

TÉRMINO DE REFERENCIA DE SERVICIO

1. **ÁREA USUARIA:** Sección Capacitación
2. **OBJETO DE LA CONTRATACIÓN:** Servicio de capacitación: Desarrollo seguro en plataformas mainframe y distribuido en entidades financieras.
3. **FINALIDAD DEL REQUERIMIENTO.**
La presente solicitud tiene como finalidad contratar una capacitación especializada en Desarrollo seguro en plataformas mainframe y distribuido en entidades financieras, con el objetivo de fortalecer las competencias técnicas del personal involucrado en el diseño, desarrollo, implementación y mantenimiento de sistemas críticos, promoviendo el uso de prácticas seguras que garanticen la integridad, confidencialidad y disponibilidad de la información en entornos financieros tanto centralizados como distribuidos.
4. **OBJETIVOS DE LA CONTRATACIÓN**
El área solicitante tiene como finalidad desarrollar competencias técnicas y metodológicas en prácticas de desarrollo seguro, orientadas a plataformas mainframe y distribuidas, a fin de mejorar la capacidad institucional para prevenir vulnerabilidades, mitigar riesgos y asegurar el cumplimiento de normativas de seguridad en el ciclo de vida del software. Se busca fomentar la aplicación de estándares internacionales, la integración de controles de seguridad desde las primeras fases del desarrollo y la colaboración efectiva entre equipos técnicos en entornos complejos y de alta criticidad operativa.
5. **PLAN OPERATIVO INSTITUCIONAL- POI**
El vínculo que tiene el objeto de la contratación OEI 10: Garantizar la estabilidad operativa
6. **CATALOGO UNICO DE BIENES, SERVICIOS Y OBRAS- CUBSO:**
Código de Servicios educativos y de capacitación, curso en temas de tecnología de la información 8610160100229192
7. **ALCANCES Y DESCRIPCIÓN DEL SERVICIO**
Se adjuntan puntos a ser considerados según el objeto de contratación.



SERVICIO DE CAPACITACIÓN	
Concepto	Descripción
Actividad de Capacitación	Desarrollo seguro en plataformas mainframe y distribuido.
Requerimiento	Necesidad de capacitación contemplado PAEC 2025 – CG - 094
No. de Participantes	30 participantes distribuido en: Curso 1: Desarrollo Seguro en Plataforma Mainframe- 15 participantes. Curso 2: Desarrollo Seguro en Plataformas Distribuidas- 15 participantes.
Público objetivo	Trabajadores de la Gerencia de Tecnologías de Información

<p>Temario de las actividades de capacitación</p>	<p>CURSO 1: Desarrollo Seguro en Plataforma Mainframe</p> <p>Módulo 1: Introducción al mainframe y Desarrollo Seguro</p> <ul style="list-style-type: none"> Arquitectura del mainframe: Introducción a los mainframes y su papel en la informática empresarial. <ul style="list-style-type: none"> Bucles (PERFORM). Gestión de archivos: <ul style="list-style-type: none"> Acceso secuencial a archivos. Definición y uso de archivos VSAM. Tipos de datos en COBOL: <ul style="list-style-type: none"> Definición de variables. Manejo de arrays de manera óptima. <p>Módulo 3: Introducción a Desarrollo Seguro CICS</p> <ul style="list-style-type: none"> Fundamentos de CICS: <ul style="list-style-type: none"> Qué es CICS y cómo funciona en el entorno mainframe. Estructura básica de un programa CICS. Transacciones y comunicación entre programas. Comandos básicos de CICS: <ul style="list-style-type: none"> EXEC CICS para gestionar transacciones, archivos y mapas. Uso de SEND, RECEIVE, START, XCTL, LINK, RETURN. Soporte de Mapas BMS (Mapas Básicos): <ul style="list-style-type: none"> Definición y uso de mapas BMS para interacción con el usuario. Cómo crear y gestionar mapas. Modificación de mapas y campos. <p>Módulo 4: Principios de Seguridad en COBOL</p> <ul style="list-style-type: none"> Principios de Seguridad en COBOL <ul style="list-style-type: none"> Minimización de Privilegios Validación de Entrada Manejo Seguro de Datos. Prácticas de Seguridad en COBOL <ul style="list-style-type: none"> Control de Acceso a Archivos Validación de Datos de Entrada Uso de Cifrado Manejo de Errores Auditoría y Logging Consideraciones Adicionales <ul style="list-style-type: none"> Actualizaciones y Parches Entrenamiento y Conciencia Pruebas de Seguridad
	<p>CURSO 2: Curso de Desarrollo Seguro en Plataformas Distribuidas (40 HORAS)</p> <p>Módulo 1: Introducción al Desarrollo Seguro</p> <p>Fundamentos del JCL:</p> <ul style="list-style-type: none"> Sintaxis y estructura del JCL. Comandos del JCL: JOB, EXEC, DD. <p>A. Evolución del OWASP TOP 10 Web</p> <ul style="list-style-type: none"> A1:2021 Inadecuado Control de Accesos



Módulo 4: Principios de Seguridad en COBOL

- Principios de Seguridad en COBOL
 - Minimización de Privilegios
 - Validación de Entrada
 - Manejo Seguro de Datos.
- Prácticas de Seguridad en COBOL
 - Control de Acceso a Archivos
 - Validación de Datos de Entrada
 - Uso de Cifrado
 - Manejo de Errores
 - Auditoría y Logging
- Consideraciones Adicionales
 - Actualizaciones y Parches
 - Entrenamiento y Conciencia
 - Pruebas de Seguridad

CURSO 2: Curso de Desarrollo Seguro en Plataformas Distribuidas (40 HORAS)

Módulo 1: Introducción al Desarrollo Seguro

Fundamentos del JCL:

- Sintaxis y estructura del JCL.
- Comandos del JCL: JOB, EXEC, DD.

A. Evolución del OWASP TOP 10 Web

- A1:2021 Inadecuado Control de Accesos
 - Escenarios de Ataque
 - Ejemplo de Explotación.
 - ¿Cómo Prevenir este Riesgo?
- A2:2021 Fallos Criptográficos.
 - Escenarios de Ataque
 - Ejemplo de Explotación.
 - ¿Cómo prevenir este riesgo?
- A3:2021 Inyección
 - Escenarios de Ataque
 - Ejemplo de Explotación.
 - ¿Cómo prevenir este riesgo?
- A4:2021 Diseño Inseguro
 - Escenarios de Ataque-
 - Ejemplo de Explotación.
 - ¿Cómo prevenir este riesgo?
- A5:2021 Configuración Insegura
 - Escenarios de Ataque
 - Ejemplo de Explotación.
 - ¿Cómo prevenir este riesgo?
- A6:2021 Componentes Vulnerables y Obsoletos
 - Escenarios de Ataque
 - Ejemplo de Explotación.
 - ¿Cómo prevenir este riesgo?
- A6:2021 Fallos de Identificación y Autorización
 - Escenarios de Ataque



- Ejemplos de Explotación.
- ¿Cómo prevenir este riesgo?
- A7:2021 Fallos de Integridad de Datos y Software
 - Escenarios de Ataque
 - Ejemplo de Explotación
 - ¿Cómo prevenir este riesgo?
- A8:2021 Fallos de Registro y Monitoreo de Seguridad
 - Escenarios de Ataque.
 - Ejemplo de Explotación.
 - ¿Cómo prevenir estos riesgos?
- A9:2021 Server Side Request Forgery
 - Escenarios de Ataque
 - Ejemplo de Explotación
 - ¿Cómo prevenir este riesgo?

B. Análisis cambios OWASP Top 10 - 2017 vs 2021

- A.1 Inyección
 - Explotando una inyección SQL
 - ¿Cómo prevenir las inyecciones?
- A.2 Problemas de autenticación
 - Explotando problemas de autenticación
 - ¿Cómo prevenir los problemas de autenticación?
- A.3 Exposición de datos sensibles
 - Explotando servicios que exponen datos servicios.
 - ¿Cómo prevenir la exposición de datos sensibles?
- A.4 XML External Entities (XXE)
 - Explotando una inyección de XXE
 - ¿Cómo prevenir la inyección de XML External Entities?
- A.5 Inadecuado Control de Accesos
 - Explotando el Inadecuado Control de Accesos.
 - ¿Cómo Prevenir Problemas con el Control de Accesos?
- A.6 Configuración de Seguridad Incorrecta
 - Explotando la Configuración Insegura.
 - ¿Cómo Prevenir la Configuración Insegura
- A.7 Cross Site Scripting (XSS)
 - Explotando un Cross Site Scripting (XSS)
 - ¿Cómo prevenir el Cross Site Scripting (XSS)?
- A.8 Deserialización Insegura
 - Explotando la Deserialización Insegura
 - ¿Cómo Prevenir la deserialización insegura?
- A.9 Uso de Componentes con Vulnerabilidades Conocidas
 - Explotando Vulnerabilidades Conocidas.
 - ¿Cómo Prevenir las Vulnerabilidades Conocidas?
- A10. Registro y Monitoreo Insuficiente
 - Explotando el Registro y Monitoreo Insuficiente
 - ¿Cómo prevenir el monitoreo y registro insuficiente?

C. Proyectos complementarios al OWASP Top 10 Web

Módulo 2: Desarrollo de Software Seguro

- A. Instalando el Programa VirtualBox**
- Instalación de Laboratorio Virtual
 - Descarga de Archivos Desde Google Drive
 - Configurando Correctamente la Máquina Virtual



	<ul style="list-style-type: none"> • Iniciando la Máquina Virtual • Actualizando Cuenta Usuario Visual Studio - config de red <p>B. Desarrollo de Software Seguro</p> <ul style="list-style-type: none"> • Los mitos en el desarrollo de Software • Vulnerabilidad Cross-Site Scripting • Seguridad Desde el Diseño • Vulnerabilidad Path Traversal • Los 7 touch points, como aplicar la seguridad en el desarrollo de software • Vulnerabilidad Ejecución remota de Comandos • Gestión de Riesgos de Software • Ataque de Fuerza Bruta, Utilizando Owasp ZAP • Fases del Pentest • Vulnerabilidad Cross-site request forgery • Casos de Abuso • Abusando de la Encodificación Base64 • Seguridad en las Operaciones • Vulnerabilidad Inyección SQL • Integración de conceptos en el ciclo de desarrollo de software <p>C. Contra Medidas</p> <ul style="list-style-type: none"> • Actualizando la Configuración • Protegiendo contra XSS
--	---



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.



Para la contratación de personas naturales, en base al objeto de contratación y actividades a desarrollar NO se constituye como SUJETO OBLIGADO asimismo la presente contratación NO CALIFICA como un servicio de consultoría para presentar declaración jurada de intereses.

Teniendo conocimiento de lo anteriormente mencionado, la contratación NO CALIFICA como un servicio de consultoría.

8. REQUISITOS DEL PROVEEDOR

Los requisitos del proveedor para servicios son:

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



EXPERIENCIA

El postor deberá acumulado al equivalente de experiencia a S/10,000.00 (diez mil con 00/100 soles) por la contratación de servicios iguales o similares al objeto de contratación, durante los últimos cinco (05) años anteriores a la fecha de la prestación de su cotización que se computaran desde la fecha de conformidad o emisión del comprobante de pago, según corresponda .

Se consideran servicios similares:

- Capacitación en desarrollo seguro de software en entornos mainframe.
- Capacitación en desarrollo seguro de software en plataformas distribuidas.
- Implementación de estándares de seguridad de la información en entornos de desarrollo (ISO/IEC 27001, OWASP, PCI DSS, entre otros).

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[1], correspondientes a un máximo de veinte (20) contrataciones.

En el caso de cambio del docente, el proveedor deberá notificar, vía correo electrónico, al área usuaria con un mínimo de 15 días calendario; caso contrario estará sujeto a la penalidad correspondiente.

Formación Académica: egresado de carrera técnica o superior en ingeniería de Sistemas o Ingeniería Informática o Ingeniería en computación o Ingeniería de Software o Ingeniería Electrónica o administración de sistemas de información o carreras afines a informática.

Acreditación: Copia simple de constancia, diploma, título u otros documentos

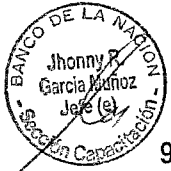


Experiencia:

Experiencia General: Mínimo 2 años en dictado de cursos en el sector público y/o privado
Experiencia Específica: Mínimo 1 año en asesoría y dictado de cursos a fines a la materia

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.



9. ENTREGABLE (S):

La presentación o consultoría consta de/ los siguiente(s) entregable (s):

- Contenido de los cursos virtuales descritos
- Entrega de material digitales a los participantes



Dentro de los cinco días de finalizado el servicio, el proveedor deberá remitir al área usuaria vía correo electrónico **y por separado** los siguientes documentos:

1. El reporte académico
2. Reporte de asistencia
3. Los certificados digitales individuales donde debe indicar apellidos y nombres en mayúscula de los participantes aprobados (nota mínima aprobatoria 14 y asistencia mínima 80%)
4. Informe final de la capacitación con recomendaciones

10. ÉTICA Y 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 indirectamente 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.



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.

11. PLAZO DE EJECUCIÓN DEL SERVICIO

El servicio se desarrollará en un plazo máximo de 120 días calendarios, computados a partir del día siguiente hábil de la notificación de la carta de aprobación vía correo electrónico.

12. LUGAR DE PRESTACIÓN DEL SERVICIO

La presentación del servicio será de manera virtual en la plataforma digital contratada por el proveedor designado.

13. FORMA DE PAGO

El pago se realiza 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 un solo pago finalizado el servicio.

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

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

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.

14. RESPONSABLE DE DAR CONFORMIDAD A LA PRESTACIÓN

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

La conformidad será otorgada por la Subgerencia de Desarrollo de Talento con la verificación del cumplimiento del servicio de la Sección Capacitación en un plazo máximo de (7) días calendario de presentado el entregable.

15. CONFIDENCIALIDAD:

EL PROVEEDOR se obliga a guardar estricta reserva sobre toda la información relacionada con EL BANCO y que sea de su conocimiento en el curso del cumplimiento de sus prestaciones, la cual no podrá ser utilizada sin previa autorización de este último, configurándose en causal de resolución de pleno derecho el incumplimiento de la indicada obligación, sin perjuicio de la indemnización de daños y perjuicios a que hubiere lugar. En este contexto, toda la información referida a clientes, personal, contabilidad, finanzas, productos, tráfico de llamadas telefónicas, tráfico de Internet, mensajería electrónica, actividades de comercialización, planes de negocio, acuerdos y actas de directorio, técnicas de marketing, procesos, servicios, políticas de precios, estrategias, buenas prácticas, metodología de trabajo, especificaciones técnicas, hardware, software, diseños, planos, dibujos, prototipos, nombres o marcas comerciales, modelos, descubrimientos, investigaciones, desarrollos, procesos, procedimientos, propiedad intelectual, sistemas de seguridad, estructura y distribución de las oficinas, sucursales y agencias, y también toda aquella información obtenida de terceras partes para EL BANCO, se considera confidencial y está considerada como parte de la obligación de reserva absoluta que asume EL PROVEEDOR por el presente instrumento. La obligación de mantener la confidencialidad de la información subsistirá incluso luego de finalizado la carta de aprobación.

16. PENALIDAD

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, hasta por un monto máximo equivalente al 5% del monto del entregable correspondiente, que puede descontarse del entregable o del pago final. En todos los casos, la penalidad se aplica automáticamente y se calcula de acuerdo con la siguiente fórmula:

$$\text{Penalidad diaria} = \frac{0.10 \times \text{monto del entregable correspondiente}}{0.5 \times \text{plazo del entregable}}$$

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

17. OTRAS PENALIDADES APLICABLES

N°	CONDICIONES	PENALIDAD	PROCEDIMIENTOS
1	No cumplir con el plazo establecido para notificar el cambio del docente.	5% del importe del servicio	Mediante correo electrónico, la Sección Capacitación comunicará el motivo de la penalización.

18. RESOLUCIÓN DE LA CONTRATACIÓN

Cualquiera de las partes puede resolver el contrato, de conformidad con el numeral 68.1 del artículo 68 de la Ley N° 32069, Ley General de Contrataciones Públicas y Artículo N° 122 de su Reglamento.

De encontrarse en alguno de los supuestos de resolución del contrato, LAS PARTES procederán de acuerdo con lo establecido en el artículo 122 del Reglamento de la Ley N° 32069, Ley General de Contrataciones Públicas, aprobado mediante Decreto Supremo N° 009-2025-EF.

Se puede resolver la carta de aprobación, en los siguientes casos:

- 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.
- 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.
- El BANCO puede resolver la carta de aprobación cuando la penalidad aplicada excede el 10% del monto contractual.
- 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.



19. SOLUCIÓN DE CONTROVERSIAS

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

20. OTRAS CARACTERÍSTICAS QUE SEAN RELEVANTES PARA LA CONTRATACIÓN

Nota:



I. Esta contratación de servicios corresponde a la necesidad del área y se ratifica no estar dividiendo la contratación (FRACCIONANDO), para evadir la aplicación de la Ley General de Contrataciones Públicas y su reglamento. Asimismo, el presente requerimiento SI SE ENCUENTRA PROGRAMADO en el PAC.

II. En todo lo no previsto expresamente en el presente termino de referencia, resulta aplicable la circular - CONTRATOS MENORES A NIVEL NACIONAL

FIRMA Y SELLO / ÁREA USUARIA

