TÉRMINOS DE REFERENCIA

SERVICIO DE IDENTIFICACION DE BRECHAS TECNOLÓGICAS EN LA INFRAESTRUCTURA TECNOLÓGICA DEL MTC A TRAVÉS DEL PROCESO DE ETHICAL HACKING.

Unidad Orgánica:	Oficina General de Tecnología de la Información.
Meta Presupuestaria:	Sec. Fun. 0295 - Desarrollo y Mantenimiento de los Sistemas Informáticos.
Actividad del POI	AO100107200151 Gestión de la Infraestructura Tecnológica y Seguridad Informática.

1. DENOMINACIÓN DE LA CONTRATACIÓN

Servicio de identificación de brechas tecnológicas en la infraestructura tecnológica del MTC a través del proceso de Ethical Hacking.

2. OBJETIVO

Contratar el servicio de identificación de brechas tecnológicas en la infraestructura tecnológica del MTC a través del proceso de hacking ético con alcance a nivel interno y externo en el código fuente de los sistemas informáticos, servidores de procesamiento de datos, redes y comunicaciones que permitan verificar, evaluar y analizar las posibles fallas de seguridad, amenazas, vulnerabilidades y riesgos de los servicios digitales del MTC

3. ANTECEDENTES

Que, la Resolución Ministerial N° 658-2021-MTC/01, aprueba el Texto Integrado del Reglamento de Organización y Funciones del Ministerio de Transportes y Comunicaciones, en su artículo 83 precisa:

*"Funciones de la Oficina de Infraestructura Tecnológica y Seguridad Informática del Reglamento de Organización y Funciones: "Diseña lineamientos, directivas, protocolos y otros documentos de gestión para la implementación de las **materias de seguridad informática**, en coordinación con el órgano competente del ministerio; así como realizar acciones de seguimiento para su cumplimiento".*

4. FINALIDAD PÚBLICA

Verificar, evaluar y analizar las posibles fallas de seguridad que pueden presentar los servicios digitales que el MTC brinda a los ciudadanos, los cuales deben ser brindados con todas las medidas necesarias que permitan salvaguardar la información y los datos personales de los usuarios.

5. ACTIVIDADES A REALIZAR

5.1. ALCANCE Y DESCRIPCIÓN DEL SERVICIO

La evaluación de seguridad de la plataforma tecnológica del MTC se dará a través de la de identificación de brechas tecnológicas en el código fuente de los sistemas informáticos, servidores, infraestructura de red y datos de sus componentes.

- ✓ La ejecución del servicio no debe causar daño alguno en el funcionamiento de los sistemas o en el desempeño de la red del MTC.

FIRMA DIGITAL
Firmado digitalmente por: ORTIZ ALBERCA Carlos Joet FAU 20131379944 hard
Motivo: Soy el autor del documento
Fecha: 09/01/2025 13:00:26-0500

- ✓ El MTC designará a una persona responsable del proyecto, quien tendrá la responsabilidad de coordinar y facilitar el acceso a los recursos, servicios e información necesaria para la ejecución del servicio.
- ✓ El contratista en coordinación con el personal técnico del MTC, elaborará los cronogramas para la ejecución de la evaluación de seguridad y pruebas de penetración (pentesting).
- ✓ El contratista deberá indicar las herramientas, equipos y/o productos que utilizará durante la ejecución de la evaluación de seguridad y pruebas de penetración.
- ✓ La metodología utilizada para la ejecución del servicio, debe estar basada en los manuales de seguridad OSSTM (Open Source Security Test Metodology), OWASP (Open Web Application Security Project), ISSAF (Information System Security Assessment Framework) e ITSAM (Information Technology Security Assessment Methodology).
- ✓ Las vulnerabilidades detectadas en la evaluación de seguridad y pruebas de penetración deben de calificarse y reportarse en base a la aplicación del Common Vulnerability Score System (CVSS).
- ✓ Las recomendaciones emitidas por el contratista surgidas del análisis efectuado a la seguridad y pruebas de penetración, deberán ser aplicables y ejecutadas por el personal del MTC para subsanar las vulnerabilidades sin afectar los servicios revisados.
- ✓ El servicio de análisis de Ethical Hacking debe comprender las siguientes cantidades de activos informáticos:

Plataforma	Cantidad
Aplicaciones web	286
Aplicaciones de escritorio	5
Servidores windows/linux	300
Estaciones de trabajo windows	3500

5.2. CARACTERÍSTICAS DEL SERVICIO

La prestación del servicio debe considerar las siguientes etapas de análisis:

FASE 1 – COMPONENTE DE GESTIÓN DEL SERVICIO

Para el componente gestión del proyecto se deberá utilizar la Guía del PMBOK (Project Management Body of Knowledge). Se debe considerar los siguientes puntos en el Plan de Gestión del Proyecto:

- o Alcance del Servicio
- o Cronograma de actividades
- o Actividades del Proyecto
- o Gestión de Recursos Humanos
- o Riesgos del Proyecto

FASE 2 – ANÁLISIS DE VULNERABILIDADES EN APLICACIONES

- ✓ La metodología aplicada por el PROVEEDOR para la verificación de seguridad de aplicaciones, se centrará en la evaluación de controles utilizados para la autenticación, manejo de sesiones y validación de datos de entrada.

Asimismo, se identificarán problemas de configuración, transmisión insegura de datos y divulgación de información sensible.

- ✓ Como producto de la evaluación se obtienen las vulnerabilidades de las aplicaciones Web clasificadas según el nivel de riesgo, las cuales son acompañadas con recomendaciones aplicables a su mitigación.
- ✓ La metodología desarrollada por el PROVEEDOR deberá cubrir todos los aspectos recomendados por la metodología OTP (OWASP Testing Project).

FASE 3 - PRUEBAS DINÁMICAS SOBRE APLICACIONES

Se debe realizar la evaluación sobre los sistemas de información en funcionamiento. El tipo de prueba a realizar sobre las aplicaciones a evaluar será del tipo CAJA GRIS (Gray Box), para esto se proporcionará credenciales de acceso al sistema de información correspondientes a un (01) perfil del sistema.

Las pruebas deberán incluir las siguientes actividades:

Obtención de Información

- ✓ Realizar el descubrimiento y reconocimiento de divulgación de información, basados en motores de búsqueda.
- ✓ Identificar el software de web.
- ✓ Revisar archivos con metadata en búsqueda de divulgación de información
- ✓ Identificar los puntos de entrada de las aplicaciones.
- ✓ Mapear las rutas de ejecución a través de las aplicaciones.
- ✓ Identificar el Framework usado por las aplicaciones
- ✓ Identificar la aplicación
- ✓ Mapear la arquitectura de las aplicaciones

Evaluación de la Gestión de Configuración y Despliegue

- ✓ Evaluar el manejo de las extensiones de nombres de archivos en búsqueda de información sensible.
- ✓ Buscar información sensible en archivos de copia de seguridad y no referenciados.
- ✓ Enumerar las interfaces de administración de infraestructura y de las aplicaciones.
- ✓ Evaluar los métodos HTTP.
- ✓ Evaluar la seguridad estricta en el transporte vía HTTP.

Evaluación de la Autenticación

- ✓ Evaluación de credenciales transportadas sobre un canal no encriptado
- ✓ Evaluar las credenciales default
- ✓ Evaluar los mecanismos débiles de bloqueo de cuentas
- ✓ Evaluar la evasión del esquema de autenticación
- ✓ Evaluar la funcionalidad de recordar contraseña
- ✓ Evaluar las debilidades del caché del browser
- ✓ Evaluar las políticas de contraseña débiles
- ✓ Evaluar los mecanismos débiles de recuperación de acceso mediante pregunta/respuesta
- ✓ Evaluar funcionalidades débiles de cambio de contraseña o reinicialización
- ✓ Evaluar autenticaciones débiles mediante canales alternos.

Evaluación de Autorización

- ✓ Evaluar el recorrido de directorios/inclusión de archivos.
- ✓ Evaluar la evasión del esquema de autorización.

- ✓ Evaluar el escalamiento de privilegios.
- ✓ Evaluar las referencias inseguras a objetos de forma directa.

Evaluar el manejo de sesiones

- ✓ Evaluar la evasión del esquema de manejo de sesiones.
- ✓ Evaluar los atributos de las cookies.
- ✓ Evaluar la "fijación de sesiones".
- ✓ Evaluar variables de sesiones expuestas.
- ✓ Evaluar la ocurrencia de falsificación de requerimientos cruzados (Cross Site Request Forgery)
- ✓ Evaluar la funcionalidad de termino de sesión (logout)

Evaluar la validación de datos

- ✓ Evaluar Cross Site Scripting Reflejado.
- ✓ Evaluar Cross Site Scripting Almacenado.
- ✓ Evaluar la manipulación de verbos HTTP.
- ✓ Evaluar la "contaminación" de parámetros HTTP
- ✓ Evaluar inyecciones de SQL
- ✓ Evaluar inyecciones de XML
- ✓ Evaluar inyecciones de código.
- ✓ Evaluar inyecciones de comandos.
- ✓ Evaluar desbordamiento de buffer.
- ✓ Evaluar la división y/o encubrimiento de tráfico HTTP.

Manejo de Errores.

- ✓ Análisis de códigos de error.
- ✓ Análisis de trazados de pila.
- ✓ Evaluar cifrados débiles de SSL/TSL, protección protecciones insuficientes en el transporte.
- ✓ Evaluar ataques del tipo "Padding Oracle".
- ✓ Evaluar información sensible enviada por canales no encriptados.

Evaluación del Lado Cliente

- ✓ Evaluar Cross Site Scripting basados en DOM (Document Object Model)
- ✓ Evaluar la ejecución de JavaScript
- ✓ Evaluar inyecciones de HTML.
- ✓ Evaluar redirecciones de URL en el Lado Cliente.
- ✓ Evaluar inyecciones de CSS.
- ✓ Evaluar la manipulación de recursos del Lado Cliente.
- ✓ Evaluar "Cross Origin Resource Sharing".
- ✓ Evaluar "Clickjacking".
- ✓ Evaluar almacenamiento local

FASE 4 - PRUEBAS ESTÁTICAS SOBRE APLICACIONES:

Se debe realizar la evaluación estática en las aplicaciones web designadas por el MTC. Para la realización de la evaluación estática el MTC hará entrega del código fuente de los sistemas de información para que estos sean evaluados a nivel de vulnerabilidades y deficiencias de seguridad informática.

La evaluación deberá ser realizada en base a la metodología OWASP – Code Review Guide Pre Alpha. La revisión considerará como mínimo la revisión de los siguientes procesos:

- Proceso de ingreso a la aplicación.
- Proceso de logout de la aplicación.
- Proceso de recuperación de contraseña.
- Proceso de manejo de cookies y sesiones.
- Procesos críticos del sistema a evaluar.

El servicio de Ethical Hacking deberá comprender el análisis de código estático de quince (15) aplicaciones, cada una de ellas con un mínimo de 10,000 líneas de código en lenguaje de programación PHP, .NET y Java.[1]

FASE 5 – HALLAZGOS Y RECOMENDACIONES:
Se debe realizar el informe final del servicio en la que se describa lo encontrado durante el servicio y las actividades realizadas a fin de mitigar el nivel de vulnerabilidades. Asimismo, deberá exponer las recomendaciones propuestas a fin de mejorar la seguridad informática del MTC.

6. PLAZO Y LUGAR DE EJECUCIÓN

6.1 PLAZO DE EJECUCIÓN DEL SERVICIO

El plazo del servicio será de hasta ochenta (80) días calendario[2], contados desde el día siguiente de la suscripción del contrato.

6.2 LUGAR DE PRESTACIÓN DEL SERVICIO

El servicio se brindará en la Oficina de Infraestructura Tecnológica y Seguridad Informática de la Oficina General de Tecnología de la Información del Ministerio de Transportes y Comunicaciones, sito en Jr. Zorritos N.º 1203, cercado de Lima.

Para aquellas actividades que no puedan realizarse de manera presencial, debido a la naturaleza de la misma y que se requiera ejecutar fuera del horario laborable, se permitirá que se realicen remotamente a través de un canal seguro VPN.[3]

7. ENTREGABLES

La presentación de los entregables se realizará de acuerdo a lo indicado a continuación:

TABLA N° 01

ENTREGABLE	NOMBRE	DESCRIPCIÓN	ENTREGA[4]
Entregable 1	Plan de gestión del proyecto.	Fase 1 - Componente de gestión del servicio.	Hasta cinco (5) días calendario, contados a partir del día siguiente de la suscripción del contrato.
Entregable 2	Informe técnico detallado.	Fase 2 - Análisis de vulnerabilidades en aplicaciones. Fase 3 - Pruebas dinámicas sobre aplicaciones. Fase 4 - Pruebas estáticas sobre aplicaciones.	Hasta cincuenta y cinco (55) días calendario, contados a partir del día siguiente de la presentación del primer entregable.

[1] Se incluye párrafo en atención a las Consulta N° 03 del participante HYNET S.A.C., Consulta N° 04 del participante KUNAK CONSULTING S.A.C. y Consulta N° 15 del participante BIGSECURE S.A.C
[2] Se modifica en atención a la Consulta N° 2 del participante HYNET S.A.C y Consulta N° 5 del participante KUNAK CONSULTING S.A.C.
[3] Se incluye párrafo en atención a la consulta N° 7 del participante KUNAK CONSULTING S.A.C.
[4] Se modifica en atención a la Consulta N° 2 de HYNET S.A.C y Consulta N° 5 de KUNAK CONSULTING S.A.C.

Entregable 3	Informe final	Fase 5 – Hallazgos y recomendaciones	Hasta veinte (20) días calendario, contados a partir del día siguiente de la presentación del segundo entregable.

8. REQUISITOS DEL PROVEEDOR

8.1 RECURSOS A SER PROVISTOS POR EL CONTRATISTA

8.1.1. DEL PERSONAL CLAVE

a) Un (01) jefe del Proyecto:

Actividades

Será el responsable de la coordinación y gestión durante toda la etapa de ejecución del servicio.

Perfil

✓ **Experiencia**

Debe contar con una experiencia mínima de cinco (05) años y haber participado como líder o gerente o jefe en proyectos relacionados a Ethical Hacking o Análisis de Vulnerabilidades o Implementación de SGSI basado en ISO 27001 o Auditoría de Sistemas o Consultorías en Seguridad de la Información o Proyectos en TI relacionados a Seguridad Digital[5].

✓ **Formación Académica**

- Profesional Titulado en alguna de las siguientes carreras: Ingeniería Informática, o Ingeniería de Computación y Sistema, o Ingeniería de Sistemas, o Ingeniería de Telecomunicaciones, o Ingeniería de Seguridad Informática, o Ingeniería Electrónica, o Ingeniería Empresarial y de Sistemas[6].
- Deberá contar con al menos dos (02) de las siguientes certificaciones: ISO 27001 Lead Implementer, ISO 27001 Lead Auditor, CISSO (Certified Information Systems Security Officer), CISA (Certified Information Systems Auditor), CRISC (Certified in Risk and Information Systems Control), ITIL Foundation, Certificación PMP o curso oficial basado en PMP con una duración mínima de cuarenta y ocho (48) horas.

b) Un (01) Especialista en Seguridad Digital.

Actividades

Será el responsable de la ejecución de las tareas comprendidas en el servicio.

Perfil

✓ **Experiencia**

Debe contar con una experiencia mínima de cinco (05) años como Consultor Senior en Seguridad de la Información o Pentester Profesional en el campo de las Tecnologías de la información

[5] Se incorpora en atención a Consulta N° 16 del participante BIGSECURE S.A.C.
[6] Se incorpora en atención a la Consulta N° 1 del participante HYNET S.A.C.

enfocado en servicios de Análisis y Vulnerabilidades, Hacking Ético, Pentesting.

✓ **Formación Académica**

- Profesional titulado en alguna de las siguientes carreras: Computación e Informática, o Ingeniería Informática, o Ingeniería de Computación y Sistemas, o Ingeniería de Sistemas, o Ingeniería de Redes y Comunicaciones de datos, o Ingeniería de Seguridad Informática, o Ingeniería Electrónica, o Ingeniería de Sistemas e Informática[7].
- Deberá contar con al menos dos (02) de las siguientes certificaciones: C|EH (Certified Ethical Hacker), CPTE (Certified Penetration Testing Engineer), CPEH (Certified Professional Ethical Hacker), OCSP (Offensive Security Certified Professional), ECSA (EC-Council Certified Security Analyst), CHFI (Computer Hacking Forensic Investigator).

Nota:

- Las certificaciones deberán ser presentadas como parte de la documentación para perfeccionar el contrato.
- La experiencia se contabiliza desde la obtención del grado de bachiller.

9. FORMA DE PAGO

Único pago del 100% luego de la conformidad del servicio.

La entidad debe pagar las contraprestaciones pactadas a favor del contratista dentro de los diez (10) días calendarios siguientes a la conformidad del informe final y las condiciones establecidas en el contrato para ello.

Para efectos del pago de las contraprestaciones ejecutadas por el contratista, la Entidad debe contar con la siguiente documentación:

✓ Informe del funcionario responsable de la Oficina de Infraestructura Tecnológica y Seguridad Informática.
✓ Comprobante de pago.
✓ Presentación de los entregables indicados en el numeral 7.

La documentación se debe presentar en la Oficina de Atención al Ciudadano y Gestión Documental del MTC, sito en Jr. Zorritos N.º 1203 –Cercado de Lima, en el horario de 8:30 horas a 17:30 horas, o a través de Mesa de Partes Virtual del MTC, accediendo desde el siguiente link: https://mpv.mtc.gob.pe, siendo que los remitidos luego del horario antes indicado serán recepcionados como si hubiesen sido entregados al día siguiente hábil.

10. PENALIDADES

10.1 Penalidad por mora

En caso de retraso injustificado en la ejecución de las prestaciones objeto del contrato, la Entidad le aplica automáticamente una penalidad por mora por cada

[7] Se incorpora en atención a la Consulta N° 17 del participante BIGSECURE S.A.C.

día de atraso. La penalidad se aplica automáticamente y se calcula de acuerdo a la siguiente fórmula:

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

Donde:

F = 0.25 para plazos mayores a sesenta (60) días o;
F = 0.40 para plazos menores o iguales a sesenta (60) días.

Tanto el monto como el plazo se refieren, según corresponda, al monto vigente del contrato o ítem que debió ejecutarse o, en caso que estos involucraran obligaciones de ejecución periódica o entregas parciales, a la prestación individual que fuera materia de retraso.

El retraso se justifica a través de la solicitud de ampliación de plazo debidamente aprobado. Adicionalmente, se considera justificado el retraso y en consecuencia no se aplica penalidad, cuando el contratista acredite, de modo objetivamente sustentado, que el mayor tiempo transcurrido no le resulta imputable. En ese último caso, la calificación del retraso como justificado por parte de la Entidad no da lugar al pago de gastos generales ni costos directos de ningún tipo.

10.2 OTRAS PENALIDADES[8]

De acuerdo con el artículo 163 del Reglamento se considerarán además la siguiente penalidad:

Tabla N° 02

N°	Supuestos de aplicación de penalidad	Procedimiento	Forma de cálculo (% por valor del servicio)
01	Por exceder el tiempo de presentación de los entregables.	Tiempo empleado por el CONTRATISTA para realizar la presentación de los entregables correspondientes a la prestación principal y accesoria. El tiempo se contabiliza conforme a lo indicado en el ítem 7. La Oficina de Infraestructura Tecnológica y Seguridad Informática, emitirá un informe técnico.	1% del valor de una (01) UIT por cada día de retraso.

UIT: Unidad Impositiva Tributaria.

Nota: Se precisa que, para la aplicación de penalidad, el cálculo se efectuará sobre la base de la UIT vigente a la fecha de haberse producido el incumplimiento.

11. MEDIDAS DE CONTROL DURANTE LA EJECUCIÓN CONTRACTUAL

11.1 ÁREA QUE COORDINARÁ CON EL CONTRATISTA

El área que coordinará con el contratista es la Oficina de Infraestructura Tecnológica y Seguridad Informática de la Oficina General de Tecnología de la Información.

12. CONFORMIDAD

La conformidad será otorgada por la Oficina de Infraestructura Tecnológica y Seguridad Informática de la Oficina General de Tecnología de la Información, en un plazo de siete (07) días calendario previa verificación del entregable correspondiente.

[8] Se incorpora en atención a la Consulta N° 11 del participante KUNAK CONSULTING S.A.C.

13. RESPONSABILIDAD POR VICIOS OCULTOS

El contratista es el responsable por la calidad ofrecida y por los vicios ocultos de los bienes ofertados por un plazo de un (01) año, contados a partir de la conformidad otorgada por la Oficina de Infraestructura Tecnológica y Seguridad Informática[9].

14. OTRAS CONDICIONES PARA LA EJECUCION DE LA PRESTACION

14.1 Subcontratación

El contratista se encuentra en la obligación expresamente a no subcontratar y/o transferir y/o ceder y/o traspasar y/o subarrendar a terceros, total o parcialmente el servicio.

14.2 Confidencialidad

El contratista se encuentra en la obligación de mantener absoluta confidencialidad y reserva sobre cualquier información a la que tenga acceso en el cumplimiento de las obligaciones durante el periodo de contratación, en tal sentido, el contratista se compromete a no divulgar la información a la que tuvo acceso en el ejercicio de sus obligaciones.

14.3 Sistema de contratación

A suma Alzada.

15. NORMA ANTICORRUPCIÓN

EL CONTRATISTA acepta expresamente que no llevará a cabo, acciones que están prohibidas por las leyes locales u otras leyes anticorrupción. Sin limitar lo anterior, EL CONTRATISTA se obliga a no efectuar algún pago, ni ofrecerá o transferirá algo de valor, a un funcionario o empleado gubernamental o a cualquier tercero relacionado con el servicio aquí establecido de manera que pudiese violar las leyes locales u otras leyes anticorrupción, sin restricción alguna.

En forma especial, EL CONTRATISTA declara con carácter de declaración jurada que no se encuentra inmerso en ningún procedimiento de carácter penal vinculado a presuntos ilícitos penales contra el Estado Peruano, constituyendo su declaración, la firma del mismo en el contrato de la que estos términos de referencia forman parte integrante.

16. NORMA ANTISOBORNO

EL CONTRATISTA, no debe ofrecer, negociar o efectuar, cualquier pago, objeto de valor o cualquier dádiva en general, o cualquier beneficio o incentivo ilegal en relación al contrato, que puedan constituir un incumplimiento a la ley, tales como robo, fraude, cohecho o tráfico de influencias, directa o indirectamente, o a través de socios, integrantes de los órganos de administración, apoderado, representantes legales, funcionarios, asesores o personas vinculadas.

Asimismo, el contratista se obliga a conducirse en todo momento, durante la ejecución del contrato. Con honestidad, probidad, veracidad e integridad y de no cometer actos ilegales o de corrupción, directa o indirectamente o a través de sus socios, accionistas, participantes de los órganos de administración apoderados, representantes legales,

[9] Se precisa en atención a la Consulta N° 9 del participante N° KUNAK CONSULTING S.A.C.

funcionarios, asesores y personas vinculadas en virtud a lo establecido en el artículo 11º de la Ley de Contrataciones del Estado y el artículo 7º de su Reglamento.

Asimismo, el contratista se compromete a comunicar a las autoridades competentes, de manera directa y oportuna, cualquier acto o conducta ilícita o corrupta de la que tuviere conocimiento; así también en adoptar medidas técnicas, prácticas, a través de los canales dispuestos por el MTC.

De la misma manera, el proveedor es consciente que, de no cumplir con lo anteriormente expuesto, se someterá a la resolución del contrato y a las acciones civiles y/o penales que el MTC pueda accionar.

17. CLAUSULA DE CONFIDENCIALIDAD

Toda información del MTC a que tenga acceso el CONTRATISTA, producto del desarrollo del servicio contratado es estrictamente confidencial. El CONTRATISTA y su personal, deben comprometerse a mantener las reservas del caso y no transmitirla a ninguna persona (natural o jurídica) sin la autorización expresa y por escrito de la Oficina General de Tecnología de la Información.

18. REQUISITOS DE CALIFICACIÓN

B	**CAPACIDAD TÉCNICA Y PROFESIONAL**
B.3	**CALIFICACIONES DEL PERSONAL CLAVE**
B.3.1	**FORMACIÓN ACADÉMICA**
	Requisitos: **Un (01) Jefe del proyecto** Profesional titulado en alguna de las siguientes carreras: Ingeniería Informática, o Ingeniería Computación y Sistema, o Ingeniería de Sistemas, o Ingeniería de Telecomunicaciones, o Ingeniería de Seguridad e Informática, o Ingeniería Electrónica, o Ingeniería Empresarial y de Sistemas[10]. **Un (01) Especialista en Seguridad Digital** Profesional titulado en alguna de las siguientes carreras: Computación e Informática, o Ingeniería informática, o Ingeniería de Computación y Sistemas, o Ingeniería de Sistemas, o Ingeniería de Redes y Comunicaciones de datos, o Ingeniería de Seguridad Informática, o Ingeniería Electrónica o Ingeniería de Sistemas e Informática[11]. Acreditación: El grado académico será verificado por el órgano encargado de las contrataciones o comité de selección, según corresponda, en el Registro Nacional de Grados Académicos y Títulos Profesionales en el portal web de la Superintendencia Nacional de Educación Superior Universitaria - SUNEDU a través del siguiente link: *https://enlinea.sunedu.gob.pe//* o en el Registro Nacional de Certificados, Grados y Títulos a cargo del Ministerio de Educación a través del siguiente link: *https://titulosinstitutos.minedu.gob.pe/*, según corresponda. En caso el grado académico no se encuentre inscrito en el referido registro, el postor debe presentar la copia del diploma respectivo a fin de acreditar la formación académica requerida.
B.4	**EXPERIENCIA DEL PERSONAL CLAVE**
	Requisitos: **Un (01) Jefe del proyecto** Debe contar con una experiencia mínima de cinco (05) años y haber participado como líder o gerente o jefe en proyectos relacionados a Ethical Hacking o Análisis de Vulnerabilidades o Implementación de SGSI basado en ISO 27001 o Auditoría de Sistemas o Consultorías en Seguridad de la Información o

[10] Se incorpora en atención a la Consulta N° 1 del participante HYNET S.A.C.
[11] Se incorpora en atención a la Consulta N° 17 del participante BIGSECURE S.A.C.

	Proyectos en TI relacionados a Seguridad Digital[12]. **Un (01) Especialista en Seguridad Digital** Debe contar con una experiencia mínima de cinco (05) años como Consultor Senior en Seguridad de la Información o Pentester Profesional en el campo de las Tecnologías de la información, enfocado en servicios de Análisis de vulnerabilidades o Hacking Ético o Pentesting. De presentarse experiencia ejecutada paralelamente (traslape), para el cómputo del tiempo de dicha experiencia sólo se considerará una vez el periodo traslapado. Acreditación: La experiencia del personal clave se acreditará con cualquiera de los siguientes documentos: (i) copia simple de contratos y su respectiva conformidad o (ii) constancias o (iii) certificados o (iv) cualquier otra documentación que, de manera fehaciente demuestre la experiencia del personal propuesto. **Importante** • ***Los documentos que acreditan la experiencia deben incluir los nombres y apellidos del personal clave, el cargo desempeñado, el plazo de la prestación indicando el día, mes y año de inicio y culminación, el nombre de la Entidad u organización que emite el documento, la fecha de emisión y nombres y apellidos de quien suscribe el documento*** • ***En caso los documentos para acreditar la experiencia establezcan el plazo de la experiencia adquirida por el personal clave en meses sin especificar los días se debe considerar el mes completo.*** • ***Se considerará aquella experiencia que no tenga una antigüedad mayor a veinticinco (25) años anteriores a la fecha de la presentación de ofertas.*** • ***Al calificar la experiencia del personal, se debe valorar de manera integral los documentos presentados por el postor para acreditar dicha experiencia. En tal sentido, aun cuando en los documentos presentados la denominación del cargo o puesto no coincida literalmente con aquella prevista en las bases, se deberá validar la experiencia si las actividades que realizó el personal corresponden con la función propia del cargo o puesto requerido en las bases.***
C	**EXPERIENCIA DEL POSTOR EN LA ESPECIALIDAD**
	Requisitos: El postor debe acreditar un monto facturado acumulado equivalente a S/. 200,000.00 (doscientos mil con 00/100 soles), por la contratación de servicios iguales o similares al objeto de la convocatoria, durante los ocho (8) años anteriores a la fecha de la presentación de ofertas que se computarán desde la fecha de la conformidad o emisión del comprobante de pago, según corresponda. En el caso de postores que declaren en el Anexo N.° 1 tener la condición de micro y pequeña empresa, se acredita una experiencia de S/ 25,000.00 (veinte cinco mil con 00/100 soles) por la venta de servicios iguales o similares al objeto de la convocatoria, durante los ocho (8) años anteriores a la fecha de la presentación de ofertas que se computarán desde la fecha de la conformidad o emisión del comprobante de pago, según corresponda. En el caso de consorcios, todos los integrantes deben contar con la condición de micro y pequeña empresa. Se consideran servicios similares a los siguientes: servicios se seguridad perimetral o servicios de ethical hacking o servicios de análisis de vulnerabilidades o servicios de pentesting. Acreditación: La experiencia del postor en la especialidad 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 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[13], correspondientes a un máximo de veinte (20) contrataciones. En caso los postores presenten varios comprobantes de pago para acreditar una sola contratación, se debe acreditar que corresponden a dicha contratación; de lo contrario, se asumirá que los comprobantes

[12] Se incorpora en atención a Consulta N° 16 del participante BIGSECURE S.A.C.

[13] Cabe precisar que, de acuerdo con la **Resolución N° 0065-2018-TCE-S1 del Tribunal de Contrataciones del Estado**:
"… el solo sello de cancelado en el comprobante, cuando ha sido colocado por el propio postor, no puede ser considerado como una acreditación que produzca fehaciencia en relación a que se encuentra cancelado. Admitir ello

	acreditan contrataciones independientes, en cuyo caso solo se considerará, para la evaluación, las veinte (20) primeras contrataciones indicadas en el **Anexo Nº 8** referido a la Experiencia del Postor en la Especialidad. En el caso de servicios de ejecución periódica o continuada, solo se considera como experiencia la parte del contrato que haya sido ejecutada durante los ocho (8) años anteriores a la fecha de presentación de ofertas, debiendo adjuntarse copia de las conformidades correspondientes a tal parte o los respectivos comprobantes de pago cancelados. En los casos que se acredite experiencia adquirida en consorcio, debe presentarse la promesa de consorcio o el contrato de consorcio del cual se desprenda fehacientemente el porcentaje de las obligaciones que se asumió en el contrato presentado; de lo contrario, no se computará la experiencia proveniente de dicho contrato. Asimismo, cuando se presenten contratos derivados de procesos de selección convocados antes del 20.09.2012, la calificación se ceñirá al método descrito en la Directiva "Participación de Proveedores en Consorcio en las Contrataciones del Estado", debiendo presumirse que el porcentaje de las obligaciones equivale al porcentaje de participación de la promesa de consorcio o del contrato de consorcio. En caso que en dichos documentos no se consigne el porcentaje de participación se presumirá que las obligaciones se ejecutaron en partes iguales. Si el titular de la experiencia no es el postor, consignar si dicha experiencia corresponde a la matriz en caso que el postor sea sucursal, o fue transmitida por reorganización societaria, debiendo acompañar la documentación sustentatoria correspondiente. Si el postor acredita experiencia de otra persona jurídica como consecuencia de una reorganización societaria, debe presentar adicionalmente el **Anexo N° 9.** Cuando en los contratos, órdenes de servicios o comprobantes de pago el monto facturado se encuentre expresado en moneda extranjera, debe indicarse el tipo de cambio venta publicado por la Superintendencia de Banca, Seguros y AFP correspondiente a la fecha de suscripción del contrato, de emisión de la orden de servicios o de cancelación del comprobante de pago, según corresponda. Sin perjuicio de lo anterior, los postores deben llenar y presentar el **Anexo Nº 8** referido a la Experiencia del Postor en la Especialidad **Importante** • ***Al calificar la experiencia del postor, se debe valorar de manera integral los documentos presentados por el postor para acreditar dicha experiencia. En tal sentido, aun cuando en los documentos presentados la denominación del objeto contractual no coincida literalmente con el previsto en las bases, se deberá validar la experiencia si las actividades que ejecutó el postor corresponden a la experiencia requerida.*** • ***En el caso de consorcios, solo se considera la experiencia de aquellos integrantes que se hayan comprometido, según la promesa de consorcio, a ejecutar el objeto materia de la convocatoria, conforme a la Directiva "Participación de Proveedores en Consorcio en las Contrataciones del Estado".***

CARLOS JOET ORTIZ ALBERCA
Director
Oficina de Infraestructura Tecnológica y Seguridad Informática

equivaldría a considerar como válida la sola declaración del postor afirmando que el comprobante de pago ha sido cancelado"
(…)
"Situación diferente se suscita ante el sello colocado por el cliente del postor [sea utilizando el término "cancelado" o "pagado"] supuesto en el cual sí se contaría con la declaración de un tercero que brinde certeza, ante la cual debiera reconocerse la validez de la experiencia".