SERVICIO DE MONITOREO ANTIPHISHING - PREVENTIVO

I. TÉRMINOS DE REFERENCIA

1. AREA USUARIA:

Gerencia de Tecnologías de Información - Oficina de Seguridad Informática - Sección Ciberseguridad.

2. OBJETO DE LA CONTRATACIÓN:

Contratar un servicio especializado de monitoreo preventivo de amenazas digitales y protección de marca, orientado a la detección temprana de actividades maliciosas que puedan afectar la seguridad de la información, la reputación institucional y a los usuarios del Banco de la Nación, incluyendo la identificación de campañas de phishing, pharming, abuso de marca, filtraciones de información y otras amenazas cibernéticas asociadas a los canales digitales del Banco.

3. FINALIDAD DEL REQUERIMIENTO:

La transformación digital ha impulsado el crecimiento de los servicios en línea, pero también ha generado un incremento en la frecuencia y sofisticación de los fraudes cibernéticos. Modalidades como el phishing, el pharming, el abuso de marca en redes sociales, entre otros, se han convertido en amenazas persistentes, organizadas y en constante evolución, que afectan de manera directa a las entidades del sector financiero.

Estos ciberataques no solo comprometen la seguridad de la información, sino que también ponen en riesgo la reputación institucional, un activo crítico para organizaciones financieras como el Banco de la Nación. En este contexto, se hace necesario implementar mecanismos preventivos que permitan anticipar y mitigar dichos riesgos.

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

Por tal motivo, el Banco de la Nación requiere la contratación de una empresa especializada en ciberseguridad que brinde un servicio de monitoreo preventivo para la detección de amenazas digitales, incluyendo la vigilancia en la dark web, el monitoreo de reputación de marca, la identificación de filtraciones de datos, y la detección de sitios de phishing y otros contenidos maliciosos relacionados.

BANCO DE LA NACION
Jymmy Hands Quesquén Rivas
Analista
Sección Ciberseguridad
Gerencia de Tecnologías de Información

Este servicio contribuirá a la protección de los usuarios frente a fraudes electrónicos en los canales digitales del Banco, facilitará la adopción de medidas tempranas ante publicaciones falsas y/o difamatorias, y permitirá reducir la exposición al riesgo operativo, mejorando los niveles de confianza y seguridad en las transacciones en línea para beneficio de los clientes y del propio Banco.

4. OBJETIVOS DE LA CONTRATACIÓN:

BANCO DE LA NACION
Ana Maria Li Manrique
Jefe
Secc. Ciberseguridad
Of. de Seguridad Informática
Gerencia de Tecnologías de Información

Objetivo General:

Contratar los servicios de una empresa especializada en ciberseguridad que brinde una solución integral de monitoreo preventivo orientada a la detección temprana, mitigación y respuesta frente a amenazas digitales como phishing, pharming, carding, malware, malware móvil y otras formas de fraude electrónico. La solución deberá incluir el monitoreo de la marca del Banco de la Nación en canales digitales, redes sociales, web superficial y dark web, así como la identificación de filtraciones de datos y contenidos difamatorios que afecten la reputación del Banco de la Nación. Todo ello en cumplimiento de buenas prácticas internacionales y marcos de referencia como PCI DSS 4.0, NIST CSF 2.0 y MITRE ATT&CK, a fin de proteger las operaciones financieras por internet, reducir la exposición al riesgo y fortalecer la confianza de los clientes en los servicios digitales del Banco.

Objetivo Específicos:

1. Monitorear de forma continua sitios web, dominios, redes sociales, aplicaciones móviles, tiendas de aplicaciones y la dark web para identificar amenazas digitales relacionadas con campañas de phishing, pharming, carding, malware y otros fraudes electrónicos.

   Alineado con:

   NIST CSF 2.0 - DE.AE-1 (Anomalous activity is detected)
   MITRE ATT&CK - T1566 (Phishing)

2. Detectar anticipadamente sitios o contenidos maliciosos que suplanten la identidad del Banco de la Nación, utilizando su imagen o marca sin autorización, con el objetivo de prevenir impactos negativos en los clientes y en la reputación institucional.

   Alineado con:

   NIST CSF 2.0 - ID.RA-1 (Risk identification)
   PCI DSS 4.0 - Req. 10.6.1 (Monitoreo de seguridad continuo)

3. Implementar mecanismos de respuesta y mitigación, incluyendo el proceso de takedown de sitios fraudulentos, en coordinación con autoridades y proveedores de infraestructura digital, para reducir el tiempo de exposición de las amenazas detectadas.

   Alineado con:
   NINIST CSF 2.0 - RS.MI-1 (Response and mitigation processes are executed)
   MITRE ATT&CK - Takedown and remediation tactics

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

4. Identificar filtraciones de información sensible o confidencial, detectando su exposición o comercialización en fuentes no autorizadas, como foros clandestinos, redes sociales o la dark web, para activar medidas de contención.

   Alineado con:

   PCI DSS 4.0 - Req. 12.10.5 (Identificación y respuesta ante filtración de datos)
   NIST CSF 2.0 - DE.CM-7 (Detection of unauthorized access to sensitive information)
   MITRE ATT&CK - T1586 (Data leak sites)

BANCO DE LA NACION
Jymmy Hands Quesquén Rivas
Analista
Sección Ciberseguridad
Gerencia de Tecnologías de Información

5. Monitorear publicaciones falsas, engañosas o difamatorias que puedan afectar la imagen del Banco, permitiendo activar estrategias de respuesta comunicacional y jurídica.

   Alineado con:

   NIST CSF 2.0 - ID.RA-4 (Identification of reputational threats)

BANCO DE LA NACION
Ana María Livanrique Ledo
Sección Ciberseguridad
Of. de Seguridad Informática
Gerencia de Tecnologías de Información

6. Generar reportes periódicos de inteligencia digital, incluyendo indicadores de compromiso (IoCs), análisis de tendencias, mapas de calor de actividad maliciosa y recomendaciones de mejora continua en la postura de ciberseguridad del Banco.

   Alineado con:

   PCI DSS 4.0 - Req. 10.7 (Reporting on security events)
   NIST CSF 2.0 - IM-2 (Security information is used for continuous improvement)

7. Asegurar la trazabilidad, confidencialidad e integridad de la información recolectada y procesada, conforme a buenas prácticas y normas de ciberseguridad reconocidas internacionalmente.

   Alineado con:

   PSI DSS 4.0 - Req. 3 y 10 (Protección y monitoreo de la información)
   NIST CSF 2.0 - PR.DS-1 al PR.DS-5 (Protección de datos en tránsito y en reposo)..

5. PLAN OPERATIVO INSTITUCIONAL - POI/PEI

La presente contratación se encuentra vinculado al Plan Estratégico Institucional 2022 - 2026 del Banco de la Nación, con los Objetivos Estratégicos:

- OE N° 4: Mejorar la Experiencia del Cliente.
- OE N° 6: Incrementar las operaciones y clientes digitales.

6. ANTECEDENTES.

Desde el año 2010, el Banco de la Nación viene contratando los servicios de una empresa especializada en monitoreo preventivo antiphishing, con el objetivo de identificar, rastrear, mitigar y responder de manera oportuna a intentos de fraude electrónico, tales como phishing, pharming, malware, carding, malware móvil y crimeware.

Actualmente, el Banco cuenta con un contrato vigente para este servicio, suscrito el 23 de diciembre de 2022, bajo el Contrato N° 029079-2022-BN, correspondiente al Concurso Público N° 0032-2022-BN, denominado "Servicio de Monitoreo Antiphishing - Preventivo". En el marco de la evolución constante de las amenazas cibernéticas, se requiere la continuidad de este servicio con mejoras sustanciales que incorporen las últimas capacidades tecnológicas y buenas prácticas en ciberseguridad.....

7. ALCANCES Y DESCRIPCION DEL SERVICIO

7.1. DESCRIPCION

El servicio deberá proporcionar una solución integral para la **detección temprana, mitigación y respuesta ante amenazas digitales** que comprometan los canales digitales del Banco, con énfasis en la protección de la Banca por Internet y la imagen institucional. La solución deberá operar de forma continua (24x7) los 365 días del año, permitiendo el **monitoreo activo del entorno digital** para identificar campañas de phishing, pharming, malware, carding, malware móvil, y otras modalidades de fraude electrónico. Asimismo, deberá incluir el seguimiento de publicaciones en línea con contenido falso o difamatorio que pueda afectar la reputación del Banco. La plataforma o herramienta empleada deberá contar con capacidades de **alerta temprana, trazabilidad de amenazas, generación de reportes ejecutivos y técnicos**, así como mecanismos automatizados o manuales para la **gestión de incidentes y solicitud de baja de contenidos maliciosos** ante terceros (takedown).

El servicio deberá prestarse mediante infraestructura propia del contratista o a través de plataformas en la nube que cumplan con estándares internacionales de seguridad, sin perjuicio de que se garantice la **disponibilidad, confidencialidad e integridad de la información procesada**. Además, el contratista deberá asegurar la ejecución del servicio conforme a las disposiciones vigentes en materia de ciberseguridad, así como los protocolos sanitarios establecidos por las autoridades competentes. Finalmente, el servicio deberá incluir actividades que garanticen su continuidad operativa.

ALCANCE DE LA MONITORIZACIÓN	
N° de marcas	20
N° de dominios	55
N° de direcciones IP	254
N° de activos tecnológicos	100
N° de identidades digitales (VIPs)	20
N° de *bincodes*	50

7.2. CARACTERÍSTICAS DEL SERVICIO A CONTRATAR

a) Descripción Detallada del Servicio a Contratar

La Contratación comprende lo siguiente:

PRESTACIÓN PRINCIPAL

Denominación	U.M.	Cantidad
Servicio de Monitoreo Antiphishing - Preventivo	Servicio	Un servicio por el período de sesenta (60) días calendario.

b) Actividades y Procedimientos

Se deben realizar las siguientes actividades que permitan realizar el seguimiento, prevención control y/o remediación, dependiendo del tipo de ciberataque:

REPUTACIÓN Y MARCA:

Dominios Sospechosos	Se debe detectar, reportar y monitorear aquellos nombres de dominio que contengan en su nombre palabras clave directamente relacionadas con la institución. Este módulo se complementa además con capacidades typosquatting en algoritmos de similitud y proximidad: Similitud: Reemplazando ciertos caracteres por otros similares o deformando las palabras para que sean visualmente iguales. Proximidad: Eliminando o reemplazando ciertos caracteres. Además, se proporcionará siempre que esté disponible, la información de registro **(WHOIS)** asociada a los dominios sospechosos identificados. Para ello se debe consultar las bases de datos de los dominios de alto nivel (TLDs, incluyendo ccTLD y los nuevos gTLD), tomando como referencia los dominios registrados por la institución.
Uso no autorizado de marca	Se debe identificar aquellos sitios web y contenidos en redes sociales u otras plataformas que pretendan suplantar o aprovecharse de la imagen y reputación de la institución para confundir al usuario final mediante el uso de su marca, logo o imagen Para ello se debe monitorizar redes sociales, canales relacionados en el sector Banca, publicidad y blogs en busca de usos no autorizados.

	Se debe incluir identidad visual, incluyendo logos, slogans, colores institucionales y perfiles apócrifos en redes sociales, apps móviles, blogs, canales de YouTube, foros y sitios web. Se deberán aplicar reglas de similitud, correlación histórica y geolocalización para priorizar los hallazgos de mayor riesgo.
Contenidos Ofensivos	Se debe identificar opiniones de usuarios y tendencias conforme a los productos o marcas de la institución para detectar contenidos ofensivos que dañen directamente su imagen o la reputación de sus marcas. Para ello se debe monitorizar redes sociales, canales relacionados con su sector, blogs y foros, en busca de publicaciones o comentarios que resulten ofensivos, amenazantes, difamatorios, etc. Dado el gran volumen de la información que se puede detectar, el Servicio realizará una valoración de la relevancia de cada información detectada y se acordará con la institución el umbral mínimo, a partir de la cual dicha información será comunicada.
Seguimiento de Identidad Digital	El servicio debe monitorizar información publicada en Internet relacionada con las identidades digitales facilitadas por la institución, poniendo foco en un conjunto de identidades directamente relacionadas con la empresa (Alta Dirección, personalidades, etc.), con el fin de identificar situaciones de sobreexposición de información personal (no corporativa), críticas contra los directivos y creación de perfiles fraudulentos en redes sociales que suplantan a los VIPs o hacen uso no autorizado de su imagen. Para ello se debe monitorizar información y referencias publicadas por terceros, principalmente en redes sociales, foros y blogs. Se debe disponer de la información suficiente y necesaria para identificar en la red, sin opción a dudas, a las personas físicas seleccionadas por la institución.

BANCO DE LA NACIÓN - Jymmy Hands Quesquen Rivas - Analista - Sección Ciberseguridad - Gerencia de Tecnologías de Información

DISRUPCIÓN DEL NEGOCIO:

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

BANCO DE LA NACIÓN - Ana María Li Martínez - Sección Ciberseguridad - Of. de Seguridad Informática - Gerencia de Tecnologías de Información

Exposición de Información	Se debe localizar información sensible o confidencial que no deben estar publicada o ser accesible desde internet, de acuerdo con las indicaciones de la institución respecto a su documentación sensible y/o confidencial, clasificada o restringida. Para ello se debe monitorizar repositorios documentales y de ficheros, plataformas de compartición de información (pastes) y la información publicada en los canales oficiales de la institución. Así como sitios de la Dark Web, en caso de haber contratado dicho ámbito de monitorización.
Hacktivismo	Se debe localizar anuncios de grupos hacktivistas con intenciones de realizar ataques contra los activos en red facilitados por la institución (DDoS, defacement, XSS, SQLinjection, ...) o publicaciones donde afirman que estos activos han sido vulnerados. Para ello se debe monitorizar redes sociales (perfiles y colectivos hacktivistas), medios de comunicación (locales, sectoriales, sindicales,

	etc.), plataformas de peticiones y firmas, plataformas de compartición de información y manifiestos (pastes). Así como sitios de la Dark Web, en caso de haber contratado dicho ámbito de monitorización.
Activismo	Se debe identificar las intenciones de grupos activistas que muestren conductas peligrosas o dañinas hacia la institución, tales como manifestaciones, escraches, protestas, campañas de recogida de firmas, peticiones de boicot, etc. Para ello se debe monitorizar redes sociales (perfiles y colectivos activistas), medios de comunicación (locales, sectoriales, sindicales, etc.), plataformas de peticiones y firmas, plataformas de compartición de información y manifiestos (pastes).
Vulneración de mecanismos de seguridad	Se debe identificar aquellas publicaciones, tutoriales o videos que revelen fallos de seguridad en activos lógicos o físicos de la institución. Para ello se debe monitorizar canales utilizados para la difusión de tutoriales enfocados a la evasión de medidas de seguridad. Así como sitios de la Dark Web, en caso de haber contratado dicho ámbito de monitorización.
CVEs y boletín de seguridad	Se debe identificar vulnerabilidades con un CVSS igual o superior a 7, vulnerabilidades 0-day, que no han sido todavía evaluadas, y exploits que pueden afectar a los sistemas, plataforma y software utilizados en la institución, así como a activos de las principales tecnologías software. Asimismo, se debe notificar a través de boletines de seguridad y Security Advisory de los principales fabricantes (como Microsoft, Cisco o Adobe, entre otros), que contienen información sobre vulnerabilidades y actualizaciones de seguridad de sus productos. Para ello se debe monitorizar la National Vulnerability Database del NIST, así como distintas fuentes de exploits.
Robo de Credenciales	Se debe identificar credenciales comprometidas que correspondan con permisos de acceso a sistemas, instalaciones y procesos relacionados con la institución. Para ello se debe monitorizar fuentes públicas como plataformas de compartición de información (pastes), así como fuentes de la Deep Web como mercados negros de credenciales e información recolectada por botnets (crime servers), en caso de haber contratado dicho ámbito de monitorización. Se debe proporcionar información disponible del contexto del robo: nombre de usuario, contraseña (en caso de ser de servicios de terceros o de pertenecer a colaboradores o clientes de la institución se mostrará ofuscada), url del servicio afectado, tipo de usuario afectado, ubicación del servicio afectado, organización del servicio afectado, fecha de compromiso, dominio del usuario comprometido, host del servicio afectado, puerto del servicio afectado, tipo de botnet asociada, evidencia. El servicio requerido no necesariamente incluye la verificación de la validez o vigencia de las credenciales.

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

BANCO DE LA NACIÓN
Jymmy Hands Quesquén Rivas
Analista
Sección Ciberseguridad
Gerencia de Tecnologías de Información

BANCO DE LA NACIÓN
Ana María Li Mayorque
Secc. Ciberseguridad
Of. de Seguridad Informática
Gerencia de Tecnologías de Información

FRAUDE ONLINE:

Phishing y Pharming	Se debe localizar sitios web que simulen ser las páginas legítimas de la institución con el propósito de confundir a usuarios finales y obtener sus credenciales de acceso y otros datos confidenciales. Se debe identificar direcciones IP y dominios involucrados, así como la información de contexto que esté disponible (registrador y localización). Para ello se debe monitorizar fuentes oficiales procedentes de organismos internacionales en la lucha contra el cibercrimen (APWG) y fuentes de confianza dedicadas a denunciar sitios fraudulentos, así como bases de datos de dominios. Para tener una mayor precisión y volumen de detecciones relativas al módulo de Phishing y Pharming, el proveedor es libre de proponer herramientas, agentes, etc. De cara a facilitar su instalación, el proveedor debe proporcionar un guía rápido para su correcta implementación.
Malware	Se debe identificar aquellas muestras de "malware" que tengan como objetivo o se relacionen explícitamente con la institución (URLs, direcciones IP, nombres de dominio o marcas comerciales). Para ello se debe monitorizar fuentes de confianza sobre ficheros maliciosos tracking de familias de malware, repositorios de ficheros y sistemas de compartición de archivos.
Aplicaciones Móviles sospechosas	Se debe detectar la publicación de aplicaciones móviles sospechosas relacionadas con la institución o la suplantación de las aplicaciones oficiales, con el posible objetivo de confundir a sus usuarios para obtener credenciales, datos personales o infectarlos con algún tipo de malware. Para ello se debe monitorizar los mercados móviles oficiales (Apple Store, Google Play), así como mercados móviles alternativos, identificando aquellas aplicaciones móviles con referencias a la institución o a su marca.
Carding	Se debe recopilar los datos de aquellas tarjetas bancarias que se hayan visto comprometidas y que correspondan con los "bincodes" pertenecientes a la institución. Para ello se debe monitorizar fuentes públicas como plataformas de compartición de información (pastes), así como fuentes de la Deep Web, con datos recopilados por botnets y mercados UnderGround. El alcance debe limitarse a los bincodes facilitados por la institución, asociados al número de bincodes contratados. Se debe entregar toda la información de contexto disponible: fecha de recuperación, bincode, número de la tarjeta, tarjeta expirada (sí/no), fecha de expiración, fuente, marca (Visa, Mastercard, Diners Club, etc.), tipo (Crédito/Débito), emisora. El servicio no necesariamente incluye la verificación de la validez o vigencia de las tarjetas recuperadas.

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

BANCO DE LA NACIÓN
Jymmy Hands Quesquen Rivas
Analista
Sección Ciberseguridad
Gerencia de Tecnologías de Información

BANCO DE LA NACIÓN
Ana María Li Mayaute
Secc. Ciberseguridad
Of. de Seguridad Informática

7.3. ACTIVIDADES

El servicio se brindará remotamente a través de un Centro de Operaciones de Seguridad (SOC), el cual debe tener la capacidad de interactuar a nivel mundial con cualquier ISPs, instalaciones de hosting y dueños inocentes de computadoras comprometidas en sus idiomas nativos.

El Servicio se realizará con una frecuencia de 24x7 los sesenta (60) días calendario para todas las funciones, debiendo destacar el contratista a las instalaciones del Banco a un **Ingeniero Residente** especializado, quien prestará el servicio de 08:30 horas a las 17:30 horas de Lunes a Viernes, la continuidad del servicio de 17:30 horas hasta las 8:30 horas estará a cargo del Centro de Operaciones de Seguridad (SOC), incluyendo sábados, domingos y feriados.

El servicio deberá incluir interacción directa mediante correos electrónicos y llamadas telefónicas y, en casos críticos o de severidad S1, el acceso a canales de comunicación directa con el equipo de Respuesta a Incidentes (Incident Response – IR) del contratista.

Se debe realizar reuniones semanales presenciales para evaluación de las amenazas descubiertas en la semana anterior.

El servicio para contratar debe incluir la detección de incidentes de diferentes tipos de ataques de phishing, pharming, smishing y crimeware, entre otros.

El contratista deberá indicar las herramientas de alto valor tecnológico para la búsqueda automática en Internet.

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

El Servicio debe poseer las siguientes fuentes de información:

- Webs convencionales, con independencia del idioma y la localización geográfica.
- Redes Sociales
- Deep Web (Páginas web no listadas en los motores de búsqueda y directorios)
- Underground ChatRooms/IRC
- Redes peer-to-peer
- Newsgroups.
- Páginas de hacking, Information Security Web Pages, Vulnerabilities webpages, etc.
- Bases de datos de Spam.
- Registradores de dominios (gTLD y ccTLD).
- Servidores DNS.
- Black lists feeds.
- Fuentes de inteligencia en comunidades underground (Telegram, Discord y foros de cibercrimen).

BANCO DE LA NACION
Jymmy Hands Quesquen Rivas
Analista
Sección Ciberseguridad
Gerencia de Tecnologías de Información

El servicio debe anticiparse, identificando las amenazas y vulnerabilidades, así como los factores desencadenantes de las actuaciones maliciosas, recomendando contramedidas y respuestas frente a éstas, a través de la definición de estrategias de seguridad adecuadas.

BANCO DE LA NACION
Ana María Linares Enrique
Secc. Ciberseguridad
Of. de Seguridad Informática
Gerencia de Tecnologías de Información

Se requiere que, ante la detección de cualquier IoC (Indicador de Compromiso), incluyendo venta o filtración de credenciales de usuarios, accesos remotos o bases de datos, que impacte o pueda impactar los activos digitales del Banco de la Nación, el ingeniero residente del proveedor notifique inmediatamente al Área de Ciberseguridad. Esto permitirá la aplicación inmediata de los IoC en los controles de seguridad (firewall, WAF, EDR/XDR, IPS, etc.) para su bloqueo, contención y mitigación.

El servicio debe brindar la evaluación de la postura de seguridad de servicios informáticos en Internet, para lo cual debe utilizar un software de las siguientes características:

- La solución debe operar bajo la modalidad de Software como servicio (SaaS).
- La solución propuesta debe estar basada sobre una infraestructura en la nube que posea alguna de las certificaciones bajo la norma ISO 27001, ISO 27017 y/o ISO 27018 relevantes a la zona o región desde donde se provee el servicio.
- El software debe disponer de informes del nivel de seguridad informática de una organización en particular sin tener límites de subdominios para cada organización, si no se dispone del informe de seguridad de una organización se deberá incluir otras fuentes de información para obtener el nivel de seguridad informático.
- El software debe permitir realizar como mínimos las evaluaciones siguientes:
- Para cada subdominio se deberá verificar si la información es vigente o histórica.
- Se deberán verificar los puertos abiertos TCP y UDP por cada subdominio; así como el servicio asociado.
- Se deberá indicar el nivel de certificados SSL/TLS de cada subdominio (en los casos que aplique) y protocolos soportados
- Se deberá identificar y extraer la Información de las cabeceras de los servicios web identificando tipología e información no segura
- Se deberá identificar indicadores de compromiso; así como actividades sospechosas como malware y spam.
- Deberá de clasificar y puntuar las vulnerabilidades de acuerdo a la criticidad, con la finalidad de proporcionar a la entidad evaluada una clasificación de seguridad en un contexto de riesgo de ciberseguridad.
- El software debe permitir la identificación de vulnerabilidades de seguridad de los servicios informáticos y/o aplicaciones que están expuestos en internet, y sobre los cuales las empresas supervisadas evaluadas deben implementar controles a fin de evitar la explotación de una vulnerabilidad que pueda generar un incidente de ciberseguridad.
- La solución debe permitir la visualización del score de riesgo y detalle de la vulnerabilidad identificada.
- La solución debe permitir la monitorización continúa para analizar el Nivel de Ciberseguridad del Banco de la Nación el cual comprende la exposición en Internet y Deep/Dark Web. Se aceptarán soluciones que el nivel de seguridad es actualizado de forma continua o en tiempo real en un máximo de 48 horas.
- La solución deberá permitir algún mecanismo para la agrupación y comparación de diferentes entidades evaluadas.
- La solución deberá proveer algún mecanismo para contar con la información histórica de las puntuaciones de las entidades evaluadas; así como visualizar su evolución.
- La solución deberá proveer los respectivos mecanismos para la configuración y generación de alertas ante posibles variaciones del Nivel de Ciberseguridad o cuando la puntuación de su empresa caiga por debajo de un cierto umbral o en una cierta cantidad de puntos.

La solución debe proporcionar reportes personalizables (ad-hoc), gráficos, tanto en tiempo real como información histórica, mediante ejecución manual o programación de tiempo predefinida por cada tipo de reporte. Los reportes pueden enviarse por correo electrónico.

Los informes deberán ser exportables en varios formatos, tales como PDF, XLSX y CSV.

La solución debe incluir actividades para conocer el comportamiento y actividades de los ciberatacantes, tales como:

- Dilución: Introducción de datos ficticios
- Señuelos: usando cuentas ficticias y reales.
- Recolección de datos introducidos por los clientes en las páginas fraudulentas, cuando los casos lo permitan.
- Presentar los casos y advertencias a los motores de búsqueda y proveedores email para la inclusión en listas negras
- Cierre de Webs y monitorización de re-aperturas.

La solución debe facilitar al Banco de la Nación el acceso a la información derivada como parte del servicio a través de un Portal Web; para ello se debe considerar lo siguiente:

- Acceso de manera segura a través de un Portal de Vigilancia Digital en idioma español, donde se debe registrar toda la información actualizada.
- Acceso para realizar seguimientos a los casos que se reportan, cuando estos, están abiertos, no bloqueados.
- Debe Permitir monitorizar el estado de alertas.
- Debe permitir la representación de las detecciones por número y riesgo.
- Debe mostrar el listado de las detecciones, el estado de cada una y acceso al detalle de cada detección. Detalle de los casos, gráficos históricos, indicadores claves y umbrales de exposición.
- Las alertas pueden ser creadas por el Banco o por el contratista.
- El portal debe disponer de características de dashboards y reportes estadísticos.
- Informes iniciales que incluyan descripción de alto nivel de la información del ataque.
- Informes detallados que describan las acciones derivadas como parte del análisis y/o detección.
- Información relevante respecto a incidentes presentados a nivel mundial.
- Información respecto a estadísticas, tendencias y metodologías generales de ataques, preguntas frecuentes
- La información recibida por el Banco de la Nación como parte de los informes debe contener como mínimo en caso un ataque, lo siguiente:

  - ID del ataque
  - URLS
  - ISP (Geolocalización)
  - Bloqueo en los ISP indicando en cuales se ha realizado
  - Sitio bajado - si / no
  - Severidad
  - Información Análisis Forense
  - Copia del Correo o evidencia del ataque
  - Detalles generales
  - Los reportes deben poder filtrarse y exportarse a un formato Excel.
  - Los reportes deben ser en Tiempo Real y permitir abrir casos.

El servicio debe incluir como mínimo los siguientes métodos de detección proactiva de ataques:

- IP/URL (sitios falsos - phishing sites), monitorear y analizar URL sospechosas, así como direcciones IP con una frecuencia de 24x7, para determinar si éstos están siendo usado como hosts de ataques de phishing.
- Bank Trojans, monitorear y detectar diferentes variantes de crimeware, abuso de marca, malware, pharming y phishing a través de sus diferentes conexiones a Internet.
- Correos electrónicos falsos, que incluyen un enlace al sitio de phishing falso o no.

- Detección temprana (antes que el ataque sea lanzado), análisis de los registros web, de esta manera permitir detectar actividades sospechosas relacionadas con la creación de sitios de phishing, ataques de pharming y crimeware.
- Detección de ataques Post, realizar un monitoreo permanente de los sitios de phishing que fueron reportados, para saber si estos han sido cerrados, reabiertos y si nuevamente son usados para ataques, de confirmarse nuevos ataques de estos sitios la solución deberá notificar al usuario y comenzar el proceso de mitigación.
- La solución debe constantemente verificar los servidores raíces de DNS y los servidores autoritarios del DNS en un extremo, e ISPs seleccionados, así como servidores de DNS en el otro extremo para comprobar si hay nombres de servidores válidos y respuestas de direcciones IP que corresponden con los dominios legítimos de la Institución.
- Detección de dominios falsos como variantes del dominio del Banco en buscadores y redes sociales.
- Detección de correos falsos enmascarados con el dominio del Banco y conteniendo enlaces a sitios de phishing.
- Capacidad para analizar cabeceras de correos fraudulentos, capacidad para realizar análisis forense de cualquier caso de phishing. Tener interacción con google y otros buscadores para que pueda gestionar la eliminación de publicaciones que llevan a sitios web fraudulentos contra el Banco.

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

Como estrategias de mitigación debe contar por lo menos con:

- Phish tagging (baits).
- Enlaces disponibles con barras de herramientas antiphishing y browsers.

BANCO DE LA NACIÓN Jymmy Hands Quesquen Rivas Analista Sección Ciberseguridad Gerencia de Tecnologías de Información

Atención de Requerimientos por parte del Banco de la Nación

El servicio debe incluir la atención de solicitudes reportadas por el Banco, solicitudes de baja de sitios web falsos. Dichas solicitudes, deberán ser verificadas y validadas por el personal especializado del SOC. Las solicitudes deberán hacerse a través del Portal de Vigilancia Digital propuesto por el contratista, vía email y/o teléfono. Luego de la verificación, deberá ingresar al proceso de mitigación de incidentes. El servicio deberá considerar la mitigación proactiva 24x7 de los sitios web falsos detectados y en paralelo informar al banco de las acciones ejecutadas.

BANCO DE LA NACIÓN Ana María Li Enrique Seguridad de Seguridad Informática Gerencia de Tecnologías de Información

Mitigación de Incidentes

El contratista del servicio deberá ofrecer la activación de red de bloqueos (aviso de página de phishing en los principales navegadores / proveedores de correo) como método de mitigación, con tiempos promedio de la industria que garanticen una adecuada gestión de los incidentes de phishing en el Banco de la Nación.

El contratista deberá gestionar el bloqueo con los ISP a nivel nacional y continuar la gestión hasta el bloqueo en el origen. Se deberá informar al Banco de la acción tomada en cada instancia de bloqueo conforme estas se vayan realizando o escalando.

Servicio Post- Ataque / Análisis Forense

El servicio debe coberturar para el soporte post ataque, desarrollando:

- El Análisis Forense de Phishing, pharming, exposición de información y crimeware encontrados en los equipamientos del Banco, debiendo colectar la siguiente información:

- Copia del correo electrónico del ataque Phishing
- Código HTML fuente del ataque Phishing, pharming y crimeware
- Información adicional dependiendo del tipo de ataque.
- Se deberá realizar una investigación del ataque y se deberá recopilar las evidencias y datos expuestos. El servicio deberá incluir el análisis forense de los casos que el Banco solicite.

Servicio de Protección de Marca y Reputación

- Monitoreo del uso no autorizado de marca, logos e imagen seguimiento de dominios.
- Búsqueda y gestión de la eliminación de la información que afecte la marca y reputación del Banco.
- Monitoreo de Canales alternativos de venta de productos, con uso de la marca.
- Monitoreo de Falsificación de identidades digitales.
- Monitoreo de información confidencial del Banco.
- Protección contra Trolls y perfiles 'no oficiales' en Redes Sociales, uso no autorizado de logos y brand en páginas no oficiales", abuso y tráfico de dominios, Cybersquating y Typosquatting.
- Uso de la marca del Banco para redirigir el tráfico a las webs donde se venden productos similares de la competencia.
- Detección del uso no autorizado de logos en webs para promocionar la venta de servicios no relacionados con el Banco, como las campañas SPAM.
- Monitoreo de la marca en redes sociales.
- Monitoreo de buscadores para detectar y gestionar a baja de páginas falsas posicionadas en ellos.
- Monitoreo de Mercados Negros y foros clandestinos que trafican con información de tarjetas y clientes.
- Monitoreo de dominios y de aplicaciones móviles además de redes sociales.
- Monitoreo en tiempo real de medios sociales como Facebook, Google+, los más importantes portales de noticias, Youtube, Twiter, Fickr, Linkedin, Reddit, Delicious y otros similares que se presenten.
- El contratista deberá notificar inmediatamente al Banco sobre cualquier impostor o cuenta social sospechosa detectada. Al detectar cualquier actividad maliciosa que viole los términos legales de uso de las redes sociales, el contratista a solicitud del Banco inmediatamente presentara un reporte formal a las partes correspondientes en el sitio involucrado para que se realce el bloqueo o la desactivación del elemento malicioso. Esto incluye cuentas impostoras que quieran suplantar la identidad del Banco. Todos los incidentes que ocurran en las redes sociales serán incluidos en un reporte mensual y el contratista se encargara de investigar cualquier cuenta, mención o incidente que el Banco solicite.
- El contratista deberá monitorear las principales tiendas de aplicaciones como Apple iTunes, Google Play y tiendas de terceros. Las aplicaciones legítimas deberán ser registradas en el servicio y en caso de detectar aplicaciones sospechosas, se enviarán las notificaciones oportunas al Banco. El contratista deberá investigar los dominios más recientes en busca de material asociado a la identidad y marca del Banco
- El contratista deberá monitorear constantemente los servicios de registro de dominios en busca de actividad sospechosa que pueda resultar en ataques de fraude online. Todos los dominios sospechosos deberán ser clasificados para su revisión en el portal para el cliente e inmediatamente se deben activar las notificaciones al Banco
- El servicio de detección proactiva de ataques en tiempo real debe considerar:

- Monitoreo de buzón de correo. El Banco pondrá a disposición del proveedor un buzón oficial para la recepción de correos electrónicos sospechosos reportados por los usuarios internos.
- Monitoreo y análisis de registros de servidores Web
- Monitoreo de correos con URL falsos
- Monitoreo de dominio y protección de marca en todos los ámbitos de internet
- Monitoreo y observación de diversas fuentes públicas (www, blogs, redes sociale, P2P), fuentes internas del proveedor, acuerdo y alianzas, fuentes hacking y underground, autoridades y otras fuentes oficiales
- Vigilancia de Servidores DNS para detectar posibles casos de pharming
- Monitoreo Global de Dominios
- Buzones trampas en diferentes ISPs a nivel mundial. El proveedor deberá detallar el despliegue de los buzones y la estrategia de esta característica.
- Detectar al crear páginas similares fraudulentas, mediante el registro de un código oculto en la página verdadera. Este Código deberá ser entregado al Banco y será responsabilidad del contratista la instalación y pruebas del mismo con la supervisión de los especialistas del Banco.
- El Centro de Detección de Fraudes (SOC) deberá realizar la verificación de la validez de las alertas detectadas
- El personal del Centro de Detección de Fraudes (SOC) asignado para el servicio, debe tener los conocimientos necesarios para realizar una selección y calificación manual de la alerta.
- Toda alerta debe ser informada al Banco, para ello el contratista entregará diferentes tipos de canales de reporte como vía Telefónica, lista de correos, mensajes; estableciéndose el procedimiento de escalamiento respectivo.
- Toda alerta debe ser registrada con su respectiva severidad proveyendo al Banco de la Nación información valiosa y oportuna de manera que puedan ser tomadas. Dicha información deberá estar reflejada en el portal en idioma español
- La determinación de la severidad de la alerta debe basarse de manera objetiva a través de estadísticas predefinidas, modelos y/u otros.

BANCO DE LA NACIÓN - Jymmy Hands Quesquen Rivas - Analista - Sección Ciberseguridad - Gerencia de Tecnologías de Información

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

7.4. Plan de Trabajo:

El contratista presentará en un plazo máximo de cinco (5) días calendarios contabilizados a partir del día siguiente hábil de la notificación de la contratación. El plan de trabajo el cual deberá contar como mínimo con la siguiente información:

BANCO DE LA NACIÓN - Ana María Li Mendoza - Jefe - Secc. Ciberseguridad - Of. de Seguridad Informática - Gerencia de Tecnologías de Información

- Plan de Implementación, detallando la identidad digital del Banco de la Nación, sus necesidades y requisitos.
- Actividades a realizar durante la ejecución del servicio
- Procedimiento de atención de casos, desde el momento en que se detecta el incidente o recepcionado el reporte hasta el informe indicando la baja de sitios web falsos, canales no oficiales en redes sociales.

Presentación del Plan de Trabajo

El Plan de Trabajo podrá ser presentado a través de los siguientes medios:

- **Mesa de Partes Física:**
  Sección Trámite Documentario de la Oficina Principal del Banco de la Nación, con atención a la Oficina de Seguridad Informática, en el horario de 08:30 a.m. a 04:30 p.m., ubicada en la Calle Arqueología N° 120 - San Borja - Distrito de San Borja.

- **Mesa de Partes Digital:**
  https://www.bn.com.pe/mesa-de-partes/mesa-de-partes.asp

Complementariamente deberá ser presentado al correo electrónico: seginformatica@bn.com.pe.

Revisión y Aprobación del Plan de Trabajo

La Sección Ciberseguridad de la Oficina de Seguridad Informática del Banco de la Nación evaluará el Plan de Trabajo y comunicará las observaciones que correspondan en un plazo máximo de tres (03) días calendario.

En caso dicho plazo venza el sábado, domingo o feriado, el levantamiento de observaciones podrá ser recibido en el siguiente día hábil, sin que ello afecte el cronograma contractual.

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.

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.

8. **PRESTACIONES ACCESORIAS A LA PRESTACIÓN PRINCIPAL.**
   NO corresponde

9. **REGLAMENTOS TECNICOS, NORMAS METROLOGICAS Y/O SANITARIAS**
   NO corresponde

10. REQUISITOS DEL PROVEEDOR

Los requisitos obligatorios para servicios son:

- Persona jurídica, con RUC en estado activo y habido.
- Contar con RNP vigente – Registro de servicios.
- 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 EN LA ESPECIALIDAD

El proveedor debe acreditar un monto facturado acumulado equivalente a S/ 120,000.00 (Ciento veinte mil 00/100 Soles) por la contratación de servicios iguales o similares al objeto de contratación, durante los cinco (5) años anteriores a la fecha de la presentación de su cotización que se computaran desde la fecha de la conformidad o emisión del comprobante de pago, según corresponda.

Se consideran servicios similares: Ciberinteligencia, Inteligencia para la Defensa, Protección de Marca, Prevención del Fraude, Ciberseguridad, Detección de Fuga de Información, Inteligencia e Amenazas, Monitoreo de Deep & Dark Web, Cyber Threat inteligence (Inteligencia de Ciber amenazas), Servicios de Ethical Hacking, Servicios de Gestión de Seguridad, Outsourcing de Seguridad Gestionada, Soluciones Antispam; (siempre y cuando se acredite funcionalidades de Antiphishing).

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

Acreditación:

La experiencia se acredita con copia simple de (i) contratos u órdenes de servicios, y su respectiva conformidad o constancia de prestación; o (ii) comprobantes de pago cuya cancelación se acredite documental y fehacientemente, con voucher de depósito, nota de abono, reporte de estado de cuenta, cualquier otro documento emitido por Entidad del sistema financiero que acredite el abono o mediante cancelación en el mismo comprobante de pago, correspondientes a un máximo de veinte (20) contrataciones. En caso el postor sustente su experiencia en la especialidad mediante contrataciones realizadas con privados, para acreditarla debe presentar de forma obligatoria lo indicado en el numeral (ii) del presente párrafo; no es posible que acredite su experiencia únicamente con la presentación de contratos u órdenes de compra con conformidad o constancia de prestación.

BANCO DE LA NACIÓN Jymmy Hands Quesquen Rivas Analista Sección Ciberseguridad Gerencia de Tecnologías de Información

PERSONAL PROPUESTO

1) **Formación Académica:**

Acreditar como mínimo el grado de bachiller en la carrera de Ingeniería de Sistemas o Telecomunicaciones o Electrónica o Informática o Ingeniería de Software o Industrial con mención en Sistemas o Ingeniería Computacional o Ingeniería de Redes o Ingeniería Telemática o Ingeniería en Ciberseguridad, del personal clave requerido como Ingeniero Residente.

Acreditación:

Con copia simple de constancia, diploma u título que acredite la formación académica requerida.
El grado de bachiller o título profesional requerido será verificado por los evaluadores en el Registro Nacional de Grados Académicos y Títulos Profesionales en el portal web de la Superintendencia Nacional de Educación Superior Universitaria - SUNEDU a través del siguiente link: https://enlinea.sunedu.gob.pe/ o en el Registro Nacional de Certificados, Grados y Títulos a cargo del Ministerio de Educación a través del siguiente link:

BANCO DE LA NACIÓN Analista Sección Ciberseguridad Of. de Seguridad Informática Gerencia de Tecnologías de Información

https://titulosinstitutos.minedu.gob.pe/, según corresponda.

2) **Certificación u otro requisito:**
El Ingeniero Residente deberá estar especializado en las distintas áreas de Ciberseguridad y sus conocimientos deberán estar avalados con al menos una de las siguientes Certificaciones Técnicas vigentes:

- EC - Council Threat Intelligence Essentials ó
- CEH - Certified Ethical Hacker

Acreditación: se acreditará con copia simple de constancias, certificados, u otros documentos. Para el caso de certificaciones internacionales emitidas en idioma distinto al castellano, deberá presentarse adicionalmente traducción simple.

3) **Capacitación:**
El Ingeniero Residente deberá acreditar como mínimo ochenta (80) horas de capacitación, las cuales podrán ser lectivas, académicas y/o pedagógicas, en materias directamente relacionadas con las actividades a ejecutar en el servicio objeto de la convocatoria, tales como:

- Ciberseguridad
- Seguridad de la Información
- Inteligencia de Amenazas (Threat Intelligence)
- Monitoreo y detección de Phishing, Smishing y Fraude Digital
- Protección de Marca Digital
- Análisis de amenazas en Deep Web y Dark Web.
- Prevención del fraude digital y fuga de información

Acreditación: Las horas de capacitación exigidas se acreditará con copia simple de constancias, certificados u otros documentos.

4) **Experiencia:**
El personal clave: Ingeniero Residente debe acreditar como mínimo con un (1) año de experiencia en servicios de monitoreo de Antiphishing - preventivo y/o Ciberseguridad y/o Seguridad Informática y/o Inteligencia para la defensa y/o Protección de Marca y/o Prevención del fraude y/o detección de Fugas de Información y/o Inteligencia de Amenazas y/o Monitoreo de Deep & Dark Web.

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.

11. VISITA TECNICA
NO corresponde.

12. ENTREGABLES:
La prestación del servicio consta de los siguientes entregables:

Periodo de la prestación del Servicio	Entregables
Se presentará a los cinco (5) días calendario, contados a partir del día siguiente hábil de la notificación de la contratación.	- Plan de Trabajo.
Se presentará a los (25) días calendario, contados a partir de la aprobación del plan de trabajo.	- Primer Informe.
Se presentará a los (30) días calendario, contados a partir del primer informe	- Segundo Informe

Presentado cada uno de los entregables en los plazos establecidos, el Banco de la Nación tiene tres (3) 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.

13. ÉTICA Y ANTICORRUPCIÓN:

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.

14. 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

15. SEGURO COMPLEMENTARIO DE TRABAJO DE RIESGO

Para los requerimientos que se traten de intermediación laboral, tercerización o por la naturaleza de la prestación el personal del proveedor realice labores de riesgo y para la persona natural que realice actividades dentro de las instalaciones de la institución, por el cual el área usuaria deberá coordinar con la Sección Seguridad y Salud en el Trabajo.

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

SCTR:

El Proveedor debe adquirir las pólizas de SCTR salud y pensión; de acuerdo a la Ley No 26790 (Decreto Supremo N° 009-97-SA Decreto Supremo N° 003-98-SA)

BANCO DE LA NACIÓN Jymmy Hands Quesquen Rivas Analista Sección Ciberseguridad Gerencia de Tecnologías de Información

- SCTR Salud: Proporciona cobertura médica completa al 100 %, en caso de accidentes de trabajo o enfermedades profesionales, incluyendo atención médica, medicamentos, hospitalización, cirugías, rehabilitación y prótesis hasta la recuperación y alta del paciente.
- SCTR Pensión: Otorga beneficios económicos, como pensiones por invalidez o sobrevivencia (a beneficiarios en caso de fallecimiento del trabajador) y reembolso de gastos de sepelio.

VIDA LEY

El Proveedor debe adquirir la póliza de Vida Ley de acuerdo con el decreto Legislativo No 688 el cual debe contar como mínimo con las coberturas de ley.

BANCO DE LA NACIÓN

- Muerte Natural: Indemnización de 16 remuneraciones mensuales asegurables.
- Muerte Accidental: Indemnización de 32 remuneraciones mensuales asegurables.
- Invalidez Total y Permanente por Accidente: Indemnización de 32 remuneraciones mensuales asegurables.

Otras consideraciones

- El Proveedor se obliga a entregar a BANCO DE LA NACIÓN de manera previa al inicio de las actividades dentro de sus instalaciones, copia de las Pólizas, el cronograma de pago y de las constancias de pago de las respectivas primas.
- Las Pólizas deberán ser otorgadas por compañías de seguros de primer nivel (en adelante, el "Asegurador"), entendiéndose por éstas a las compañías de seguros calificadas como Categoría A conforme con lo establecido en el Reglamento para la Clasificación de Empresas de los Sistemas Financieros y de Seguros aprobado mediante la Resolución SBS N° 18400-2010, o la norma que la sustituya o modifique.
- El Proveedor acepta que será de su total responsabilidad y asumirá a su total riesgo y responsabilidad, toda responsabilidad, gastos y costos por pérdidas y/o daños materiales y/o daños corporales, incapacidad o muerte de cualquier personas o personas, en la eventualidad que un accidente ocurra y el Proveedor no haya provisto adecuadas coberturas cuando fuesen necesarias durante el desarrollo del presente Contrato.
- Todos y cada uno de los deducibles y el pago de las primas de seguros correspondientes a

las Pólizas, serán asumidas por el Proveedor.

- El Proveedor deberá cumplir con acreditar la renovación de las Pólizas (si corresponde) y, además, deberá comunicar a BANCO DE LA NACIÓN dentro de los treinta (30) Días calendario previo al vencimiento de cada una de las Pólizas la renovación de las mismas, adjuntando el cronograma de pago y las constancias de pago respectivas.
- Si llegase a ocurrir un siniestro cuyo costo implique un monto mayor al asegurado por las Pólizas del Proveedor, éste se compromete a resarcir todos los daños ocasionados, comprometiéndose a mantener indemne a BANCO DE LA NACIÓN.
- Es responsabilidad del Proveedor obtener coberturas adicionales a las señaladas y/o pólizas cuando sea necesario y/o aplicable a la naturaleza del servicio a contratarse.
- La no contratación de pólizas necesarias y adicionales, no libera de responsabilidad al proveedor por los daños y/o pérdidas ocasionadas a la Entidad.
- En el supuesto caso que los límites contratados en las pólizas de seguros sean insuficientes o estas no puedan ejecutarse por cualquier motivo ante la eventualidad de un siniestro, el Proveedor asumirá directamente el pago de la indemnización a terceras personas, así como a la Entidad y/o a sus trabajadores.
- El Proveedor deberá evidenciar el pago de los seguros requeridos. comprenden la oferta.
- Las coberturas de la presente póliza son primarias, respecto a los intereses de la Entidad y cualquier otro seguro mantenido por la Entidad. En caso de que los seguros presentados tengan una vigencia menor al contrato, el proveedor deberá de presentar antes de la suscripción un compromiso de renovación antes del término de la vigencia del seguro presentado.
- Las sumas aseguradas no deben ser limitadas por evento o reclamante
- Las pólizas deberán indicar expresamente que el Asegurador renuncia a su derecho de subrogación contra BANCO DE LA NACIÓN y/o funcionarios y/o empleados y/o clientes.
- Las Pólizas deberán especificar que BANCO DE LA NACIÓN y/o funcionarios y/o empleados y/o clientes son asegurados adicionales, e incluir una cláusula en donde se especifique que serán considerados también como terceros en caso de siniestro.

BANCO DE LA NACION - Jymmy Hanns Quesquen Rivas - Analista - Sección Ciberseguridad - Gerencia de Tecnologías de Información

BANCO DE LA NACION - Ana [illegible] - Sección Ciberseguridad - Oficina de Seguridad Informática

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

16. RECURSOS A SER PROVISTOS DEL PROVEEDOR

NO corresponde

17. PLAZO DE EJECUCIÓN DEL SERVICIO.

El servicio se desarrollará en un plazo de sesenta (60) días calendarios, computados a partir del día siguiente hábil de la notificación de la contratación o de la publicación de la adjudicación en la PLADICOP y/o vía correo electrónico.

18. LUGAR DE PRESTACIÓN DEL SERVICIO.

La prestación del servicio se realizará de manera remota.

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.

19. FORMA DE PAGO:

El pago se realiza en un plazo máximo de diez días hábiles luego de otorgada la conformidad por parte del área usuaria y es prorrogable, previa justificación de la demora, por cinco días hábiles; de conformidad con lo establecido en el artículo 67 de la Ley General de Contrataciones Públicas. El Banco de la Nación realizará el pago de la contraprestación pactada a favor del contratista en Soles (s/) y en dos (2) pagos, conforme a la siguiente distribución:

Entregables	%Porcentaje del Monto Contractual	Plazo
1er Entregable	Pago 50% del monto contractual	Plazo de hasta 10 días hábiles de emitido la conformidad del Primer Informe.
2do Entregable	Pago 50% del monto contractual	Plazo de hasta 10 días hábiles de emitido la conformidad del Segundo Informe.

Para efecto del pago descrito líneas arriba, se debe presentar la siguiente documentación:

- Carta simple dirigida al Subgerente de Compras de la Gerencia de Administración y Logística.
- Comprobante de pago.
- Copia simple del documento de contratación
- Acta de conformidad suscrita por la Oficina de Seguridad Informática. Previo informe técnico de la Sección de Ciberseguridad – Sub Gerencia de Seguridad Informática – Gerencia de Tecnologías de Información.

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 16:00 horas

20. 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 unidad orgánica responsable (Sección, Subgerencia o Gerencia solicitante) o quien hagas sus veces, en un plazo máximo de (7) días calendario o 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, o si se trata de consultorías.

21. 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.

22. PENALIDAD

Penalidad por Mora en la ejecución de la prestación:
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:

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

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.

23. OTRAS PENALIDADES.

Asimismo; teniendo en cuenta el tipo bien, se podrá establecer penalidades distintas a las mencionadas, las mismas que deberán ser objetivas, razonables, congruentes y proporcionales con el objeto de contratación y no afectar el equilibrio económico financiero del contrato, conforme al principio de valor por dinero.

Otras Penalidades			
N°	**Supuestos de aplicación de penalidad**	**Forma de cálculo**	**Procedimiento**
1	El contratista cambie al personal propuesto sin contar con la autorización previa de la Entidad	1 UIT Vigente a la fecha de la Penalidad	Para la aplicación de la penalidad se seguirá el siguiente procedimiento: 1.- En caso el contratista cambie el personal clave presentado en su oferta, sin haber mediado comunicación alguna a la Sección Ciberseguridad, y aun existiendo una solicitud de cambio de personal clave por parte del contratista y esta sección no haya comunicado la aceptación de dicha solicitud al contratista. 2.- La sección Ciberseguridad como área usuaria, registrará y contabilizará cada incumplimiento que se haya presentado dentro de cada mes y posteriormente realizará la sumatoria de las ocurrencias y calculará el monto a ser descontado al contratista, de acuerdo a la siguiente formula: Monto a Descontar= X*Y Donde los valores de X e Y son: X= Nro. de incumplimiento en el mes Y= 1 UIT vigente a la fecha del incumplimiento El monto a descontar será deducido en el pago

			mensual donde se presentó los incumplimientos. 3.- La Sección Ciberseguridad, al culminar el mes, emitirá un acta de conformidad y un informe técnico en donde se indicará la cantidad de incumplimientos y el monto que será descontado al Contratista en su factura mensual.

La suma de la aplicación de las penalidades por mora y de otras penalidades no puede exceder el 10% del monto del entregable correspondiente.

24. 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 carta de aprobación, 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 remitir a la otra parte una carta 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 carta de aprobación 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 Carta de aprobación.
h. Por incumplimiento de la cláusula anticorrupción.

25. 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.

26. 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.

27. OTROS CARACTERISTICAS QUE SEAN RELEVANTES PARA LA CONTRATACIÓN

Esta contratación de servicios 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-homologacionaprobadas.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
Jymmy Hands Quesquen Rivas
Analista
Sección Ciberseguridad
Gerencia de Tecnologías de Información

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

BANCO DE LA NACION
Ana María Li Martínez
Jefa
Sección Ciberseguridad
Oficina de Seguridad Informática

Jefe de la Sección Ciberseguridad
Oficina Seguridad Informática
Gerencia de Tecnologías de Información