ANEXO N° 2

TERMINO DE REFERENCIA PARA LA CONTRATACIÓN DEL SERVICIO DE GESTION DE VULNERABILIDADES DE INFRAESTRUCTURA DE RED

1. **AREA USUARIA:**
   Gerencia de Tecnologías de Información – Oficina de Seguridad Informática.

2. **OBJETO DE LA CONTRATACIÓN:**
   Contratar los servicios de una compañía especializada y experimentada en la instalación y despliegue de una solución que permita identificar y gestionar efectivamente las vulnerabilidades de los activos tecnológicos.

3. **FINALIDAD DEL REQUERIMIENTO:**
   La Finalidad de este servicio es realizar una identificación temprana de las vulnerabilidades de la infraestructura de red, mediante la detección y alerta sobre posibles riesgos en la seguridad de la red. Asimismo, contribuye al cumplimiento de la Resolución S.B.S. N° 504-2021, que establece el Reglamento para la Gestión de la Seguridad de la Información y la Ciberseguridad, así como del estándar internacional PCI DSS 4.0, relativo a la Seguridad de los Datos del Sector de Pagos con Tarjetas. Además, al detectar y solucionar las vulnerabilidades tempranamente, el Banco de la Nación puede ahorrar costos en términos de daño reputacional, perdida de datos o tiempo de inactividad o indisponibilidad de los servicios.

BANCO DE LA NACIÓN - Jhosep Alan Valenzuela Matutti - Subgerente - Oficina de Seguridad Informática

4. **OBJETIVOS DE LA CONTRATACIÓN:**
   Objetivo General:

   Identificar de manera temprana las vulnerabilidades en la infraestructura de red del Banco de la Nación, mediante la detección proactiva y la generación de alertas sobre posibles riesgos de seguridad, con el fin de fortalecer la ciberseguridad institucional, garantizar la continuidad operativa, y contribuir al cumplimiento de la Resolución S.B.S. N° 504-2021 y del estándar PCI DSS 4.0.

   Objetivo Específicos:

   1. Detectar y alertar proactivamente sobre vulnerabilidades en la infraestructura de red, a fin de mitigar riesgos antes de que se materialicen.
   2. Reducir los costos asociados a incidentes de seguridad, tales como daño reputacional, pérdida de datos, tiempo de inactividad o indisponibilidad de los servicios.
   3. Contribuir al cumplimiento normativo, específicamente con lo establecido en la Resolución S.B.S. N° 504-2021 y el estándar PCI DSS 4.0, asegurando una adecuada gestión de la seguridad de la información.

BANCO DE LA NACIÓN - Carlos Alberto Arana Orrego - Analista - Sección Control de Operaciones de Seguridad - Gerencia de Tecnologías de Información

5. **PLAN OPERATIVO INSTITUCIONAL - POI:**
   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.

6. ALCANCES Y DESCRIPCION DEL SERVICIO

6.1. DESCRIPCION

El Banco de la Nación requiere contar con una solución de Gestión de Vulnerabilidades de Infraestructura de Red, considerando lo siguiente:

Prestación Principal

Descripción	Plazo de entrega
Entrega de los componentes e implementación de la solución.	Treinta (30) días calendarios contabilizados a partir del día siguiente de la recepción de Carta de Aprobación por parte del Contratista.

Descripción	Plazo del servicio
Suscripciones para la solución de Gestión de Vulnerabilidades de Infraestructura de Red incluyendo las actualizaciones de software y soporte técnico (escalamiento) del fabricante.	Un (01) año contabilizado a partir de la fecha de la fecha indicada en el Acta de Conformidad de Implementación.

Prestación Accesoria

Descripción	Plazo
Servicio de mesa de ayuda y soporte técnico local 24 x 7.	Un (01) año contabilizado a partir de la fecha indicada en el Acta de Conformidad de Implementación.
Capacitación.	Dentro del plazo de tres (03) meses contabilizados a partir de la fecha indicada en el Acta de Conformidad de Implementación.

El servicio consiste en:

- Instalación y despliegue de una solución de Gestión de Vulnerabilidades de Infraestructura de Red, considerando los siguientes componentes:

  ✓ Una (01) Consola de Gestión On-premise
  ✓ Un (01) Escáner de Vulnerabilidades

Condiciones generales

- Se requiere una solución que permita identificar y gestionar efectivamente las vulnerabilidades de los activos tecnológicos.
- Se requiere la contratación de suscripciones por el periodo de un (1) año para la Gestión de Vulnerabilidades de quinientos (500) activos de red del Banco de la Nación, entre ellos estaciones de trabajo, servidores, dispositivos de red, plataformas de virtualización y otros sistemas conectados a red.
- La solución deberá ser virtual y deberá estar basada en un sistema de gestión centralizada On-Premisse y múltiples escáneres distribuidos sin límites en cantidad de instancias o el despliegue de agentes instalados en los servidores escaneados.
- El proveedor deberá proporcionar todo licenciamiento, suscripciones y servicios que puedan requerirse para la correcta operación de la solución, sin que el Banco de la Nación incurra en ningún costo adicional.
- El proveedor deberá proporcionar, con el correspondiente respaldo del fabricante, el licenciamiento, suscripciones y los servicios de mantenimiento de software y soporte técnico para la solución, por el periodo de un (01) año contabilizado a partir de la firma del acta de conformidad de implementación de la solución.
- El proveedor deberá contar con autorización del fabricante o su representante, para comercializar la marca y brindar los servicios solicitados, dicha autorización deberá ser presentada en la oferta.
- El proveedor deberá presentar una relación descriptiva de los componentes proporcionados, incluyendo sus códigos comerciales (en tanto sea aplicable), dicha información deberá ser presentada a la recepción de la orden de compra.

BANCO DE LA NACION
Jhosep Alan Valenzuela Matutti
Subgerente
Oficina de Seguridad Informática

Condiciones especificas

- Los appliances virtuales que forman parte de la solución deberán ser compatibles con: VMware vSphere 7.0 o superior. Tanto la consola como los escáneres deberán ser desplegables en modalidad software y appliance virtual en VMware y Hyper-V.
- El Banco de la Nación proporcionará el software hypervisor y los requerimientos de infraestructura de plataforma (procesadores, memoria, almacenamiento) para la operación de la solución, los cuales se detallan a continuación:

BANCO DE LA NACION
Carlos Alberto Arana Ortego
Analista
Sección Control de Operaciones de Seguridad
Gerencia de Tecnologías de Información

✓ <u>Consola de gestión</u>
- vCPUs: 8
- RAM: 16 GB
- Disco: 500 GB

✓ <u>Escáner</u>
- vCPUs: 16
- RAM: 40 GB
- Disco: 500 GB

- La solución deberá estar basado en un catálogo de vulnerabilidades que incluyan más de 170 mil evaluaciones diferentes y al menos 70 mil vulnerabilidades conocidas por un periodo no menor a 15 años.
- Deberá contar con actualizaciones de base de datos de vulnerabilidades, amenazas avanzadas, día cero (0 day) y nuevos tipos de configuraciones de cumplimiento regulatorio.
- La solución deberá proveer un mecanismo de priorización de vulnerabilidades automático basado en la probabilidad de explotación y que ofrezca información alternativa CVSS (Common Vulnerability Scoring System) basada en inteligencia de amenazas reales, recabada de diversas fuentes como Deep Web, Dark Web, redes sociales, sitios de divulgación y otros centros de investigación.
- La solución deberá ser capaz de evaluar, no solo vulnerabilidades, sino auditar configuraciones y compararlas contra las mejores prácticas y frameworks de seguridad tales como CIS, CERT, CISA, STIG, PCI, entre otros para la totalidad de activos licenciados, incluidos equipos de red, infraestructura de virtualización, Windows, Linux, Base de Datos, Aplicaciones y otros sistemas.
- Deberá contar con la posibilidad de definir objetivos para ser cumplidos por las diferentes áreas de la Gerencia de Tecnologías de Información, a fin de asegurar y medir la efectividad de las prácticas de gestión mediante un tablero de cumplimiento. Dichos objetivos pueden estar alineados con normativas como CIS, ISO, PCI o personalizada y utilizar métricas de evaluación.
- La solución deberá crear automáticamente planes de remediación con actividades recomendadas y estimaciones sobre cuál será el impacto en la reducción de riesgo previo a su ejecución. Esta capacidad deberá ser global y permitirá aplicar filtros por grupo de activos especifico.
- Todos los elementos que conforman la solución deberán ser actualizables automáticamente con intervención opcional de un especialista, incluyendo nuevas versiones de software/firmware, updates de contenido (nuevas vulnerabilidades) y feeds de inteligencia.
- La solución deberá contar con un API completa para integración mediante scripting automatizado y exportación de datos mediante llamados. Esta API deberá estar liberada y documentada y no deberá tener limitaciones de licencias en cantidad de llamados o sistemas que la consultan.
- Deberá tener la posibilidad de realizar escaneos con credenciales y sin credenciales.
- La solución deberá ser capaz de generar un inventario de activos, poblándolo mediante escaneos de descubrimiento sin límites de licenciamiento. Deberá también permitir agregar activos importándolos desde fuentes externas. Deberá auto-clasificar los activos por diversos criterios tales como localización, red en la que se encuentra, tipo de dispositivo, propietario o responsable del dispositivo, criticidad para la organización, si el activo ha sido escaneado o no, si se cuentan con credenciales funcionales o no, si está comprometido por malware y otros criterios de agrupamiento.
- La solución deberá agrupar activos que posean una base de datos, que posean aplicaciones web, que no resuelvan nombre, que contengan vulnerabilidades explotables y otras agrupaciones dinámicas mediante reglas.

BANCO DE LA NACION
Jhosep Alan Valenzuela Matutti
Subgerente
Oficina de Seguridad Informática

BANCO DE LA NACION
Carlos Alberto Arana Orrego
Analista
Sección Control de Operaciones de Seguridad
Gerencia de Tecnologías de Información

- Deberá contar con escaneos que solo auditen la existencia o inexistencia de parches de todo tipo de sistemas (Windows Desktop, Unix/Linux, equipos de red, aplicaciones y otras plataformas).
- Deberá mantener registro de estado de vulnerabilidades por activo, de modo de identificar vulnerabilidades que, habiendo sido remediadas, volvieron a surgir en nuevos escaneos. Deberán registrarse las fechas de primera aparición, última aparición y reaparición.
- La solución deberá ser capaz de identificar sistemas comprometidos por malware y otros códigos maliciosos. También deberá ser capaz de identificar la ejecución y nivel de firmas del sistema de Antimalware presente en el dispositivo.
- Deberá reportar vulnerabilidades que sean explotables.
- La solución deberá tener la posibilidad de realizar escaneos selectivos.
- La solución deberá tener la posibilidad de realizar escaneos programados, a demanda, por horas y recurrentes.
- La solución deberá tener la posibilidad de realizar priorización de acciones de remediación y recomendaciones para su corrección.
- La solución deberá tener la posibilidad de categorizar la vulnerabilidad encontrada por nivel de criticidad.
- La solución deberá tener la posibilidad de realizar escaneos basado en agentes.

Gestión y monitoreo

- La administración de la solución deberá realizarse en forma centralizada, no importando el número de dispositivos en la red y escáneres desplegados.
- Deberá permitir la autenticación segura (ya sea mediante HTTPS o SSH).
- Toda la comunicación entre la consola y el appliance virtual de escaneo deberá estar cifrada con algoritmos criptográficos robustos.
- La administración y configuración de la solución deberá ser por medio de interfaz gráfica.
- La solución deberá tener una gestión de usuarios con las siguientes características:

  ✓ Deberá estar basada en roles (RBAC) y permisos que limiten el acceso a conjuntos de datos puntuales, grupos de activos y a acciones concretas tales como reportes, análisis, escaneo, aceptar riesgos o reclasificarlos, etc.

  ✓ Las credenciales de acceso a la consola deberán ser locales o integradas a un SLDAP (por ejemplo, Active Directory).

  ✓ Deberá permitir autenticación SAML para integración con soluciones de Single Sign-On.

- Los administradores deberán contar con perfiles de acceso con privilegios de lectura/escritura o con privilegio de solo lectura para cada una de las funciones de administración.

BANCO DE LA NACION
Jhosep Alan Valenzuela Matutti
Subgerente
Oficina de Seguridad Informática

BANCO DE LA NACION
Carlos Alberto Arana Orrego
Analista
Sección Control de Operaciones de Seguridad
Gerencia de Tecnologías de Información

Registro y reportes

- La solución deberá proveer esquemas de reportes predefinidos que permitan personalización.
- La solución deberá contar con capacidades de reporting y dashboards completamente personalizables mediante gráficos, texto, filtros, querys y lógicas complejas. Además, deberá contar con más de 300 templates listos para ser usados y editables.
- Deberá incluir plantillas de cumplimiento CIS, PCI, ISO 27001 entre otras.
- Los reportes generados deberán ser de tipo ejecutivo (gráficos), detallado (matriz / tabla) o una combinación de ambos.
- Deberá contar con funcionalidades integradas a un Centro de Operaciones de Seguridad (SOC) mediante alertas automatizadas independientes y nativas en el producto, así como integrarse a una solución de SIEM y de orquestación (SOAR). Se espera que la solución alerte cuando se detecten nuevas vulnerabilidades críticas en sistemas relevantes, nuevas vulnerabilidades asociadas a una amenaza conocida y otras reglas personalizables.

Actualizaciones de software

- Deberá proporcionar el acceso, autorizado por el fabricante, a las actualizaciones del software provisto, lo cual debe incluir el suministro de nuevas versiones (releases) y reparaciones (denominadas comercialmente como patches, temporary fixes y updates).
- El proveedor deberá notificar al Banco de la Nación, mediante correo electrónico, respecto a las actualizaciones que libere el fabricante y cuya aplicación sea recomendada o requerida.

Vigencia Tecnológica

- En caso de presentarse, en cualquier momento anterior a la entrega definitiva de la solución, versiones nuevas de cualquiera de los componentes de la misma, se deberán entregar tales elementos actualizados, sin costo adicional, contando con autorización previa del Banco de la Nación.
- Si durante el periodo de servicio el fabricante realiza un cambio de denominación del licenciamiento, suscripciones y servicios que fueron implementados, deberán proporcionarse los componentes equivalentes necesarios para mantener el cumplimiento de las prestaciones contratadas y sin costo adicional para el Banco de la Nación.

BANCO DE LA NACION
Jhosep Alan Valenzuela Matutti
Subgerente
Oficina de Seguridad Informática

Mesa de Ayuda y Soporte Técnico

- Brindar el servicio de soporte técnico a los especialistas del Banco de la Nación, por el periodo de vigencia del servicio, a través de la línea telefónica, correo electrónico, sistemas en línea o en sitio cuando se requiera.
- Contar con una mesa de ayuda disponible las 24 horas del día, los 7 días de la semana (24x7) y un procedimiento para el reporte de incidentes que incluya los niveles de escalamiento correspondientes y que contemple, entre otras cosas, la asignación, en un plazo no mayor a dos (2) horas, de numero de atención (ticket) que facilite el seguimiento de los incidentes reportados.
- El máximo tiempo de respuesta para visitas de soporte técnico será de ocho (8) horas, a partir del momento en que se determine tal necesidad.

BANCO DE LA NACION
Carlos Alberto Arana Orrego
Analista
Sección Control de Operaciones de Seguridad
Gerencia de Tecnologías de Información

- Garantizar en toda circunstancia la posibilidad de escalamiento del servicio con el fabricante (incluyendo el reporte directo, por parte del Banco de la Nación), para una oportuna solución de los eventos que puedan presentarse.

6.2. ACTIVIDADES

Dentro de las tareas a ejecutar en la implementación, el proveedor deberá cumplir como mínimo con:

- Despliegue de la consola de gestión central
- Despliegue del appliance virtual de escaneo y su integración con la consola de gestión central
- Demostración de la configuración de escaneos a demanda, programados, recurrentes de auditoría y cumplimiento.
- Configuración de reportes y dashboards

6.3. SLA DE SOPORTE

En la tabla anexa se muestran los tiempos de respuesta contemplados de acuerdo con el nivel de asistencia técnica seleccionada:

Severidad	Tiempo de Respuesta	Tiempo de Restauración
Incidente	2 horas	24 horas
Consultas Técnicas	1 día hábil	-

BANCO DE LA NACION
Jhosep Alan Valenzuela Matutti
Subgerente
Oficina de Seguridad Informática

BANCO DE LA NACION
Carlos Alberto Arana Orrego
Analista
Sección Control de Operaciones de Seguridad
Gerencia de Tecnologías de Información

6.4. CONDICIONES Y CLASIFICACIÓN DEL SERVICIO CONTRATADO

La persona natural o jurídica que brindará el servicio queda estrictamente prohibida de usar nombres o signos distintivos del Banco de la Nación para cualquier comunicación interna o externa, entendiéndose como signos distintivos palabras, lemas o frases que identifiquen al Banco, así como, imágenes, símbolo, gráficos, logotipos y sonidos.
En base al objeto de contratación y actividades a desarrollar, el contratista No se constituye como SUJETO OBLIGADO para presentar declaración jurada de intereses
De igual forma, según lo dispuesto en la Ley N° 31559 - Ley que crea el Registro para el Control de Contratos de Consultoría en el Estado y la Directiva N° 013-2024-CG/PREVI - Registro para el Control de Contratos de Consultoría en el Estado, se califica que la contratación no obedece a un servicio de consultoría.
Para que el área usuaria califique el servicio solicitado en relación a los supuestos señalados anteriormente, es necesario que verifique previamente el cumplimiento concurrente de estas condiciones:

- Que el objeto, actividades, y/u obligaciones a realizar en el servicio contratado revista cierta especialización o complejidad.
- Que tales características del servicio hayan conllevado a que se establezca un perfil profesional altamente calificado.

Si el servicio se encuentra calificado se procederá a registrar la contratación en el Sistema de Registro para el Control de Contratos de Consultoría del Estado – SIRICC de la Contraloría General de la República.
Teniendo conocimiento de lo anteriormente mencionado, la contratación NO CALIFICA como un servicio de consultoría.

7. REQUISITOS DEL PROVEEDOR

Los requisitos del proveedor para servicios son:

- Persona natural o jurídica, con RUC en estado activo y habido.
- Contar con RNP vigente – Registro de servicios o Consultor de obras, para contrataciones superiores a 01 UIT.
- No tener impedimento para contratar con el estado, conforme a lo dispuesto el artículo N° 30 de la Ley General de Contrataciones Públicas y el artículo N° 39 de su Reglamento.

EXPERIENCIA

El postor deberá demostrar su experiencia con una facturación acumulada de las prestaciones efectuadas con empresas privadas y/o entidades públicas en los últimos 15 años por un monto mínimo de S/25,000.00 (veinticinco mil soles con 00/100) en servicios iguales o similares; lo cual deberá acreditar con copia simple de (i) contratos u órdenes de servicios y su respectiva conformidad o constancia o certificados 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.

BANCO DE LA NACION
Jhosep Alan Valenzuela Matutti
Subgerente
Oficina de Seguridad Informática

Servicios similares: Venta y/o servicios de implementación de soluciones de Ciberseguridad, Gestor de Vulnerabilidades, escáner de vulnerabilidades.

El equipo deberá estar conformado como mínimo por:

BANCO DE LA NACION
Carlos Alberto Arana Orrego
Analista
Sección Control de Operaciones de Seguridad
Gerencia de Tecnologías de Información

Especialista (01)

- **Formación académica:** en Ingeniería de Sistemas, Ingeniería de Computación y de Sistemas, Ingeniería Electrónica o carreras afines (*). El postor deberá acreditarlo con la presentación de copia simple de constancia del título técnico, bachiller o título profesional.

(*) Afines, entre otros son: Computación, Electrónica, Licenciatura en Computación, Ingeniería de Computación y de Sistemas, Ingeniería de Computación e Informática, Ingeniería de Sistemas e Informática, Ingeniería de Sistemas Empresariales, Ingeniería de Software, Ingeniería de Sistemas de Información, Ingeniería Informática y de Sistemas, Ingeniería de Sistemas, Ingeniería Informática, Ingeniería de Telecomunicaciones, Ingeniería Industrial y de Sistemas, Ingeniería de Telecomunicaciones y Redes, Ingeniería de Redes y Comunicaciones, Ingeniería de Seguridad Informática, Ingeniería Mecatrónica y Sistemas Computacionales, Ingeniería electrónica, Ingeniería de Tecnologías de Información y Sistemas.

- **Conocimiento:** Acreditarlo con la presentación de **certificaciones técnicas** emitidas por el fabricante, las mismas que podrán estar vigentes o que no supere el año de caducidad.
  No se aceptarán certificaciones del tipo Entry, Junior, Sales, Marketing, Foundations o aquella que no cuenta con un examen de certificación oficial.

- **Experiencia:** mínima de un (01) año, en la instalación, implementación, mantenimiento preventivo y soporte técnico, en la línea de soluciones de gestión de vulnerabilidades del fabricante de la solución propuesta.
  Deberá acreditarlo con cualquiera de los siguientes documentos: copia simple de contratos o constancias o certificados o declaración jurada o cualquiera otra documentación que, de manera fehaciente demuestren la experiencia del personal propuesto (en las labores realizadas y su tiempo de ejecución).

- El mencionado personal técnico será encargado de brindar los servicios de implementación, soporte y mantenimiento. En caso de que durante la vigencia del servicio se realice el reemplazo del especialista, sólo se podrá considerar personal que cumpla con las calificaciones profesionales y experiencia, similares o superiores a los requerimientos solicitados para el personal clave, y previa conformidad del Banco de la Nación.

BANCO DE LA NACIÓN - Jhosep Alan Valenzuela Matutti - Subgerente - Oficina de Seguridad Informática

8. ENTREGABLES:

La prestación del servicio consta de los siguientes entregables:

BANCO DE LA NACIÓN - Carlos Alberto Arana Orrego - Analista - Sección Control de Operaciones de Seguridad - Gerencia de Tecnologías de Información

Prestación Principal:

- Plan de implementación
- Documentación de la arquitectura de la solución
- Documentación técnica de la solución
- Informe final de la implementación de la solución
- Documentación técnica de la solución
- Manuales de administración y operación de la solución

Prestación Accesoria:

- **Soporte:** El soporte técnico para la plataforma estará disponible 24 x 7, durante los 365 días del año contabilizados a partir de la fecha indicada en el Acta de Conformidad de Implementación, y se brindará bajo demanda. Brindar un reporte mensual del estado de los tickets de soporte generados en el último mes.

- **Capacitación:** Proporcionar un curso de capacitación práctico, sobre la solución ofertada, para el personal técnico del Banco de la Nación, con una duración de como mínimo seis (06) horas. La capacitación deberá ser programada considerando un total de quince (15) participantes y deberá ser realizada dentro de los primeros tres (03) meses del servicio, en forma online o presencial en la ciudad de Lima (sin costos adicionales para el Banco de la Nación). La capacitación será dictada por al menos un especialista según en acápite 8. REQUISITOS DEL PROVEEDOR. Se deben incluir las constancias de participación correspondientes.

Presentado cada uno de los entregables en los plazos establecidos, el Banco de la Nación tiene cinco (5) días calendario para emitir las conformidades u observaciones, en caso el Banco presente observaciones el Contratista tiene un plazo máximo de cinco (5) días calendario para su subsanación.

La persona jurídica que brindará el servicio queda estrictamente prohibida de usar nombres o signos distintivos del Banco de la Nación para cualquier comunicación interna o externa, entendiéndose como signos distintivos palabras, lemas o frases que identifiquen al Banco, así como, imágenes, símbolo, gráficos, logotipos y sonidos.

BANCO DE LA NACIÓN
Jhosep Alan Valenzuela Matutti
Subgerente
Oficina de Seguridad Informática

9. ÉTICA, ANTICORRUPCIÓN Y ANTISOBORNO

BANCO DE LA NACIÓN
Carlos Alberto Arana Orrego
Analista
Sección Control de Operaciones de Seguridad
Gerencia de Tecnologías de Información

A la recepción del documento contractual, EL CONTRATISTA declara y garantiza no haber ofrecido, negociado, prometido o efectuado ningún pago o entrega de cualquier beneficio o incentivo ilegal, de manera directa o indirecta, a los evaluadores del contrato menor o cualquier servidor de la entidad contratante. Asimismo, EL CONTRATISTA se obliga a mantener una conducta proba e íntegra durante la vigencia del contrato, y después de culminado el mismo en caso existan controversias pendientes de resolver, lo que supone actuar con probidad, sin cometer actos ilícitos, directa o indirectamente. Aunado a ello, EL CONTRATISTA se obliga a abstenerse de ofrecer, negociar, prometer o dar regalos, cortesías, invitaciones, donativos o cualquier beneficio o incentivo ilegal, directa o indirectamente, a funcionarios públicos, servidores públicos, locadores de servicios o proveedores de servicios del área usuaria, de la dependencia encargada de la contratación, actores del proceso de contratación y/o cualquier servidor de la entidad contratante, con la finalidad de obtener alguna ventaja indebida o beneficio ilícito. En esa línea, se obliga a adoptar las medidas técnicas, organizativas y/o de personal necesarias para asegurar que no se practiquen los actos previamente señalados.

Adicionalmente, EL CONTRATISTA se compromete a denunciar oportunamente ante las autoridades competentes los actos de corrupción o de inconducta funcional de los cuales tuviera conocimiento durante la ejecución del contrato con LA ENTIDAD CONTRATANTE. Tratándose de una persona jurídica, lo anterior se extiende a sus accionistas, participacionistas, integrantes de los órganos de administración, apoderados, representantes legales, funcionarios, asesores o cualquier persona vinculada a la persona jurídica que representa; comprometiéndose a informarles sobre los alcances de las obligaciones asumidas en virtud del presente contrato.

Asimismo, declara no tener, ni conocer actualmente ningún conflicto de interés para la ejecución de prestaciones contratadas. Por otro lado, se compromete a informar, de manera inmediata, al área usuaria y a la Gerencia de Oficialía de Cumplimiento Normativo y Conducta de Mercado (integridadbn@bn.com.pe) en caso tome conocimiento de una situación de conflicto de interés, debiendo inhibirse inmediatamente de intervenir en las actividades que directa o indirectamente se relacionen con el conflicto de interés advertido.

En consecuencia, el CONTRATISTA se compromete –en lo que le resulte aplicable- a cumplir en todo momento con lo establecido en el Código de Ética del Banco y normas de integridad publicadas en https://www.bn.com.pe/integridad/integridad.asp

Finalmente, el incumplimiento de las obligaciones establecidas en esta cláusula, durante la ejecución contractual, otorga a LA ENTIDAD CONTRATANTE el derecho de resolver total o parcialmente el contrato. En ningún caso, dichas medidas impiden el inicio de las acciones civiles, penales y administrativas a que hubiera lugar.

BANCO DE LA NACION
Jhosep Alan Valenzuela Matutti
Subgerente
Oficina de Seguridad Informática

10. RESPONSABILIDAD POR VICIOS OCULTOS

La conformidad del servicio por parte del Banco de la Nación no enerva su derecho a reclamar posteriormente por defectos o vicios ocultos.
El plazo máximo de responsabilidad del contratista es de un (01) año, contado a partir de la conformidad otorgada.

11. PLAZO DE EJECUCIÓN DEL SERVICIO.

BANCO DE LA NACION
Carlos Alberto Arana Orrego
Analista
Sección Control de Operaciones de Seguridad
Gerencia de Tecnologías de Información

El plazo de ejecución de la prestación principal (que incluye: entrega de los componentes e implementación de la solución y las suscripciones para la solución de vulnerabilidades de infraestructura de red incluyendo las actualizaciones de software y soporte técnico) será de treinta (30) días calendarios como máximo, contados a partir del día siguiente de notificada la carta de aprobación, mediante correo electrónico.

El plazo de ejecución de la prestación accesoria será:

- **Capacitación:** Dentro de los primeros tres (03) meses de servicio, contados a partir del siguiente día de la emisión del Acta de Conformidad de la Prestación Principal.

- **Servicio de Soporte Técnico:** Un (01) año, contados a partir del siguiente día de la emisión del Acta de Conformidad de la Prestación Principal.

12. LUGAR DE PRESTACIÓN DEL SERVICIO.

La prestación del servicio se realizará de manera presencial.
Para aquellas situaciones en las cuales EL PROVEEDOR requiera hacer trabajo en modo presencial en el Banco de la Nación - Sede Principal (Av. Javier Prado Este 2499, San Borja), deberá contar con el Seguro Complementario de Trabajo de Riesgo (SCTR) para el desarrollo de sus actividades en el Banco.

13. FORMA DE PAGO:

El pago se realiza de conformidad con lo establecido en el artículo 67 de la Ley General de Contrataciones Públicas:

PRESTACIÓN PRINCIPAL

- **El 85%**, previa conformidad emitida por la Oficina de Seguridad Informática, de acuerdo a lo señalado en el acápite 7. ENTREGABLES, en moneda nacional y a la presentación del comprobante de pago por parte del CONTRATISTA.

PRESTACIÓN ACCESORIA

- **El 5%**, previa conformidad emitida por la Oficina de Seguridad Informática, de la realización de la Capacitación, de acuerdo a lo señalado en el acápite 7. ENTREGABLES.
- **El 10%** al finalizar el año del servicio, previa conformidad emitida por la Oficina de Seguridad Informática, de la realización del Servicio Soporte Técnico.

BANCO DE LA NACION - Jhosep Alan Valenzuela Matutti - Subgerente - Oficina de Seguridad Informática

BANCO DE LA NACION - Carlos Alberto Arana Orrego - Analista I - Sección Control de Operaciones de Seguridad - Gerencia de Tecnologías de Información

Para iniciar el trámite de pago de las contraprestaciones ejecutadas por el contratista, el Banco de la Nación debe contar con la siguiente documentación:

- Carta simple dirigida a la Subgerencia de Compras.
- Comprobante de pago.
- Copia simple de Carta de aprobación.
- Acta de conformidad original debe ser visada por el Jefe de la Sección Control de Operaciones de Seguridad y Subgerencia de la Oficina de Seguridad Informática.
- Informe Técnico visado por el analista, el Jefe de la Sección Control de Operaciones de Seguridad y la Subgerencia de la oficina de Seguridad Informatica.

Dicha documentación se debe presentar en mesa de partes Módulo de Logística de la Gerencia de Administración y Logística – Av. Javier Prado Este N° 2499 – San Borja, Lima, en el horario de 09:00am a 16:00horas.

14. RESPONSABLE DE DAR CONFORMIDAD A LA PRESTACIÓN:

Según lo señalado en el Artículo 144 del Reglamento de la Ley N° 32069 – Ley General de Contrataciones Públicas:

La conformidad será otorgada por la Oficina de Seguridad Informática, en un plazo máximo de (7) días calendario contado desde el día siguiente de recibido el entregable o máximo veinte (20) días en caso se requiera efectuar pruebas que permitan verificar el cumplimiento de la obligación.

15. CONFIDENCIALIDAD:

EL PROVEEDOR se obliga a guardar estricta reserva sobre toda la información relacionada con EL BANCO y que sea de su conocimiento en el curso del cumplimiento de sus prestaciones, la cual no podrá ser utilizada sin previa autorización de este último, configurándose en causal de resolución de pleno derecho el incumplimiento de la indicada obligación, sin perjuicio de la indemnización de daños y perjuicios a que hubiere lugar. En este contexto, 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, acuerdos y actas de directorio, técnicas de marketing, procesos, servicios, políticas de precios, estrategias, buenas prácticas, metodología de trabajo, especificaciones técnicas, hardware, software, diseños, planos, dibujos, prototipos, 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 PROVEEDOR por el presente instrumento. La obligación de mantener la confidencialidad de la información subsistirá incluso luego de finalizado la contratación.

BANCO DE LA NACIÓN - Jhosep Alan Valenzuela Matutti - Subgerente - Oficina de Seguridad Informática

16. PENALIDAD:

Penalidad por Mora en la ejecución de la prestación:

BANCO DE LA NACIÓN - Carlos Alberto Arana Orrego - Analista - Sección Control de Operaciones de Seguridad - Gerencia de Tecnologías de Información

Las penalidades serán aplicadas según lo señalado en el artículo 119 y 120 del Reglamento de la Ley General de Contrataciones Públicas, en caso de retraso injustificado del contratista en la ejecución de las prestaciones objeto del contrato menor, se aplica al proveedor una penalidad por cada día de atraso que le sea imputable.
La suma de la aplicación de las penalidades por mora y de otras penalidades no puede exceder el 10% del monto del contrato o, de ser el caso del entregable correspondiente

En todos los casos, la penalidad se aplica automáticamente y se calcula de acuerdo con la siguiente formula:

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

Donde F tiene los siguientes valores:

Para Bienes y Servicios F= 0.40

Una vez que se llega al monto máximo de la penalidad por mora, la entidad contratante puede optar por resolver el contrato menor.

17. OTRAS PENALIDADES.

Asimismo; no se contempla otras penalidades.

18. RESOLUCIÓN DE LA CONTRATACIÓN.

Cualquiera de las partes puede resolver el contrato, de conformidad con el artículo 68 de la Ley N° 32069, Ley General de Contrataciones Públicas, y artículo 229 de su Reglamento aprobado mediante Decreto Supremo N° 009-2025-EF.

Se puede resolver la contratación, en los siguientes casos:

a) Por incumplimiento de alguna de LAS PARTES de las obligaciones asumidas en los términos de referencia, para lo cual la parte perjudicada con el incumplimiento deberá notificar a la otra parte comunicando la causal invocada.
b) Por incumplimiento del requerimiento de presentar la Declaración Jurada de Intereses conforme el numeral 11.5 del artículo 11 del Reglamento del Decreto de Urgencia 020-2019 o la presentación de la Declaración Jurada de Interés con información inexacta o falsa, solo en el caso que el servicio sea prestado por persona natural con obligación de presentar declaración jurada de intereses de acuerdo con lo señalado por el área usuaria.
c) El BANCO puede resolver la contratación cuando la penalidad aplicada excede el 10% del monto contractual.
d) De corresponder a servicios profesionales de asesoría, servicios de consultoría y servicios legales: la presentación con información inexacta o falsa de la Declaración Jurada de Prohibiciones e Incompatibilidades a que se hace referencia en la Ley de prevención y mitigación del conflicto de intereses en el acceso y salida de personal del servicio público. Asimismo, en caso se incumpla con los impedimentos señalados en el artículo 5 de dicha ley se aplicará la inhabilitación por cinco años para contratar o prestar servicios al Estado, bajo cualquier modalidad.
e) Paralización o reducción injustificada de la ejecución de la prestación, pese a haber sido requerido para corregir tal situación.
f) Por mutuo acuerdo entre el proveedor y el Banco de la Nación, previa solicitud el área usuaria.
g) Por caso fortuito o fuerza mayor, que imposibilite al Banco de la Nación de manera definitiva continuar con la contratación.
h) Por incumplimiento de la cláusula anticorrupción.

BANCO DE LA NACIÓN
Jhosep Alan Valenzuela Matutti
Subgerente
Oficina de Seguridad Informática

BANCO DE LA NACIÓN
Carlos Alberto Arana Orrego
Analista
Sección Control de Operaciones de Seguridad
Gerencia de Tecnologías de Información

19. SOLUCIÓN DE CONTROVERSIAS

Todas las controversias que surjan entre las partes sobre la validez, nulidad, interpretación, ejecución, terminación o eficacia de los contratos menores se resuelven mediante conciliación.

20. CLÁUSULA GESTION DE RIESGOS

Las partes realizan la gestión de riesgos de acuerdo con lo establecido en el presente documento, a fin de tomar decisiones informadas, aprovechando el impacto de riesgos positivos y disminuyendo la probabilidad de los riesgos negativos y su impacto durante la ejecución contractual, considerando la finalidad pública de la contratación

21. OTROS CARACTERISTICAS QUE SEAN RELEVANTES PARA LA CONTRATACIÓN

Esta contratación corresponde a la necesidad del área y se ratifica no estar dividiendo la contratación (FRACCIONANDO), para evadir la aplicación de un procedimiento de selección mayor a las 08 UIT. Asimismo, se ha verificado que el presente requerimiento NO SE ENCUENTRA PROGRAMADO en el PAC; en caso de tratarse de una necesidad imprevista se procederá con lo dispuesto en el artículo 50° de la Ley N° 32069 y artículo 45° de su reglamento.

Se ha verificado que el objeto de contratación no se encuentra en el Listado de Bienes y Servicios Comunes (https://www.gob.pe/8194-consultar-el-listado-de-bienes-y-servicios-comunes-lbsc), así como en la relación de las fichas de homologación (https://central.perucompras.gob.pe/homologacion/relacion-fichas-homologacion-aprobadas.php).

En todo lo no previsto expresamente en el presente termino de referencia, resulta aplicable la Ley General de Contrataciones Públicas - Ley N° 32069 y su Reglamento aprobado por Decreto Supremo N° 009-2025-EF

BANCO DE LA NACION
Jhosep Alan Valenzuela Matutti
Subgerente
Oficina de Seguridad Informática

BANCO DE LA NACION
Carlos Alberto Arana Orrego
Analista
Sección Control de Operaciones de Seguridad
Gerencia de Tecnologías de Información

Carlos Alberto Arana Orrego
Analista Control de Operaciones de Seguridad - Gestión de Vulnerabilidades
Oficina de Seguridad Informática
Gerencia de Tecnologías de la Información