecha el Banco de la Nación no cuenta con soluciones avanzadas que permitan prevenir, detectar y actuar ante amenazas presentes en sus Endpoints y/o en la Red interna, y estas no se encuentran integradas con el resto de las soluciones de seguridad.

1.4. OBJETIVOS

El Banco de la Nación requiere contar con soluciones que le permitan prevenir, detectar y mitigar en tiempo real amenazas en sus equipos (endpoints) y en la red interna a través de una solución que le permita correlacionar eventos de seguridad de las soluciones de seguridad existentes

1.5. SISTEMA DE CONTRATACIÓN

Sistema de Contratación de Suma Alzada

1.6. FINALIDAD PÚBLICA

Con la contratación del servicio de solución para la protección avanzada en endpoints y la red interna, el Banco de la Nación (en adelante BN) logrará fortalecer y optimizar sus procesos de gestión de incidentes de seguridad, en cumplimiento del Reglamento para la Gestión de la Seguridad de la Información y la Ciberseguridad (Resolución SBS 504-2021), en el cual se indica que toda empresa que cuenta con presencia en el ciberespacio debe mantener con carácter permanente un Programa de Ciberseguridad, el cual contempla protección frente a las amenazas a los activos, detección y respuesta de incidentes de ciberseguridad.

Asimismo, este servicio permitirá al BN alinearse a las normas de seguridad de datos para la industria de tarjetas de pago, impartidas por PCI DSS (Payment Card Industry Data Security Standard) y por consiguiente al artículo 16 del Reglamento de las Tarjetas de Crédito y Débito Resolución SBS 6523-2013 y sus modificatorias, en lo que respecta a protección contra malware y actualización de los programas o software antivirus en endpoint.

Como consecuencia de ello, se implementará los siguientes puntos:

- ✓ XDR (Solución para Detección y Respuesta Extendida)
- ✓ EDR (Solución para Detección y Respuesta de Endpoints)
- ✓ NDR (Solución para Detección y Respuesta en la RED)
- ✓ Acceso confiable y seguro a la red de comunicaciones que garantice la integridad la información de los clientes del BN.
- ✓ Mejorar los accesos a la red con mayores niveles de confidencialidad, encriptación e integridad.

1.7. VINCULACIÓN CON LOS OBJETIVOS DEL PLAN ESTRATÉGICO INSTITUCIONAL VIGENTE (2022-2026) DEL BN

El servicio contribuye a alcanzar Objetivo Estratégico Institucional OEI 10: Garantizar la estabilidad operativa, del Plan Estratégico Institucional 2022 - 2026 del Banco de la Nación

2. ALCANCES Y DESCRIPCIÓN DEL SERVICIO

El servicio será ejecutado por un periodo de treinta y seis (36) meses e inicia al día siguiente de firmado al Acta de Conformidad de implementación del Servicio según lo indicado en el numeral 3.4.

El servicio consta de; Soluciones de seguridad, Mantenimiento Preventivo, Mantenimiento Correctivo, residente de seguridad y Servicio de Respuesta ante Incidentes, según el siguiente detalle:

Soluciones de Seguridad:
Se requiere de una solución para la protección avanzada en endpoints y la red del banco de la nación, según el siguiente detalle:

Solución para Detección y Respuesta Extendida (XDR)
Solución para Detección y Respuesta de Endpoints (EDR)
Solución para Detección y Respuesta en la RED (NDR)

Solución para Detección y Respuesta Extendida (XDR)
Se requiere que la solución para Detección y Respuesta Extendida se brinde mediante un servicio SaaS y ser la última versión liberada por el fabricante, además deberá:

- Integrar las soluciones de EDR y NDR que forman parte de las soluciones requeridas.
- Incluir inteligencia de amenazas propia o integrada con terceros para predecir futuros ataques o brindar contexto de incidentes presentados.
- Detectar las técnicas, tácticas y procedimientos presentes en una o en un conjunto de alertas relacionadas con cada incidente detectado, de acuerdo con al framework de ciberseguridad MITRE ATT&CK y la solución propuesta deberá haber obtenido el nivel de protección en al menos 12 de las 13 pruebas en el escenario Protection de la evaluación Turla de MITRE ATT&CK. Esto será corroborado por la Entidad ingresando al link de dicho framework corroborando el cumplimiento de cada solución propuesta.

- Realizar acciones automatizadas para responder ante un incidente.
- Correlacionar logs provenientes de la infraestructura de soluciones de seguridad del BN y centralizar la visibilidad de todos los eventos y alertas de seguridad, permitiendo la integración de las soluciones de seguridad que tiene el BN:
  Firewalls, IPS, Filtro Web, Antispam, WAF, Anibol, Directorio Activo (AD), CGBS.

Solución para Detección y Respuesta de Endpoints (EDR)
Se requiere que la solución para Detección y Respuesta de Endpoint se brinde mediante un servicio SaaS y ser la última versión liberada por el fabricante, además deberá:

- Asegurar 8000 endpoint (estaciones de trabajo, laptops, servidores y cajeros - ATMs) que el BN cuenta distribuidos en su red.
- Supervisar y recopilar datos de actividad de puntos finales (endpoints) que podrían indicar una amenaza, y analizar estos datos para identificar patrones de amenazas.
- Responder automáticamente a las amenazas identificadas para eliminarlas o contenerlas, y notificar al personal de seguridad.
- Tener herramientas forenses y de análisis para investigar amenazas identificadas y buscar actividades sospechosas.

Solución para Detección y Respuesta en la RED (NDR)
Se requiere de dos (02) equipos (appliance) de uso específico, basado en hardware y sistema operativo del mismo fabricante y deberá ser el último modelo liberado por el fabricante. No podrán usarse servidores o sistemas operativos diferentes o que requieran alguna otra licencia no provista por el fabricante.

Centro de Datos	Cantidad Equipos
Centro de Datos Principal (CDP) en San Borja	1
Centro de Datos de Respaldo (CDR) en San Isidro	1

Los equipos deberán estar en alta disponibilidad entre sites.
Los equipos deberán integrarse al XDR adquirido.
La solución para Detección y Respuesta en la RED deberá:

- Contar con mecanismos de detección de amenazas conocidas presentes en la red.
- Contar con la capacidad de utilizar bases de datos de indicadores de compromiso actualizada de terceros.
- Tener capacidades de detección y respuesta frente a amenazas de día cero, basado en técnicas de machine learning y anomalías en la red.
- Brindar respuesta de acción inmediata para bloquear toda comunicación detectada como maliciosa.

El servicio deberá, ante defectos de diseño y/o fabricación y/o averías y/o fallas de funcionamiento y/o pérdida total de los bienes contratados no detectados al momento de su implementación, dar la solución del mismo. En caso de que el defecto no pueda ser solucionado, el proveedor deberá proceder al reemplazo de

las partes y/o del equipo afectado por otro equipo de igual o superiores características del mismo fabricante, sin costo para el Banco de la Nación.

Mantenimiento Preventivo

EL ganador de la buena pro deberá considerar un (01) mantenimiento preventivo cada 6 meses (semestral) durante todo el plazo de ejecución del servicio, para cada uno de los equipos en alquiler.

Los mantenimientos preventivos deberán ser programados al inicio de cada año de servicio, a través del Plan de Mantenimiento respectivo que será entregado a la Oficina de Seguridad Informática de la Gerencia de Tecnologías de Información.

El mantenimiento preventivo será para todos los componentes de la solución, tanto en CDP como en CDR y será con personal técnico in-situ.

El Contratista deberá tener una disponibilidad de 24x7x365 para estas actividades; la cual deberá ser asistida con soporte directo del fabricante, vía web, correo y telefónicamente de ser el caso.

Las actividades a ejecutar son:

- ✓ Realizar la verificación de las configuraciones de los equipos.
- ✓ Realizar el backup de las configuraciones de los equipos de seguridad de la solución implementada por el Contratista, antes de iniciar los trabajos de mantenimiento preventivo.
- ✓ De ser necesario, actualizar el software de todos los equipos de la plataforma de seguridad a la última versión liberada y estable, la cual debe ser informada, evaluada y aprobada previamente por el BN. Esto permitirá minimizar las vulnerabilidades. Como medida preventiva en este escenario, el Contratista deberá asegurar la continuidad operatividad del servicio a través de la conmutación al sistema de respaldo.
- ✓ Realizar la revisión y análisis de logs.
- ✓ Realizar el diagnóstico de la salud óptimo de todos los equipos, garantizando que los mismos vengan operando y aplicando las políticas, perfiles y protocolos de seguridad ininterrumpidamente.

EL CONTRATISTA deberá indicar el periodo de tiempo de duración de las actividades del mantenimiento preventivo por parte de su personal, el cual no deberá exceder cuatro (04) horas de labores, fuera de horario de atención al público y en el horario que el BN disponga.

El informe de Mantenimiento Preventivo emitido por el CONTRATISTA deberá ser presentado luego de culminado todas las actividades descritas anteriormente y formará parte de la documentación necesaria para expedir el acta de conformidad del servicio.

Mantenimiento Correctivo

Comprende la resolución de las averías y/o incidentes (hardware y/o software) con la reparación y/o reemplazos de los equipos en alquiler y de las soluciones adquiridas, para el correcto funcionamiento de los mismos.

La realización del servicio estará sujeto a lo siguiente:

Llamadas de Servicio

- ✓ Durante todo el periodo de duración del servicio el BN deberá tener la libertad de abrir casos con EL CONTRATISTA mediante "Llamadas de Servicio" o

través para hacer consultas, reportar incidentes y solicitar atención para la resolución de problemas.

- ✓ EL CONTRATISTA pondrá a disposición del BN un número telefónico gratuito (0800 o equivalente), o correo electrónico, considerándose todas estas formas igualmente válidas para la atención y reparación de las averías en el servicio.
- ✓ La atención de las llamadas de servicio se podrá realizar de lunes a domingo, incluyendo feriados, desde las 00:00 hasta las 24:00 horas.

Atención de las averías y/o incidentes:

El CONTRATISTA deberá asistir a la Sede del BN donde se produjo la avería en el esquema (24) horas x siete (7) días de la semana durante el periodo de la prestación del servicio o asistir de manera remota para el caso de las soluciones adquiridas.

Reparación de las averías y/o incidentes:

El SLA del tiempo de reparación de las averías y/o incidentes se señala en el Anexo A.

Todos los costos asociados a la reparación de las averías y/o incidentes serán asumidos por el Contratista.

Para los equipos en alquiler se deberán considerar lo siguiente:

- En el caso que el equipo dañado no pueda ser reparado, éste será reemplazado por un equipo nuevo teniendo en consideración lo siguiente:
- El equipo deberá ser del mismo modelo o superior, del mismo fabricante y compatible con la plataforma de seguridad con que cuenta el Banco.
- En caso se requiera un cambio o nueva configuración, ésta se realizará previo a un reporte elaborado por EL CONTRATISTA y aprobado por el BN, manejando un control de cambios.
- Deberá contar con garantía del fabricante

Cierre de la avería y/o incidente.

El Contratista mediante correo electrónico dirigido a la jefatura y al personal de la Oficina de Seguridad Informática detallará las acciones realizadas para resolver la avería y/o incidente, el personal técnico de dicha oficina decidirá el cierre de la avería y/o incidente confirmando la normalización de la operatividad de los bienes en alquiler y/o soluciones involucrados en el incidente.

Dentro de los tres (3) días calendario, luego de realizado el soporte técnico, el Contratista presentará un informe al Banco, en el que se indicará el detalle de las tareas realizadas, así como observaciones, sugerencias y recomendaciones a realizar a fin de que la avería y/o incidentes presentada no vuelva a ocurrir. Si fuera el caso, el Banco podrá realizar las observaciones que crea necesarias a este informe dentro de los cinco (5) días calendario de haber recibido este informe. El contratista deberá enviar dentro de los tres (3) días calendario luego de haber recibido las observaciones, un nuevo informe con las correcciones solicitadas.

El informe como mínimo deberá constar de lo siguiente:

1. Fecha, hora y duración de la avería
2. Diagnóstico
3. Impacto

4. Acciones de corrección
5. Estado del servicio afectado
6. Acciones de mejora
7. Conclusiones y recomendaciones

Estos puntos deben contener la explicación técnica necesaria, la cual debe estar sustentada con evidencias.

Residente de seguridad:
El contratista asignará un residente de seguridad, el cual deberá administrar las soluciones durante todo el periodo que dure el servicio en las instalaciones del Banco de la Nación de la sede San Borja u otro local que se le asigne. El banco facilitará el espacio físico, punto de red al residente de seguridad y el horario de labores será de 08:30 a 17:30 horas y las actividades a realizar se encuentran descritas en el numeral 3.3.
Para horario fuera de oficina de horario de oficina y feriados, el contratista deberá atender desde su SOC asegurando la atención 24/7.

Servicio de Respuesta ante Incidentes

El Contratista deberá ofertar un servicio de respuesta ante incidentes y emergencia de seguridad informática, con el objetivo de apoyar al BN en la contención, mitigación, y solución de las incidencias, así como en la preparación de la respuesta ante dichas emergencias. Este servicio abarcará las soluciones ofertadas.

El servicio deber proveer un modelo de anticipación y respuesta frente a crisis derivadas de incidentes graves de seguridad, así como debe diseñar todos los mecanismos necesarios de análisis, contención, respuesta, erradicación y recuperación como parte de la gestión de incidentes de seguridad. Para ello el Contratista debe contar con un equipo de respuesta ante incidentes de seguridad informática CSIRT (Computer Security Incident Response Team). Las instalaciones y el personal que operan el CSIRT del Contratista, deben estar ubicados en la ciudad de Lima, Perú o en el extranjero.

El equipo de respuesta antes incidentes del contratista debe estar registrado como miembro de FIRST (Forum of Incident Response and Security Teams).

Este servicio se activará bajo demanda (requerido explícitamente por el BN) en el transcurso del periodo del servicio. El resultado del servicio será un informe por ocurrencia del análisis de incidentes, las medidas de contención y respuesta implementadas y el estado de recuperación de los servicios o activos.

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

Este servicio debe basarse en las siguientes políticas:

Realizar el registro, clasificación y atención de los incidentes de seguridad.

- Apoyar y asesorar al BN en la evaluación de los daños ocasionados por los incidentes de seguridad, siendo los responsables de la evaluación los administradores de los activos del lado del BN.
- Asesorar en la etapa de erradicación y recuperación del incidente al BN.
- Reportar los resultados de la gestión de incidentes notificados.
- El servicio debe ser prestado en la modalidad 24x7.
- El Contratista accederá a la información obtenida y procesada resultante de la gestión de incidentes.
- Toda la información generada y procesada es propiedad del BN, siendo además confidencial.
- El Contratista deberá implementar los mecanismos de seguridad para garantizar que la información que produzca este servicio se mantenga confidencial, integra y disponible.
- Comunicar al BN cualquier información relevante que permita gestionar de manera adecuada el incidente notificado.
- Asesorar al BN en las medidas a tomar respecto de la gestión de incidentes.
- Elaborar un informe que contenga las actividades realizadas para la gestión de los incidentes notificados.
- Informar al BN en cuanto se advierta la ocurrencia de un incidente de Ciberseguridad que presente un impacto significativo adverso verificado o presumible de:

  - Pérdida o hurto de información de la empresa o de clientes.
  - Fraude interno o externo.
  - Impacto negativo en la imagen o reputación de la empresa.
  - Interrupción de operaciones.

3. CARACTERÍSTICAS Y CONDICIONES DEL SERVICIO

3.1 CARACTERÍSTICAS TÉCNICAS

El proveedor debe garantizar una alta disponibilidad del servicio (incluye los 3 componentes. XDR, EDR y NDR), de tal forma que no se requiera reconfigurar el servicio ante la ocurrencia de interrupciones del servicio para continuar operando.

Solución para Detección y Respuesta Extendida (XDR)
La solución para Detección y Respuesta Extendida deberá:

a. La solución debe ser una plataforma basada 100% en la nube, que permita integrar fuentes de servicios en nube y recolectar logs de eventos en premisas a través de colectores, los cuales pueden ser servidores físicos, servidores virtuales o máquinas virtuales.
b. La solución debe tener la capacidad de integrar +300 tecnologías de seguridad de otras marcas o fabricantes, las integraciones pueden ser nativas o a través de API, protocolos de colección como Syslog o colección basada en CSV, FTP, Bases de datos. Esto será corroborado por la Entidad ingresando al link público del fabricante.
c. La solución debe soportar el análisis de tráfico de al menos 10000 eventos por segundo (EPS) o 24 Terabytes de información por mes.
d. La solución debe poder centralizar los datos recibidos para una visibilidad de las amenazas y vulnerabilidades, asimismo proporcionar un flujo de trabajo de incidentes para rastrear eventos.

e. La solución debe soportar operaciones booleanas como AND, OR y NOT y funciones adicionales para búsquedas específicas.
f. La solución debe proporcionar dentro de la misma, la creación de casos a través diferentes clasificaciones, como pueden ser: denegación de servicio, código malicioso, reconocimiento, phishing, violación de políticas, entre otros.
g. Debe utilizar un lenguaje de análisis de datos para consultas de eventos para su posterior análisis, soportando operaciones booleanas como AND, OR y NOT y expresiones regulares.
h. La solución debe soportar dentro de la anatomía del lenguaje utilizado al menos los siguientes aspectos: búsquedas, filtros, elementos sintaxis como día y hora, operadores de comparación, histograma.
i. La solución debe proveer la capacidad de asignar un nombre de clase genérico que se refiere a eventos, por ejemplo, proxies: forcepoint, firewall: CheckPoint.
j. Para el tránsito de todos los datos, debe realizarse con un cifrado SSL/TLS
k. La solución debe soportar una consola maestra de alertas, la cual posea la capacidad de personalizar dashboards, búsquedas, resultados de búsquedas.
l. La solución debe proporcionar y actualizar indicadores provenientes del fabricante y su red de inteligencia de amenazas, así mismo, permitir la personalización de esos indicadores, permitiendo la carga de archivos CSV o JSON.
m. Debe contar con un panel informativo que muestre información sobre: estadísticas de eventos por segundo, estado general del dispositivo, eficacia o estado de salud de los sensores.
n. Se debe mostrar en las tablas de alertas al menos la siguiente información: riesgo, tipo, origen, primer evento, último evento, sumario, estado, hash.
o. La solución debe soportar la personalización de tablas de alertas.
p. La solución debe incluir una vista sobre consejos de investigación, que permitan ofrecer un detalle más profundo a través de preguntas con consultas de búsqueda asociadas y así tener una mejor comprensión de la amenaza, además deberá tener la capacidad de mostrar feed de Threat Intelligence en la vista de incidentes.
q. El proveedor deberá realizar cacería de amenazas durante todo el tiempo de contrato usando la solución ofertada.
r. El servicio de cacería de amenazas deberá realizar investigaciones proactivas asociadas a campañas de ataque para saber si existe incidencias dentro de la red de la Entidad.
s. La consola de gestión deberá tener un panel dedicado para que los analistas de cacería de amenazas puedan informar sus hallazgos, sobre este panel la Entidad tendrá la potestad de hacer preguntas y consultas a los analistas de cacería de amenazas.
t. El servicio deberá estar disponible 24x7 y los 365 días del año.
u. Cada incidente identificado por los analistas de cacería de amenazas deberá generar un registro en la consola de gestión.
v. El análisis realizado por el servicio de cacería de amenazas deberá tener cobertura de los eventos generados en los endpoints, la red, la nube y otras fuentes de diferentes marcas.
w. El servicio de cacería de amenazas deberá enviar reportes mensuales con el resumen y eventos importantes de las investigaciones realizadas.
x. La recolección de eventos debe permitir los siguientes tipos de log: Security log, system log, application log, PowerShell Log, IIS log o logs del sistema operativo mediante tecnologías nativas de Windows como Windows Event Collector (WEC).

y. La solución debe ser capaz de procesar los logs provenientes de los Next Generation Firewall.
z. Deberá ser capaz de recolectar eventos de Office 365 vía API, tales como: auditoría de Office 365, Azure AD, Exchange, Sharepoint, metadata de correos electrónicos.
aa. Deberá ser capaz de recolectar eventos de AWS CloudTrail, AWS CloudWatch, Microsoft Event Hub, Google Cloud Platform.
bb. Eventos de Active Directory (Window Event Logs), tales como: búsquedas de LDAP, gestión de grupos y usuarios de dominio, gestionar de computadoras del dominio.
cc. Deberá ser capaz de recolectar eventos de otras fuentes de diferentes marcas a través del protocolo Syslog, pudiendo soportar al menos los formatos CEF y LEEF.
dd. La solución de XDR deberá ser capaz de configurar un formato y tabular (parsing) los eventos recibidos de las diferentes fuentes.
ee. La solución debe soportar el análisis de la correlación sobre todos los eventos recolectados de las diferentes fuentes.
ff. Debe de soportar la detección de actividad sospechosa a través del comportamiento dentro de varios detectores dentro de los cuales se destacan: Beacon Detection, DNS Entropy Detection, DNS Fast-flux Detection, Credetial Misuse Detection, Unacknowledged Connection Detection, Port Scanning Detection, Port Probing Detection, Data Theft (outbond) exfiltration Detection, Inbound Connections Detection, Server outbound Connections Detection, VPN Compromised Account Detection, User agent sospechoso, Cantidad de interacciones de red inusuales, Query LDAP inusual, Creación de reglas de firewall inusuales, Sesión WinRM anómala, Servidor Python inicializado, Proceso raro ejecutado en la institución, Elevación de privilegios con usuario SYSTEM de manera anómala, Firewall de Linux desactivado de manera anómala, Tarea programada creada de forma inusual, Ejecución de arp.exe anómala, Cantidad inusual de screenshots tomados, Cantidad excesiva y anómala de información subida a internet, Conexión RDP inusual, Escaneo de puertos sospechoso, Creación de una máquina en el dominio, Creación de usuario con permisos de domain admin, Usuario imprime una cantidad inusual de archivos, Conexiones VPN sospechosas, Logueo VPN desde una cuenta de servicio, Uso de aplicación no habitual, Cantidad inusual de solicitudes DNS generadas, Actividad inusual en nube como: borrado de RDS, creación de usuarios, borrado de recursos o con motores de comportamiento que permitan la detección.
gg. La solución debe incluir capacidades de UEBA (User and Entity Behavior Analytics) así como la detección de movimiento lateral y otras amenazas, basado en la recolección de eventos de diferentes fuentes de la entidad.
hh. La plataforma deberá ser capaz de recolectar eventos por al menos 30 días y en base a toda esa data generar perfiles de comportamientos de los usuarios y generar alertas de seguridad si una determinada acción sale del perfil de comportamiento aprendido.
ii. Las capacidades de UEBA deberán generar los perfiles de comportamiento al menos de los eventos recolectados por los endpoints y dispositivos de seguridad perimetral.
jj. Deberá estar integrado al Active Directory para generar un score de riesgo en base al usuario y grupo al cual pertenece. La solución deberá dar contexto del puesto de trabajo y área laboral a la cual pertenece el usuario en base a la

información recolectada por el LDAP de tal manera que el analista tenga mayor contexto del incidente.

kk. El postor podrá incorporar otro agente de la misma marca o una marca tercera para poder cumplir los requerimientos de UEBA, deberá estar licenciado para 8000 usuarios.

ll. La solución debe ser compatible para procesar registro a través de los siguientes métodos: syslog, CEF, CSV o FTP, DB.

mm. La solución debe proporcionar la detección, validación, e investigación de alertas/amenazas, para así reconstruir el killchain de un ataque.

nn. Se requiere contar con capacidades para categorizar los eventos basado en riesgo.

oo. Deberá contar con un scoring de riesgo que permita dar una valoración cuantitativa a los incidentes de seguridad identificados.

Solución para Detección y Respuesta de Endpoints (EDR)

a. La solución EDR deberá soportar:
   - Servidores y estaciones de trabajo Windows de 32 y 64 bits.
   - Sistema operativo Mac OS.
   - Sistema operativo Linux.

b. La solución deberá soportar los siguientes navegadores de internet para acceder a la consola de administración:
   - Google Chrome
   - Microsoft Edge
   - Mozilla Firefox
   - Microsoft Internet Explorer y otros navegadores standart del mercado.

c. La solución EDR deberá contar con administración centralizada para gestionar los equipos finales sin importar la ubicación física de los equipos, dentro o fuera de la red de la entidad.

d. La consola de administración deberá soportar administración por roles.

e. La solución EDR deberá contar con administración para gestionar los equipos finales sin importar la ubicación física de los equipos, dentro o fuera de la red de la entidad.

f. La solución debe ofrecer distintos modelos de gestión: On-Premises o SaaS.

g. La consola de administración podrá enviar actualizaciones a los agentes de EDR.

h. La comunicación entre los agentes y la consola de administración deberá utilizar un túnel de seguridad SSL/TLS cifrado.

i. La solución debe contar con los mecanismos de protección para no poder ser desinstalada o desactivada por el usuario.

j. La solución deberá permitir configurar excepciones que le permitan convivir con otros agentes en el endpoint, en caso ocurra algún conflicto.

k. Se deben poder habilitar o deshabilitar los módulos de protección sin ser desinstalados del sistema.

l. La solución EDR podrá ser desplegado en equipos físicos y virtuales a través de un único agente, proporcionando las mismas funcionalidades a cualquiera de los equipos.

m. La solución deberá contar con capacidad de procesamiento y analítica de datos directamente en la nube.

n. Debe identificar y bloquear técnicas de explotación sin necesidad de utilizar firmas y/o heurísticas. La solución no deberá tener ningún componente que requiera actualizar una base de datos de firmas.

x. El bloqueo de exploits deberá ser posible incluso en procesos desarrollados inhouse, la solución deberá permitir especificar los nombres de los procesos que serán protegidos contra exploits.
p. Deberá proteger la explotación de vulnerabilidades de sistemas operativos y aplicaciones que incluso se encuentren sin el parche de seguridad instalado. Esta funcionalidad podrá ser cubierta con un agente tercero en caso el postor lo requiera.
q. La protección contra vulnerabilidades deberá ser independiente al CVE identificado, la solución deberá proteger cualquier intento de explotación incluyendo a vulnerabilidades de día cero que no tengan un CVE.
r. Bloquear técnicas de explotación de vulnerabilidades, como mínimo Return Oriented Programming (ROP), Heap Spray, Jit Spray, Shell link, Structured Exception Handler, CPL Execution Process.
s. Identificación y prevención de intentos de escalamiento de privilegios a nivel de Kernel.
t. Deberá ser capaz de proteger contra ataques a vulnerabilidades conocidas y desconocidas (día cero).
u. La solución de EDR deberá usar Inteligencia Artificial y aprendizaje de máquina, por lo que no deberá estar basada en firmas, de tal forma que los agentes no tengan que actualizarse diariamente sobre definiciones de virus o ataques.
v. La solución EDR deberá contar con la capacidad de detectar y prevenir intentos de borrado de respaldo del sistema, realizados por ataques de tipo ransomware.
w. La solución EDR deberá detectar y prevenir los procesos de cifrado de archivos relacionados a extensiones usadas por ataques de tipo ransomware.
x. La solución EDR deberá detectar y prevenir los procesos asociados a accesos indiscriminados al sistema de archivos asociados a ataques de tipo ransomware.
y. La solución EDR deberá identificar y bloquear malware orientado al sector financiero.
z. La solución de EDR deberá contar con capacidades de aprendizaje de máquina de forma local en cada dispositivo.
aa. El postor deberá incluir y licenciar una plataforma de sandbox integrada a la solución EDR o XDR, la cual permita realizar análisis dinámico del malware identificado localmente.
bb. El sandbox deberá soportar el análisis dinámico en sistemas Windows, Linux y MacOS.
cc. El sandbox deberá tener una capacidad mínima de análisis dinámico de 120000 archivos por día, además deberá admitir el envío de archivos de hasta 100 MB al sanbox, sin generar costos adicionales a la Entidad.
dd. Deberá mostrar un reporte con el detalle del análisis realizado por el sandbox
ee. Deberá permitir solicitar la corrección del veredicto del sandbox en caso se trate de un falso positivo.
ff. El sandbox podrá estar basado en nube o en un appliance onpremise.
gg. En caso de ofertar un sandbox en nube deberá ser del mismo fabricante del software EDR, XDR.
hh. En caso de ofertar un sandbox onpremise deberá cumplir los siguientes requerimientos:
* Estar desplegado en Alta Disponibilidad entre sites, cada nodo deberá ofrecer el mismo performance solicitado.
ii. La solución de EDR deberá mostrar gráficamente la trazabilidad de las conexiones de los procesos o ejecuciones de la amenaza.

jj. La solución de EDR deberá contar con funcionalidades de aprendizaje para un análisis exhaustivo.
kk. La solución de EDR deberá detectar ataques a través de análisis de comportamiento.
ll. La solución de EDR deberá contar con la capacidad de poner en cuarentena a un dispositivo o archivo.
mm. La solución de EDR deberá contar con la capacidad de devolver a un dispositivo que se envió previamente a cuarentena.
nn. La solución de EDR deberá detectar ataques de tipo file less.
oo. La solución de EDR deberá contar con la capacidad de definir un estado de retorno de sistema tras un intento de ataque de tipo ransomware y devolver la información a su estado original.
pp. La solución de EDR deberá considerar los elementos de MITRE ATT&CK Framework para tener visibilidad sobre las Técnicas, Tácticas y Procedimientos.
qq. La solución de EDR deberá considerar los elementos de MITRE ATT&CK Framework para realizar análisis sobre las posibles amenazas o incidentes detectados en la organización.
rr. La solución deberá haber sido evaluado por MITRE ATT&CK y haber tenido un resultado de al menos 77% en las pruebas de Cobertura por Analítica (Analytic Coverage) y al menos un 98% de Visibilidad, según la evaluación del 2022, además de la evaluación del 2023 la solución debe haber detectado al menos 70 de las 76 técnicas en el escenario Carbon y 60 de las 67 técnicas en el escenario Snake, correspondientes a la evaluación Turla de MITRE ATT&CK.
ss. La solución de EDR deberá contar con Inteligencia Artificial que permita realizar un análisis guiado sobre una posible amenaza o incidente, permitiendo la reducción en el tiempo para detectar y reaccionar ante amenazas.
tt. La solución deberá contar con la capacidad de información que permita la documentación de los siguientes elementos:
    - Personal asignado a un caso de investigación
    - Artefactos clave y detalles de apoyo
    - Sistemas involucrados en la investigación
    - Reputación de artefactos relevantes (Archivo, IP, Virus Total)
    - Campos abiertos que permita la toma de notas del proceso de investigación por parte del analista.
    - Clasificación del comportamiento dentro del marco MITRE ATT&CK
uu. La solución debe contar con la capacidad de monitorear en tiempo real y reportar a la consola para su análisis.
vv. La solución de EDR deberá permitir la búsqueda de históricos como mínimo de 30 días, para los eventos de telemetría recolectada de los endpoints y diversas fuentes integradas y 180 días para el dashboard y reportes de alertas e incidentes.
ww. La solución debe permitir asignar diferentes estados de acuerdo con la etapa de investigación o análisis en que se encuentre.
xx. El agente deberá poder capturar, como mínimo, las siguientes acciones en equipos Windows:
    - Proceso ejecutado, incluyendo el tiempo de inicio, el tamaño del archivo asociado.
    - Actividades de creación, escritura, renombre, eliminación, modificación de archivos.
    - Archivos DLL: ruta completa, dirección base, id del proceso, tamaño de la imagen, firma, valores hash calculados con los algoritmos MD5 y SHA256 del archivo DLL.

- Creación y terminación de los procesos, incluyendo los siguientes atributos: nombre del proceso padre, ID del proceso, ruta completa, argumentos de la línea de comando, nivel de integridad para determinar si el proceso está siendo ejecutado con privilegios elevados, valores hash calculados con los algoritmos MD5 y SHA256, detalles de la firma o el certificado utilizado para firmar el archivo.
- Inyecciones en hilos de procesos: ID del hilo padre, ID del hilo nuevo o que se da terminado, proceso que inició el hilo (en caso de ser un proceso distinto).
- Interacciones de red de cada endpoint: IP y puerto origen y destino, estado de conexión (exitosa o fallida), protocolo usado (TCP, UDP), resolución de dominio (hostname), tráfico entrante y saliente, país destino de la IP pública.
- Estadísticas de red: volumen de tráfico en eventos de subida y descarga de tráfico TCP.
- Acciones sobre los registros de Windows: Configuración o eliminación de valores del registro. Creación, modificación, eliminación, edición, restauración y guardar llaves del registro. Con los siguientes parámetros: ruta del registro del valor o llave que fue modificado, Nombre del valor o llave modificado, Datos del valor modificado,
- Sesiones del sistema operativo: inicio de sesión, cierre de sesión, conexión y desconexión. Considerando los siguientes atributos: inicio de sesión interactivo, id de la sesión, estado de la sesión, y si la sesión es local o remota.
- Logs de eventos de Windows.

yy. El agente deberá poder capturar, como mínimo, las siguientes acciones en equipos MacOS:

- Actividades de creación, escritura, renombre, eliminación, modificación de archivos.
- Inicio y detención de procesos, con los siguientes parámetros: PID de proceso del proceso padre, PID del proceso, ruta completa, argumentos de la línea de comando, nivel de integridad para determinar si el proceso está siendo ejecutado con privilegios elevados, valores hash calculados con los algoritmos MD5 y SHA256, detalles de la firma o el certificado utilizado para firmar el archivo.
- Interacciones de red de cada endpoint: IP y puerto origen y destino, estado de conexión (exitosa o fallida), protocolo usado (TCP, UDP).
- Las siguientes acciones de red: accept, connect, connect failure, disconnect, listen, statistics.
- Logs de eventos de autenticación

zz. El agente deberá poder capturar, como mínimo, las siguientes acciones en equipos Linux:

- Para los archivos: las acciones de creación, apertura, escritura y eliminación, incluyendo la ruta completa del archivo y el hash del archivo (para ciertos archivos y sólo si el archivo fue escrito). Información del copiado o renombrado de los archivos, incluyendo las rutas completas tanto del archivo original como del modificado. Las acciones para cambiar el dueño (chown) y el modo (chmod) de los archivos, incluyendo la ruta completa del archivo, así como el nuevo dueño o nuevos atributos.
- Inicio y detención de procesos, con los siguientes parámetros: PID de proceso del proceso padre, PID del proceso, ruta completa, argumentos de la línea de comando, nivel de integridad para determinar si el proceso está siendo ejecutado con privilegios elevados, valores hash calculados con los

algoritmos MD5 y SHA256, detalles de la firma o el certificado utilizado para firmar el archivo.
- Interacciones de red de cada endpoint: IP y puerto origen y destino, estado de conexión (exitosa o fallida), protocolo usado (TCP, UDP).
- Las siguientes acciones de red: accept, connect, connect failure, disconnect, listen, statistics.
- Logs de eventos de autenticación.

aaa. La solución permite crear investigaciones de las posibles amenazas en un dispositivo para validar los procesos o conexiones que se han detectado en el dispositivo, así como su comportamiento.

bbb. La solución debe contar con contención inmediata si una actividad maliciosa es detectada, sin perder conexión y reporteo a la consola para poder realizar la investigación de la amenaza.

ccc. Se debe poder configurar acciones en dispositivos sobre infecciones identificadas:
- Finalizar el proceso
- Finalizar y eliminar
- Enviar a cuarentena el dispositivo
- Finalizar la cuarentena del dispositivo

ddd. La solución debe contar con mecanismos de protección a ejecución de scripts maliciosos de IE, sean JavaScript o VBScript.

eee. La solución debe permitir mecanismos de contención y remediación remotos en el dispositivo.

fff. La solución debe colectar información del filesystem.

ggg. La solución debe permitir eliminar archivos de forma remota.

hhh. La solución permite búsqueda de patrones mediante reglas Yara o un lenguaje equivalente.

iii. La solución deberá mostrar el hilo de acciones que un proceso ejecuto dentro de un host o estación de trabajo con la finalidad de identificar procesos principales, secundarios, conexiones y módulos que puedan estar siendo afectados en un usuario determinado e identificar posibles objetivos de la actividad anómala.

jjj. Con el objetivo de identificar amenazas latentes (existentes, pero no ejecutadas) dentro de EL CLIENTE, la solución deberá permitir la ejecución de búsquedas condicionales de archivos o artefactos de manera histórica y en tiempo real en la organización.

kkk. La solución debe colectar información de Bash/Shell históricamente

lll. La solución de EDR deberá contar con la capacidad de integrarse con plataformas de SIEM y XDR.

mmm. La solución debe contar con la capacidad de integrarse y recibir actualizaciones de reputación de un sistema de inteligencia o indicadores de compromiso contra amenazas mediante el uso de protocolo abierto de comunicación, con la capacidad de actualizar todas las máquinas del ambiente en tiempo real.

nnn. La consola deberá estar basada en nube o híbrida (on-premise y nube). La nube del fabricante deberá contar con las siguientes certificaciones:
- Contar con la certificación SOC2 Tipo II de AICPA, ISO 27001 para soluciones en Nube.
- Contar con doble factor de autenticación para el login para soluciones en Nube.
- Opcionalmente deberá permitir el acceso solo desde un rango de IP pública de la Entidad.

ooo. La consola debe permitir la gestión de usuarios mediante roles preconfigurados y debe ser capaz de crear roles personalizados
ppp. El proveedor de ser necesario deberá desinstalar la solución actual con la finalidad de no tener problemas de compatibilidad.

Solución para Detección y Respuesta en la RED (NDR)

a. El hardware provisto debe soportar la capacidad de ser gestionado por medio de una interfaz tipo serial o consola, desde donde se puedan configurar los parámetros básicos del equipo.
b. La solución debe tener capacidad de análisis de mínimamente de 8 Gbps.
c. Los accesorios de conectividad deben ser capaces de operar en modo en línea interceptando hasta dos (02) pares RJ45 de 10b o cuatro (04) interfaces de RJ45 de 1Gb, y adicionalmente cuatro (04) pares fibra óptica de 10Gb SPF o 8 interfaces 10Gb SPF de fibra óptica por cada equipo.
d. Se debe proveer la cantidad de hardware (equipos appliance) necesario para cubrir con las necesidades de la entidad de acuerdo con la arquitectura más acertada de inspección y protección, brindando todos los SFPs/SFP+ necesarios para la interconexión de los componentes. La solución deberá permitir 150 mil nuevas conexiones/sesiones por segundo o 8GB de throughput como mínimo.
e. Deberá estar integrado y/o ser un componente de la plataforma de XDR.
f. Deberá poseer la capacidad de analizar la navegación vía port-mirroring para el monitoreo o vía in-line, la interceptación (bloqueo) podrá realizarse de forma directa (in-line) o a través de la integración con plataformas de seguridad perimetral existentes, dicha integración con las diferentes plataformas de seguridad deberá estar a cargo del proveedor sin costo para el Banco de la Nación.
g. Debe permitir y estar licenciada la apertura y desencriptado de tráfico cifrado (HTTPS) a través del propio equipo, permitiendo así crear exclusiones de tráfico por categoría de sitios web (tales como, financiero, internet, motores de búsqueda, contenido de adultos, etc.). También se aceptarán tecnologías que analicen el tráfico cifrado utilizando ML (Machine Learning) e IA (Inteligencia Artificial) sin la necesidad de descifrarlo
h. Debe implementar la funcionalidad de inspección SSL para el análisis de tráfico cifrado y permitir la duplicación del tráfico descifrado usando otra interfaz física para permitir el análisis de soluciones de otras partes. También se aceptarán tecnologías que analicen el tráfico cifrado utilizando ML (Machine Learning) e IA (Inteligencia Artificial) sin la necesidad de descifrarlo
i. Debe poseer la capacidad de operar en modo sigiloso, sin dirección IP asociada con los puertos de detección.
j. La solución debe incluir mecanismos de detección de amenazas desconocidas o día cero, este método de detección no debe requerir conectarse a ningún otro dispositivo cuya función sea proporcionar firmas de malware.
k. La solución debe contar con una tecnología sandbox con virtualización propietaria que soporta sistema Windows x86 y x64, además de MacOS y Linux, integrándose con la red de datos existente de forma autónoma. El mecanismo Sandbox también debería poder externalizarse a través de hardware dedicado o en la nube del fabricante, este sistema de virtualización no debe ser una solución comercial para no tener técnicas de evasión en la explotación por virtualización de los sistemas Operativos señuelo. Este sistema de virtualización

no debe ser una solución comercial para no tener técnicas de evasión en la explotación por virtualización de los sistemas Operativos señuelo. La solución de NDR deberá ser capaz de enviar al menos cinco mil (5,000) archivos por hora al sandbox. Para tecnologías cuya detección y contención se centre principalmente en el análisis de comportamiento y la utilización de Inteligencia Artificial aplicado al análisis de los archivos no se requerirá la utilización de un sandbox.

l. Debe tener la capacidad de bloquear el tráfico malicioso en tiempo real, proporcionando un sistema avanzado de protección contra amenazas, protección contra ataques cibernéticos generados por grupos de "Hacktivismo", Crimen Organizado, Espionaje y Ciberterrorismo.

m. El sistema de protección contra malware debe tener la capacidad de bloquear llamadas a servidores remotos (devoluciones de llamada). En el caso de ataques de día cero, el Sistema de Protección contra Malware debe bloquear la capacidad del malware para realizar llamadas C&C (comando y control), dejándolo inerte y evitando la pérdida de información. Esto significa que debe detectar y prevenir malware avanzado, ataques Zero Day y amenazas persistentes avanzadas dirigidas sin haber sido reconocido previamente por una base de suscripción.

n. La herramienta debe ser capaz de analizar todo el código sospechoso, las URL y varios tipos de archivos en un entorno de inspección o a través de la utilización de más de 650 métricas utilizadas en el modelado del comportamiento sin la necesidad de utilizar un entorno de inspección.

o. La solución debe permitir incorporar reglas SNORT personalizadas para implementar bloqueos customizados sobre el contenido del tráfico o a través de la utilización de IoCs y decisiones de contención autónomas sin la necesidad de utilizar reglas estáticas.

p. En caso se identifique un malware de día cero, éste deberá ser notificado automáticamente a la nube de inteligencia de amenazas del fabricante y ser distribuido a nivel global, incluyendo la capacidad de que la solución de endpoint del mismo fabricante pueda bloquear este mismo malware de manera local Tecnologías de NDR de diferente fabricante deberán bloquear el malware a nivel de la red y notificar a la tecnología de endpoint del fabricante seleccionado para llevar el bloqueo de manera local.

q. La solución debe tener capacidades para: Detectar, Investigar y Contener Malware, Botnets, APTs, Malware Polimórfico y ZeroDays independientemente del mecanismo de deteccion utilizado, sin generar costos adicionales a la Entidad. asimismo, deberá ser capaz de reportar esta amenaza generado en el endpoint, asegurando la contención de las infecciones entrantes y manteniendo así la integridad de los equipos que integran la red.

r. Debe admitir la ejecución e inspección de al menos los siguientes tipos de archivos: 3gp, asf, avi, bat, chm, cmd, com, csv, dll, doc, docx, exe, flv, gif, hqp, html, htm, hwp, ico jar, jpg, js, lnk, midi, mov, mp3, mp4, mpg, pdf, ppsx, ppt, pptx, qt, rm, rmi, rtf, swf, tiff, url, vbs, vcf, vcs, wav, wma, wsf, xls, xlsx, xml.

s. La solución debe tener la capacidad de bloquear las comunicaciones de comando y control (C&C), evitando la pérdida de información y otros daños a la red de la empresa.

t. Disponer de firmas de detección basadas en vulnerabilidades y también detección de ataques desconocidos mediante el análisis de anomalías en el tráfico de red.

u. El sistema de protección de malware debe detectar malware de día cero, malware polimórfico, Botnets y otros APT (Advanced persistent Threats –

Amenazas Persistentes Avanzadas) en la red interna y en las comunicaciones hacia y desde internet (tráfico inbound y tráfico outbound).

v. La plataforma deberá tener la capacidad de detectar software o tráfico malicioso que se aprovecha de vulnerabilidades conocidas.

vi. Permitir la identificación de ataques a protocolos que utilizan puertos aleatorios.

x. La solución debe tener la capacidad de bloquear llamadas a servidores remotos (Callbacks). En el caso de ataques de Día Cero, el Sistema de Protección de Malware deberá bloquear la habilidad del Malware para realizar llamadas C&C (comando & control), de esa manera dejándolo inerte y previniendo pérdida de información.

y. Debe actuar de tal manera que el bloqueo de un intento de intrusión en particular no interfiera con el resto del tráfico de la red.

z. El equipo debe contar con mecanismos de lista blanca reglas basadas en subredes IP, nombres de dominio o puertos de destino para omitir TODOS los análisis y la detección de tráfico adicionales.

aa. La solución debe ser capaz de llevar a cabo protecciones en la dirección "Norte-Sur", para el tráfico entrante y saliente de la organización, y "Este-Oeste", para el tráfico interno de la organización, detectando movimiento lateral. Para esto detectar en al menos los siguientes protocolos:

- DNS • HTTP • HTTPS • FTP • WebSocket/WSS DCERPC/MSRPC • SMB • SMB2 • SSL/TLS • DCERPC • DHCP • DNS • FTP • HTTP • HTTPS • ICMP • IMAP • IRC • ISCSI • KRB o KERBEROS • MySQL • LDAP • NetBIOS • NFS • NNTP • NTP • POP3 • Radius • RDP • rlogin • RSH • RTSP •SCADA • SIP • SMB • SMB2 • SMTP • SNMP • SSL/TLS • TCP • Telnet • TFTP • UDP

bb. Debe permitir mostrar detalles sobre las alertas con al menos las siguientes: Acciones de bloqueo, tipo de aplicación, tipo de archivo, Peap, triage, entre otros.

cc. La solución debe incluir en actividades de movimiento lateral una descripción de la actividad, proporcionar detalles de cómo realizar la investigación y las asignaciones correspondientes hacia que categoría está identificada dentro del marco de seguridad mitre ATT&CK.

dd. La solución debe tener mecanismos para detectar WebShells en PHP, WAR JSP, ASP y ASPX.

ee. Debe permitir y disponer de APIs para facilitar la integración de otras soluciones.

ff. La solución se requiere mecanismos de Machine Learning y/o inteligencia artificial como complemento, pero debe basar la detección en inteligencia, análisis y detección de amenazas reales.

gg. La solución debe enfocar su detección en análisis dinámicos, estáticos, como firmas, IoC, exploits/vulnerabilidades, u otros, estos deben ser complemento de los diferentes mecanismos de detección con los que cuenta la solución.

hh. La solución por ofertar debe tener la capacidad de detectar la explotación de vulnerabilidades de día cero, payload polimórfico y archivo malicioso. También técnicas de ofuscación en javascript. Todo esto en tiempo real, con la posibilidad de bloquear esta actividad maliciosa.

ii. Deberá estar integrada a la tecnología XDR, para que en caso de que el EDR identifique IPs internas maliciosas, éstas sean informadas inmediatamente a la solución XDR y éste realice el bloqueo del tráfico de red generado por estas IPs maliciosas, de manera automática

jj. Deberá disponer de una interfaz web para la administración del sistema y el monitoreo de eventos, con capacidad de utilizar protocolos encriptados (tipo SSL, SSH) para proteger las comunicaciones

kk. Debe contar con la capacidad de gestionar diferentes niveles de usuario (derechos de administrador / Monitor / Operador / Analista).

ll. Deberá contar la capacidad de generar reportes que permita obtener información sobre las principales alertas, al menos con los siguientes criterios: estáticos / programados.

mm. La solución deberá permitir enviar notificaciones en diversos formatos requeridos como: Syslog, SNMP, http, SMTP y estar sincronizado mediante NTP.

nn. La solución por ofertar deberá tener la posibilidad de exportar sus informes en formato CSV y PDF de manera automática (programada) o manual.

3.2 CABLEADO ESTRUCTURADO

- **Cableado vertical y horizontal.**

✓ Como parte de las labores de instalación y puesta en operación de los equipos en cada uno de los Gabinetes o Racks (de la respectiva sede CDP y CDR) se debe efectuar el Cableado Estructurado (entre los Gabinetes o Racks, los Gabinetes que tienen instalados los Switches Core de Centro de Datos). Esto es, efectuar el Cableado Estructurado de los Racks de Comunicaciones.

La ejecución debe estar basada en los estándares y recomendaciones nacionales e internaciones que se detallan seguidamente:

- EIA/TIA-568C: Norma cableado de fibra óptica.
- ANSI/EIA/TIA-569B: Comercial Building Standard for Telecommunications Pathways and Spaces.
- BICSI.
- ANSI/EIA/TIA-606A: Administration Standard for the Telecommunications Infrastructure of Comercial Buildings.
- ANSI/EIA/TIA-607.
- ANSI/EIA/TIA-310.
- National Fire Protection Agency (NFPA).
- National Electrical Code (NEC).

✓ El cableado estructurado a ser instalado está conformado por los siguientes tipos de cables:

- Cables UTP Categoría 6A.
- Cables de Fibra óptica MMF (multimodo).

✓ Todo el cableado a realizar debe ser realizado de acuerdo a los estándares y normas de cada Administrador de los Data Center (CDP y CDR) y con el Banco, Subgerencia de Producción de la Gerencia de Tecnologías de Información.

✓ EL CONTRATISTA deberá hacer adecuaciones eléctricas para poner en operación la solución propuesta.

- ✓ La topología de la entidad es del tipo End of Row y con el sistema de cableado IMVISION (que incluye (Ptach , patch panels inteligentes y todos los elementos necesarios para su adecuado funcionamiento); todo cableado a implementar deberá integrarse y ser registrado en el Sistema IMVISION del Banco (Será responsabilidad del Banco la integración de los nuevos componentes al Sistema IMVISION), para ello EL CONTRATISTA deberá proveer Controladores , Patchs Panels Inteligentes de Fibra y/o UTP , conectores , acopladores , módulos de fibra y/o UTP , en caso sea necesario y sin costo adicional al Banco.
- ✓ Los insumos o materiales a utilizar deben ser certificados (UL o ISO) y ser de uso exclusivo para cableado estructurado. Estos insumos o materiales deberán estar debidamente sustentados a través de sus respectivas hojas técnicas y número de parte.
- ✓ El servicio de rotulación (incluido como parte de las labores a efectuar por personal de EL CONTRATISTA) deberá ser coordinado con el personal técnico del BN antes de efectuar el mismo. Incluye equipos y cables de datos.
- ✓ EL POSTOR podrá realizar visita de inspección a los locales del BN donde se implementará la solución (CDP y CDR) a fin de evaluar la naturaleza del requerimiento (necesaria para la formulación de su propuesta técnica) hasta cinco (05) días útiles antes de la entrega de la propuesta, en horario laboral (de 08:30 horas a 17:30 horas). La persona encargada de coordinar las visitas será:
  - Sr Levi Cotrina Herrera - email lcotrinah@bn.com.pe, para la visita en el CDR y CDP
- ✓ Para las labores de cableado estructurado que requieran realizar obras civiles, estas deberán ser formuladas por EL CONTRATISTA a fin de que sean validadas y aprobadas por el área especialista del BN (Subgerencia de Producción)

3.3 PERFIL MÍNIMO DEL PERSONAL

El Contratista deberá presentar para la firma del contrato la documentación que acredite la formación académica y capacitación, correspondiente al personal NO CLAVE

a) **Personal clave: Un (01) especialista en Solución para Detección y Respuesta Extendida (XDR) y Solución para Detección y Respuesta de Endpoints (EDR)**

- ✓ **Formación académica**: Técnico Titulado o Bachiller o Profesional Titulado en la especialidad de ingeniería en Sistemas o Telecomunicaciones o Informática o Electrónica o Ingeniería de Seguridad y Auditoría Informática o Ingeniería de Sistemas y Cómputo o Ingeniería de Computación o Ingeniería Informática o Ingeniería de Sistemas Empresariales o Ingeniería de Sistemas y Computación o Ingeniería de redes y comunicación o Ingeniería de software.
  - **Acreditación:** Se acreditará con copia simple de Título de Técnico o grado de Bachiller o Título Profesional.
- ✓ **Capacitación:** Certificación Oficial vigente en la solución XDR y/o EDR ofertada expedida por el fabricante (Nivel técnico vigente)

- **Acreditación:** Se acreditará con copia simple de constancia, certificado u otro documento, según corresponda

✓ **Experiencia:** Experiencia mínima dos (02) años en implementación de soluciones de XDR y EDR

- **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.

✓ **Actividades del Especialista en XDR y EDR.**

- Puesta en producción de las soluciones de XDR y EDR propuestas.

b) **Personal clave: Un (01) especialista en Solución para Detección y Respuesta en la RED (NDR)**

✓ **Formación académica**: Técnico Titulado o Bachiller o Profesional Titulado en la especialidad de ingeniería en Sistemas o Telecomunicaciones o Informática o Electrónica o Ingeniería de Sistemas y Computo o Ingeniería de Computación o Ingeniería Informática o Ingeniería de Sistemas Empresariales o Ingeniería de Sistemas y Computación o Ingeniería de redes y comunicación o Ingeniería de software.

- **Acreditación:** Se acreditará con copia simple de Título de Técnico o grado de Bachiller o Título Profesional.

✓ **Capacitación:** Certificación Oficial de fabricante de la solución NDR propuesta (Nivel técnico vigente)

- **Acreditación:** Se acreditará con copia simple de constancia, certificado u otro documento, según corresponda

✓ **Experiencia:** Experiencia mínima dos (02) años en implementación de solución de NDR

- **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.

✓ **Actividades del Especialista en NDR.**

- Puesta en producción de la solución NDR propuesta.

c) **Personal clave: Un (01) Jefe de Proyecto**

✓ **Formación académica:** La condición mínima para esta persona deberá ser la del profesional Titulado en Ingeniería de la especialidad de Sistemas o Telecomunicaciones o Informática o Electrónica o Ingeniero Informático y de Sistemas o Ingeniería de Sistemas y Computo o Ingeniería de Computación o Ingeniería Informática o Ingeniería de Sistemas Empresariales o Ingeniería de Sistemas y Computación o Ingeniería de Seguridad o Auditoria Informática o Ingeniería Industrial.

- **Acreditación:** Se acreditará con copia simple del Título Profesional

- ✓ Capacitación: Certificación PMP (Project Management Profesional) vigente o diplomado de especialización en dirección y gestión de proyectos bajo el enfoque PMI con un mínimo de 360 horas de duración o diplomado de especialización en dirección y gestión de proyectos bajo el enfoque PMI con un mínimo 24 créditos académicos.
  - Acreditación: Se acreditará con copia simple de constancia, certificado u otro documento según corresponda.
- ✓ Experiencia: Experiencia mínima de dos (02) años de experiencia en la gestión de proyectos de TIC.
  - 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.
- ✓ Actividades del Jefe de Proyecto.
  - Deberá supervisar el cumplimiento y hacer seguimiento de la puesta en producción de las soluciones (XDR, EDR y NDR) propuestas

d) Personal NO CLAVE: Un (01) residente de seguridad

- ✓ Formación académica: Técnico Titulado o Bachiller o Profesional Titulado en la especialidad de ingeniería en Sistemas o Telecomunicaciones o Informática o Electrónica o Redes y Comunicaciones o Computación e Informativa o Ingeniería de Sistemas o Sistemas de Telecomunicaciones o Redes de Computadoras y Comunicación de Datos o Ingeniería de Software.
  - Acreditación: Se acreditará con copia simple de Título de Técnico o grado de Bachiller o Título Profesional, a la firma del contrato
- ✓ Capacitación: Certificación Oficial de fabricante de las soluciones propuestas XDR y/o EDR y NDR (Nivel técnico vigente)
  - Acreditación: Se acreditará con copia simple de constancia, certificado u otro documento, según corresponda a la firma del contrato
- ✓ Experiencia: Experiencia mínima de dos (02) años en la instalación y/o mantenimiento y/o implementación y/o administración y/o soporte de soluciones de XDR, EDR y NDR.
  - Acreditación: La experiencia del personal no 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, a la firma del contrato.
- ✓ Actividades del Residente de seguridad.
  - Monitoreo de recursos y verificación de alarmas de las funciones de seguridad:
    - Detección de Eventos e Incidentes
    - Atención de Averías
  - Optimización de la plataforma

- Revisión de profile de las soluciones propuestas luego del descubrimiento durante un periodo en coordinación conjunta con el Banco de la Nación.
- Afinamiento de políticas de seguridad en coordinación con el Banco de la Nación.
- Revisión de excepciones mensuales.

- Elaboración de reportes mensuales de eventos de seguridad por cada servicio crítico:
  - Reporte de ataques, duración y estado de bloqueo.
  - Clasificación por criticidad y protocolo.
- Revisión mensual de nuevos releáse de software y validación de aplicación según nuevos BUGS/HOTFIX.
- Elaboración de reportes de estado de salud de los equipos de la solución
- Atención de requerimientos para la plataforma.
- Mantenimiento y respaldo de información de toda la plataforma.
- Gestionar y canalizar escalamientos de soporte de modo presencial o remoto (internet) de toda la plataforma hasta que se tenga solucionado el evento reportado
- Informe mensual de tipo gerencial que relacione como mínimo los eventos detectados, correlacionados y notificados, los hallazgos más relevantes del periodo, el estado de salud/capacidad de la plataforma gestionada y las acciones de mejora sugeridas.
- Reporte mensual de casos de servicio abiertos.
- Informe mensual de cumplimiento de los SLAs
- Reporte mensual de estado de salud del servicio y de las soluciones implementadas.
- Reporte a demanda de la solución implementada.

Si debiera producirse un reemplazo, el/la reemplazante deberá ser aprobado por la Oficina de Seguridad Informática y reunir al menos las mismas habilidades, competencias y experiencia que el/la reemplazado/a; el reemplazo deberá ser después de tres (03) días calendario como máximo después de notificar al BN el cambio y no afectara el periodo de implementación establecido.

3.4 INSTALACIÓN E IMPLEMENTACIÓN DEL SERVICIO

El proceso de instalación de los equipos e implementación de las soluciones adquiridas incluirá el uso de sus recursos humanos, herramientas, útiles y materiales de trabajo, por lo que el servicio deberá ser presupuestado a todo costo, y por lo tanto al BN le debe significar ningún costo adicional.

EL CONTRATISTA deberá realizar todas las configuraciones necesarias para lograr el objetivo descrito en el alcance, así como realizará otras configuraciones involucradas y que no están mencionadas en el presente documento con el fin de

dejar todo el sistema de red operativo, y sin perder la continuidad del servicio que se brinda actualmente. Dado que los equipos solicitados están íntimamente relacionados a la continuidad operativa del Banco de la Nación.

El ganador de la buena pro debe asegurar que durante la instalación e implementación de los equipos de la solución tendrá acompañamiento por al menos un especialista del área de servicios profesionales del fabricante de la solución ofertada (debe ser refrendado con una carta del fabricante) durante al menos las dos primeras semanas de instalación, a fin de asegurar la adecuada integración de las soluciones adquiridas con los endpoints y la red del banco.

El Plazo de Entrega máximo del servicio será de noventa (90) días calendario (contados a partir del día siguiente de la fecha de suscripción del Contrato)

Para la implementación del servicio el contratista deberá cumplir con lo siguiente.

- ✓ Designar un Jefe de Proyectos el cual tendrá la responsabilidad de gestionar el proceso de implementación con el BN.
- ✓ El Jefe de Proyectos deberá seguir las mejores prácticas según la metodología PMP.
- ✓ EL CONTRATISTA, dentro de los cinco (05) días calendario posteriores de firmado el contrato deberá organizar una reunión kick off en coordinación con el BN, donde serán presentados los contactos de las diferentes áreas y otros proveedores quienes estarán involucrados en la ejecución del proyecto.
- ✓ En dicha reunión (Kick off), el jefe de proyecto deberá presentar un Plan/Cronograma de implementación, mismo que será ratificado por el BN dentro de los 05 días calendario siguientes. Este Plan/Cronograma de implementación debe cubrir todas las tareas a llevarse a cabo desde la firma del contrato hasta la entrega del Acta de Conformidad de Aceptación. El plan de trabajo, debe establecer plazos mínimos y máximos para cada una de las tareas a cumplir, diferenciándose claramente las que debe cumplir el BN, EL CONTRATISTA en forma exclusiva, y las que deben asumir en forma compartida.
- ✓ El Jefe de Proyectos tendrá que reportar semanalmente los avances del proyecto, así como sus riesgos, al personal encargado de administrar el servicio en el BN, este reporte será en físico y lógico
- ✓ El CONTRATISTA debe gestionar el servicio con un enfoque de proyecto bajo el estándar PMI y estará obligado a presentar los siguientes entregables de gestión además de los relacionados al producto o servicio propiamente dicho:

  - **Fase de Iniciación:**
    - Project Charter del Proyecto
    - Identificación de todos los involucrados
  - **Fase de Planificación:**
    - WBS (Estructura de desglose del trabajo)
    - Cronograma en detalle
    - Plan de Gestión del Proyecto
  - **Fase de Ejecución:**

- Actividades de detalle orientadas a la puesta en servicio como objetivo del proyecto.
- Manejo de las expectativas de los involucrados.

- **Fase de Seguimiento y Control:**
  - Actas de Reuniones
  - Peticiones o Solicitudes de Cambios aprobadas.
  - Informes de avances periódicos según el cronograma.

- **Fase de Cierre:**
  - Lecciones aprendidas
  - Acta de Conformidad de implementación del Servicio.

Para el Acta de Conformidad de implementación del Servicio el Contratista debe entregar el informe el cual debe incluir:

- ✓ Diseño descriptivo de las soluciones implementadas.
- ✓ Diagrama Esquemático implementada en los Centros de Datos (CDP, CDR).
- ✓ Diagrama unifilar de interconexión de los equipos instalados en los Centros de Datos (CDP, CDR).
- ✓ Documentación Técnica y/o Manual de la instalación, configuración y administración de los equipos y soluciones adquiridas.
- ✓ Inventario de Equipos.

4. CARACTERÍSTICAS Y CONDICIONES DE LA PRESTACIÓN ACCESORIA AL SERVICIO.

La Prestación Accesoria está compuesta por Entrenamiento, el cual deberá ser provistos de acuerdo a lo señalado en el presente documento.

4.1. ENTRENAMIENTO

EL CONTRATISTA deberá incluir como parte de su propuesta los siguientes cursos, los cuales deber ser dictados durante los primeros seis (6) meses del Servicio:

Un curso de las soluciones propuestos el cual debe cumplir con lo siguiente:

- ✓ Ser un curso oficial y certificado por parte del fabricante de las soluciones ofertadas (XDR, EDR, NDR)
- ✓ Dictado en una institución autorizada y certificada por el fabricante en modo presencial o remoto. El proveedor deberá acreditar el dictado del entrenamiento con una carta de la institución especializada.
- ✓ Abarca los tópicos referidos a todas las prestaciones de las soluciones ofertadas. Podemos incluir troubleshooting.
- ✓ 24 horas efectivas de dictado
- ✓ Dirigido a seis (06) personas del BN
- ✓ Se entregará material didáctico a cada asistente

- ✓ Para verificar el nivel de asimilación de cada participante en el curso, el mismo debe contener:
  - Prácticas calificadas.
  - Pruebas escritas de conocimientos.

5. OTRAS OBLIGACIONES A CARGO DEL CONTRATISTA

El contratista se compromete a cumplir y a observar los Resolución Ministerial N° 031-2023-MINSA que aprueba a Directiva Administrativa N° 339-MINSA/DGIESP-2023, "Directiva Administrativa que establece las disposiciones para la vigilancia, prevención y control de la salud de los trabajadores con riesgo de exposición a SARS-CoV-2, Manteniendo en sus trabajadores la sensibilización de la prevención del contagio en el centro de trabajo a través de las capacitaciones en temas de la COVID-19, así como de las medidas preventivas personales dotándoles de equipos de protección personal en la prevención de la COVID-19. Asimismo, bajo el cuidado de la salud de los trabajadores en el contexto COVID-19, deberán realizar la vigilancia de la salud de sus trabajadores de manera permanente.

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.

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.

8. OTRAS PENALIDADES

Se aplican las penalidades indicadas en el Anexo A

7. REQUISITOS DE CALIFICACIÓN

A EXPERIENCIA DEL POSTOR EN LA ESPECIALIDAD

Requisitos:

El postor debe acreditar un monto facturado acumulado equivalente a S./10'000,000.00 (diez Millones y 00/00 Soles), por la contratación de servicios iguales o similares al objeto de la convocatoria, durante los ocho (08) años anteriores a la fecha de la presentación de ofertas que se computarán desde la fecha de la conformidad o emisión del comprobante de pago, según corresponda

Se consideran servicios similares a los siguientes: Servicio de Licencias o Servicio de CYBERSOC o Administración y Monitoreo de Plataformas de Seguridad o Correlación de Eventos de Seguridad o Servicio de soporte de mantenimiento o Servicio de monitoreo y administración de plataformas de seguridad TI o Servicio de monitoreo de eventos de seguridad (SOC) o Servicio de CyberSOC, Servicio de Red Team o Servicio de monitoreo de equipamiento de seguridad o Servicio de seguridad Gestionada o Servicio de Solución Integral Tecnológica de Ciberseguridad – SIEM o Servicio de soporte de plataforma de seguridad y correlación o Servicio de Ciberseguridad o Servicios Gestionados de seguridad o Soporte Local o Ethical Hacking o Servicio de Seguridad de la Red Interna y Perimetral o Servicio de Detección y Respuesta ante Amenazas o Servicio de Operación de la Seguridad y Servicio de CyberSOC o Servicios de Ciberseguridad y ciberdefensa o Servicio de seguridad de informática o TI o Seguridad de la información o Seguridad gestionada o Servicio de Ciberseguridad o Servicio de Cyber Defense.

Acreditación:

La experiencia del postor en la especialidad se acreditará con copia simple de (i) contratos u órdenes de compra, 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, correspondientes a un máximo de treinta (30) contrataciones.

B CAPACIDAD TÉCNICA Y PROFESIONAL

B.1 EXPERIENCIA DEL PERSONAL CLAVE

Requisitos:

- Un (01) especialista con experiencia mínima dos (02) años en implementación de soluciones de XDR y EDR.
- Un (01) especialista con experiencia mínima dos (02) años en implementación de solución de NDR.
- Un (01) Jefe de Proyecto con experiencia mínima de dos (02) años de experiencia en la gestión de proyectos de TIC.

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.

B.2 FORMACIÓN ACADÉMICA DEL PERSONAL CLAVE

Requisitos:

- Un (01) especialista con Formación académica: Técnico Titulado o Bachiller o Profesional Titulado en la especialidad de Ingeniería en Sistemas o Telecomunicaciones o Informática o Electrónica o Ingeniería de Seguridad y Auditoria Informática o Ingeniería de Sistemas y Computo o Ingeniería de Computación o Ingeniería Informática o Ingeniería de Sistemas Empresariales o Ingeniería de Sistemas y Computación o Ingeniería de redes y comunicación o Ingeniería de software.
- Un (01) especialista con Formación académica: Técnico Titulado o Bachiller o Profesional Titulado en la especialidad de Ingeniería en Sistemas o Telecomunicaciones o Informática o Electrónica o Ingeniería de Sistemas y Computo o Ingeniería de Computación o Ingeniería Informática o Ingeniería de Sistemas Empresariales o Ingeniería de Sistemas y Computación o Ingeniería de redes y comunicación o Ingeniería de software.
- Un (01) Jefe de Proyecto con Formación académica: Titulado en Ingeniería de la especialidad de Sistemas o Telecomunicaciones o Informática o Electrónica o Ingeniero Informático y de Sistemas o Ingeniería de Sistemas y Computo o Ingeniería de Computación o Ingeniería Informática o Ingeniería de Sistemas Empresariales o Ingeniería de Sistemas y Computación o Ingeniería de Seguridad o Auditoria Informática o Ingeniería Industrial.

Acreditación:
Se acreditará con copia simple de Título de Técnico o grado de Bachiller o Título Profesional.

B.3 CAPACITACIÓN DEL PERSONAL CLAVE

Requisitos:

- Un (01) especialista con Certificación Oficial vigente en la solución XDR y/o EDR ofertada expedida por el fabricante (Nivel técnico vigente).
- Un (01) especialista con Certificación Oficial de fabricante de la solución NDR propuesta (Nivel técnico vigente).
- Un (01) Jefe de Proyecto con Certificación PMP (Project Management Profesional) vigente o diplomado de especialización en dirección y gestión de proyectos bajo el enfoque PMI con un mínimo de 360 horas de duración o diplomado de especialización en dirección y gestión de proyectos bajo el

enfoque PMI con un mínimo 24 créditos académicos.

Acreditación:
Se acreditará con copia simple de constancia, certificado u otro documento, según corresponda.

8. PLAZO DE ENTREGA

- **Servicio:**

  El Plazo de Entrega máximo del servicio será de noventa (90) días calendarios (contados a partir del día siguiente de la fecha de suscripción del Contrato) para la entrega de los equipos, licencias y la respectiva configuración, instalación y puesta en producción del servicio a plena satisfacción del BN.

- **Prestación Accesoria:**

  El plazo de la prestación accesoria será durante los primeros seis (6) meses del Servicio.

9. LUGAR DE PRESTACIÓN DEL SERVICIO

EL CONTRATISTA suministrará los equipos (hardware/software, licenciamiento y accesorios) en la cantidad y especificaciones técnicas referidas en el presente documento.

EL CONTRATISTA implementará el servicio, en los lugares que se muestran a continuación:

NODO	DEPENDENCIA	DIRECCION
1	Centro de Datos Principal BN (CDP)	Av. Javier Prado Este 2499 – San Borja – Lima
2	Centro de Datos de Respaldo BN (CDR)	Av. Arequipa 2720 San Isidro – Lima

10. FORMA DE PAGO

10.1 SERVICIO

El pago del servicio será de manera mensual.

Previo al pago del servicio, el CONTRATISTA deberá entregar un informe y este informe formará parte de la documentación necesaria para expedir el acta de conformidad del servicio, el informe debe contener lo siguiente:

- Informe mensual de tipo gerencial que relacione como mínimo los eventos detectados, correlacionados y notificados, los hallazgos más relevantes del periodo, el estado de salud/capacidad de la plataforma gestionada y las acciones de mejora sugeridas.
- Reporte mensual de estado de salud del servicio y de las soluciones implementadas.

Para tal efecto la Oficina de Seguridad Informática de la Gerencia de Tecnologías de Información del BN emitirá el acta de conformidad del servicio previo informe técnico emitido por la Oficina de Seguridad Informática y visado por la subgerencia de Producción en un plazo que no excederá de los diez (10) días calendario de ser recibida la documentación correspondiente del Contratista.

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

a. Comprobante de pago.
b. Acta de Conformidad emitida por la Oficina de Seguridad Informática de la Gerencia de Tecnologías de Información.
c. Informe Técnico del funcionario de la Oficina de Seguridad Informática de la Gerencia de Tecnologías de Información.

10.2 PRESTACIÓN ACCESORIA

Previo al pago de la prestación accesoria, el CONTRATISTA deberá entregar un informe donde se indique todas las actividades ejecutadas, este informe formará parte de la documentación necesaria para expedir el acta de conformidad de la Prestación Accesoria.

La prestación Accesoria se pagará en un solo pago, en soles.

- ✓ El Entrenamiento en el semestre en que se realizó la misma.

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

a) Comprobante de pago.
b) Acta de Conformidad emitida por la Oficina de Seguridad Informática.
c) Informe del funcionario responsable de Oficina de Seguridad Informática, emitiendo la conformidad de la prestación efectuada

11. ÁREA RESPONSABLE

La conformidad del servicio será otorgada por la Oficina de Seguridad Informática de la Gerencia de Tecnologías de Información, en su calidad de área usuaria y técnica, quienes deberán verificar el cumplimiento de las condiciones contractuales.

12. 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 de responsabilidad del contratista es de treinta y seis (36) meses, contado a partir de la conformidad otorgada por LA ENTIDAD

13. SUBCONTRATACIÓN

No se permitirá la subcontratación.

14. GESTIÓN INTEGRAL DE RIESGOS Y AUDITORIA

- El proveedor está obligado a permitir la revisión, supervisión e inspección de los servicios prestados y de las condiciones que garanticen la seguridad de información

protección de datos personales, continuidad del negocio y gestión de sus riesgos, por parte de la dependencia responsable del contrato, el Órgano de Auditoria Interna del Banco, de la sociedad auditora externa, así como por parte de la Superintendencia, en la oportunidad que cualquiera de estos órganos lo solicite, con un aviso previo por escrito de veinticuatro (24) horas, el cual será remitido a la dirección indicada por el proveedor en el contrato. En dicho comunicado se designarán a las personas que efectuarán la mencionada revisión, supervisión e inspección. Consecuentemente, el proveedor se compromete a facilitar todos los recursos y medios necesarios a las personas antes mencionadas para efectuar dicha revisión.

- El incumplimiento de las obligaciones que asume el proveedor en las cláusulas referidas, constituyen causal de resolución automática y de pleno derecho del presente contrato, de conformidad con lo previsto en el Artículo 165° del Reglamento de la Ley N° 30225 "Ley de contrataciones del Estado" (en el caso de contratos dentro del marco de la Ley de Contrataciones), y el artículo N° 1430° del Código Civil, sin perjuicio de la obligación del proveedor de pagar al Banco la indemnización correspondiente.
- En caso el Banco incurriera en costos y/o multas establecidas por parte de un organismo regulador u otro, mediante una resolución o sentencia firme producto de la interrupción y/o algún error o falla en las condiciones de la prestación del servicio por causas imputables al proveedor, éste se hará totalmente responsable de dichas penalidades, asumiendo el importe de las mismas sin reserva ni limitación alguna. Por lo que, el Banco podrá evaluar la aplicación de penalidades o el pago de indemnización mediante las cláusulas de penalidades que correspondan por la no operatividad del servicio, conforme al SLA que haya definido en los Términos de Referencia.

El CONTRATISTA deberá cumplir con los siguientes requerimientos:

14.1. SEGURIDAD DE LA INFORMACIÓN

- Para garantizar la integridad, disponibilidad y confidencialidad de la información el CONTRATISTA debe implementar y cumplir con los lineamientos de seguridad de la información que apliquen al servicio contratado.
- El CONTRATISTA se obliga a adoptar las medidas necesarias para sus trabajadores, representantes y personal o terceros subcontratados que intervengan para el cumplimiento del servicio contratado, cumplan con las disposiciones sobre la seguridad y confidencialidad de la información.
- El CONTRATISTA es el responsable del resguardo y protección de los activos de información (equipos, dispositivos informáticos, aplicaciones, información, entre otros) de propiedad del Banco de la Nación, involucrados en el servicio contratado, que se encuentren bajo la administración del CONTRATISTA o que formen parte del servicio contratado.
- El Banco en coordinación con el contratista, adoptarán las medidas de seguridad en los sistemas tecnológicos involucrados en el servicio contratado, a fin de mitigar los riesgos y asegurar que la información se proteja de forma segura. Estas medidas deberán ser plasmadas en un documento y ejecutadas en la etapa de implementación y ante cualquier incidente o mejora del servicio.
- Antes de realizar cualquier cambio o mantenimiento de los sistemas tecnológicos relacionados al servicio contratado, el CONTRATISTA deberá

coordinar con el Banco, a fin de definir las acciones pertinentes para dicha actividad.

- El Banco y el CONTRATISTA restringirán el acceso a la información física y lógica, así como a los sistemas informáticos inmersos en el servicio, sólo al personal autorizado del Banco y del CONTRATISTA, por lo que ningún tercero no autorizado tendrá acceso a la información relacionada con el servicio contratado.
- En la etapa de implementación, el CONTRATISTA en coordinación con el Banco definirán el proceso de cómo se gestionarán los riesgos, alertas o incidentes de seguridad de la información, relacionados con el servicio contratado.
- El CONTRATISTA permitirá, facilitará y/u otorgará al Banco la revisión del cumplimiento de las normas de seguridad de la información relacionados con el servicio asociado al contratado.
- De aplicar desarrollo de softwares, aplicativos que el CONTRATISTA proporcione para el Banco, en el marco del servicio contratado, estos serán de titularidad del Banco, durante la ejecución del contrato, por lo tanto, el CONTRATISTA no podrá asumir ningún derecho sobre ellos.

14.2. PROTECCIÓN DEL SECRETO BANCARIO, TELECOMUNICACIONES Y DATOS PERSONALES

- El Banco y el CONTRATISTA declaran conocer que están obligados a salvaguardar y mantener la confidencialidad del secreto bancario, de las telecomunicaciones y de los datos personales de los usuarios y clientes del Banco de la Nación, de acuerdo con la Constitución Política del Perú, Ley N°29733 Ley de Protección de datos personales, su Reglamento y Directivas de Seguridad, Ley N°26702, Secreto Bancario y la Ley N° 28096 Ley de Telecomunicaciones, sus modificatorias y actualizaciones; aplicables a los servicios objeto del contrato.
- El CONTRATISTA debe poner en conocimiento de su personal y de los terceros que requiera para ejecutar el contrato, que tuvieran acceso a la información del Banco, la obligación de salvaguardar y mantener la confidencialidad del secreto bancario, de las telecomunicaciones y de los datos personales, esta obligación se mantendrá vigente inclusive luego de haber concluido el presente contrato, salvo que medie autorización expresa de estos últimos para su tratamiento.
- Los datos personales que el Banco le proporcione al CONTRATISTA a lo largo de la prestación del servicio, el CONTRATISTA deberá cumplir con el tratamiento de datos personales de acuerdo a las disposiciones establecidas en la Ley N° 29733, Ley de Protección de Datos Personales, su Reglamento y Directiva de seguridad.
- Cualquier información que se intercambie y se genere bajo cualquier formato y medio, como parte del servicio, es de propiedad exclusiva del Banco y por ningún motivo pueda ser utilizada por el contratista para un fin distinto al contrato y no debe divulgarla a terceros salvo autorización expresa del Banco.
- El CONTRATISTA declara conocer las sanciones tipificadas en la Ley N° 3096, Ley de Delitos Informáticos (integridad de datos informáticos, tráfico ilegal de

datos, interceptación de datos informáticos), así como dar cumplimiento de las mismas.

14.3. CONFIDENCIALIDAD DE LA INFORMACIÓN

- Como parte del servicio el CONTRATISTA tomará conocimiento de la información del Banco. Esta información es confidencial, por lo tanto, el CONTRATISTA y todo su personal mantendrá la confidencialidad de la misma. El compromiso de confidencialidad se prolonga indefinidamente aún después de terminado el servicio, y se hace extensivo al personal que el CONTRATISTA subcontrate aun cuando hayan dejado de tener vínculo laboral con el CONTRATISTA.
- El CONTRATISTA se compromete a mantener toda información suministrada por el Banco en estricta reserva y absoluta confidencialidad, así como de adoptar las medidas que resulten necesarias para impedir que la Información Confidencial sea conocida o revelada a terceros o que sea utilizada para fines distintos para los cuales fue entregada.
- Se entiende que la obligación asumida está referida no sólo a documentos e informaciones señalados por la otra parte como "confidenciales" sino a todos los documentos e informaciones que, en razón del referido intercambio, pueda ser conocida por cualquier medio, incluyendo, sin limitarse a ella, a programas de cómputo, nombres de clientes, estrategias financieras o comerciales, etc.
- El CONTRATISTA se obliga a tomar todas las medidas y precauciones razonables para que sus trabajadores y en general cualquier persona con la que tenga relación, no divulgue a ningún tercero los documentos o información a los que tengan acceso, haciéndose responsables por la divulgación que se pueda producir y asumiendo el pago de la indemnización por daños y perjuicios. Estas medidas incluyen, aunque no se limitan a: (i) poner en disposición la información confidencial sólo a un número restringido de personas; (ii) permitir que sus trabajadores, agentes o terceros, accedan a la información confidencial sólo hasta donde sea necesario para la prestación de los servicios; (iii) exigir a su personal o trabajadores como condición previa al acceso a la información confidencial que se obliguen por escrito a respetar esta cláusula de confidencialidad. El compromiso de confidencialidad se prolonga por 10 años después de terminado el servicio, y se hace extensivo al personal que el proveedor subcontrate aun cuando hayan dejado de tener vínculo laboral con el CONTRATISTA.
- El CONTRATISTA reconoce que la información que se le entregue, procese, facilite o genere en razón a su desempeño y/o ejecución del presente contrato, se considera un activo del Banco, por consiguiente, el CONTRATISTA se obliga a:

  1. Mantener en confidencial dicha información, sin divulgarla, ni entregarla, directa o indirectamente a terceras personas naturales o jurídicas.
  2. No usarla para cualquier otro fin que no sea en relación con la prestación de los servicios; ni obtener un beneficio propio o de terceros de ella.
  3. No entregarla o revelarla, de manera total o parcial, pública o privada, a ninguna persona sea en el Perú como en el extranjero, sin el consentimiento escrito previo del Banco, aun cuando se encuentre obligado con alguna de las partes por un acuerdo de confidencialidad

similar, salvo a los empleados de cada una de ellas o de cualquier otra persona que se encuentre en una relación contractual o de confianza con el proveedor y que requiera dicha información para utilizarla para asuntos relacionados con los servicios.

4. El CONTRATISTA debe asegurar de que toda la Información Confidencial sea usada para el exclusivo beneficio de los servicios que se prestan en virtud del contrato. Por tal razón, la violación de cualquiera de las disposiciones establecidas en esta cláusula obligará al proveedor a indemnizar todos los perjuicios directos que cause con motivo de ello y, de caso ser necesario, a resolver de manera automática el contrato.

- Se considera como violación de la confidencialidad y, por tanto, una conducta desleal, la divulgación o explotación sin autorización de la otra parte, de la información a la que tendrá acceso legítimamente, pero con deber de reserva.
- Se entiende que la obligación asumida está referida no sólo a documentos e informaciones señalados por la otra parte como "confidenciales" sino a todos los documentos e informaciones que, en razón del referido intercambio, pueda ser conocida por cualquier medio, incluyendo sin limitarse a ella, características técnicas, sistemas, programación de instalación, ubicación física, información de las Oficina, etc.
- El CONTRATISTA se obliga a mantener y guardar en estricta reserva y absoluta confidencialidad todos los documentos e informaciones que reciban del Banco durante las negociaciones y ejecución del servicio.
- Para la prestación del servicio el proveedor se compromete a firmar un acuerdo de confidencialidad de la información.
- Para la prestación del servicio el CONTRATISTA se compromete a firmar un acuerdo de confidencialidad.

14.4. CONTINUIDAD DEL NEGOCIO

EL PROVEEDOR debe desarrollar la gestión de continuidad para el servicio objeto del contrato, mediante la aplicación de la Resolución S.B.S N° 877-2020 Reglamento para la gestión de la continuidad del negocio o buenas prácticas para la Gestión de Continuidad del Negocio (ISO 20301) para este tipo de servicio.

EL PROVEEDOR se compromete a mantener la continuidad del servicio contratado por EL BANCO para lo cual, debe contar con procedimientos documentados que permitan responder, recuperar, reanudar y restaurar el servicio objeto del contrato; además, los referidos procedimientos deben formar parte de un Plan de Recuperación de Tecnología de Información o en su defecto de un Plan de Continuidad de Negocio, de tal modo que su ejecución asegure la alta disponibilidad.

EL PROVEEDOR debe entregar a EL BANCO, el Plan de Recuperación de Tecnología de Información / Plan de Continuidad de Negocio, los cuales deban estar actualizados y probados cuando menos una vez al año; asimismo, EL PROVEEDOR deberá contar con un Programa de Pruebas respecto a los procedimientos documentados. Al respecto, EL PROVEEDOR deberá remitir cada primer trimestre del año el Plan(es) y Programa de Pruebas, así como un reporte que resuma los resultados alcanzados de las pruebas efectuadas.

EL PROVEEDOR programará las pruebas en horarios de madrugada a fin de reducir la afectación del servicio en coordinación con la Oficina de Seguridad Informática; para casos de pruebas que implique la interrupción del servicio, estas deben ser identificadas y comunicadas desde su programación. Asimismo, EL BANCO podrá solicitar su participación en el desarrollo de dichas pruebas, y de tener alguna observación sobre los resultados de las pruebas podrá remitirla a EL PROVEEDOR para que lo evalúe y responda en un periodo no mayor a treinta (30) días con un plan de acción y fecha estimada para subsanar la(s) observación(es).

Ante la eventual interrupción del servicio objeto del contrato por causales imputables a EL PROVEEDOR, siempre que dicha interrupción sea continúa y se mantenga por un periodo mayor a una (01) hora; EL PROVEEDOR deberá comunicar a EL BANCO (con copia al correo electrónico de la Oficina de Seguridad Informática) de forma inmediata o máximo al día siguiente de ocurrida la incidencia y posterior a ello deberá remitir un informe técnico detallado de la interrupción (incluyendo como mínimo el detalle de: la fecha, hora, duración, causa/origen, diagnostico, impacto, acciones para la recuperación del servicio, estado del servicio afectado, acciones de mejora, conclusiones y recomendaciones), en un plazo máximo de cinco (05) días hábiles, ambos periodos contabilizados a partir de la ocurrencia del evento.

Para casos que EL PROVEEDOR realice cambios a sus configuraciones u otros componentes que involucren/afecten la operatividad del servicio objeto del contrato, deben ser comunicados a EL BANCO con cinco (05) días hábiles de anticipación a la Oficina de Seguridad Informática.

EL PROVEEDOR se compromete a entregar a EL BANCO toda la documentación y/o información que pueda ser necesaria para el correcto funcionamiento del servicio objeto del contrato y que además permita a EL BANCO tener un nivel de independencia en sus mantenimientos y mejoras, así como mantener una operación adecuada

14.5. RIESGO OPERATIVO

El proveedor debe aplicar las medidas de control para la gestión de los riesgos operacionales, que sean aplicables al servicio contratado por el Banco; que permita identificar, evaluar, tratar, controlar y monitorear los diversos riesgos asociados a dicho servicio, siendo responsable frente al Banco en caso de la materialización de algún riesgo operativo que, en el marco de la prestación del servicio, afecte a Banco y/o sus clientes.

15. SEGURIDAD Y SALUD EN EL TRABAJO

El ganador de la Buena Pro a la suscripción del contrato deberá presentar la siguiente documentación:

1. Política y Objetivo de Seguridad y Salud en el Trabajo de la empresa.
2. Reglamento Interno de Seguridad y Salud en el Trabajo de la empresa.
3. Matriz IPERC de los puestos de trabajo que realizarán labores dentro de las instalaciones del Banco de la Nación.
4. Registro de Capacitación en temas relacionados a la prevención de los riesgos laborales, así como al COVID-19 en el Trabajo, el registro debe estar acorde

con la R.M. N° 050-2013-TR, el formato debe contener la información solicitada.

5. Registro de entrega de Equipos de Protección Personal en relación con la prevención de los riesgos laborales, así como al COVID-19 en el Trabajo, el registro debe estar acorde con la R.M. N° 050-2013-TR, el formato debe contener la información solicitada.
5. Personal Apto para cumplir las funciones del puesto de trabajo, corroborado por su Certificado de Aptitud Médico Ocupacional.

16. PREVENCIÓN DEL LAVADO ACTIVOS Y DEL FINANCIAMIENTO DEL TERRORISMO

A la suscripción del contrato, el ganador de la buena pro deberá presentar la siguiente información:

- Nombres y Apellidos completos o denominación o razón social, el caso se trate de una persona jurídica.
- Registro Único de Contribuyentes (RUC), o registro equivalente para no domiciliados, de ser el caso.
- Tipo y número de documento de Identidad, en caso de trate de una persona natural.
- Dirección de la oficina o local principal.
- Años de Experiencia en el mercado.
- Rubros en los que el proveedor brinda sus productos o servicios.
- Identificación de los accionistas, socios o asociados que tengan directa o indirectamente el 25 % del capital social, aporte o participación de la persona jurídica y del nombre del representante legal, considerando la información requerida para las personas naturales.
- Declaración Jurada de no contar con antecedentes penales del proveedor, de ser el caso.
- No encontrarse incluido en la lista emitida por la Oficina de Control de Activos Extranjeros del Departamento de Tesoro de los Estados Unidos de América (OFAC).

17. REGISTRO DE DEUDORES DE REPARACIÓN CIVIL – REDERECI

A la suscripción del contrato, el ganador de la buena pro deberá presentar Declaración Jurada de no encontrarse inscritos en el Registro de Deudores de Reparación Civil

18. ANEXOS

ANEXO A

ACUERDO DE NIVEL DE SERVICIO (SLA) Y PENALIDADES

1 Definición

Establecer el nivel operativo de funcionamiento, penalizaciones, limitación de responsabilidades por no atención del servicio, tales como interrupción de la Continuidad Operativa del BN durante el proceso de implementación, retraso en la ejecución del mantenimiento preventivo, por retraso en la reparación averías y/o incidentes.

GERENCIA DE TECNOLOGÍAS DE INFORMACIÓN	SERVICIO DE SOLUCION PARA LA PROTECCION AVANZADA EN ENDPOINTS Y LA RED DEL BANCO DE LA NACION	

Para efectos de los Acuerdos de Niveles de Servicio las averías y/o incidentes las clasificamos en:

- Críticas: Cuando el equipo está inoperativo.
- Urgentes: Cuando el equipo se encuentra en condición de "alarmado".

2 **Acuerdos de Nivel de Servicio (SLA) y Otras Penalidades**

Penalidades			
N°	**Supuestos de aplicación de Penalidad**	**Forma de Cálculo**	**Procedimiento**
1	Incumplimiento en la ejecución de acciones correctivas en la atención de incidentes, aplicable por ocurrencia.	Demora de hasta 10 minutos: 0.20% de la UIT vigente a la fecha	Según informe de la Oficina de Seguridad Informática de la Gerencia de Tecnologías de Información. Se verificará con la atención y cierre de incidentes.
		Demora de hasta 20 minutos: 0.30% de la UIT vigente a la fecha	
		Demora de hasta 30 minutos: 0.40% de la UIT vigente a la fecha	
		Demora de hasta 40 minutos: 0.50% de la UIT vigente a la fecha	
		Demora después de 40 minutos: 01 UIT vigente a la fecha	
2	Incumplimiento en la entrega de los informes técnicos, aplicable por ocurrencia de acuerdo al requerimiento del BN.	Demora de hasta 1 día calendario: 0.25 de la UIT vigente a la fecha	Según informe de la Oficina de Seguridad Informática de la Gerencia de Tecnologías de Información. Se verificará con la fecha de recepción del documento por mesa de partes y/o correo electrónico.
		Demora de hasta 2 día calendario: 0.50 de la UIT vigente a la fecha	
		Demora de hasta 3 día calendario: 0.75 de la UIT vigente a la fecha	
		Demora después del 3 día calendario: 01 de la UIT	

Penalidades			
N°	Supuestos de aplicación de Penalidad	Forma de Cálculo	Procedimiento
		vigente a la fecha.	
3	El contratista cambia al personal propuesto sin contar con la autorización previa del Banco de la Nación.	1 UIT vigente a la fecha (La penalidad se aplicará por ocurrencia)	Se verificará con los documentos de acreditación de los profesionales propuestos en el expediente de contratación, en el caso de que el personal que efectuará el servicio sea diferente al propuesto y de no mediar comunicación alguna por parte del Contratista con el BANCO, en donde se indique la solicitud de cambio de personal por uno equivalente, se procederá a aplicar la penalidad correspondiente, se indica que la penalidad se aplicará por ocurrencia.
4	Por el incumplimiento de los Protocolos Sanitarios y demás disposiciones vigentes que hayan sido dictados por los Sectores y Autoridades Competentes, que se señalan en el numeral 16	10% de 01 UIT vigente a la fecha por incumplimiento Reportado	Para la aplicación de la penalidad se aplicará el siguiente procedimiento: 1.- La Oficina de Seguridad Informática de la Gerencia de Tecnologías de Información comunica el incidente al Contratista 2.- La Oficina de Seguridad Informática de la Gerencia de Tecnologías de Información registra cada incumplimiento y calcula el monto de la penalidad 3.- Solicitar al área encargada de hacer los pagos a los proveedores, realizar el descuento al contratista

Anexo N° 2

Cronograma del Proceso de Concurso de Méritos

N°	Etapa	Periodo
1	Convocatoria	El 15/11/2023
2	Formulación de consultas	Del 16/11/2023 al 24/11/2023
3	Absolución de consultas	El 15/12/2023
4	Integración de Bases	El 15/12/2023
5	Presentación de Propuestas (Acto Público) A las 09:00 horas en el piso 8 de la Sede Central del BN (Av. Javier Prado Este N° 2499 - San Borja)	El 19/12/2023
6	Evaluación de propuestas	Del 20/12/2023 al 21/12/2023
7	Otorgamiento de la buena pro	El 22/12/2023
8	Comunicación de resultados	El 22/12/2023

Anexo N° 3

CONTRATO DE SERVICIO FINANCIERO PARA LA CONTRATACIÓN DEL SERVICIO DE SOLUCIÓN PARA LA PROTECCIÓN AVANZADA EN ENDPOINTS Y LA RED DEL BANCO DE LA NACIÓN

Importante

Dependiendo del objeto del contrato, de resultar indispensable, puede incluirse cláusulas adicionales o la adecuación de las propuestas en el presente documento, previo acuerdo de partes.

Conste por el presente documento, el contrato de Servicio Financiero para **la contratación del servicio de Solución para la Protección Avanzada en Endpoints y la Red del Banco de la Nación**, en adelante EL CONTRATO, que celebran:

BANCO DE LA NACIÓN, en adelante EL BANCO, con RUC N° 20100030595, con domicilio legal en Avenida Javier Prado Este N° 2499, distrito de San Borja, provincia y departamento de Lima , representada por [.....], identificado con DNI N° [.....] y por [.....], identificado con DNI N° [.....],con facultades inscritas en la Partida Electrónica N° 11013341 del Registro de Personas Jurídicas de Lima, y de otra parte [CONSIGNAR NOMBRE DE CONTRATISTA], con RUC N° [.....], con domicilio legal en [.....], inscrita en la Ficha N° [.....] Asiento N° [.....] del Registro de Personas Jurídicas de la ciudad de [.....], debidamente representado por su Representante Legal, [.....], con DNI N° [.....], según poder inscrito en la Ficha N° [.....], Asiento N° [.....] del Registro de Personas Jurídicas de la ciudad de [.....], a quien en adelante se le denominará EL CONTRATISTA.

El BANCO Y CONTRATISTA serán denominados en adelante como LAS PARTES, EL CONTRATO consta de los términos y condiciones siguientes:

CLÁUSULA PRIMERA: ANTECEDENTES

1.1 **EL BANCO** es una empresa estatal con potestades públicas, integrante del sector Economía y Finanzas de la República del Perú, que opera con autonomía económica, financiera y administrativa, creada mediante Ley N° 16000 de fecha 28 de enero de 1966, que se encuentra regulado por su Estatuto aprobado mediante Decreto Supremo N° 07-94-EF de fecha 26 de enero de 1994, el Decreto Legislativo N° 1031 que promueve la eficiencia de la actividad empresarial del Estado y su Reglamento, y el artículo 33° de la Ley N° 26702, Ley General del Sistema Financiero y del Sistema de Seguros y Orgánica de la Superintendencia de Banca y Seguros, y supletoriamente por los demás artículos de dicha Ley General o sus modificatorias.

1.2 EL CONTRATISTA es una empresa constituida en el Perú, que se dedica a [.....]

1.3 El servicio a contratar consta de soluciones de seguridad, mantenimiento preventivo, mantenimiento correctivo, residente de seguridad y servicio de respuesta ante incidentes, que incluya una solución de seguridad para protección avanzada en endpoints y la red del Banco de la Nación, que comprenda acceso confiable y seguro a la red de comunicaciones que garantice la integridad de la información de los clientes del Banco, así como mejorar los accesos a la red con mayores niveles de confidencialidad, encriptación e integridad.

1.4 De conformidad con lo establecido en el artículo 4° literal a) del Texto Único Ordenado de la Ley N° 30225 - Ley de Contrataciones del Estado, aprobado por Decreto Supremo N° 082-2019-EF, el Decreto Supremo N° 169-2022-EF que precisa el alcance de lo dispuesto en el literal a) del artículo 4 de la Ley N° 30225, Ley de Contrataciones del Estado, lo señalado por la Ley General del Sistema Financiero y del Sistema de Seguros y Orgánica de la Superintendencia de

Banca, Seguros y AFP – Ley N° 26702 sobre el término "servicio financiero" incluido en el Anexo – Glosario y el artículo 12.20 del Capítulo 12 del Acuerdo Comercial con los Estados Unidos (TLC), el presente constituye un contrato de naturaleza financiera, por lo que se encuentra fuera del ámbito de aplicación de la Ley de Contrataciones del Estado.

1.5 En el marco del Concurso de Méritos N° [.....], EL CONTRATISTA presentó su propuesta adjuntando la Propuesta Económica y la Propuesta Técnica, las que formaran parte integrante del presente contrato como **Anexo I "Oferta Ganadora"**, otorgándole el Comité de Selección del mencionado Concurso de Méritos, la Buena Pro.

CLÁUSULA SEGUNDA: OBJETO DEL CONTRATO

Por medio de EL CONTRATO, EL BANCO contrata a EL CONTRATISTA para que brinde el servicio financiero de Solución para la Protección Avanzada en Endpoints y la Red del Banco de la Nación, en adelante el SERVICIO. Queda establecido que EL SERVICIO comprende a la:

1. **Prestación Principal**: Soluciones de seguridad, Mantenimiento preventivo, Mantenimiento correctivo, Residente de seguridad y Servicio de respuesta ante incidentes.
2. **Prestación Accesoria**: Entrenamiento.

Las características técnicas del SERVICIO se establecen en el **Anexo II "Especificaciones Técnicas para la Contratación de Servicios: Solución para la Protección Avanzada en Endpoints y la Red del Banco de la Nación"**, el cual forma parte integrante de EL CONTRATO, y que EL CONTRATISTA se compromete a cumplir en su integridad.

CLÁUSULA TERCERA: PLAZO DE VIGENCIA Y LUGAR DE PRESTACIÓN DE EL SERVICIO

3.1 Plazo de vigencia

El presente Contrato tendrá vigencia de **treinta y seis (36) meses** y comenzará a regir a partir del día siguiente de firmada el Acta de Conformidad de Implementación del Servicio por EL BANCO y EL CONTRATISTA. Sin perjuicio de ello, EL CONTRATISTA se obliga a cumplir con los plazos de entrega del SERVICIO y de la prestación accesoria que forma parte del servicio, conforme se detalla en el **Anexo II "Especificaciones Técnicas para la Contratación de Servicios: Solución para la Protección Avanzada en Endpoints y la Red del Banco de la Nación"**.

3.2 Lugar de prestación del servicio

EL CONTRATISTA implementará el SERVICIO, en los lugares que se muestran a continuación:

NODO	DEPENDENCIA	DIRECCION
1	Centro de Datos Principal BN (CDP)	Av. Javier Prado Este 2499 – San Borja – Lima
2	Centro de Datos de Respaldo BN (CDR)	Av. Arequipa 2720 San Isidro – Lima

CLÁUSULA CUARTA: MONTO CONTRACTUAL

EL BANCO y EL CONTRATISTA acuerdan que la contraprestación total por el presente contrato asciende a la suma de [.....(.....00/100 Soles)] de acuerdo al siguiente detalle:

Descripción		contraprestación
Servicio de solución para la protección avanzada en Endpoints y la Red del Banco de la Nación	Prestación Principal	
	Prestación Accesoria	
Total		

La forma y oportunidad para el pago de la contraprestación será la descrita en la cláusula quinta de EL CONTRATO.

Este monto comprende el costo por todo el SERVICIO, todos los impuestos de Ley, seguros, transporte, inspecciones, pruebas y cualquier otro gasto o costo que incurra EL CONTRATISTA, así como todo concepto que pueda tener incidencia sobre la ejecución de la prestación materia del presente contrato.

CLÁUSULA QUINTA: DEL PAGO DEL SERVICIO

5.1 Pago de la Prestación Principal

El pago de la prestación principal del SERVICIO será de manera mensual.

Previo al pago de la prestación principal del SERVICIO, el CONTRATISTA deberá entregar un informe y este informe formará parte de la documentación necesaria para expedir el acta de conformidad del servicio, el informe debe contener lo siguiente:

- Informe mensual de tipo gerencial que relacione como mínimo los eventos detectados, correlacionados y notificados, los hallazgos más relevantes del periodo, el estado de salud/capacidad de la plataforma gestionada y las acciones de mejora sugeridas.
- Reporte mensual de estado de salud del servicio y de las soluciones implementadas.

Para tal efecto la Oficina de Seguridad Informática de la Gerencia de Tecnologías de Información de EL BANCO emitirá el acta de conformidad del servicio previo informe técnico emitido por la Oficina de Seguridad Informática y visado por la subgerencia de Producción en un plazo que no excederá de los diez (10) días calendario de ser recibida la documentación correspondiente del CONTRATISTA.

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

d. Comprobante de pago.
e. Acta de Conformidad emitida por la Oficina de Seguridad Informática de la Gerencia de Tecnologías de Información de EL BANCO.
f. Informe Técnico del funcionario de la Oficina de Seguridad Informática de la Gerencia de Tecnologías de Información de EL BANCO.

5.2 Pago de la Prestación Accesoria

Previo al pago de la prestación accesoria que forma parte del SERVICIO, EL CONTRATISTA deberá entregar un informe donde se indique todas las actividades ejecutadas, este informe formará parte de la documentación necesaria para expedir el acta de conformidad de la prestación accesoria.

La prestación accesoria se pagará en un solo pago, en soles, en el semestre en que se realizó la misma.

Para efectos del pago de la prestación accesoria ejecutada por EL CONTRATISTA, la Entidad debe contar con la siguiente documentación:

d) Comprobante de pago.
e) Acta de Conformidad emitida por la Oficina de Seguridad Informática de EL BANCO.
f) Informe del funcionario responsable de Oficina de Seguridad Informática, emitiendo la conformidad de la prestación efectuada de EL BANCO.

De existir observaciones, EL BANCO las comunicará a EL 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 dos (2) ni mayor de quince (15) días. Si pese al plazo otorgado, si EL CONTRATISTA no cumpliese a cabalidad con la subsanación, EL BANCO puede otorgar a EL CONTRATISTA periodos adicionales para las correcciones pertinentes. En este supuesto, corresponde aplicar la penalidad desde el vencimiento del plazo para subsanar.

Este procedimiento no resulta aplicable cuando el SERVICIO o la prestación accesoria manifiestamente no cumplan con las características y condiciones ofrecidas, en cuyo caso EL BANCO no efectúa la recepción y/o no otorga la conformidad, según corresponda, debiendo considerarse como no ejecutada la prestación, aplicándose la penalidad que corresponda por cada día de atraso.

La conformidad del SERVICIO, inclusive de la prestación accesoria, por parte de EL BANCO no enerva su derecho a reclamar posteriormente por defectos o vicios ocultos, durante el plazo de treinta y seis (36) meses; plazo que inicia luego de emitida(s) la(s) acta(s) de conformidad respectiva(s), por lo que EL CONTRATISTA será responsable de subsanar y/o reparar los vicios ocultos, sin perjuicio de asumir los daños y perjuicios que ello hubiere generado a EL BANCO.
EL BANCO debe pagar las contraprestaciones pactadas a favor de EL CONTRATISTA dentro de los [..... (.....)] días calendarios siguientes a la presentación de los documentos que debe presentar EL CONTRATISTA, que se detallan en la presente cláusula.

CLÁUSULA SEXTA: OBLIGACIONES DE EL CONTRATISTA

Además de las obligaciones asumidas en EL CONTRATO y el **Anexo II "Especificaciones Técnicas para la Contratación de Servicios: Solución para la Protección Avanzada en Endpoints y la Red del Banco de la Nación"**, EL CONTRATISTA se obliga frente a EL BANCO, conforme a lo siguiente:

- EL CONTRATISTA es responsable directo y absoluto de las actividades que realizará para el cumplimiento del objeto de EL CONTRATO, sea directamente o a través de su personal, debiendo responder por la ejecución de la prestación. EL CONTRATISTA estará sujeto a las adecuaciones que hubieran por cambios mandatorios de tecnología, seguridad de la información, seguridad de datos, ciberseguridad u otros relacionados, parte de SBS, BN (EL BANCO) u otras entidades.
- EL CONTRATISTA está impedido de subcontratar alguna de las actividades establecidas en el **Anexo II "Especificaciones Técnicas para la Contratación de Servicios: Solución para la Protección Avanzada en Endpointe y la Red del Banco de la Nación"**.
- EL CONTRATISTA se obliga a efectuar los controles de calidad. EL BANCO realizará las tareas de Auditoria que estime necesarias para verificar la calidad y forma de entrega del SERVICIO, a fin de dar por cumplida en forma satisfactoria su entrega por EL CONTRATISTA. Cualquier observación emitida por EL BANCO será notificada en forma fehaciente a EL CONTRATISTA, a efectos de que este pueda resolver la falta en cuestión y así dar cumplimiento satisfactorio a la(s) prestación(es) a su cargo.
- EL CONTRATISTA, previo a la formalización de EL CONTRATO, debe entregar a EL BANCO una garantía de Fiel Cumplimiento por una suma equivalente al 10% del monto contractual pactado; la cual se mantiene vigente hasta la conformidad de la recepción de la(s) prestación(es) conforme a lo establecido en la Cláusula Tercera de EL CONTRATO. Dicha garantía debe ser incondicional, solidaria, irrevocable, sin beneficio de excusión y de realización automática, a solo requerimiento de EL BANCO, las cual debe ser emitida por una empresa

supervisada por la SBS y que cuenta 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.

- Informar a EL BANCO en caso de transformación, fusión, absorción, disolución, liquidación, reorganización u otros actos que afecten la identidad o existencia de EL CONTRATISTA con no menos de quince (15) días hábiles antes de producido el hecho.

El incumplimiento de las obligaciones que asume EL CONTRATISTA en la presente cláusula y las demás obligaciones que se establecen en EL CONTRATO y su **Anexo II "Especificaciones Técnicas para la Contratación de Servicios: Solución para la Protección Avanzada en Endpoints y la Red del Banco de la Nación"**, constituyen causal de resolución automática y de pleno derecho de EL CONTRATO, de conformidad con lo previsto en el artículo 1430° del Código Civil, sin perjuicio de la obligación de EL CONTRATISTA de reparar a EL BANCO los daños y perjuicios que le hubiere causado con dicho incumplimiento.

CLÁUSULA SÉPTIMA: OBLIGACIONES DE EL BANCO

- EL BANCO asume la obligación de efectuar el(los) pago(s) de la contraprestación contractual, conforme a lo pactado en EL CONTRATO.
- EL BANCO se obliga a emitir la(s) Acta(s) de Conformidad, así como el(los) informe(s) técnico(s) respectivo(s), siempre y cuando EL CONTRATISTA haya cumplido a cabalidad con sus obligaciones, de acuerdo a lo establecido en EL CONTRATO.
- EL BANCO se compromete a efectuar la recepción de la prestación a cargo de El CONTRATISTA, de acuerdo a lo pactado y acorde a los términos establecidos en EL CONTRATO.

CLAUSULA OCTAVA: PENALIDADES

Si EL CONTRATISTA incurre en retraso injustificado en la ejecución de las prestaciones objeto del contrato, EL BANCO le aplica automáticamente una penalidad por mora por cada día de atraso hasta por un máximo equivalente al diez por ciento (10%) del monto del contrato, 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
Por monto y plazo se entenderá lo pactado en el contrato.
Se puede considerar justificado el retraso y en consecuencia no se aplica penalidad, cuando EL CONTRATISTA acredite documentalmente que el mayor tiempo transcurrido no le resulta imputable y que es por motivo de fuerza mayor o caso fortuito. En este último caso la calificación del retraso como justificado por parte de EL BANCO no da lugar al pago de gastos generales ni costos directos de ningún tipo.

Asimismo, será aplicable a EL CONTRATISTA las penalidades establecidas en el **Anexo III "Acuerdo de Nivel de Servicio (SLA) y Penalidades"** del presente Contrato.

EL CONTRATISTA reconoce y acepta como válida(s) la(s) penalidad(es) detallada(s) en la presente cláusula y en el **Anexo III "Acuerdo de Nivel de Servicio (SLA) y Penalidades"**, declarando a su vez que **EL BANCO** tiene plena facultad de aplicarlas, descontándolas del monto correspondiente a la contraprestación de EL CONTRATISTA o si fuese necesario se cobrará del monto resultante de la ejecución de la garantía.

Cuando se llegue a cubrir el monto máximo de la penalidad por mora o el monto máximo para otras penalidades, en caso se hubiesen pactado, EL BANCO tiene la facultad de resolver el

contrato por incumplimiento, de conformidad con el artículo 1430° del Código Civil, sin perjuicio de la obligación de EL CONTRATISTA de reparar a EL BANCO los daños y perjuicios que le hubiere causado con dicho incumplimiento.

Por su parte, en caso EL BANCO incurriera en costos y/o multas establecidas por parte de un Organismo Regulador, Autoridad competente u otro, mediante una resolución o sentencia firme producto de la interrupción y/o algún error o falla en las condiciones de la prestación del servicio por causas imputables a EL CONTRATISTA, este se hará totalmente responsable de dichas multas o penalidades, asumiendo el 100% del importe de las mismas sin reserva ni limitación alguna, sin perjuicio de la obligación de EL CONTRATISTA de reparar a EL BANCO los daños y perjuicios que le hubiere causado con dicho incumplimiento.

CLAUSULA NOVENA: NATURALEZA DEL CONTRATO

Dado la naturaleza bancaria/financiera del vincula que origina este CONTRATO entre EL CONTRATISTA y EL BANCO, los trabajadores de EL CONTRATISTA o los terceros de los que este se valga para ejecutar todas las prestaciones a su cargo provenientes del presente CONTRATO, mantendrán relación contractual, ya sea laboral o civil, única y exclusivamente con EL CONTRATISTA, por lo que el otorgamiento de beneficios laborales así como el cumplimiento de las obligaciones derivadas de una relación laboral son de su exclusiva responsabilidad.

EL BANCO podrá solicitar por escrito a EL CONTRATISTA una corrección, variación, sustitución, adecuación, etc. de los servicios contratados y EL CONTRATISTA evaluará el alcance de dichas modificaciones a fin de poder comunicar por escrito la viabilidad técnica y económica de las mismas dentro del plazo concedido por EL BANCO.

EL CONTRATISTA cumplirá con la ejecución integral de los servicios materia de este CONTRATO de manera autónoma, utilizando para ello todos sus conocimientos y experiencia. EL CONTRATISTA tendrá a cargo la dirección, supervisión y fiscalización de las labores de su personal, sin participación absoluta de EL BANCO.

Queda entendido que el personal de EL CONTRATISTA que ejecute los servicios, no tendrá vínculo directo alguno y/o subordinación con EL BANCO, el mismo que ni dirigirá ni supervisará sus labores en forma alguna ya que los referidos trabajadores mantendrán dependencia y subordinación exclusivamente con EL CONTRATISTA. El referido personal de EL CONTRATISTA deberá estar debidamente identificado.

CLAUSULA DÉCIMA: DE NO EXCLUSIVIDAD Y CESIÓN DEL SERVICIO

Queda expresamente convenido entre LAS PARTES, que el presente CONTRATO no tiene carácter de exclusividad, lo cual implica que EL CONTRATISTA, está plenamente facultado para atender servicios similares o diferentes con sus clientes actuales y los futuros que tenga.
El presente CONTRATO no será transferible por concepto alguno, no podrá ser objeto de cesiones de derechos o de posición contractual, debiendo LAS PARTES sujetarse estrictamente a sus estipulaciones. Asimismo, para todo lo no previsto en el mismo, se regirán por lo estipulado en la Ley N° 26702, el Código Civil y demás normas aplicables.
En la medida que el presente Contrato no involucra una prestación de servicios que involucre el desplazamiento continuo de personal a centros de trabajo o de operaciones de EL BANCO, sino que su ejecución se llevará a cabo en centros de trabajo de EL CONTRATISTA, no resulta de aplicación la Ley N° 29245, ni normas complementarias, de acuerdo con lo establecido en el artículo 2° del Decreto Supremo N. ° 006-2008-TR.

Teniendo en cuenta la naturaleza civil del presente Contrato, las Partes declaran que cada una es exclusivamente responsable de sus obligaciones en materia laboral, tributaria, administrativa y, en general, por la obtención de sus permisos y licencias necesarios para el normal desarrollo de su negocio, actividades y el fiel cumplimiento del presente Contrato.

CLÁUSULA DÉCIMA PRIMERA: RESPONSABILIDADES ADICIONALES

Responsabilidad General

Teniendo en consideración los alcances, límites y otras condiciones expresadas en EL CONTRATO, EL CONTRATISTA será responsable por los daños que sufra EL BANCO como consecuencia o con motivo del incumplimiento de las obligaciones asumidas en EL CONTRATO.

EL CONTRATISTA se compromete a liberar de responsabilidad a EL BANCO por los reclamos, quejas, daños, pérdidas, penalidades, multas, acciones judiciales y/o administrativas cuando sean por causas imputables de EL CONTRATISTA, según corresponda por disposición legal o según las obligaciones derivadas de EL CONTRATO, debiendo EL CONTRATISTA cumplir la Ley o EL CONTRATO asumir y abonar los costos, costas y gastos de EL BANCO, incluyendo honorarios legales que dichas acciones traigan aparejadas, cualquiera fuera la naturaleza de las mismas. En caso EL BANCO deba pagar a cualquier tercero o autoridad alguna suma de dinero como consecuencia o con motivo de que EL CONTRATISTA incumplió una de sus obligaciones de EL CONTRATO y/o obligaciones que les correspondan por disposición legal o contractual, dichos costos, costas, gastos y honorarios EL CONTRATISTA deberá resarcir a EL BANCO procediendo con el pago integro de dichos conceptos a favor de EL BANCO.

EL CONTRATISTA no será responsable por ninguna imprecisión o error debidamente acreditado contenidos en, o derivados de la información suministrada por EL BANCO para la prestación de los servicios. EL CONTRATISTA será plenamente responsable del uso y manejo de la información brindada por EL BANCO.

EL CONTRATISTA se compromete a defender, indemnizar y liberar de responsabilidad a EL BANCO y/o sus directores, gerentes y/o empleados, salvo dolo contra todo reclamo que surja de lo siguiente:

(a) La falta de cumplimiento por EL CONTRATISTA de cualquiera de las obligaciones a su cargo bajo los términos de EL CONTRATO y las consecuencias derivadas de dicho incumplimiento.

(b) La pérdida de materiales, registros, datos procesados o sin procesar o cualquier otro elemento en las instalaciones de EL CONTRATISTA.

CLAUSULA DÉCIMO SEGUNDA: DE GESTIÓN INTEGRAL DE RIESGOS Y AUDITORIA

EL CONTRATISTA se obliga a cumplir con las condiciones que garanticen la seguridad de información, protección de datos personales y gestión de sus riesgos, asociados al servicio contratado por EL BANCO.

EL CONTRATISTA se obliga a permitir la revisión, supervisión e inspección de los servicios prestados y de las condiciones que garanticen la seguridad de información, protección de datos personales, continuidad del negocio y gestión de sus riesgos, por parte dependencia responsable del contrato o del personal autorizado por EL BANCO, el Órgano de Auditoria Interna del Banco, de la Sociedad Auditora Externa, así como de la Superintendencia de Banca, Seguros y AFP, Autoridad de Protección de Datos Personales o cualquier otro ente regulador, supervisor o fiscalizador de las actividades materia del contrato, en la oportunidad que cualquiera de estos lo solicite, con un aviso previo por escrito de veinticuatro (24) horas, el cual será remitido a la dirección indicada por EL CONTRATISTA en el presente contrato. En dicho comunicado se designarán a las personas que efectuarán la mencionada revisión, supervisión e inspección. Consecuentemente, EL CONTRATISTA se compromete a facilitar todos los recursos y medios necesarios a las personas antes mencionadas para efectuar dicha revisión.

El incumplimiento de las obligaciones que asume EL CONTRATISTA en la presente cláusula constituye causal de resolución automática y de pleno derecho del presente contrato, de

conformidad con lo previsto en el artículo N° 1430° del Código Civil, sin perjuicio de la obligación del proveedor de pagar al Banco la indemnización correspondiente.

En caso el Banco incurriera en costos y/o multas establecidas por parte de un organismo regulador u otro, mediante una resolución o sentencia firme producto de la interrupción y/o algún error o falla en las condiciones de la prestación del servicio por causas imputables al proveedor, éste se hará totalmente responsable de dichas penalidades, asumiendo el importe de las mismas sin reserva ni limitación alguna. Por lo que, el Banco podrá evaluar la aplicación de penalidades o el pago de indemnización por la no operatividad del servicio, conforme al SLA que haya definido en los Términos de Referencia.

El CONTRATISTA deberá cumplir con los siguientes requerimientos:

12.1 Seguridad de la Información

- Para garantizar la integridad, disponibilidad y confidencialidad de la información el CONTRATISTA debe implementar y cumplir con los lineamientos de seguridad de la información que apliquen al servicio contratado.

- El CONTRATISTA se obliga a adoptar las medidas necesarias para sus trabajadores, representantes y personal o terceros subcontratados que intervengan para el cumplimiento del servicio contratado, cumplan con las disposiciones sobre la seguridad y confidencialidad de la información.

- El CONTRATISTA es el responsable del resguardo y protección de los activos de información (equipos, dispositivos informáticos, aplicaciones, información, entre otros) de propiedad del Banco de la Nación, involucrados en el servicio contratado, que se encuentren bajo la administración del CONTRATISTA o que formen parte del servicio contratado.

- El Banco en coordinación con EL CONTRATISTA, adoptarán las medidas de seguridad en los sistemas tecnológicos involucrados en el servicio contratado, a fin de mitigar los riesgos y asegurar que la información se proteja de forma segura. Estas medidas deberán ser plasmadas en un documento y ejecutadas en la etapa de implementación y ante cualquier incidente o mejora del servicio.

- Antes de realizar cualquier cambio o mantenimiento de los sistemas tecnológicos relacionados al servicio contratado, el CONTRATISTA deberá coordinar con el Banco, a fin de definir las acciones pertinentes para dicha actividad.

- El Banco y el CONTRATISTA restringirán el acceso a la información física y lógica, así como a los sistemas informáticos inmersos en el servicio; sólo al personal autorizado del Banco y del CONTRATISTA, por lo que ningún tercero no autorizado tendrá acceso a la información relacionada con el servicio contratado.

- En la etapa de implementación, el CONTRATISTA en coordinación con el Banco definirán el proceso de cómo se gestionarán los riesgos, alertas e incidentes de seguridad de la información, relacionados con el servicio contratado.

- El CONTRATISTA permitirá, facilitará y/u otorgará al Banco la revisión del cumplimiento de las normas de seguridad de la información relacionados con el servicio asociado al contratado.

- De aplicar desarrollo de softwares, aplicativos que el CONTRATISTA proporcione para el Banco, en el marco del servicio contratado, estos serán de titularidad

del Banco, durante la ejecución del contrato, por lo tanto, el CONTRATISTA no podrá asumir ningún derecho sobre ellos.

➢ EL CONTRATISTA permitirá, facilitará y/u otorgará a EL BANCO, ante requerimiento de este; la revisión del cumplimiento de las normas de seguridad de la información relacionados con el servicio asociado al contratado.

➢ EL CONTRATISTA deberá adoptar las medidas de índole técnica y organizativas necesarias para garantizar la seguridad de la información de carácter confidencial y evitar su adulteración, pérdida, tratamiento o acceso no autorizado, la naturaleza de los datos suministrados y los riesgos a que están expuestos, ya provengan de la acción humana o del medio físico o natural. Para ello acepta cumplir bajo responsabilidad, con las políticas, lineamientos y protocolos de seguridad que le haga llegar EL BANCO.

12.2 Protección del Secreto Bancario, Telecomunicaciones y Datos Personales

➢ El Banco y el CONTRATISTA declaran conocer que están obligados a salvaguardar y mantener la confidencialidad del secreto bancario, de las telecomunicaciones y de los datos personales de los usuarios y clientes del Banco de la Nación, de acuerdo con la Constitución Política del Perú, Ley N°29733 Ley de Protección de datos personales, su Reglamento y Directivas de Seguridad, Ley N°26702, Secreto Bancario y la Ley N° 26096 Ley de Telecomunicaciones, sus modificatorias y actualizaciones; aplicables a los servicios objeto del contrato.

➢ El CONTRATISTA debe poner en conocimiento de su personal y de los terceros que requiera para ejecutar el contrato, que tuvieran acceso a la información del Banco; la obligación de salvaguardar y mantener la confidencialidad del secreto bancario, de las telecomunicaciones y de los datos personales, esta obligación se mantendrá vigente inclusive luego de haber concluido el presente contrato, salvo que medie autorización expresa de estos últimos para su tratamiento.

➢ Los datos personales que el Banco le proporcione al CONTRATISTA a lo largo de la prestación del servicio, el CONTRATISTA deberá cumplir con el tratamiento de datos personales de acuerdo a las disposiciones establecidas en la Ley N° 29733, Ley de Protección de Datos Personales, su Reglamento y Directiva de seguridad.

➢ Cualquier información que se intercambie y se genere bajo cualquier formato y medio, como parte del servicio, es de propiedad exclusiva del Banco y por ningún motivo puede ser utilizada por EL CONTRATISTA para un fin distinto al contrato y no debe divulgarla a terceros salvo autorización expresa del Banco.

➢ En caso EL BANCO le proporcionen a EL CONTRATISTA datos personales de sus colaboradores, clientes o terceros o éste último deba recopilarlos o generarlos, en el marco del cumplimiento del Contrato, ello no implicará de modo alguno la transferencia de los mismos, debiendo EL CONTRATISTA asumir en dichos casos, la condición de encargado del tratamiento. De igual modo, EL CONTRATISTA podrá proporcionar datos personales de sus colaboradores, clientes o terceros a EL BANCO, para su tratamiento, así como generarlos o recopilarlos cuando estos resulten necesarios en el marco del Contrato, sin que ello implique de modo alguno la transferencia de los mismos, debiendo EL BANCO asumir en dichos casos, la condición de encargado del tratamiento.

➢ EL CONTRATISTA declara conocer que asume la condición de encargado del tratamiento cuando EL BANCO entrega o pone a disposición de manera directa o indirecta a EL CONTRATISTA información que contiene datos personales en virtud de una relación jurídica que los vincula. Dicha relación jurídica delimita el ámbito de actuación de EL CONTRATISTA. En ese sentido, EL CONTRATISTA se compromete a:

a) No Utilizar o tratar los datos personales proporcionados, generados o recopilados con una finalidad distinta a aquella por la que le fueron entregados o por la que son generados o recopilados.

b) No Transferir o divulgar estos datos personales a terceros, con excepción de entidades públicas, cuando estas lo soliciten en el marco del cumplimiento de sus funciones debidamente sustentadas o el poder judicial cuando sea solicitado mediante la orden judicial correspondiente, debiendo notificar de ello a EL BANCO, según corresponda, dentro de las 24 horas de recibido el requerimiento.

c) Que los datos personales proporcionados por EL BANCO, serán tratados en forma confidencial y estarán sujetos a estrictas medidas de seguridad, conforme lo dispone la Ley de Protección de Datos Personales su reglamento, directiva y demás normas conexas, complementarias, modificatorias y/o sustitutorias.

➢ En caso EL CONTRATISTA transfiera datos personales a EL BANCO, EL CONTRATISTA declara que cuenta con el consentimiento libre, voluntario, previo, expreso, informado e inequívoco de los titulares de los datos personales de sus colaboradores, clientes o de terceros que, como parte del cumplimiento del presente Contrato, hubiera entregado o pudiera entregar EL BANCO mediante transferencia de datos. En este supuesto, los datos personales transferidos por EL CONTRATISTA a EL BANCO deberán tener el mismo tratamiento que el contemplado en esta cláusula para los datos personales entregados por EL BANCO a EL CONTRATISTA.

➢ En el eventual caso que se identifique o descubra que la información proporcionada por EL CONTRATISTA sea falsa, se aplicará la máxima penalidad (severidad crítica) acordada en el contrato. En el caso que no se hayan pactado penalidades en el contrato, EL BANCO podrá determinar en su momento, dependiendo del perjuicio ocasionado, el monto a pagar a favor de EL BANCO debiendo EL CONTRATISTA de asumir el pago en las condiciones y plazos indicados por EL BANCO.

➢ EL BANCO, en caso lo crea necesario, podrá, en cualquier momento, de forma presencial o electrónica revisar o auditar a EL CONTRATISTA sobre las medidas de seguridad aplicadas en cumplimiento de la Ley de Protección de Datos Personales, su reglamento, directiva y demás normas conexas, complementarias, modificatorias y/o sustitutorias. De comprobar EL BANCO algún incumplimiento por parte de EL CONTRATISTA como resultado de la auditoría, podrá resolver / dejar sin efecto el presente Contrato, debiendo previamente enviar una comunicación por escrito a EL CONTRATISTA comunicándole el incumplimiento, y otorgándole un plazo máximo de cinco días hábiles para su cumplimiento, de perseverar EL CONTRATISTA en el incumplimiento, EL BANCO podrá dar por resuelto el presente contrato, y de considerarlo necesario interponer las acciones legales a que hubiera lugar. En ese sentido, EL CONTRATISTA será responsable por cualquier perjuicio que se cause a EL BANCO como consecuencia directa o indirecta del incumplimiento de cualquiera de las obligaciones que se desprenden de la presente cláusula de protección de datos personales.

➢ Del Flujo Transfronterizo: En caso exista flujo transfronterizo de datos personales asociado al servicio contratado, EL CONTRATISTA deberá asegurarse que la información de datos personales que se transmita y/o transfiera entre el Perú y cualquier otro país, a causa directa o indirecta del servicio o producto contratado, mantiene y mantendrá los niveles de

protección adecuados, disponiendo de las medidas de seguridad, privacidad y confidencialidad necesarias y efectivas para evitar la adulteración, pérdida, consulta o tratamiento no autorizado de los datos, y que permitan detectar desviaciones, intencionales o no, ya sea que los riesgos provengan de la acción humana o del medio técnico utilizado; verificando que todas estas medidas y acciones no sean inferiores a las dispuestas por la Ley N° 29733, su reglamento, directiva de seguridad y normas conexas, de manera tal que garanticen el nivel de seguridad apropiado para abordar los riesgos asociados al tratamiento de datos personales ya la naturaleza sensible de los datos que han de protegerse.

➢ Por otro, lado, en caso exista flujo transfronterizo asociado al servicio contratado, EL BANCO tomará como insumo la información proporcionada por EL CONTRATISTA en el presente cuadro, para registrar y/o actualizar los flujos transfronterizos aplicables a los bancos de datos personales de EL BANCO.

➢ Sobre el Secreto Bancario, LAS PARTES se comprometen a cumplir con las disposiciones señaladas en los artículos 140° , 141°, 142°, 143° y 143° - A de la Ley N° 26702 "Ley General del Sistema Financiero y del Sistema de Seguros y Orgánica de la Superintendencia de Banca y Seguros" y sus modificatorias y en la Resolución SBS N° 1132 – 2015 "Norma que regula el procedimiento de atención de las solicitudes de levantamiento de secreto bancario", siendo responsables de que la información relacionada a las cuentas de los clientes no sea entregada por ambas partes a terceros, ni que dicha información sea utilizada para fines fraudulentos, debiendo para ello establecer y garantizar las medias de seguridad correspondientes.

➢ LAS PARTES se obligan a poner en conocimiento de su personal y de los terceros de los que se valga para ejecutar el contrato - que tuvieran acceso a la información protegida - la obligación contenida en la presente cláusula, así como a instruirlos y capacitarlos periódicamente sobre la importancia de estas protecciones. Queda establecido que si cualquiera de las partes – o cualquier subcontratista de éstas - incumple la obligación a que se refiere la presente cláusula – además de las consecuencias civiles y penales del caso - quedará obligada a resarcir a la otra parte los daños que le cause, ya sea por dolo, culpa grave o culpa leve, asumiendo especialmente: (a) las sanciones administrativas y judiciales impuestas a esta última como consecuencia del referido incumplimiento; y, (b) los costos en los que la misma incurra en la defensa administrativa y judicial de sus intereses. La obligación de salvaguardar el secreto bancario y de las telecomunicaciones y la confidencialidad de los datos personales de los usuarios se mantendrá vigente inclusive luego de haber concluido el presente Contrato, salvo que medie autorización expresa de estos últimos para su tratamiento.

➢ Sin perjuicio de lo señalado, entre ambas partes se podrá compartir información que no vulnere ningún derecho de terceros ni normativa legal, para efectos del mejor cumplimiento del presente Contrato.

➢ El CONTRATISTA declara conocer las sanciones tipificadas en la Ley N° 3096, Ley de Delitos Informáticos (integridad de datos informáticos, tráfico ilegal de datos, interceptación de datos informáticos), así como dar cumplimiento de las mismas.

12.3 Confidencialidad de la Información

➢ Por el presente instrumento, EL CONTRATISTA se obliga a guardar estricta y severa reserva, confidencialidad y secreto respecto de la información que EL BANCO le proporcione, así como de la información correspondiente a las transacciones que

procesa o de la cual tome conocimiento, sea voluntaria o involuntariamente, con ocasión y a consecuencia de la prestación del servicio contratado, o por error de quien se la provee, bajo cualquier modalidad o vía de acceso, y aquella obtenida o producida por LA EL CONTRATISTA (informes o entregables) para EL BANCO en razón de la prestación del servicio, siendo su compromiso formal utilizar dicha información exclusivamente para la prestación del servicio contratado y de ningún modo en perjuicio de EL BANCO.

➢ Como parte del servicio el CONTRATISTA tomará conocimiento de la información del Banco. Esta información es confidencial, por lo tanto, el CONTRATISTA y todo su personal mantendrá la confidencialidad de la misma. El compromiso de confidencialidad se prolonga indefinidamente aún después de terminado el servicio, y se hace extensivo al personal que el CONTRATISTA subcontrate aun cuando hayan dejado de tener vínculo laboral con el CONTRATISTA.

➢ El CONTRATISTA se compromete a mantener toda información suministrada por el Banco en estricta reserva y absoluta confidencialidad, así como de adoptar las medidas que resulten necesarias para impedir que la Información Confidencial sea conocida o revelada a terceros o que sea utilizada para fines distintos para los cuales fue entregada.

➢ Se entiende que la obligación asumida está referida no sólo a documentos e informaciones señalados por la otra parte como "confidenciales" sino a todos los documentos e informaciones que, en razón del referido intercambio, pueda ser conocida por cualquier medio, incluyendo, sin limitarse a ella, a programas de cómputo, nombres de clientes, estrategias financieras o comerciales, toda la información referida a clientes, personal, contabilidad, finanzas, productos, tráfico de llamadas telefónicas, tráfico de Internet, mensajería electrónica, actividades de comercialización, planes de negocio, técnicas de marketing, procesos, servicios, políticas de precios, estrategias, buenas prácticas, metodología de trabajo, nombres o marcas comerciales, modelos, descubrimientos, investigaciones, desarrollos, procesos, procedimientos, propiedad intelectual, sistemas de seguridad, estructura y distribución de las oficinas, sucursales y agencias, y también toda aquella información obtenida de terceras partes para EL BANCO, se considera confidencial y está considerada como parte de la obligación de reserva absoluta que asume EL CONTRATISTA por el presente instrumento.

➢ El CONTRATISTA se obliga a tomar todas las medidas y precauciones razonables para que sus trabajadores y en general cualquier persona con la que tenga relación, no divulgue a ningún tercero los documentos o información a los que tengan acceso, haciéndose responsables por la divulgación que se pueda producir y asumiendo el pago de la indemnización por daños y perjuicios. Estas medidas incluyen, aunque no se limitan a: (i) poner en disposición la información confidencial sólo a un número restringido de personas; (ii) permitir que sus trabajadores, agentes o terceros, accedan a la información confidencial sólo hasta donde sea necesario para la prestación de los servicios; (iii) exigir a su personal o trabajadores como condición previa al acceso a la información confidencial que se obliguen por escrito a respetar esta cláusula de confidencialidad. El compromiso de confidencialidad se prolonga por 10 años después de terminado el servicio, y se hace extensivo al personal que el proveedor subcontrate aun cuando hayan dejado de tener vínculo laboral con el CONTRATISTA.

➢ El CONTRATISTA reconoce que la información que se le entregue, procese, facilite o genere en razón a su desempeño y/o ejecución del presente contrato, se

considera un activo del Banco, por consiguiente, el CONTRATISTA se obliga a:

1. Mantener en confidencial dicha información, sin divulgarla, ni entregarla, directa o indirectamente a terceros, sean personas naturales o jurídicas.
2. No usarla para cualquier otro fin que no sea en relación con la prestación de los servicios; ni obtener un beneficio propio o de terceros de ella.
3. No entregarla o revelarla, de manera total o parcial, pública o privada, a ninguna persona sea en el Perú como en el extranjero, sin el consentimiento escrito previo del Banco, aun cuando se encuentre obligado con alguna de las partes por un acuerdo de confidencialidad similar; salvo a los empleados de cada una de ellas o de cualquier otra persona que se encuentre en una relación contractual o de confianza con el proveedor y que requiera dicha información para utilizarla para asuntos relacionados con los servicios.
4. El CONTRATISTA debe asegurar de que toda la Información Confidencial sea usada para el exclusivo beneficio de los servicios que se prestan en virtud del contrato. Por tal razón, la violación de cualquiera de las disposiciones establecidas en esta cláusula obligará al proveedor a indemnizar todos los perjuicios directos que cause con motivo de ello y, de caso ser necesario, a resolver de manera automática el contrato.

➢ Se considera como violación de la confidencialidad y, por tanto, una conducta desleal, la divulgación o explotación sin autorización de la otra parte, de la información a la que tendrá acceso legítimamente, pero con deber de reserva.

➢ Se entiende que la obligación asumida está referida no sólo a documentos e informaciones señalados por la otra parte como "confidenciales" sino a todos los documentos e informaciones que, en razón del referido intercambio, pueda ser conocida por cualquier medio, incluyendo sin limitarse a ella, características técnicas, sistemas, programación de instalación, ubicación física, información de las Oficina, etc.

➢ El CONTRATISTA se obliga a mantener y guardar en estricta reserva y absoluta confidencialidad todos los documentos e informaciones que reciban del Banco, durante las negociaciones y ejecución del servicio.

➢ Para la prestación del servicio el proveedor se compromete a firmar un acuerdo de confidencialidad de la información.

➢ Para la prestación del servicio el CONTRATISTA se compromete a firmar un acuerdo de confidencialidad.

EL CONTRATISTA declara tener total conocimiento que la infracción del compromiso de reserva, confidencialidad y secreto será considerada como incumplimiento contractual y, en consecuencia, será causal de resolución automática del CONTRATO, de conformidad con el artículo 1430° del Código Civil. No obstante, EL CONTRATISTA queda exenta de responsabilidad si la información o documentación es difundida por razón de mandato judicial, legalmente requerida, o por terceros sin vinculación a él.

12.4 Continuidad del Negocio

El CONTRATISTA debe desarrollar la gestión de continuidad para el servicio objeto del contrato, mediante la aplicación de la Resolución S.B.S N° 877-2020 Reglamento para la gestión de la continuidad del negocio o buenas prácticas para la Gestión de Continuidad del Negocio (ISO 20301) para este tipo de servicio.

El CONTRATISTA se compromete a mantener la continuidad del servicio contratado por EL BANCO; para lo cual, debe contar con procedimientos documentados que permitan responder, recuperar, reanudar y restaurar el servicio objeto del contrato; además, los referidos procedimientos deben formar parte de un Plan de Recuperación de Tecnología de Información o en su defecto de un Plan de Continuidad de Negocio, de tal modo que su ejecución asegure la alta disponibilidad.

El CONTRATISTA debe entregar a EL BANCO: el Plan de Recuperación de Tecnología de Información / Plan de Continuidad de Negocio, los cuales deban estar actualizados y probados cuando menos una vez al año; asimismo, El CONTRATISTA deberá contar con un Programa de Pruebas respecto a los procedimientos documentados. Al respecto, El CONTRATISTA deberá remitir cada primer trimestre del año el Plan(es) y Programa de Pruebas, así como un reporte que resuma los resultados alcanzados de las pruebas efectuadas.

El CONTRATISTA programará las pruebas en horarios de madrugada a fin de reducir la afectación del servicio en coordinación con la Oficina de Seguridad Informática; para casos de pruebas que implique la interrupción del servicio, estas deben ser identificadas y comunicadas desde su programación. Asimismo, EL BANCO podrá solicitar su participación en el desarrollo de dichas pruebas, y de tener alguna observación sobre los resultados de las pruebas podrá remitirla a El CONTRATISTA para que lo evalúe y responda en un periodo no mayor a treinta (30) días con un plan de acción y fecha estimada para subsanar la(s) observación(es).

Ante la eventual interrupción del servicio objeto del contrato por causales imputables a El CONTRATISTA, siempre que dicha interrupción sea continúa y se mantenga por un periodo mayor a una (01) hora; El CONTRATISTA deberá comunicar a EL BANCO (con copia al correo electrónico de la Oficina de Seguridad Informática) de forma inmediata o máximo al día siguiente de ocurrida la incidencia y posterior a ello deberá remitir un informe técnico detallado de la interrupción (incluyendo como mínimo el detalle de: la fecha, hora, duración, causa/origen, diagnostico, impacto, acciones para la recuperación del servicio, estado del servicio afectado, acciones de mejora, conclusiones y recomendaciones), en un plazo máximo de cinco (05) días hábiles, ambos periodos contabilizados a partir de la ocurrencia del evento.

Para casos que El CONTRATISTA realice cambios a sus configuraciones u otros componentes que involucren/afecten la operatividad del servicio objeto del contrato, deben ser comunicados a EL BANCO con cinco (05) días hábiles de anticipación a la Oficina de Seguridad Informática.

El CONTRATISTA se compromete a entregar a EL BANCO toda la documentación y/o información que pueda ser necesaria para el correcto funcionamiento del servicio objeto del contrato y que además permita a EL BANCO tener un nivel de independencia en sus mantenimientos y mejoras, así como mantener una operación adecuada

12.5 Riesgo Operativo

EL CONTRATISTA debe aplicar las medidas de control para la gestión de los riesgos operacionales, que sean aplicables al servicio contratado por EL BANCO; que permita identificar, evaluar, tratar, controlar y monitorear los diversos riesgos asociados a dicho servicio, siendo responsable frente a EL BANCO en caso de la materialización de algún riesgo operativo que, en el marco de la prestación del servicio, afecte a Banco y/o sus clientes.

Para garantizar la adecuada gestión de los riesgos asociados al servicio contratado, EL CONTRATISTA debe implementar y cumplir con los lineamientos para la gestión de riesgo operacional que apliquen al servicio contratado, indicados en la Resolución SBS N° 2116-2009 - "Reglamento para la Gestión del Riesgo Operacional".

EL CONTRATISTA se obliga a cumplir con contar obligatoriamente con un procedimiento orientado a gestionar el riesgo operacional de los servicios contratados por EL BANCO, que permita identificar, evaluar, tratar, medir, controlar, monitorear y reportar los diversos riesgos que enfrentan, siendo responsable frente a este último, en caso de culpa leve o culpa inexcusable. Este procedimiento y el resultado de la gestión de riesgos deberá ser entregado al finalizar la etapa de implementación y posterior a ella de forma semestral.

CLÁUSULA DECIMA TERCERA: DEL CODIGO DE ÉTICA DEL BANCO DE LA NACIÓN

EL CONTRATISTA declara bajo juramento conocer que **EL BANCO** cuenta con un Código de Ética, cuyo objetivo principal está orientado a establecer valores institucionales, principios, derechos, deberes y prohibiciones éticos. Por tanto, **EL CONTRATISTA** se compromete a tomar conocimiento del contenido del mismo, a través del enlace http://www.bn.com.pe/nosotros/codigo-etica.asp.

EL BANCO sólo contrata con quienes mantengan los más altos estándares de honestidad, ética y profesionalismo en la gestión de sus negocios. EL BANCO toma muy en serio e investigará cualquier indicio, denuncia, sugerencia o evidencia que indique que EL CONTRATISTA pueda estar involucrada en prácticas prohibidas o indebidas de corrupción, o en caso éste haya ejercitado actos coercitivos indebidos, incentivos indebidos, ofertas indebidas, chantaje o violencia, para obtener ventaja contractual. Estas son prácticas que EL BANCO rechaza, por lo que EL BANCO no efectúa ningún tipo de negocio o contrato con aquellas organizaciones que se gestionen con esas prácticas indebidas. En caso EL BANCO descubra que EL CONTRATISTA está involucrado en tales prácticas, EL BANCO estará facultada para resolver de inmediato el contrato y podrá retener los montos comprometidos en tales prácticas indebidas. Esta disposición será aplicada en todo su rigor.

En particular, EL BANCO prohíbe expresamente a todos sus proveedores de realizar ofrecimientos, o prometer cualquier pago ilegal, impropio o indebido, o transferir cualquier bien o valor a favor de cualquier autoridad (nacional, regional o local), tercera parte, o trabajador de EL BANCO, a fin de sostener o entablar negocios con EL BANCO. EL BANCO exige asimismo que toda documentación que le sea remitida, incluyendo la documentación por reembolso de gastos o facturas sean completas y ajustadas a los montos reales y acordes con la naturaleza de los servicios prestados o gastos incurridos. EL CONTRATISTA acuerda en cooperar con EL BANCO en remitirle cualquier documentación o justificación derivada del contrato que le sea requerida a EL CONTRATISTA sobre el particular. EL BANCO no realizará pagos a EL CONTRATISTA contra facturas o solicitudes de pago que no estén debidamente sustentados.

EL CONTRATISTA garantiza que, en relación con el presente contrato, no ha realizado, directa o indirectamente, ofrecimiento o promesa indebida, irregular, ilícita o ilegal alguna, y se obliga a no realizar ofrecimiento alguno o promesa, pago o transferencia ilícita de cualquier valor o bien, a cualquier autoridad, terceras partes, o trabajadores de EL BANCO; y asimismo, EL CONTRATISTA se obliga a cumplir con las normas legales aplicables a la ejecución del presente contrato. El incumplimiento de estas obligaciones o la remisión de información falsa, darán lugar a la resolución inmediata del contrato, sin perjuicio de los demás recursos y remedios establecidos en el presente contrato.

CLÁUSULA DECIMA CUARTA: PREVENCION DEL LAVADO DE ACTIVOS Y DEL FINANCIAMIENTO DEL TERRORISMO Y ANTISOBORNO

EL CONTRATISTA declara conocer que EL BANCO es una empresa sujeta a la Resolución SBS N° 2660-2015-Reglamento de gestión de riesgo de Lavado de Activos y del Financiamiento del Terrorismo, cuya finalidad es mantener un sistema de prevención de LA/FT con componentes de cumplimiento y de gestión de riesgo de LA/FT. Por tanto, EL CONTRATISTA se obliga a respetar la mencionada norma, así como cualquier otra norma legal sobre esta materia, desde su entrada en vigencia. La información a la que tiene acceso EL CONTRATISTA sólo podrá ser utilizada, para los fines señalados en el presente contrato.

EL BANCO es responsable de asegurar el cumplimiento de la normatividad emitida por la Superintendencia de Banca, Seguros y AFPs (SBS), por lo que EL CONTRATISTA declara conocerla y se obliga a facilitar a EL BANCO previo a la firma del presente contrato y durante la vigencia del mismo, en la oportunidad y a solo requerimiento de EL BANCO, toda la información y documentación referida a las actividades comerciales de EL CONTRATISTA, así como de sus socios y/o accionistas y/o representantes legales.

Dicha información comprenderá como mínimo el formato currículo vitae, ficha RUC, vigencia de poderes y/o copia literal de la partida, copia de los documentos de identidad de los accionistas y representante legal, estados financieros; así como cualquier otra documentación que se requiera para cumplir con la debida diligencia de Contrapartes y Gestión de los Riesgos de LA/FT a los que se encuentra expuestos EL BANCO, sin que esta enumeración resulte limitativa. Ante el requerimiento por parte de EL BANCO, EL CONTRATISTA se obliga a proporcionar la información en un plazo razonable. Asimismo, las partes establecen que la información requerida solo podrá versar sobre la referente al presente contrato o toda aquella que pueda generar un impacto importante respecto de lo establecido en la presente cláusula.

EL CONTRATISTA declara que los fondos con los que se conformó el capital de la empresa se originaron en negocios lícitos, que todas las actividades e ingresos que se perciben provienen de actividades lícitas; y que, ni EL CONTRATISTAS, ni sus socios y/o accionistas, ni su representante legal, se encuentra/n en ninguna lista de reportes internacionales, nacionales o bloqueados por actividades de narcotráfico, lavado de activos o terrorismo. Asimismo, declara que tampoco existe en su contra, ni sus socios y/o accionistas, ni su representante legal ningún procedimiento o proceso en instancias nacionales o internacionales por ninguno de los aspectos anteriores. Por lo que, EL CONTRATISTA reconoce que de incurrir en alguna/s de la/s situación/es previstas en este párrafo, el presente contrato quedará resuelto de forma automática.

Asimismo, en relación con el cumplimiento de las obligaciones derivadas del presente Contrato, EL CONTRATISTA declara estar de acuerdo y garantiza que:

a) No ha violado y no violará las leyes vigentes de lucha contra el lavado de activos, financiamiento del terrorismo, corrupción y sus regulaciones.

b) No ha realizado, y se compromete a no realizar o a participar en las siguientes conductas: realización de pagos o transferencias de valor, ofertas, promesas o la concesión de cualquier ventaja económica o de otro tipo, solicitudes, acuerdos para recibir o aceptar cualquier ventaja financiera o de otro tipo, ya sea directa o indirectamente, que tenga el propósito, el efecto, la aceptación o la conformidad del soborno público o comercial o cualquier otro medio ilegal o indebido de obtener o retener un negocio, una ventaja comercial o de la mala ejecución de

cualquier función o actividad.

c) Deberá procurar el cumplimiento de las obligaciones mencionadas en los literales a) y b) de sus propios asociados, agentes o subcontratistas que puedan ser utilizados por EL CONTRATISTA para el cumplimiento de las obligaciones en virtud del presente contrato.

d) EL CONTRATISTA deberá contar con políticas y procedimientos diseñados para prevenir la existencia de actos que puedan calificar como lavado de activos, terrorismo, soborno o corrupción en la ejecución del presente contrato, EL CONTRATISTA deberá cumplir estas obligaciones a partir de sus propias personas, asociadas, agentes o subcontratistas que puedan ser utilizados en la ejecución del presente contrato.

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

El incumplimiento de las obligaciones asumidas por EL CONTRATISTA a través de la presente cláusula constituye causal de resolución automática del presente contrato, de conformidad con el artículo 1430° del Código Civil, siendo responsable EL CONTRATISTA, de todas las multas y sanciones impuestas a EL BANCO derivadas directamente de este tipo de incumplimientos.

CLAUSULA DÉCIMA QUINTA: RIESGO OPERATIVO

El CONTRATISTA debe aplicar las medidas de control para la gestión de los riesgos operacionales, que sean aplicables al servicio contratado por el Banco; que permita identificar, evaluar, tratar, controlar y monitorear los diversos riesgos asociados a dicho servicio, siendo responsable frente a EL BANCO en caso de la materialización de algún riesgo operativo que, en el marco de la prestación del servicio, afecte a EL BANCO y/o sus clientes.

Para garantizar la adecuada gestión de los riesgos asociados al servicio contratado, EL CONTRATISTA debe implementar y cumplir con los lineamientos para la gestión de riesgo operacional que apliquen al servicio contratado, indicados en la Resolución SBS N° 2116-2009 - "Reglamento para la Gestión del Riesgo Operacional".

EL CONTRATISTA se obliga a cumplir con contar obligatoriamente con un procedimiento orientado a gestionar el riesgo operacional de los servicios contratados por EL BANCO, que permita identificar, evaluar, tratar, medir, controlar, monitorear y reportar los diversos riesgos que enfrentan, siendo responsable frente a este último, en caso de culpa leve o culpa inexcusable. Este procedimiento y el resultado de la gestión de riesgos deberá ser entregado al finalizar la etapa de implementación y posterior a ella de forma semestral.

CLAUSULA DÉCIMO SEXTA: PREVENCION DEL LAVADO DE ACTIVOS Y DEL FINANCIAMIENTO DEL TERRORISMO Y ANTISOBORNO

EL CONTRATISTA declara conocer que EL BANCO es una empresa sujeta a la Resolución SBS N° 2660-2015-Reglamento de gestión de riesgo de Lavado de Activos y del Financiamiento del Terrorismo, cuya finalidad es mantener un sistema de prevención de LA/FT con componentes de cumplimiento y de gestión de riesgo de LA/FT. Por tanto, EL CONTRATISTA se obliga a respetar la mencionada norma, así como cualquier otra norma legal sobre esta materia, desde su entrada en vigencia. La información a la que tiene acceso EL CONTRATISTA sólo podrá ser utilizada, para los fines señalados en el presente contrato.

EL BANCO es responsable de asegurar el cumplimiento de la normatividad emitida por la

Superintendencia de Banca, Seguros y AFPs (SBS), por lo que EL CONTRATISTA declara conocerla y se obliga a facilitar a EL BANCO previo a la firma del presente contrato y durante la vigencia del mismo, en la oportunidad y a solo requerimiento de EL BANCO, toda la información y documentación referida a las actividades comerciales de EL CONTRATISTA, así como de sus socios y/o accionistas y/o representantes legales.

Dicha información comprenderá como mínimo el formato currículo vitae, ficha RUC, vigencia de poderes y/o copia literal de la partida, copia de los documentos de identidad de los accionistas y representante legal, estados financieros; así como cualquier otra documentación que se requiera para cumplir con la debida diligencia de Contrapartes y Gestión de los Riesgos de LA/FT a los que se encuentra expuestos EL BANCO, sin que esta enumeración resulte limitativa. Ante el requerimiento por parte de EL BANCO, EL CONTRATISTA se obliga a proporcionar la información en un plazo razonable. Asimismo, las partes establecen que la información requerida solo podrá versar sobre la referente al presente contrato o toda aquella que pueda generar un impacto importante respecto de lo establecido en la presente cláusula.

EL CONTRATISTA declara que los fondos con los que se conformó el capital de la empresa se originaron en negocios lícitos, que todas las actividades e ingresos que se perciben provienen de actividades lícitas; y que, ni EL CONTRATISTAS, ni sus socios y/o accionistas, ni su representante legal, se encuentra/n en ninguna lista de reportes internacionales, nacionales o bloqueados por actividades de narcotráfico, lavado de activos o terrorismo. Asimismo, declara que tampoco existe en su contra, ni sus socios y/o accionistas, ni su representante legal ningún procedimiento o proceso en instancias nacionales o internacionales por ninguno de los aspectos anteriores. Por lo que, EL CONTRATISTA reconoce que de incurrir en alguna/s de la/s situación/es previstas en este párrafo, el presente contrato quedará resuelto de forma automática.

Asimismo, en relación con el cumplimiento de las obligaciones derivadas del presente Contrato, EL CONTRATISTA declara estar de acuerdo y garantiza que:

e) No ha violado y no violará las leyes vigentes de lucha contra el lavado de activos, financiamiento del terrorismo, corrupción y sus regulaciones.
f) No ha realizado, y se compromete a no realizar o a participar en las siguientes conductas: realización de pagos o transferencias de valor, ofertas, promesas o la concesión de cualquier ventaja económica o de otro tipo, solicitudes, acuerdos para recibir o aceptar cualquier ventaja financiera o de otro tipo, ya sea directa o indirectamente, que tenga el propósito, el efecto, la aceptación o la conformidad del soborno público o comercial o cualquier otro medio ilegal o indebido de obtener o retener un negocio, una ventaja comercial o de la mala ejecución de cualquier función o actividad.
g) Deberá procurar el cumplimiento de las obligaciones mencionadas en los literales a) y b) de sus propios asociados, agentes o subcontratistas que puedan ser utilizados por EL CONTRATISTA para el cumplimiento de las obligaciones en virtud del presente contrato.
h) EL CONTRATISTA deberá contar con políticas y procedimientos diseñados para prevenir la existencia de actos que puedan calificar como lavado de activos, terrorismo, soborno o corrupción en la ejecución del presente contrato, EL CONTRATISTA deberá cumplir estas obligaciones a partir de sus propias personas, asociadas, agentes o subcontratistas que puedan ser utilizados en la ejecución del presente contrato.

En caso de que EL CONTRATISTA tuviera noticia de la ocurrencia de alguno de estos hechos en el marco del presente contrato que actual o potencialmente pudieran impactar de cualquier

forma a EL BANCO sea en su responsabilidad penal, civil o crédito y reputación, deberá informar de inmediato de este hecho a EL BANCO; sin perjuicio de tomar todas las medidas necesarias para evitar o mitigar estos efectos. Asimismo, EL CONTRATISTA se compromete a entregar a EL BANCO toda la información que éste le requiera en el marco de las investigaciones internas, sean éstas de carácter meramente preventivo o cuándo se indague sobre hechos constitutivos de delito, sea que estas investigaciones tengan carácter sistemático o aleatorio.

El incumplimiento de las obligaciones asumidas por EL CONTRATISTA a través de la presente cláusula, constituye causal de resolución automática del presente contrato, de conformidad con el artículo 1430° del Código Civil, siendo responsable EL CONTRATISTA, de todas las multas y sanciones impuestas a EL BANCO derivadas directamente de este tipo de incumplimientos.

CLÁUSULA DÉCIMA SÉPTIMA: ACUERDOS DE NIVELES DE SERVICIOS - SLA

El Acuerdo de Niveles de Servicios - SLA son estándares mínimos requeridos para la prestación según el objeto de la contratación, siendo que los SLA aceptados por ambas partes, se establecen en el **Anexo III "Acuerdos de Niveles de Servicios – SLA y Penalidades"** de EL CONTRATO, los cuales son de obligatorio cumplimiento por parte de EL CONTRATISTA. Por otro lado, EL CONTRATISTA se compromete y acepta dar cumplimiento a todos los plazos, obligaciones, especificaciones y compromisos que allí se detallan.

Por lo cual EL CONTRATISTA se obliga a cumplir, con lo siguiente:

- EL CONTRATISTA declara y garantiza que cuenta y contara durante toda la vigencia de EL CONTRATO con las instalaciones, el personal, el equipamiento, los sistemas, la capacidad, la experiencia técnica y tecnológica y los conocimientos necesarios para cumplir con la prestación en las condiciones pactadas y exigidas por el BANCO, por la regulación peruana y requerimiento de la SBS.

- EL CONTRATISTA se obliga a cubrir los gastos que requiera para resolver cualquier tipo de emergencia que sea de su competencia y que afecten la continuidad de la prestación de los servicios de ésta.

CLÁUSULA DÉCIMA OCTAVA: PARTES INTEGRANTES DEL CONTRATO

EL CONTRATO está conformado por:

- Anexo I "Oferta Ganadora"
- Anexo II "Especificaciones Técnicas para la Contratación de Servicios: Solución para la Protección Avanzada en Endpoints y la Red del Banco de la Nación"
- Anexo III "Acuerdos de Niveles de Servicios – SLA y Penalidades"

CLÁUSULA DÉCIMA NOVENA: DECLARACIONES Y GARANTÍAS

EL BANCO y el CONTRATISTA manifiestan y declaran que a la fecha de suscripción de EL CONTRATO:

a) Son personas jurídicas legalmente constituidas y que operan y han operado de acuerdo a las leyes, decretos, reglamentos y demás normas aplicables en el Perú.

b) EL CONTRATO y el cumplimiento de las obligaciones establecidas en el mismo, constituyen actos jurídicos que pueden ser legalmente realizados en mérito a las respectivas disposiciones legales y estatutarias que rigen sus actividades; y que EL CONTRATO se suscribe, celebra y otorga reuniendo todas las aprobaciones necesarias, sin violación de disposición legal,

estatuaria, ni contractual alguna. La celebración de el CONTRATO y la asunción de cualquier otro compromiso vinculado con el mismo, no viola contratos o compromisos anteriores; y no existe mejor derecho ni gravamen que impida, prohíba, limite o de cualquier manera restrinja sus facultades y derechos o para suscribir y firmar la totalidad de la documentación que resulte para el otorgamiento y perfeccionamiento de EL CONTRATO, así como su cumplimiento.

c) 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 EL BANCO, por los conceptos, montos y vigencias siguientes:

- De fiel cumplimiento del contrato: [CONSIGNAR EL MONTO], a través de la Carta Fianza N° [INDICAR NÚMERO DEL DOCUMENTO] emitida por [SEÑALAR EMPRESA QUE LA EMITE]. Monto que es equivalente al 10, por ciento (%) del monto del contrato original, la misma que debe mantenerse vigente hasta la conformidad de la recepción de la prestación a cargo de EL CONTRATISTA, de conformidad con lo establecido en EL CONTRATO y **Anexo II "Especificaciones Técnicas para la Contratación de Servicios: Solución para la Protección Avanzada en Endpoints y la Red del Banco de la Nación"**.

d) No tienen pendiente, ni tienen conocimiento de la inminencia de litigio o procedimiento administrativo alguno ante ningún tribunal o autoridad administrativa nacional, provincia o municipal del país o del extranjero de cualquier materia, ni tampoco proceso arbitral alguno, que pueda afectar adversa y sustancialmente: (i) su capacidad de cumplir con sus obligaciones según lo previsto en el EL CONTRATO; (ii) sus negocios o su condición económica, financiera o los resultados de sus operaciones vinculadas a EL CONTRATO; o (iii) la validez, legalidad o ejecutabilidad de EL CONTRATO.

CLAUSULA VIGESIMA: LEY APLICABLE

El presente Contrato se encuentra sujeto a las disposiciones de la Ley N° 26702, el Código Civil y a cualquier otra disposición vigente en materia de regulación bancaria.

Desde ya EL CONTRATISTA se obliga frente a EL BANCO a cumplir con todos y cada uno de los requerimientos que EL BANCO le solicite en su oportunidad a efectos de dar estricto cumplimiento a la Ley y demás normas pertinentes. Desde ya EL CONTRATISTA se compromete a suscribir la/las adendas(s) correspondiente(s) a este CONTRATO a efectos de incluir los mencionados requerimientos que EL BANCO le pida en el marco de la regulación vigente y el presente contrato.

CLÁUSULA VIGESIMA PRIMERA: DESIGNACION DE REPRESENTANTES

Para efectos de las coordinaciones que resulten necesarias en el marco de este Contrato, las partes designan como sus principales representantes:

EL CONTRATISTA a su Gerente General o quien haga sus veces.
EL BANCO a su Gerente ..... o quien haga sus veces.

Sin perjuicio de lo señalado en el párrafo precedente, cada parte podrá designar un representante operativo, el que tendrá bajo su responsabilidad la coordinación de las acciones necesarias para permanente y buen desarrollo de EL CONTRATO.

Los representantes operativos tendrán la autoridad suficiente para tomar las acciones que sean necesarias para la adecuada prestación de los servicios contratados.

Cada una de las partes informará a la otra, por escrito, el nombre de los representantes operativos y de los representantes auxiliares si los hubiera. En caso una de las partes no designe representantes operativos, las coordinaciones se realizarán con el representante principal.

Los procedimientos operativos así como cualquier otro asunto no previsto expresamente en EL **CONTRATO** y sus Anexos, serán fijados por ambas partes de común acuerdo mediante el intercambio de correspondencia, las que una vez cursadas y aceptadas por la parte destinataria serán consideradas como parte integrante de EL CONTRATO.

CLÁUSULA VIGÉSIMA SEGUNDA: RESOLUCIÓN DEL CONTRATO

LAS PARTES acuerdan y reconocen que EL CONTRATO podrá resolverse de pleno derecho por incumplimiento de cualquiera de las obligaciones pactadas en atención al artículo 1430° del Código Civil; sin embargo, la parte afectada tiene la facultad contractual de requerir a su contraparte que cumpla primero con su obligación dentro de un plazo de 15 días hábiles, y si la obligación no se cumple dentro de dicho plazo, EL CONTRATO se resolverá de pleno derecho, sin perjuicio del pago de la indemnización por daños y perjuicios correspondientes.

E L CONTRATO podrá resolverse por acuerdo mutuo entre EL BANCO y EL **CONTRATISTA** para lo cual suscribirán el documento correspondiente.

LAS PARTES expresamente acuerdan que en caso cualquiera de ellas optara por la resolución de EL CONTRATO, la resolución no libera a las mismas del cumplimiento de todas las obligaciones adquiridas con anterioridad a la resolución y que se encuentren pendientes de ejecución hasta el momento de la resolución efectiva, en los términos y condiciones establecidos en EL CONTRATO.

CLAUSULA VIGESIMA TERCERA: SOLUCIÓN DE CONTROVERSIAS

Todo litigio, controversia, desavenencia, reclamación o interpretación resultante, o relacionada o derivada de este Contrato o que guarde relación con él, incluidas las relativas a su nulidad, validez, eficacia o terminación incluso las del convenio arbitraje serán resueltas mediante conciliación y/o arbitraje ante el Centro Arbitraje de la Pontificia Universidad Católica del Perú, de conformidad con los reglamentos de dicho Centro.

Si la conciliación concluyera por inasistencia de una o ambas partes, con un acuerdo parcial o sin acuerdo, las partes se someterán a un Arbitraje de Derecho para que resuelvan las controversias definitivamente. No es obligatoria la conciliación previa al Arbitraje.

El arbitraje antes referido tendrá las siguientes características y regulaciones:

✓ El arbitraje será de derecho e institucional, bajo la administración del Centro Arbitraje de la Pontificia Universidad Católica del Perú, a cuyos reglamentos y estatutos las partes acuerdan someterse en forma expresa e irrevocable. El arbitraje será en Lima y en idioma español.

✓ En caso que el monto de la cuantía de la solicitud de arbitraje sea menor a 50 (cincuenta) Unidades Impositivas Tributarias - UIT, vigentes a la fecha de la solicitud, la controversia será resuelta por Árbitro Único designado por el Centro Arbitraje de la Pontificia Universidad Católica del Perú

✓ En caso que el monto de la cuantía de la solicitud de arbitraje sea mayor o igual a 50 (cincuenta) Unidades Impositivas Tributarias - UIT, vigentes a la fecha de la solicitud, la controversia será resuelta por un Tribunal compuesto por tres árbitros. Cada parte interviniente designará un árbitro y los dos árbitros designados escogerán al Presidente del Tribunal, a falta de acuerdo de los dos árbitros para escoger al Presidente, éste será designado por el Centro Arbitraje de la Pontificia Universidad Católica del Perú. Los árbitros podrán actuar como conciliadores y amigables componedores del asunto que se les exponga, en cualquier etapa del

arbitraje.

✓ Las partes acuerdan que respecto a los honorarios de los árbitros y del Presidente del Tribunal Arbitral, cada parte interviniente asumirá el costo de los honorarios del Árbitro que designe y además asumirá el 50% de los honorarios del Presidente del Tribunal Arbitral, de darse el caso.

✓ El laudo arbitral emitido obligará a las partes y pondrá fin al procedimiento de manera definitiva, siendo el mismo inapelable ante el Poder Judicial o cualquier instancia administrativa, tiene el valor de cosa juzgada y se ejecutará como una sentencia. Queda perfectamente entendido que las partes no le confieren al Tribunal o al Árbitro Único la posibilidad de ejecutar el laudo.

✓ Las partes acuerdan que de considerar necesario interponer recurso de anulación del laudo arbitral ante el Poder Judicial, no constituirá requisito de admisibilidad de dicho recurso la presentación de recibo de pago, comprobante de depósito bancario o fianza solidaria por el monto laudado a favor de la parte vencedora

En el caso que las partes o el árbitro tuvieran que recurrir al Poder Judicial, queda establecido que, en estos casos, serán competentes los jueces y tribunales del distrito judicial de Lima, Perú, renunciando las Partes al fuero de los jueces que les pudiera corresponder por razón de su domicilio.

Queda entendido que los acuerdos contenidos en la presente Cláusula sobrevivirán a la terminación o resolución del presente Contrato y serán aplicables a cualquier conflicto que pudiera generarse entre las partes con relación al presente Contrato y los derechos y obligaciones que se deriven de éste, incluyendo los conflictos derivados o relativos a su extinción, salvo acuerdo distinto y posterior de las partes.

CLÁUSULA VIGÉSIMA CUARTA: 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 EL BANCO: [.....]

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, las disposiciones del presente contrato y anexos, las partes lo firman por duplicado en señal de conformidad en la ciudad de [.....] al [CONSIGNAR FECHA].

"EL BANCO" "EL CONTRATISTA"

"EL BANCO" "EL CONTRATISTA"

ANEXO I

OFERTA GANADORA

ANEXO II

"ESPECIFICACIONES TÉCNICAS PARA LA CONTRATACIÓN DE SERVICIOS: SOLUCIÓN PARA LA PROTECCIÓN AVANZADA EN ENDPOINTS Y LA RED DEL BANCO DE LA NACIÓN"

ANEXO III

"ACUERDOS DE NIVELES DE SERVICIOS – SLA Y PENALIDADES"

Formatos

Formato N° 1

DECLARACIÓN JURADA DE DATOS DEL POSTOR

Señores
COMITÉ DEL CONCURSO DE MERITOS
Concurso de Méritos N° 0007-2023-BN
Presente.-

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

Razón Social :			
Domicilio Legal :			
RUC :	Teléfono(s) :		
Correo electrónico :			

Autorización de notificación por correo electrónico:

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

1. Solicitud de la descripción a detalle de todos los elementos constitutivos de la oferta.
2. Solicitud de subsanación de los requisitos para perfeccionar el contrato.
3. Solicitud al postor que ocupó el segundo lugar en el orden de prelación para presentar los documentos para perfeccionar el contrato.

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.

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

Formato N° 1

DECLARACIÓN JURADA DE DATOS DEL POSTOR

Señores
COMITÉ DEL CONCURSO DE MERITOS
Concurso de Méritos Nº 0007-2023-BN
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			
Razón Social :			
Domicilio Legal :			
RUC :	Teléfono(s) :		
Correo electrónico :			

Datos del consorciado 2			
Razón Social :			
Domicilio Legal :			
RUC :	Teléfono(s) :		
Correo electrónico :			

Datos del consorciado ...			
Razón Social :			
Domicilio Legal :			
RUC :	Teléfono(s) :		
Correo electrónico :			

Autorización de notificación por correo electrónico:

Correo electrónico del consorcio:

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

1. Solicitud de la descripción a detalle de todos los elementos constitutivos de la oferta.
2. Solicitud de subsanación de los requisitos para perfeccionar el contrato.
3. Solicitud al postor que ocupó el segundo lugar en el orden de prelación para

presentar los documentos para perfeccionar el contrato.

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.

Formato N° 2

DECLARACIÓN JURADA PARA SER POSTOR

Señores
COMITÉ DEL CONCURSO DE MERITOS
Concurso de Méritos Nº 0007-2023-BN
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 proceso de concurso de méritos ni para contratar con el Estado.

iii. Que mi información (en caso que el postor sea persona natural) o la información de la persona jurídica que represento, registrada en el RNP se encuentra actualizada.

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

v. 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.

vi. Conocer, aceptar y someterme a las bases, condiciones y reglas del proceso de concurso de méritos.

vii. Ser responsable de la veracidad de los documentos e información que presento en el presente proceso de concurso de méritos.

viii. Comprometerme a mantener la oferta presentada durante el proceso de concurso de méritos 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.

Formato Nº 3

DECLARACIÓN JURADA DE CUMPLIMIENTO DE LOS REQUISITOS, CARACTERISTICAS Y CONDICIONES TECNICAS

Señores
COMITÉ DEL CONCURSO DE MERITOS
Concurso de Méritos Nº 0007-2023-BN
Presente.-

Es grato dirigirme a usted, para hacer de su conocimiento que luego de haber examinado las bases y demás documentos del proceso de concurso de méritos de la referencia y, conociendo todos los alcances y las condiciones detalladas en dichos documentos, el postor que suscribe ofrece la prestación del **"Servicio de solución para la protección avanzada en Endpoints y la Red del Banco de la Nación"**, de conformidad con los requisitos, características y condiciones técnicas que se indican en el Anexo N° 1 – Términos de Referencia, de las bases del Concurso de Méritos N° 0007-2023-BN, así como los documentos derivados del proceso de concurso de méritos que establezcan obligaciones para las partes.

Asimismo, declaro bajo juramento conocer que el Banco de la Nación cuenta con un Código de Ética, cuyo objetivo principal está orientado a establecer valores institucionales, principios, derechos, deberes y prohibiciones éticos. Por tanto, me comprometo a tomar conocimiento del contenido del mismo, a través del enlace https://www.bn.com.pe/nosotros/archivos/CodigoEticaBN.pdf

Del mismo modo, declaro conocer que el Banco de la Nación es una empresa sujeta a la Resolución SBS N° 2660-2015 - Reglamento de Gestión de Riesgo de Lavado de Activos y del Financiamiento del Terrorismo, cuya finalidad es mantener un sistema de prevención de LA/FT con componentes de cumplimiento y de gestión de riesgo de LA/FT. Por tanto, me obligo a respetar la mencionada norma, así como cualquier otra norma legal sobre esta materia, desde su entrada en vigencia.

[CONSIGNAR CIUDAD Y FECHA]

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

Formato Nº 4

DECLARACIÓN JURADA DE PLAZO DE PRESTACIÓN

Señores
COMITÉ DEL CONCURSO DE MERITOS
Concurso de Méritos Nº 0007-2023-BN
Presente.-

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

CONSIGNAR PLAZO OFERTADO PARA LA PRESTACION DEL SERVICIO.

[CONSIGNAR CIUDAD Y FECHA]

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

Formato N° 5

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

Señores
COMITÉ DEL CONCURSO DE MERITOS
Concurso de Méritos N° 0007-2023-BN
Presente.-

Los suscritos declaramos expresamente que hemos convenido en forma irrevocable, durante el lapso que dure el proceso de concurso de méritos, para presentar una oferta conjunta al **CONCURSO DE MERITOS N° 0007-2023-BN.**

Asimismo, en caso de obtener la buena pro, nos comprometemos a formalizar el contrato de consorcio, 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 proceso de concurso de méritos, suscripción y ejecución del contrato correspondiente con [CONSIGNAR NOMBRE DE LA ENTIDAD].

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

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

e) 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] : %][1]
   [DESCRIBIR LAS OBLIGACIONES DEL CONSORCIADO 1]
2. OBLIGACIONES DE [NOMBRE, DENOMINACIÓN O RAZÓN SOCIAL DEL CONSORCIADO 2] : %][2]
   [DESCRIBIR LAS OBLIGACIONES DEL CONSORCIADO 2]

TOTAL OBLIGACIONES **100 %][3]**

[CONSIGNAR CIUDAD Y FECHA]

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

Importante

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

Las firmas de los integrantes del consorcio deben ser legalizadas.

Formato Nº 6

PRECIO DE LA OFERTA

Señores
COMITÉ DEL CONCURSO DE MERITOS
Concurso de Méritos Nº 0007-2023-BN
Presente.-

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

Descripción del Bien	Unidad de Medida	Cantidad Total	Precio Mensual (S/.)	Precio Total (S/.)
Prestación Principal: Servicio de solución para la protección avanzada en Endpoints y la Red del Banco de la Nación	Mes	36		
Prestación Accesoria: Capacitacion	Curso	1		
Precio Total de la Oferta (S/.)				

El precio de la oferta incluye todos los tributos, seguros, 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 de la prestación 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 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]".

Formato Nº 7

EXPERIENCIA DEL POSTOR EN LA ESPECIALIDAD

Señores
COMITÉ DEL CONCURSO DE MERITOS
Concurso de Méritos Nº 0007-2023-BN
Presente.-

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

Nº	CLIENTE	OBJETO DEL CONTRATO	Nº CONTRATO / O/S / COMPROBANTE DE PAGO	FECHA DEL CONTRATO O CP [4]	FECHA DE LA CONFORMIDAD DE SER EL CASO[5]	EXPERIENCIA PROVENIENTE[6] DE:	MONEDA	IMPORTE[7]	TIPO DE CAMBIO VENTA[8]	MONTO FACTURADO ACUMULADO[9]
1										
2										
3										
4										
5										
6										
	...									
TOTAL										

[CONSIGNAR CIUDAD Y FECHA]

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

---

4 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.

5 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.

6 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"*.

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

8 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.

9 Consignar en la moneda establecida en las bases.

Formato Nº 8

DECLARACIÓN JURADA DE REORGANIZACION SOCIETARIA

Señores
COMITÉ DEL CONCURSO DE MERITOS
Concurso de Méritos Nº 0007-2023-BN
Presente.-

Mediante el presente el suscrito, 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] absorbida como consecuencia de una reorganización societaria, no se encuentra sancionada.

[CONSIGNAR CIUDAD Y FECHA]

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

Formato N° 9

AUTORIZACIÓN DE NOTIFICACIONES DE LA ENTIDAD (BANCO DE LA NACION) DURANTE LA EJECUCION CONTRACTUAL MEDIANTE MEDIOS ELECTRÓNICOS DE COMUNICACIÓN

(DOCUMENTO A PRESENTAR EN EL PERFECCIONAMIENTO DEL CONTRATO)

Señores
COMITÉ DEL CONCURSO DE MERITOS
Concurso de Méritos N° 0007-2023-BN
Presente.-

El que se suscribe, [.....], Representante Legal de [.....], identificado con [CONSIGNAR TIPO DE DOCUMENTO DE IDENTIDAD] N° [CONSIGNAR NÚMERO DE DOCUMENTO DE IDENTIDAD], autorizo al Banco de la Nación que se me notifique al correo electrónico [INDICAR EL CORREO ELECTRÓNICO], las notificaciones que se realicen durante la etapa de ejecución del contrato suscrito entre ambas partes.

[CONSIGNAR CIUDAD Y FECHA]

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

Formato Nº 10

(SI ES PERSONA NATURAL)

DECLARACIÓN JURADA

RESOLUCIÓN SBS N° 2660-2015 - REGLAMENTO DE GESTIÓN DE RIESGOS DE LAVADO DE ACTIVOS Y DEL FINANCIAMIENTO DEL TERRORISMO

Señores
BANCO DE LA NACIÓN
PROCEDIMIENTO DE SELECCIÓN [CONSIGNAR]
Presente.-

[CONSIGNAR NOMBRE DE LA EMPRESA], con Registro Único de Contribuyentes Nº [CONSIGNAR], con domicilio legal en [CONSIGNAR], distrito de [CONSIGNAR], provincia y departamento de [CONSIGNAR], debidamente representada por su apoderado, el señor [CONSIGNAR], identificado con Documento de Identidad Nº [CONSIGNAR], cuyo poder obra inscrito en la Partida Electrónica Nº [CONSIGNAR], del Registro de Personas Jurídicas de [CONSIGNAR], declaro bajo juramento:

Conocer que EL BANCO DE LA NACIÓN es una Entidad Financiera sujeta al cumplimiento del Reglamento de Gestión de Riesgos de Lavado de Activos y del Financiamiento del Terrorismo, aprobado por Resolución SBS Nº 2660-2015, y que por tanto se obliga a proporcionar toda aquella información necesaria a fin de dar cumplimiento a lo dispuesto en los artículos 36º y 37º del referido Reglamento, así como a cualquier otra norma legal sobre la materia desde su entrada en vigencia, para lo cual se compromete a presentar con carácter obligatorio la siguiente documentación para la firma del contrato, la misma que se detalla:

SI ES PERSONA NATURAL:

Por el presente documento, declaro bajo juramento, lo siguiente:					
PERSONA NATURAL:					
1	Nombres:		Apellidos:		
2	**Tipo y número de documento de identidad (marque con una "X" según corresponda).**				
	DNI ( )	Pasaporte ( )	Carné de Extranjería ( )	Otro (Indique):	N°
3	Nacionalidad (en caso de extranjero):				
4	Domicilio (Indicar: Jr. - Av. - Calle - Pasaje / N° / Dpto-Int. N° /Urb - Complejo - Zona – Sector /Distrito/Provincia/Departamento):				
5	Rubros en los que el proveedor brinda sus productos o servicios:				
6	Años de experiencia en el mercado:				
7	N° Teléfono:		Correo electrónico:		
8	Declaro bajo juramento:				
	Contar con antecedentes penales ( )		No contar con antecedentes penales ( )		
9	Se encuentra incluido en la lista emitida por la Oficina de Control de Activos Extranjeros del Departamento de Tesoro de los Estados Unidos de América (OFAC) SI ☐ - NO ☐				
Afirmo y ratifico todo lo manifestado en la presente declaración jurada y me comprometo a presentarla cada dos (02) años de ejecución contractual.			**NOMBRE:**		
			FIRMA:		
			FECHA (día/mes/año):	/ /	
*Importante: - La información debe ser completada en su totalidad.					

Formato N° 10

(SI ES PERSONA JURÍDICA)
DECLARACIÓN JURADA
RESOLUCIÓN SBS N° 2660-2015 - REGLAMENTO DE GESTIÓN DE RIESGOS DE LAVADO DE ACTIVOS Y DEL FINANCIAMIENTO DEL TERRORISMO

Señores
BANCO DE LA NACIÓN
PROCEDIMIENTO DE SELECCIÓN [CONSIGNAR]
Presente.-

[CONSIGNAR NOMBRE DE LA EMPRESA], con Registro Único de Contribuyentes N° [CONSIGNAR], con domicilio legal en [CONSIGNAR], distrito de [CONSIGNAR], provincia y departamento de [CONSIGNAR], debidamente representada por su apoderado, el señor [CONSIGNAR], identificado con Documento de Identidad N° [CONSIGNAR], cuyo poder obra inscrito en la Partida Electrónica N° [CONSIGNAR], del Registro de Personas Jurídicas de [CONSIGNAR], declaro bajo juramento:

Conocer que EL BANCO DE LA NACIÓN es una Entidad Financiera sujeta al cumplimiento del Reglamento de Gestión de Riesgos de Lavado de Activos y del Financiamiento del Terrorismo, aprobado por Resolución SBS N° 2660-2015, y que por tanto se obliga a proporcionar toda aquella información necesaria a fin de dar cumplimiento a lo dispuesto en los artículos 36° y 37° del referido Reglamento, así como a cualquier otra norma legal sobre la materia desde su entrada en vigencia, para lo cual se compromete a presentar con carácter obligatorio la siguiente documentación para la firma del contrato, la misma que se detalla:

SI ES PERSONA JURÍDICA:

Por el presente documento, declaro bajo juramento, lo siguiente:				
PERSONA JURÍDICA:				
1	Denominación o razón social:			
2	Número de RUC:		Número de Registro equivalente, para no domiciliados:	
3	Dirección de la oficina o local principal donde desarrolla las actividades propias del negocio (Indicar: Jr. - Av. - Calle - Pasaje / N° / Dpto-Int. N° /Urb. - Complejo - Zona – Sector /Distrito/Provincia/Departamento):			
4	Rubros en los que el proveedor brinda sus productos o servicios:			
5	Años de experiencia en el mercado:			
6	Se encuentra incluida en la lista emitida por la Oficina de Control de Activos Extranjeros del Departamento de Tesoro de los Estados Unidos de América (OFAC) SI ☐ - NO ☐			
7	**Representante legal:**			
	Nombres y Apellidos:			
	Tipo y número de documento de identidad **(marque con una "X" según corresponda).**			
	DNI ( )	Pasaporte ( )	Carné de Extranjería ( )	Otro (Indique):
	Domicilio (Indicar: Jr. - Av. - Calle - Pasaje / N° / Dpto-Int. N° /Urb - Complejo - Zona – Sector /Distrito/Provincia/Departamento):			
	Rubros en los que el proveedor brinda sus productos o servicios:			
	Años de experiencia en el mercado:			
	Contar con antecedentes penales ( )		No contar con antecedentes penales ( )	

	Se encuentra incluido en la lista emitida por la Oficina de Control de Activos Extranjeros del Departamento de Tesoro de los Estados Unidos de América (OFAC) SI ☐ - NO ☐
8	**Identificación de los accionistas, socios o asociados, que tengan directa o indirectamente más del 25% del capital social, aporte o participación de la persona jurídica. Respecto de cada uno de ellos, se debe indicar:**
	En caso el accionista, socio o asociado sea persona natural:
	Nombres, Apellidos y porcentaje del capital social: 1. 2.
	Tipo y número de documento de identidad (marque con una "X" según corresponda).
	DNI ( ) 1. 2 | Pasaporte ( ) 1. 2 | Carné de Extranjería ( ) 1. 2 | Otro (Indique): 1. 2
	Contar con antecedentes penales ( ) No contar con antecedentes penales ( ) De marcar SI, detallar Nombre y Apellidos de dicho (s) accionista (s), socio (s) o asociado (s), que cuenta con antecedentes penales:
	Se encuentran incluidos en la lista emitida por la Oficina de Control de Activos Extranjeros del Departamento de Tesoro de los Estados Unidos de América (OFAC) SI NO De marcar SI, detallar Nombre y Apellidos de dicho (s) accionista (s), socio (s) o asociado (s), que se encuentra en la Lista OFAC:
	En caso el accionista, socio o asociado sea persona jurídica:
	Denominación o razón social:
	Número de RUC: | Número de Registro equivalente, para no domiciliados:
	Dirección de la oficina o local principal donde desarrolla las actividades propias del negocio (Indicar: Jr. - Av. - Calle - Pasaje / N° / Dpto-Int. N° /Urb. - Complejo - Zona – Sector /Distrito/Provincia/Departamento):
	Años de experiencia en el mercado y rubros en los que el proveedor brinda sus productos o servicios:
	Se encuentra incluido en la lista emitida por la Oficina de Control de Activos Extranjeros del Departamento de Tesoro de los Estados Unidos de América (OFAC) SI - NO
	N° Teléfono:

Afirmo y ratifico todo lo manifestado en la presente declaración jurada y me comprometo a presentarla cada dos (02) años de ejecución contractual	**NOMBRE:**
	FIRMA:
	FECHA (día/mes/año): / /

*Importante:
- Cuando se trate de consorcios, la presente Declaración Jurada debe ser presentada por cada uno de los integrantes del consorcio.
- La información debe ser completada en su totalidad.