TÉRMINOS DE REFERENCIA

CONTRATACION DEL SERVICIO DE EVALUACIÓN INTEGRAL DEL SGSI-C (SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN Y CIBERSEGURIDAD)

1. **Proyecto:** "Proyecto de Transformación Digital del Banco de la Nación"[1]
2. **Contrato de Préstamo:** N° 5965OC-PE
3. **Unidad Ejecutora:** Banco de la Nación
4. **Coordinación Técnica:** Unidad Implementadora de Proyecto (UIP)
5. **Tipo de consultoría:** Firma consultora.
6. **Plazo de Ejecución: 09 meses.**
7. **Responsable de la Supervisión: Coordinador Componente 3**

I. DENOMINACIÓN

Contratación del servicio de Evaluación integral del SGSI-C (Sistema de Gestión de Seguridad de la Información y Ciberseguridad)

II. FINALIDAD PÚBLICA

Contribuir a la mejora del acceso a servicios financieros adecuados a nivel nacional por parte de los usuarios del Banco de la Nación. Esto se realiza a través del fortalecimiento institucional, la modernización de la capacidad digital, la interoperabilidad de los servicios digitales y el aumento de la madurez en ciberseguridad del Banco.

III. ANTECEDENTES

El Proyecto de "Transformación Digital del Banco de la Nación", identificado como el mayor esfuerzo de modernización tecnológica de esta entidad pública peruana, tiene como objetivo fundamental mejorar el acceso a servicios financieros adecuados y oportunos a nivel nacional. Este proyecto se estructura en torno a un préstamo de US$ 40 millones otorgado por el Banco Interamericano de Desarrollo (BID), complementado con un aporte local de aproximadamente US$ 25.7 millones, sumando una inversión total superior a los S/ 240 millones (US$ 65.7 millones) para optimizar los servicios financieros, impulsar la inclusión y fortalecer la infraestructura tecnológica en beneficio de millones de usuarios en todo el país.

Sus principales ejes son el fortalecimiento de las capacidades institucionales para el diseño e implementación de productos digitales, el incremento de la capacidad digital e interoperabilidad de los servicios, y el fortalecimiento de la ciberseguridad, pilares que permitirán modernizar la gestión interna y ampliar el acceso a servicios financieros, especialmente en zonas rurales y para grupos vulnerables.

[1] *Para efectos del Prestatario y en el marco del estudio de pre-inversion a nivel de perfil, el nombre del Proyecto es "Mejoramiento de los servicios financieros del Banco de la Nación a nivel nacional".*

El proyecto se sustenta en el contrato de préstamo Nº 5965/OC-PE, suscrito el 27 de marzo de 2025 entre la República del Perú y el Banco Interamericano de Desarrollo (BID), que constituye la base financiera que da inicio al "Proyecto de Transformación Digital del Banco de la Nación". Este instrumento regula las condiciones y términos para la ejecución del proyecto, que fue declarado formalmente elegible para su ejecución el 23 de septiembre de 2025, tras cumplir satisfactoriamente las condiciones previas establecidas por el BID.

La ejecución del proyecto estará a cargo del Banco de la Nación a través de una Unidad Implementadora especializada[2], que garantizará la correcta administración y supervisión de la transformación digital. Más allá de la renovación tecnológica, esta iniciativa impulsa la inclusión financiera y la conectividad digital, facilitando el acceso a servicios bancarios ágiles, seguros y modernos para todos los peruanos.

Asimismo, para cumplir con sus objetivos, el Proyecto se encuentra estructurado en los siguientes componentes:

Componente 1. Mejoramiento de la Capacidad Institucional

Este componente se enfoca en fortalecer la estructura y competencias del Banco de la Nación para liderar y gestionar la transformación digital. Incluye la definición y ejecución de una estrategia integral de transformación digital que integre la perspectiva de género y diversidad. Se busca fortalecer las capacidades organizativas, mejorar procesos internos, implementar canales digitales, desarrollar competencias digitales del personal y asegurar el alineamiento institucional con las mejores prácticas y normativas nacionales e internacionales.

Componente 2: Mejoramiento de la Capacidad Digital

Este componente aborda la modernización tecnológica del banco a través de la renovación y mejora de sus plataformas digitales y sistemas Core bancarios. Incluye la implementación de nuevas soluciones transaccionales altamente robustas y escalables, que permitan una mayor interoperabilidad entre servicios y canales. Se contempla el desarrollo de funcionalidades para mejorar la atención al usuario final y optimizar la gestión de la información. El componente también promueve el uso de tecnologías modernas y seguras que faciliten la expansión de productos y servicios digitales accesibles para todo tipo de usuarios.

Componente 3: Mejoramiento de la Infraestructura Tecnológica con Ciberseguridad

El tercer componente está orientado a robustecer la infraestructura tecnológica del banco, enfocándose en garantizar altos estándares de seguridad y resiliencia ante ciberataques y eventos adversos. Se prevé la actualización y ampliación de los sistemas de infraestructura física y digital, incluyendo centros de datos y sistemas de contingencia. Asimismo, se fortalecen las capacidades para la gestión de riesgos tecnológicos, ciberseguridad, monitoreo continuo y recuperación ante desastres. Con ello, se asegura la continuidad operativa, la protección de los datos y la confianza de los usuarios en los servicios digitales del Banco.

[2] *En Sesión de Directorio N° 2558, de fecha 05 de mayo de 2025, se aprobó la creación de la Unidad Implementadora Proyecto BN/BID como una Unidad Orgánica Temporal dependiente de la Gerencia General del BN, encargada de la ejecución física y financiera del Proyecto.*

Dado que el proyecto se encuentra en una fase inicial de ejecución se considera oportuno realizar un análisis de brechas mediante una **Evaluación integral del SGSI-C (Sistema de Gestión de Seguridad de la Información y Ciberseguridad)** que permita que el **Componente 3** identifique el nivel de cumplimiento de:

- la **Resolución SBS N° 504-2021**,
- la **Resolución de Secretaría de Gobierno y Transformación Digital N° 003-2023-PCM/SGTD,** la cual establece la implementación y mantenimiento del Sistema de Gestión de Seguridad de la Información en las entidades públicas y
- demás relacionadas al SGSI-C, considerando al menos las indicadas en el Anexo Nº 2 - Marco de Gobierno de Seguridad y Confianza Digital,

que asegure contar con el **Plan de Acción para el cierre de brechas identificadas** como un requisito habilitante para el éxito técnico y legal de la Transformación Digital del Banco de la Nación, logrando que sea cibersegura desde la base, asegurando que el proyecto cumpla con los estándares de seguridad exigidos por el regulador peruano.

El alineamiento estratégico de esta evaluación con los componentes del proyecto incluye, entre otros beneficios, lo siguiente:

Componente del Proyecto BN	**Alineamiento con los componentes**
Componente 1. Mejoramiento de la Capacidad Institucional	La evaluación determinará si la estructura organizacional del Banco está preparada para gestionar los nuevos riesgos digitales. Define los roles que aseguran el fortalecimiento institucional sostenible.
Componente 2: Mejoramiento de la Capacidad Digital	La evaluación situacional permite identificar si los procesos actuales de desarrollo o adquisición de software cumplen con los controles que nuestras leyes y regulaciones exigen antes de la puesta en marcha.
Componente 3: Mejoramiento de la Infraestructura Tecnológica con Ciberseguridad	La evaluación busca identificar las brechas y con ello, el plan de acción para robustecer las capacidades de Ciberseguridad del BN, incluyendo entre otros, políticas, procesos, controles, Centros de Cómputo, Centro de Operaciones de Seguridad.

IV. OBJETIVO

Objetivo General:

El objetivo general del presente servicio es la Evaluación integral del SGSI-C (Sistema de Gestión de Seguridad de la Información y Ciberseguridad) que asegure contar con el **Plan de Acción para el cierre de brechas identificadas** de acuerdo con las actividades previstas como parte del Componente 3 – Mejoramiento de la Infraestructura Tecnológica con Ciberseguridad del Proyecto de Transformación Digital del Banco de la Nación, contribuyendo al logro de sus objetivos institucionales.

Objetivos Específicos:

El objetivo específico del presente servicio es la Evaluación integral del SGSI-C (Sistema de Gestión de Seguridad de la Información y Ciberseguridad) que identifique el nivel de cumplimiento de:

- la **Resolución SBS N° 504-2021**,

- la **Resolución de Secretaría de Gobierno y Transformación Digital N° 003-2023-PCM/SGTD,** la cual establece la implementación y mantenimiento del Sistema de Gestión de Seguridad de la Información en las entidades públicas y
- demás relacionadas al SGSI-C, considerando al menos las indicadas en el Anexo Nº 2 - Marco de Gobierno de Seguridad y Confianza Digital,

y asegure contar con el **Plan de Acción para el cierre de brechas identificadas** de acuerdo con las actividades previstas como parte del Componente 3 – Mejoramiento de la Infraestructura Tecnológica con Ciberseguridad del Proyecto de Transformación Digital del Banco de la Nación, contribuyendo al logro de sus objetivos institucionales.

V. JUSTIFICACIÓN

El Proyecto "Transformación Digital del Banco de la Nación", con el fin de alcanzar sus objetivos estratégicos, se encuentra estructurado en tres componentes, entre los cuales se incluye el Componente 3: Mejoramiento de la Infraestructura Tecnológica con Ciberseguridad.

Componente 3: Mejoramiento de la infraestructura tecnológica con ciberseguridad

El Banco requiere fortalecer su infraestructura tecnológica, con especial énfasis en lo concerniente a ciberseguridad con la finalidad que soporte los sistemas de información que se implementen como parte de este proyecto y garantice la disponibilidad, la integridad y confidencialidad de la información; para ello este componente aborda los siguientes factores:

- **Infraestructura tecnológica,** la cual debe ser mejorada eliminando la redundancia de componentes de arquitectura, optimizando el uso y costo de la infraestructura tecnológica, mejorando la integración entre los diferentes componentes de la arquitectura tecnológica, así como la continuidad operativa de los servicios que brinda el Banco para atender sus procesos misionales. En este sentido, las acciones de este componente se centrarán en:

    - La adquisición e instalación de infraestructura tecnológica de contingencia, incluyendo la implementación de una nube privada en las instalaciones del Banco.
    - Diseñar e implementar el centro de operaciones de ciberseguridad

- **La Ciberseguridad,** la cual debe ser fortalecida con la finalidad de reducir considerablemente la brecha en la implementación de medidas de seguridad críticas según las normas Resolución SBS N° 504-2021. NTP ISO/IEC 27001:2022 y 27002:2022, implementar completamente los servicios y/o niveles de seguridad que exige la SBS, atender e investigar todos los eventos sospechosos de ciberseguridad, aumentar la capacidad de producir software "seguro". En este sentido, el componente debe centrar sus acciones en:

    - Diseñar políticas de gestión de riesgo de ciberseguridad
    - Implementar herramientas de protección y control de acceso
    - Mejorar los planes de contingencia y recuperación ante desastres

En este contexto, se requiere la contratación de una firma consultora para evaluar el cumplimiento del Evaluación integral del SGSI-C (Sistema de Gestión de Seguridad de la Información y Ciberseguridad)

VI. ALCANCE DEL TÉRMINO DE REFERENCIA

Se contratará de una firma Consultora para la Evaluación integral del SGSI-C (Sistema de Gestión de Seguridad de la Información y Ciberseguridad)

El alcance de la consultoría es la Evaluación integral del SGSI-C (Sistema de Gestión de Seguridad de la Información y Ciberseguridad).

En este contexto, se requiere la la contratación de la Evaluación integral del SGSI-C (Sistema de Gestión de Seguridad de la Información y Ciberseguridad)

VII. METODOLOGIA DE TRABAJO

El Banco requiere evaluar el estado de implementación, madurez y efectividad de su Sistema de Gestión de Seguridad de la información y Ciberseguridad, así como el grado de cumplimiento de

- la **Resolución SBS N° 504-2021**,
- la **Resolución de Secretaría de Gobierno y Transformación Digital N° 003-2023-PCM/SGTD,** la cual establece la implementación y mantenimiento del Sistema de Gestión de Seguridad de la Información en las entidades públicas y
- demás relacionadas al SGSI-C, considerando al menos las indicadas en el Anexo Nº 2 - Marco de Gobierno de Seguridad y Confianza Digital,

Mediante esta evaluación, se identificarán brechas, riesgos residuales, oportunidades de mejora para establecer un plan de acción para su adecuación integral conforme a la normativa vigente y mejores prácticas.

El postor brindará un informe que indique resultado de la evaluación integral del SGSI-C del Banco de la Nación y del nivel de cumplimiento e implementación de cada uno de los controles de la ley, reglamentos y resoluciones. Deberá documentar cada uno de los resultados de la evaluación y presentar un Plan de Acción con el detalle de actividades a ejecutar y resultados esperados que permitan evidenciar la subsanación de la brecha.
Como parte de la evaluación de controles, el postor realizará pruebas del cumplimiento de las medidas de seguridad de la información, a los productos, servicios y canales de atención.

VIII. ACTIVIDADES A DESARROLLAR

1. Planificación y Alineamiento

- **Definición del Cronograma:** Elaboración del Plan de Trabajo detallado con hitos y fechas de inicio/fin.
- **Establecimiento del Marco:** Definición de la metodología de evaluación, basada en **Resolución SBS N° 504-2021**, NTP ISO/IEC 27001 y 27002, NIST CSF 2.0, OWASP, ASVS y MASVS que deberá ser aprobada formalmente por el Banco.

2. Fase de Descubrimiento (Recolección de Información)

- **Revisión Documental:** Análisis de políticas, procesos, manuales y procedimientos actuales del Sistema de Gestión de Seguridad de la Información y Ciberseguridad (SGSI-C).
- **Entrevistas:** Reuniones con los responsables de las áreas para entender la operatividad real frente a lo documentado.
- **Revisión de Gobierno:** Revisión de la formalización de roles, responsabilidades y gobernanza del SGSI-C.

3. Evaluación Técnica y Pruebas de Campo

Diagnóstico y/o evaluación de los controles de seguridad de los sistemas y plataformas tecnológicas que soportan productos, servicios y canales de atención, como: App-BN,

Multired Virtual, Pagalo.pe, Banca Empresarial, Red de Cajeros, Cajeros Corresponsales, Red de Agencias

- **Revisión de Configuraciones:** Análisis técnico de los activos críticos.
- **Toma de Evidencias:** Recolección de muestras técnicas, en coordinación con el BN, sin poner en riesgo la disponibilidad de los servicios.

4. Análisis de Brechas (Gap Analysis)

- **Evaluación de Cumplimiento:** Cruce de la información recolectada con las buenas prácticas, las regulaciones y la ley.
- **Medición de Madurez:** Determinar el estado de implementación y la efectividad real del SGSI-C.
- **Identificación de Hallazgos:** Cada brecha encontrada debe estar sustentada con evidencia y clasificada según el nivel de riesgo del Banco o metodología propuesta previamente aprobada por el equipo de trabajo del Banco.

5. Consolidación y Plan de Acción

- **Matriz de Cumplimiento:** Elaboración de un cuadro detallado de cumplimiento por cada artículo de las buenas prácticas, el reglamento y la ley.
- **Diagnóstico Final:** Informe integral del estado de la ciberseguridad del Banco y Programa de Ciberseguridad alineado con NIST CSF 2.0.
- **Hoja de Ruta:** Creación de un **Plan de Acción** que detalle las actividades necesarias, los resultados esperados y el cronograma para subsanar cada brecha identificada.

IX. PRODUCTOS / ENTREGABLES

A continuación, se detallan los productos a considerar:

Producto	Descripción
1	Plan de Trabajo y Cronograma de Actividades
2	Evaluación Técnica de Productos, Servicios y Canales de Atención
3	**Evaluación de cumplimiento del SGSI-C** a. Informe detallado del estado de cumplimiento de la Resolución SBS N° 504-2021 b. Informe detallado del estado de cumplimiento de la NTP ISO/IEC 27001 (incluyendo Anexo A y propuesta de declaración de aplicabilidad), c. Informe detallado del estado de cumplimiento de la NTP ISO/IEC 27002, d. Informe detallado del estado de cumplimiento de NIST CSF 2.0 e. Informe detallado del estado de cumplimiento de Marco de Gobierno de Seguridad y Confianza Digital considerando al menos la legislación, regulación y estándares incluidas en el Anexo Nº 2 - Marco de Gobierno de Seguridad y Confianza Digital f. Informe integral de cumplimiento y efectividad de los requerimientos de seguridad descritos en los puntos a, b, c, d y e
4	Programa de Ciberseguridad, alineado con NIST CSF 2.0
5	Plan de Acción para el cierre de brechas identificadas en los informes del Producto 3
6	Diagnóstico y propuesta de la estructura organizacional del Gobierno y Gestión del SGSI-C
7	Informe Final y Resumen Ejecutivo

X. PLAZO DE EJECUCIÓN DE LA CONSULTORÍA

El plazo total del servicio contratado será de hasta doscientos setenta (270) días calendario, y se contabilizará a partir del día siguiente de la firma del contrato, de acuerdo con el siguiente detalle:

Producto	Plazo
1	Hasta los diez (10) días calendario a partir del día siguiente de la firma del contrato.
2	Hasta los cuarenta (40) días calendario a partir del día siguiente de la firma del contrato
3	Hasta los ciento sesenta (160) días calendario a partir del día siguiente de la firma del contrato.
4	Hasta los ciento noventa (190)días calendario a partir del día siguiente de la firma del contrato.
5	Hasta los doscientos cincuenta (250) días calendario a partir del día siguiente de la firma del contrato.
6	Hasta los doscientos sesenta (260) días calendario a partir del día siguiente de la firma del contrato.
7	Hasta los doscientos setenta (270) días calendario a partir del día siguiente de la firma del contrato.

En caso de que el día de entrega del producto corresponda a un día no laborable, El Consultor presentará el informe correspondiente al día hábil siguiente.

Notificación de observaciones:

1. La Unidad Implementadora de Proyecto (UIP) otorgará la conformidad, en un plazo que no exceda de los 10 días calendario, computados desde el día siguiente de la recepción de los productos/entregables o de la subsanación de las observaciones formuladas por el Contratante, según corresponda.
2. En el caso que, La Unidad Implementadora de Proyecto (UIP) formule observaciones a los productos/entregables, estas deben ser efectuadas en un plazo máximo de diez (10) días calendario siguientes a la presentación de dichos **productos/entregables**, y serán comunicadas por la Coordinación Técnica (o la que haga sus veces).
3. A su vez, La Firma tendrá un plazo de hasta diez (10) días calendario posteriores para el Levantamiento de las Observaciones que correspondan, computable a partir del primer día siguiente de notificada el pliego de observaciones.
4. La Unidad Implementadora de Proyecto (UIP) podrá requerir hasta en dos (2) oportunidades la subsanación de las observaciones. A partir de culminada la última oportunidad, el requerimiento de subsanación podrá formularse bajo apercibimiento de resolución contractual.
5. Por otro lado, en caso La Unidad Implementadora de Proyecto (UIP) **se retrase y no cumpla con realizar las verificaciones necesarias y otorgar la conformidad dentro del plazo**, dicha situación no debe afectar a la Firma con la aplicación de penalidades, siendo que solo aplicará el plazo formal con el que cuenta La Unidad Implementadora de Proyecto (UIP) para su evaluación.

Dentro del plazo de la consultoría no se encuentran comprendidos los plazos que La Unidad Implementadora de Proyecto (UIP) utilice para, revisar, remitir y/o emitir observaciones, aprobaciones, inscripciones y cualquier otro acto administrativo relacionado a las gestiones que demanden los Productos mencionados. Asimismo, no se considera dentro del plazo el levantamiento de observaciones por parte del Consultor de ser el caso.

XI. PRESENTACIÓN Y RECEPCIÓN DEL PRODUCTO/ENTREGABLE

La presentación de los entregables se realizará en formato digital a través de la Mesa de Partes del Banco de la Nación[3], mediante carta dirigida al Coordinador General de la Unidad Implementadora del Proyecto, en el horario vigente para la recepción de documentos. Los entregables se presentarán en formato PDF con firma digital e incluirán los correspondientes archivos en formato editable (Word, Excel y Powerpoint), incluyendo de ser el caso, softwares utilizados y/o el programa que corresponda.

Si el día de entrega del producto / entregable establecido en estos Términos de Referencia, coincide con un día no laborable, se correrá la fecha de entrega hasta el siguiente primer día hábil, sin que sea sujeto de penalidad.

XII. CONFORMIDAD DEL PRODUCTOS/ENTREGABLES

La conformidad de los productos/entregables será realizada por el Coordinador General de la UIP, previo informe emitido por el Coordinador del Componente 3 revisado y aprobado por el Coordinador Técnico.

XIII. RECURSOS Y FACILIDADES A SER PROVISTOS POR LA ENTIDAD

1. Información y Documentación
Para que el proveedor realice la "Revisión Documental" el Banco debe facilitar:

- **Políticas, procesos y procedimientos internos** del SGSI-C.
- Documentación sobre la **Gestión de Riesgos** de Seguridad de la Información.
- Evidencias de la formalización de roles y funciones.
- Información sobre la aplicación de banca virtual (App-BN), Multired Virtual, Pagalo.pe, Banca Empresarial, Red de Cajeros, Cajeros Corresponsales, Red de Agencias.

2. Acceso a Personal y Áreas
El Banco debe garantizar la disponibilidad de su capital humano para:

- **Entrevistas:** Acceso a los responsables de las áreas involucradas para el entendimiento de la organización.
- **Presentaciones:** Participación de las áreas involucradas y la Alta Dirección para la sustentación y aprobación de los entregables.
- **Coordinación:** Equipo de trabajo, incluyendo personal de la Oficina de Seguridad Informática y la Sección Políticas de Seguridad de Información, para la revisión y levantamiento de observaciones.

3. Facilidades Técnicas y Logísticas

- **Ambientes Controlados:** El Banco debe proporcionar entornos seguros para realizar las pruebas de validación mediante el uso de herramientas, previa coordinación

XIV. PERFIL DEL CONSULTOR Y PERSONAL PROPUESTO

PERFIL DE LA FIRMA

Experiencia General

La Firma debe acreditar haber desarrollado por lo menos 3 servicios de implementación y/o evaluación del *SGSI-C* en entidades financieras reguladas por la Superintendencia de Banca, Seguros y AFP del Perú (SBS), que en acumulado no podrán ser menor a dos (02) veces el costo estimado de la contratación, durante un periodo de 5 años a la fecha de la

[3] *https://www.bn.com.pe/mesa-de-partes/mesa-de-partes.asp*

presentación de la expresión de interés.

Se considerarán como válidas, con diferencia de calificación, las experiencias en servicios vinculados al Sistema de Gestión de Seguridad de la Información bajo ISO/IEC 27001 realizados para entidades supervisadas por la SBS y servicios de validación de controles PCI en entidades bajo supervisión de la SBS.

Se considerarán como válidas, con diferencia de calificación, las experiencias entre 5 y 10 años previos a la presentación de la expresión de interés.

Se considerarán como válidas, con diferencia de calificación, las experiencias en servicios bajo otras ISO de la familia 27000, análisis de vulnerabilidades, pruebas de penetración, Ethical Hacking, Red Team, SOC (Centro de Operaciones de Seguridad), análisis de códigos seguros a entidades supervisadas por la SBS, servicios realizados en cumplimiento con el reglamento aprobado por Resolución SBS No 504-2021.

Experiencia Específica

La Firma debe acreditar haber desarrollado por lo menos un (01) servicio de implementación y/o evaluación del *SGSI-C* en una entidad financiera regulada por la Superintendencia de Banca, Seguros y AFP del Perú (SBS) o una entidad regulada por las marcas de tarjetas de pago en el Perú, que en acumulado no podrán ser menor al costo estimado de la contratación, durante un periodo de 5 años a la fecha de la presentación de la expresión de interés.

Se considerarán como válidas, con diferencia de calificación, las experiencias en servicios vinculados al Sistema de Gestión de Seguridad de la Información bajo ISO/IEC 27001 realizados para entidades supervisadas por la SBS y servicios de validación de controles PCI en entidades bajo supervisión de la SBS.

Se considerarán como válidas, con diferencia de calificación, las experiencias entre 5 y 10 años previos a la presentación de la expresión de interés.

Se considerarán como válidas, con diferencia de calificación, las experiencias en servicios como análisis de vulnerabilidades, pruebas de penetración, Ethical Hacking, Red Team, SOC (Centro de Operaciones de Seguridad), análisis de códigos seguros a entidades supervisadas por la SBS, servicios realizados en cumplimiento con el reglamento aprobado por Resolución SBS No 504-2021.

La experiencia general y específica del consultor se acreditará con copia simple de (i) contratos u órdenes de servicios, y su respectiva conformidad o constancia de prestación; o (ii) comprobantes de pago cuya cancelación se acredite documental y fehacientemente, con constancia 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.

Personal propuesto

El Consultor presentará en su propuesta el siguiente ***personal clave*** que será materia de evaluación:

- ✓ **<u>Un (01) Jefe de Proyecto</u>**

Formación académica	Grado de Bachiller en Ingeniería de Sistemas, Redes y Telecomunicaciones, Electrónica, Software o Industrial.
Capacitaciones	Contar con al menos dos (02) certificaciones vigentes:

	CISSP, CISM, CSX, ISO 27001. Se considerará, además, con calificación diferente: CEH, ECSA, CISA, ISO/IEC 27032, CSWAE, CPTE Contar con certificación vigente PMP o SCRUM o 10 años de experiencia específica
Experiencia general	Experiencia mínima de ocho (08) años en el sector público o privado
Experiencia específica	Mínimo **cinco (05) años** liderando servicios de: - Evaluación de cumplimiento **Resolución SBS N° 504-2021** - Auditorías ISO/IEC 27001 y NIST CSF 2.0. - Evaluación de Riesgos de TI o de Seguridad.
Porcentaje de participación	Participación a tiempo completo

- ✓ **Dos (02) Especialista SBS 504**

Formación académica	Grado de Bachiller en Ingeniería de Sistemas, Redes y Telecomunicaciones, Electrónica, Software o Industrial.
Capacitaciones	Contar con al menos una (01) certificación vigente: CISSP, CISM, CSX, ISO 27001. Se considerará, además, con calificación diferente: CEH, ECSA, CISA, ISO/IEC 27032, CSWAE, CPTE
Experiencia general	Experiencia mínima de cinco (05) años en el sector público o privado
Experiencia específica	Mínimo tres (03) años en servicios de: - Evaluación de cumplimiento **Resolución SBS N° 504-2021** - Ethical Hacking o Análisis de Vulnerabilidades. - Pruebas de Seguridad de Software.
Porcentaje de participación	Participación a tiempo completo

- ✓ **Un (01) Especialista ISO/IEC 27001**

Formación académica	Grado de Bachiller en Ingeniería de Sistemas, Redes y Telecomunicaciones, Electrónica, Software o Industrial.
Capacitaciones	Contar con al menos una (01) certificación vigente: CISSP, CISM, CSX, ISO 27001. Se considerará, además, con calificación diferente: CEH, ECSA, CISA, ISO/IEC 27032, CSWAE, CPTE
Experiencia general	Experiencia mínima de cinco (05) años en el sector público o privado
Experiencia específica	Mínimo tres (03) años en servicios de: - Evaluación de cumplimiento ISO/IEC 27001. - Ethical Hacking o Análisis de Vulnerabilidades. - Pruebas de Seguridad de Software.
Porcentaje de participación	Participación a tiempo completo

- ✓ **Un (01) Especialista NIST CSF 2.0.**

Formación académica	Grado de Bachiller en Ingeniería de Sistemas, Redes y Telecomunicaciones, Electrónica, Software o Industrial.
Capacitaciones	Contar con al menos una (01) certificación vigente: CISSP, CISM, CSX, ISO 27001
Experiencia general	Experiencia mínima de cinco (05) años en el sector público o privado
Experiencia específica	Mínimo tres (03) años en servicios de: - Evaluación de cumplimiento NIST CSF 2.0. - Ethical Hacking o Análisis de Vulnerabilidades. - Pruebas de Seguridad de Software.
Porcentaje de participación	Participación a tiempo completo

La formación académica del personal se acreditará mediante copia simple del grado o título profesional.

La capacitación requerida se acreditará mediante copia simple de constancias, certificados, u otros documentos, según corresponda.

La experiencia se acreditará con cualquiera de los siguientes documentos: (i) copia simple de contratos y/u orden de servicio y su respectiva conformidad o (ii) constancias o (iii) certificados o (iv) cualquier otra documentación que, de manera fehaciente acredite la experiencia. Asimismo, se contabilizará desde la obtención de condición de egresado

XV. COORDINACIÓN Y SUPERVISIÓN

La coordinación y supervisión técnica de los alcances técnicos de la consultoría estará a cargo del Coordinador del Componente 3.

La conformidad de los productos/entregables será realizada por el Coordinador General de la UIP, previo informe emitido por el Coordinador del Componente 3 revisado y aprobado por el Coordinador Técnico.

XVI. FORMA Y CONDICIONES DE PAGO

Los pagos se realizarán luego de la presentación y conformidad de los respectivos productos, según se detalla en el siguiente cuadro:

Número de Producto	% Pago
1	
2	10%
3	30%
4	10%
5	30%
6	10%
7	10%

El pago se efectuará dentro de los quince (15) días calendarios siguientes de la presentación de los productos señalados en los presentes términos de referencia, los cuales deberán adjuntar el respectivo comprobante de pago y la conformidad del producto correspondiente.

XVII. ANTICIPO

XVIII. DERECHOS DE PROPIEDAD, CONFIDENCIALIDAD Y SEGURIDAD DE LA INFORMACION

La Firma deberá declarar que en la medida de que el servicio prestado es por encargo, y el costo de su ejecución es asumida por UIP - BN; todo producto o materiales (impresos, estudios, informes, gráficos, programas, software de computación u otros), que se genere por el servicio, es de propiedad de la UIP - BN, no constituyéndose títulos de propiedad, derechos de autor y otro tipo de derechos para El Consultor; el mismo que a mérito de los presente TDR, cede en forma exclusiva y gratuita, sin generar retribución adicional a lo estipulado en el presente documento.

La Firma se obliga a mantener la confidencialidad y reserva absoluta en el manejo de información a la que se tenga acceso y que se encuentre relacionada con la prestación, quedando prohibido revelar dicha información a terceros (excepto al BID), además del cumplimiento de las Políticas de Seguridad de la Información del BN y sus procedimientos vigentes, establecidos para asegurar su cumplimiento.

En tal sentido, la Firma deberá dar cumplimiento a todas las políticas y estándares definidos por la Entidad, en materia de seguridad de la información. Dicha obligación comprende la información que se entrega, como también la que se genera durante la realización de las actividades y la información producida una vez que se haya concluido la prestación. Dicha información puede consistir en mapas, dibujos, fotografías, mosaicos, planos, informes, recomendaciones, cálculos y demás documentos e información compilados o recibidos por El Consultor.

IXX. ANTICORRUPCIÓN Y ANTISOBORNO

A la suscripción de este contrato, la Firma 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 proceso de contratación o cualquier servidor de la entidad contratante.

Asimismo, La Firma 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, la Firma 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 de la UIP -BN, 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, la Firma 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.

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 medias impiden el inicio de las acciones civiles, penales y administrativas a que hubiera lugar.

La Firma se compromete en cumplir la política antisoborno del programa aprobada y regulada mediante resolución la cual se encuentra disponible en el siguiente enlace: web: https://cdn.www.gob.pe/uploads/document/file/3248111/Resoluci%C3%B3n%20de%20Contralor%C3%ADa%20N%C2%B0%20229-2022-CG.pdf.pdf?v=1654888578.

XX. PENALIDAD

a) Penalidad diaria por mora

- La penalidad se aplica por cada día de retraso injustificado en la prestación de la ejecución del servicio.
- Penalidad diaria:
  Penalidad diaria = (0.10 x Monto del contrato) / (F x Plazo en días)
  Donde F = 0.40

b) Consideraciones generales:

- Cuando la Firma no cumpla con **la presentación de los productos/entregables de acuerdo con las características y condiciones estipuladas**, se **considera como no presentado**, aplicándose la penalidad por cada día de retraso hasta su presentación, en este escenario, la Entidad comunicará al Consultor dicho incumplimiento.
- La penalidad se deducirá de pagos parciales o finales (el criterio de aplicación de la penalidad será definido exclusivamente por la entidad).
- Se exceptúa la penalidad si la Firma acredita objetivamente que el retraso no le es imputable.
- Al alcanzar el límite máximo del 10 % acumulado de las penalidades por mora, la Entidad podrá resolver el contrato por incumplimiento.

c) Identificación del retraso injustificado:

- Cuando El Consultor **subsana las observaciones dentro del plazo otorgado**, no se aplicará penalidad.
- Cuando El Consultor **cumple con levantar las observaciones fuera del plazo otorgado en las dos** (2) **rondas de observaciones debidamente notificadas,** se considera la aplicación de penalidad por cada día de retraso contabilizado desde el día siguiente de la fecha de vencimiento del plazo otorgado.
- **Cuando vencido el plazo otorgado** para subsanar las dos (02) rondas de observaciones y La Firma/Proveedor/Contratista presenta dentro del plazo otorgado, pero **persisten las observaciones**[4]**.** La UIP en mérito a su evaluación técnica podrá

[4] Las Observaciones formuladas contarán con las rondas que se establezcan en el contrato, en caso surjan **nuevas observaciones que no hayan podido ser identificadas anteriormente, considerando la complejidad y la naturaleza de cada contratación**, **se procederá con reiniciar las rondas establecidas para estos casos específicos**.

otorgar periodos adicionales **para el levantamiento de la persistencia de observaciones**, sin perjuicio de las penalidades respectivas. En este caso, se aplica la penalidad computando los días de retraso **desde el vencimiento del plazo otorgado con la primera notificación de observación, hasta que la subsane,** incluyéndose el plazo formal con el que cuenta la UIP para su evaluación.

XXI. OTRAS CONSIDERACIONES

- Subcontratación: cada firma no podrá subcontratar para ejecutar el servicio de consultoría.
- Confidencialidad: cada firma guardará reserva de los conocimientos e información relacionada con el servicio al que tenga acceso, quedando prohibido de revelar dicha información a terceros.
- Responsabilidad por vicios ocultos: cada firma es el responsable por la calidad ofrecida y los vicios ocultos del servicio realizado, por un (01) año, contado a partir de la emisión de la conformidad del último entregable o producto.

ANEXO N° 1

CARACTERÍSTICAS Y ESTRUCTURA DE LOS DOCUMENTOS A SER PRESENTADOS POR TIPO DE PRODUCTO

1. **ESPECIFICACIONES GENERALES**
   Los informes deben redactarse teniendo en cuenta las siguientes especificaciones:

   1. Letra arial 11.
   2. Espacio simple.
   3. Carátula indicando entre otros, nombre de consultoría, nombre de consultor y número de producto.
   4. Impresión a doble cara.
   5. Páginas numeradas en la parte inferior derecha.
   6. Índice numerado de páginas.

2. **ESPECIFICACIONES POR TIPO DE PRODUCTO**

   1.1 **Plan de Trabajo**
   Tendrá la siguiente estructura:

   1. Carátula
   2. Índice
   3. Introducción
   4. Objetivo de consultoría
   5. Productos a alcanzar
   6. Actividades a cumplir por cada producto
   7. Cronograma de actividades (Gantt), sujeto a los términos de referencia
   8. Descripción de la metodología de referencia a emplear
   9. Glosario de términos
   10. Anexo(s)

   1.2 Informe del Producto
   Tendrá la siguiente estructura:

   1. Carátula
   2. Resumen ejecutivo
   3. Índice
   4. Introducción
   5. Objetivo de consultoría
   6. Productos alcanzados que contengan lo solicitado.
   7. Grado de cumplimiento del producto
   8. Dificultades y limitaciones encontradas
   9. Conclusiones y Recomendaciones
   10. Glosario de términos
   11. Anexo(s)

3. CONSIDERACIONES GENERALES DEL PRODUCTO PARA TENER EN CUENTA:

- Tapa del documento en el que se precisa el nombre de la consultoría, nombre del producto, el nombre del autor, la fecha de presentación.
- Incluir índice de capítulos, así como de tablas o cuadros y de gráficos cuando corresponda.
- Incluir una lista de abreviaturas o acrónimos, en caso de que se usen siglas en el documento.
- Incluir un glosario de términos que requieran de explicación inicial para facilitar la lectura del documento.
- El resumen ejecutivo dará cuenta de los aspectos más relevantes del trabajo encargado.
- De acuerdo con la naturaleza y características del producto a entregar, el documento se dividirá en capítulos, los que estarán debidamente numerados.

- Las páginas del documento estarán debidamente numeradas.
- Las referencias bibliográficas deberán incluirse al final del documento.
- El consultor presentará sus entregables Mesa de Partes del Banco de la Nación
- El Consultor se compromete a ceder los derechos patrimoniales de autor de los productos y documentos elaborados.
- El Consultor se compromete a guardar reserva de toda aquella información interna a la que tenga acceso para la ejecución de esta consultoría, cualquier uso de esta información, deberá ser autorizada previamente por el Banco de la Nación.
- Todos los productos deberán de ser entregados y sustentados en la forma y plazos que se indican en estos Términos de Referencia.
- A la entrega del último producto, se adjuntarán las bases de datos, códigos de programación u otros materiales utilizados por El Consultor o que le hayan sido entregados a este por el Banco de la Nación durante el proceso de ejecución de la consultoría.

ANEXO N° 2

MARCO DE GOBIERNO DE SEGURIDAD Y CONFIANZA DIGITAL

1. Decreto Supremo N° 029-2021-PCM que aprueba el Reglamento del Decreto Legislativo Nº 1412, que aprueba la Ley de Gobierno Digital, y establece disposiciones sobre las condiciones, requisitos y uso de las tecnologías y medios electrónicos en el procedimiento administrativo; en lo que respecta como mínimo a los artículos de los siguientes capítulos:
   - TÍTULO VI: INTEROPERABILIDAD
     - CAPÍTULO II: GESTIÓN DEL MARCO DE INTEROPERABILIDAD DEL ESTADO PERUANO
   - TÍTULO VII: SEGURIDAD DIGITAL
     - CAPÍTULO III: EQUIPO DE RESPUESTAS ANTE INCIDENTES DE SEGURIDAD DIGITAL
     - CAPÍTULO IV: SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN
2. Decreto Supremo N° 157-2021-PCM que aprueba el Reglamento del Decreto de Urgencia N° 006.2020 que crea el Sistema Nacional de Transformación Digital. En lo que respecta como mínimo a los artículos de los siguientes capítulos:
   - CAPÍTULO III: GOBERNANZA Y GESTIÓN DIGITAL EN LAS ENTIDADES PÚBLICAS
3. Decreto Supremo N° 126-2025-PCM que aprueba el Reglamento del Decreto de Urgencia N° 007.2020 que aprueba el marco de confianza digital y dispone medidas para su fortalecimiento. En lo que respecta como mínimo a los artículos de los siguientes capítulos:
   - TITULO II: SEGURIDAD DIGITAL
     - CAPITULO I: MEDIDAS PARA LA SEGURIDAD DIGITAL EN LA ADMINISTRACIÓN PUBLICA
     - CAPITULO III: MEDIDAS DE LOS PROVEEDORES DE SERVICIOS DIGITALES
     - CAPITULO V: INCIDENTES DE SEGURIDAD DIGITAL
4. Resolución N° 003-2023-PCM/SGTD DE SECRETARÍA DE GOBIERNO Y TRANSFORMACIÓN DIGITAL que establece la implementación y mantenimiento del Sistema de Gestión de Seguridad de la Información en las entidades públicas