TÉRMINO DE REFERENCIA DE SERVICIO

1. **AREA USUARIA:** Sección Capacitación.

2. **OBJETO DE LA CONTRATACIÓN:**
Servicio de capacitación: **Ítem 1**: Seguridad de la Información, Ciberseguridad y Protección de Datos Personales, en el Sector Financiero. **Ítem 2**: Ciberseguridad en Banco **Ítem 3:** Programa de Especialización en Seguridad de la Información y Ciberseguridad aplicado a Instituciones Financieras

3. **FINALIDAD DEL REQUERIMIENTO:**
La presente solicitud tiene como finalidad desarrollar competencias técnicas y estratégicas para la gestión de la política de Ciberseguridad en cumplimiento con la normativa vigente, reducir vulnerabilidades y asegurar el cumplimiento con estándares regulatorios en materia de procesos de TI.

4. **OBJETIVOS DE LA CONTRATACIÓN:**
El área solicitante tiene como objetivo desarrollar conocimientos sobre la normativa vigente en relación a Seguridad de la Información, Ciberseguridad y Protección de Datos Personales, con la finalidad de brindar soporte normativo a las áreas usuarias; asimismo, ejecutar auditorías especializadas en procesos de TI alineado con normas dadas por la SBS.

5. **PLAN OPERATIVO INSTITUCIONAL – POI**
O.E.I. 08: Optimizar la eficiencia de los procesos

6. **ANTECEDENTES**
(No corresponde)

7. **ALCANCES Y DESCRIPCIÓN DEL SERVICIO**

SERVICIO DE CAPACITACIÓN	
Concepto	**Descripción**
Actividad de Capacitación	**Ítem 1**: Seguridad de la Información, Ciberseguridad y Protección de Datos Personales, en el Sector Financiero. **Ítem 2**: Ciberseguridad en Banco. **Ítem 3:** Programa de Especialización en Seguridad de la Información y Ciberseguridad aplicado a Instituciones Financieras
Requerimiento	Necesidad Programada en el Plan de Capacitación 2026.
Modalidad	**Ítem 1, 2 y 3**: Presencial
Horas	**Ítem 1**: 15 horas cronológicas. **Ítem 2**: 18 horas cronológicas. **Ítem 3**: 42 horas cronológicas.
Frecuencia	**Ítem 1**: 2 veces por semana. **Ítem 2**: 2 o 3 veces por semana. **Ítem 3**: 2 veces por semana.

Alcance	**Ítem 1**: Hasta 20 trabajadores. **Ítem 2**: Hasta 06 trabajadores. **Ítem 3**: Hasta 07 trabajadores.
Público objetivo	**Ítem 1**: Trabajadores de la Gerencia de Oficialía de Cumplimiento Normativo y Conducta de Mercado. **Ítem 2**: Trabajadores de la Gerencia de Auditoría Interna **Ítem 3**: Trabajadores de la Gerencia de Riesgos
TEMARIO **Ítem 1: Seguridad de la Información, Ciberseguridad y Protección de Datos Personales, en el Sector Financiero**	Módulo 1: Marco legal de la seguridad de la información • Seguridad de la información en el sector financiero • Información financiera, datos personales y datos personales sensibles • Principios de confidencialidad, integridad y disponibilidad • Riesgos legales y de seguridad asociados a la gestión de la información
	Módulo 2: Protección de datos personales – Enfoque legal • Ley N.° 29733 y su Reglamento • Principios de protección de datos personales • Derechos ARCO y consentimiento • Obligaciones del responsable y encargado del tratamiento • Registro de bancos de datos personales • Evaluaciones de Impacto en datos personales
	Módulo 3: Ciberseguridad y riesgos digitales • Concepto de ciberseguridad y amenazas digitales • Ciberataques más frecuentes en el sector financiero (phishing, ransomware, malware, ingeniería social) • Responsabilidades legales frente a incidentes de ciberseguridad • Rol del abogado en la gestión de riesgos cibernéticos
	Módulo 4: Incidentes, cumplimiento normativo y régimen sancionador • Brechas de seguridad de la información y ciberseguridad • Deber de notificación ante incidentes • Fiscalizaciones y supervisión de la SBS • Procedimientos administrativos sancionadores • Responsabilidades administrativas, civiles y penales
TEMARIO **Ítem 2: Ciberseguridad en Banco.**	• Fundamentos de la Ciberseguridad, aplicado a una entidad financiera • Definiciones • Confidencialidad, Integridad, Disponibilidad (CIA triad) • Identidad digital, autenticación, autorización • Amenazas en el sector financieros • Fraude digital (phishing, smishing, vishing) • Malware bancario • Ataques a apps móviles • Credential stuffing • Tipos de ataques (vshing, pshing, ingeniería social, entre otros) • Gobierno y regulación de la Ciberseguridad • Regulación bancaria – SBS (Gestión de seguridad de la información, Continuidad del negocio y Gestión de terceros) • Cobit y Gobierno de TI • ISO 27001 y 27002 • NIST Cybersecurity Framework • Cultura de Seguridad

BANCO DE LA NACIÓN – Karina Lisett Gutarra Aguirre – Subgerencia Desarrollo del Talento (e)

BANCO DE LA NACIÓN – Jhonny P. García Muñoz – Sección Capacitación (e)

BANCO DE LA NACIÓN – Javier Chumpitaz Lujan – Analista – Sección Capacitación

BANCO DE LA NACIÓN – Rut[illegible] – Analista (e) – Sección Capacitación

	• Gestión de riesgos en Ciberseguridad • Identificación de riesgos • Internos (empleados) • Externos (hackers) • Tecnológicos (fallas sistemas) • Matriz de riesgos (construcción de la matriz, determinación de la probabilidad e impacto) • Evaluación de impacto financiero y reputacional • Tratamiento al riesgo • Planes de acción (KRIs y tratamiento del riesgo) • Auditoria de Ciberseguridad, planificación, ejecución, informe • Planificación basada en riesgos (identificación de procesos crítico, qué auditar y qué no - "scoping inteligente") • Técnicas de TI aplicables • Auditoria en canales digitales • Auditoría de la infraestructura tecnológica (servidores, base de datos, Active directory) • Evaluación de controles • Determinación de hallazgos • Accesos a los servidores y base de datos • Gestión de incidentes de Ciberseguridad. • Taller integrador, caso práctico de auditoría a un canal digital • Identificación y Evaluación de riesgos • Identificación y formulación de hallazgos • Trabajo Final: Elaboración de Informe
TEMARIO **Item 3: Programa de Especialización en Seguridad de la Información y Ciberseguridad aplicado a Instituciones Financieras**	Módulo 1: Auditor Líder en la Norma ISO 27001 - Seguridad de la información, ciberseguridad y protección de la privacidad • Principios y conceptos fundamentales de un sistema de gestión de seguridad de la información (SGSI) basado en ISO/IEC 27001. • Interpretar los requisitos de ISO/IEC 27001 para un SGSI desde la perspectiva de un auditor. • Evaluar la conformidad del SGSI con los requisitos de ISO/IEC 27001, de acuerdo con los principios y conceptos fundamentales de auditoría. • Planificar, realizar y cerrar una auditoría de cumplimiento con ISO/IEC 27001, de acuerdo con los requisitos de ISO/IEC 17021-1, las directrices de ISO 19011 y otras prácticas recomendadas de auditoría. • Gestionar un programa de auditoría con base en ISO/IEC 27001 Módulo 2: Ciberseguridad según el marco de referencia NIST-CSF 2.0 2.1 Fundamentos de ciberseguridad basado en NIST CSF ✓ Principales componentes del Framework CSF 2.0 ✓ Núcleo del Marco de trabajo NIST CSF 2.0 (Gobierno, Identificar, Proteger, Detectar, Responder y Recuperar). ✓ Perfiles del marco de trabajo. ✓ Establecimiento de un programa de ciberseguridad. ✓ Niveles de implementación (TIER) del marco de trabajo y entre otros disponibles.

	✓ Recursos disponibles (FFIEC, NIST Serie 800, ISO, COBIT 2019, entre otros) y relacionados con el marco de trabajo. 2.2 Auditoría de ciberseguridad ✓ Principios básicos de la auditoría. ✓ Etapas de la auditoría (Planificación, Ejecución y Cierre). ✓ Marcos de trabajos y estándares de ciberseguridad relacionados al NIST CSF. ✓ Elaborar un programa de auditoría en ciberseguridad basado en NIST CSF 2.0 2.3 Desarrollar un caso práctico ✓ Realizar una evaluación de riesgos de ciberseguridad. ✓ Aplicar el programa de auditoría basado en NIST CSF 2.0 ✓ Desarrollar un informe de auditoría de ciberseguridad. 3. Hacker ético certificado (CEH) ✓ Introducción al hacking ético, fundamentos esenciales de la seguridad de la información. ✓ Huellas y reconocimiento, utilizar las técnicas y herramientas más recientes para realizar footprinting y reconocimiento, una fase clave y fundamental en el proceso de hacking ético. ✓ Scanning Networks, diferentes técnicas de escaneo de red y contramedidas. ✓ Enumeración, diversas técnicas de enumeración, incluyendo exploits en Border Gateway Protocol (BGP) y Network File Sharing (NFS), junto con sus contramedidas. ✓ Análisis de vulnerabilidades, identificar vulnerabilidades de seguridad en la red, la infraestructura de comunicación y los sistemas finales de una organización objetivo. Además, conoce los distintos tipos de evaluación de vulnerabilidades y las herramientas más utilizadas para llevarlas a cabo. ✓ Hackeo de sistemas, conocimientos sobre diversas metodologías de hacking de sistemas empleadas para descubrir vulnerabilidades en redes y equipos, incluyendo la esteganografía, los ataques de esteganálisis y las técnicas para cubrir huellas. ✓ Amenazas de malware, conocimientos sobre los distintos tipos de malware (troyanos, virus, gusanos, entre otros), así como sobre malware APT y fileless. Aprende procedimientos de análisis y las contramedidas más efectivas para su detección y prevención. ✓ Olfatear, técnicas de rastreo de paquetes y su aplicación en la detección de vulnerabilidades de red, así como las contramedidas para protegerte frente a este tipo de ataques. ✓ Ingeniería social, conceptos y técnicas de ingeniería social, incluyendo cómo identificar intentos de fraude, auditar vulnerabilidades a nivel humano y proponer contramedidas efectivas. ✓ Denegación de servicio, distintas técnicas de ataque de denegación de servicio (DoS) y de denegación de servicio distribuido (DDoS), así como sobre las estrategias de protección más efectivas frente a ellos. ✓ Secuestro de sesiones, diferentes técnicas de secuestro de sesiones utilizadas para identificar debilidades en la gestión de sesiones a nivel de

BANCO DE LA NACION
Karina Lisett Guevara Aguirre
Subgerenta (e)
Subgerencia Desarrollo del Talento

BANCO DE LA NACION
Jhonny R. García Muñoz
Jefe (e)
Sección Capacitación

BANCO DE LA NACION
Javier Chumpitaz Lujan
Analista
Sección Capacitación

BANCO DE LA NACION
Ruby Paredes Leiva
Analista (e)
Sección Capacitación

	red, autenticación, autorización y criptografía, junto con sus contramedidas. ✓ Cómo evadir sistemas de detección de intrusos (IDS), firewalls y honeypots, Aprende sobre firewalls, sistemas de detección de intrusiones (IDS) y técnicas de evasión de honeypots, así como sobre las herramientas utilizadas para auditar el perímetro de una red en busca de debilidades y sus contramedidas. ✓ Hackeando servidores web, información sobre los ataques a servidores web, incluyendo metodologías integrales utilizadas para auditar vulnerabilidades en infraestructuras de servidores y las contramedidas correspondientes. ✓ Hackeando aplicaciones web, información sobre los ataques a aplicaciones web, incluyendo metodologías integrales de hacking utilizadas para auditar vulnerabilidades y las contramedidas correspondientes. ✓ Inyección SQL, las técnicas de ataque de inyección SQL, los métodos de evasión y las contramedidas para prevenirlas. ✓ Hackeando redes inalámbricas, diferentes tipos de cifrado, las principales amenazas, metodologías y herramientas de hacking, así como las herramientas de seguridad y contramedidas aplicadas a redes inalámbricas. ✓ Hackeando plataformas móviles, principales vectores de ataque en plataformas móviles, técnicas de hacking en Android e iOS, gestión de dispositivos móviles, pautas de seguridad y herramientas de protección. ✓ Hacking de IoT y OT, distintos tipos de ataques dirigidos al Internet de las Cosas (IoT) y a la Tecnología Operativa (OT), incluyendo metodologías y herramientas de hacking, así como las contramedidas para enfrentarlos. ✓ Computación en la nube, conceptos clave de la computación en la nube, incluyendo tecnologías de contenedores y computación sin servidor, así como las principales amenazas, ataques, metodologías de hacking y las herramientas y técnicas de seguridad en la nube. ✓ Criptografía, Obtén información sobre algoritmos de cifrado, herramientas de criptografía, infraestructura de clave pública (PKI), cifrado de correo electrónico y de disco, así como sobre ataques criptográficos y herramientas de criptoanálisis.

BANCO DE LA NACION – Karina Liseth Guerra Aguirre – Subgerente (e) – Subgerencia Desarrollo del Talento

BANCO DE LA NACION – Jhonny R. Garcia Muñoz – Jefe (e) – Sección Capacitación

BANCO DE LA NACION – Javier Chumpitaz Lujan – Analista – Sección Capacitación

De corresponder un cambio del docente, el proveedor deberá notificar, vía correo electrónico, al área usuaria con un mínimo de 15 días calendario adjuntando la documentación que acredite el cumplimiento de la formación académica, certificación y experiencia del docente propuesto, el cual debe ser aprobado por el área usuaria o caso contrario estará sujeto a la penalidad correspondiente.

BANCO DE LA NACION – Ruby Paredes Lora – Analista (e) – Sección Capacitación

Garantía:
(No corresponde).

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

Asimismo, para la contratación de personas naturales, el área usuaria deberá indicar, en base al objeto de contratación y actividades a desarrollar, el contratista **NO** se constituye como **SUJETO OBLIGADO** para presentar declaración jurada de intereses.

La presente 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 del proveedor para servicios son:
    - Persona natural o 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.

HABILITACIÓN
No corresponde

EXPERIENCIA EN LA ESPECIALIDAD
El postor deberá acumular el equivalente de experiencia a S/50,000.00 (cincuenta mil con 00/100 soles) por la contratación de servicios iguales o similares al objeto de contratación, correspondientes a los Ítems 1, 2 y 3, durante los últimos cinco (5) años anteriores a la fecha de la presentación de su cotización, que se computaran desde la fecha de conformidad o emisión del comprobante de pago, según corresponda:

Se consideran servicios y/o capacitaciones similares, en relación con los Ítems 1, 2 y 3 del presente servicio de capacitación, aquellos relacionados con capacitación en
:

- Continuidad del negocio
- Gestión de Riesgos
- Seguridad Tecnológica
- Gestión de la Seguridad
- Protección de Datos
- Gestión de Fraudes
- Gestión de Riesgo Modelo.
- Auditoria de la Continuidad de Negocio y Modelación de Riesgo de Mercado.
- Sistema de Gestión de Seguridad de la Información.
- Sistema Integral de Gestión y Administración del Riesgo.
- Sistema de Gestión de Riesgos.
- Ciberseguridad

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.

PERSONAL PROPUESTO

ITEM 1: Seguridad de la Información, Ciberseguridad y Protección de Datos Personales, en el Sector Financiero

1) **Formación Académica:**
Titulado en Ingeniería de Sistemas

Acreditación: Con copia simple de constancia o diploma o título que acredite la formación académica y/o con registro en la SUNEDU.

2) **Certificación u otro requisito:**
Master en Administración de Empresas y Certificación en Soluciones de Privacidad de Datos o Certificación en Lead Auditor 27001

Acreditación:
Se acreditará con copia simple de constancias o certificados y/o con registro en SUNEDU.

Experiencia:
Mínima 4 años en el dictado de cursos en entidades públicas o privadas en temas relacionados a: Seguridad de la información y/o Ciberseguridad y/o Protección de Datos y/o Gestión de tecnologías de la información y/o Continuidad del Negocio y/o Gestión de Riesgos y/o Gestión de Fraudes y/o afines.

Acreditación:
La experiencia 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.

ITEM 2: Ciberseguridad en Banco

3) **Formación Académica:**
Titulado en Ingeniero de Computación y Sistemas

Acreditación: Con copia simple de constancia o diploma o título que acredite la formación académica y/o con registro en la SUNEDU.

4) **Certificación u otro requisito:**
Magister en Administración de Empresas, Diplomado en Gestión de Servicios de TI

Acreditación:
Se acreditará con copia simple de constancias o certificados y/o con registro en SUNEDU.

Experiencia:
Mínimo 2 años en el dictado de cursos en entidades públicas o privadas en temas relacionados a:

- Protección de Datos.
- Gestión de Riesgo Modelo.
- Auditoria de la Continuidad de Negocio y Modelación de Riesgo de Mercado.
- Sistema de Gestión de Seguridad de la Información.
- Sistema Integral de Gestión y Administración del Riesgo.
- Sistema de Gestión de Riesgos.

Acreditación:
La experiencia 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.

ITEM 3: Programa de Especialización en Seguridad de la Información y Ciberseguridad aplicado a Instituciones Financieras

5) **Formación Académica:**
Titulado en Ingeniería de Sistemas o Ingeniería Electrónica o Ingeniería Informática.

Acreditación: Con copia simple de constancia o diploma o título que acredite la formación académica y/o con registro en la SUNEDU.

6) **Certificación u otro requisito:**
Maestro en Product Manager o Maestro en Administración de Negocios o Maestro en Ingeniería de Sistemas o Certificado Trainer en PECB ISO/IEC 27001 Lead Implementer o PECB ISO/IEC 27001 Lead Auditor.

Acreditación:
Se acreditará con copia simple de constancias o certificados y/o con registro en SUNEDU.

Experiencia:
Mínima 4 años en el dictado de cursos en entidades públicas o privadas en temas relacionados a: Seguridad de la información y/o Ciberseguridad y/o Protección de Datos y/o Gestión de tecnologías de la información y/o Continuidad del Negocio y/o Gestión de Riesgos y/o Gestión de Fraudes y/o afines.

Acreditación:
La experiencia 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 de capacitación consta de los siguientes entregables:

Periodo de la prestación del Servicio	Entregable(s)
Será de 2 días de anticipación al inicio de las actividades en coordinación con el área usuaria.	**Entregable N° 01** Entrega de material de estudio físico y virtual (PPT y/o lecturas)
Será máximo a los 20 días calendario, contados a partir de finalizada la actividad de capacitación.	**Entregable N° 02** ✓ La asistencia consolidada deberá remitirse al finalizar todas las sesiones programadas. ✓ Al concluir el proceso formativo, se deberá remitir un informe final que incluya un resumen de la ejecución, recomendaciones para futuras ediciones y el registro de incidencias, en caso correspondan. ✓ Al finalizar la capacitación, el proveedor deberá realizar una evaluación de conocimientos a todos los participantes. ✓ Certificados digitales individuales donde debe indicar apellidos y nombres en mayúscula de los participantes aprobados (nota mínima aprobatoria 14 y asistencia mínima 75%) ✓ Encuesta de satisfacción (formato proporcionado por la sección capacitación) ✓ Reporte de examen o evaluación de conocimientos o trabajos de aplicación (Sólo para el Ítems 3)

BANCO DE LA NACION - Karina Lisett Gutiérrez Aguirre - Subgerenta (e) - Subgerencia Desarrollo del Talento

BANCO DE LA NACION - Jhonny R. García Muñoz - Jefe (e) - Sección Capacitación

BANCO DE LA NACION - Javier Chumpitaz Lujan - Analista - Sección Capacitación

BANCO DE LA NACION - Paredes Jara - Analista (e) - Sección Capacitación

13. ÉTICA, ANTICORRUPCIÓN Y ANTISOBORNO:

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
No corresponde

15. SEGURO COMPLEMENTARIO DE TRABAJO DE RIEGO
No corresponde

16. RECURSOS A SER PROVISTOS DEL PROVEEDOR
No corresponde

17. PLAZO DE EJECUCIÓN DEL SERVICIO
El servicio se desarrollará en un plazo de hasta **120** días calendarios, computados a partir del día siguiente hábil de la notificación de la contratación en el PLADICOP y/o vía correo electrónico

18. LUGAR DE PRESTACIÓN DEL SERVICIO
La presentación del servicio se realizará en Av. Javier Prado Este 2499 – San Borja

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/) de la siguiente manera:

Al finalizar las actividades y la remisión del entregable N°2, el importe total asignado para la ejecución

del Item 1.
Al finalizar las actividades y la remisión del entregable N°2, el importe total asignado para la ejecución del Item 2.
Al finalizar las actividades y la remisión del entregable N°2, el importe total asignado para la ejecución del Item 3.

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

- Carta simple dirigida a la Subgerencia de Compras.
- Comprobante de pago.
- Copia simple del documento de contratación.
- Acta de conformidad original

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 09:00 am 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 Sección Capacitación, previa verificación del cumplimiento del servicio a través de una lista de chekeo, en un plazo máximo de (7) días calendario del correo de confirmación de los entregables 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:

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

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 y/o consultoría, se podrá establecer otras penalidades distintas a la penalidad por mora

Otras Penalidades			
N°	Supuestos de aplicación de penalidad	Forma de cálculo	Procedimiento
1	No cumplir con el plazo establecido para notificar el cambio del docente.	4% del importe del servicio	Mediante correo electrónico, la Sección Capacitación comunicará el motivo de la penalización.

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 contratación, en los siguientes casos:

a. Por incumplimiento de alguna de LAS PARTES de las obligaciones asumidas en los términos de referencia, para lo cual la parte perjudicada con el incumplimiento deberá notificar a la otra parte comunicando la causal invocada.
b. Por incumplimiento del requerimiento de presentar la Declaración Jurada de Intereses conforme a las normas aplicables, o la presentación tardía, incompleta o falsa, solo en el caso que el servicio sea prestado por persona natural con obligación de presentar declaración jurada de intereses de acuerdo con lo señalado por el área usuaria.
c. El BANCO puede resolver la contratación cuando la penalidad aplicada excede el 10% del monto contractual.

d. De corresponder a servicios profesionales de asesoría, servicios de consultoría y servicios legales: la presentación con información inexacta o falsa de la Declaración Jurada de Prohibiciones e Incompatibilidades a que se hace referencia en la Ley de prevención y mitigación del conflicto de intereses en el acceso y salida de personal del servicio público. Asimismo, en caso se incumpla con los impedimentos señalados en el artículo 5 de dicha ley se aplicará la inhabilitación por cinco años para contratar o prestar servicios al Estado, bajo cualquier modalidad.
e. Paralización o reducción injustificada de la ejecución de la prestación, pese a haber sido requerido para corregir tal situación.
f. Por mutuo acuerdo entre el proveedor y el Banco de la Nación, previa solicitud el área usuaria.
g. Por caso fortuito o fuerza mayor, que imposibilite al Banco de la Nación de manera definitiva continuar con la contratación.
h. Por incumplimiento de la cláusula de 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 GESTIÓN 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-homologacion-aprobadas.php).

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

FIRMA Y SELLO / ÁREA USUARIA