



TÉRMINOS DE REFERENCIA

SERVICIO DE ETHICAL HACKING MODALIDAD CAJA GRIS

I. DENOMINACIÓN DE LA PRESTACIÓN DEL SERVICIO

Contratar los servicios de una persona natural que brinde el servicio de Ethical Hacking modalidad caja gris sobre la infraestructura y servicios de ProInnovate usando técnicas de caja gris mediante la metodología OWASP.

II. FINALIDAD PÚBLICA

La presente contratación tiene por finalidad la identificación, análisis y evaluación de vulnerabilidades a la que está expuesta la infraestructura tecnológica de ProInnovate, que permita poder implementar los controles de seguridad correspondientes.

III. PERFIL PROFESIONAL

a) Formación profesional:

Profesional titulado y colegiado en las carreras de ingeniería de sistemas, ingeniería informática, sistemas e informática, ciencias de la computación y/o afines.

Deberá contar como mínimo con 3 de las siguientes certificaciones:

- ✓ CPEH (Certified Professional Ethical Hacker) de Mile2.
- ✓ CPTE (Certified Penetration Testing Engineer) de Mile 2.
- ✓ OSEH (Open Sec Ethical Hacker) de Open Sec.
- ✓ CEHPC (Ethical Hacking Professional Certification) de CertiProf.
- ✓ CEH (Certified Ethical Hacking) de EC Council.
- ✓ OSEP / Offensive Security Experienced Penetration Tester
- ✓ Offensive Security / Offensive Security Certified Professional (OSCP)
- ✓ Offensive Security / Offensive Security Certified Expert (OSCE)
- ✓ GIAC / Exploit Researcher and Advanced Penetration Tester (GXPN)
- ✓ GIAC / Certified Forensic Analyst (GCFA)
- ✓ CISSP (Certified Information Systems Security Professional) de ISC2
- ✓ CC (Certified in Cybersecurity) de ISC2.
- ✓ Cyber Security Foundation de CertiProf.
- ✓ LCSPC (Lead Cyber Security Professional Certificate) de CertiProf.
- ✓ Information Security Associate ISO 27001 de Skill Front
- ✓ Curso y/o especialización en Gerencia de Seguridad de la Información

b) Experiencia general:

Experiencia general no menor a cinco (5) años en el sector público o privado como especialista en seguridad de la información y/o ciberseguridad.

c) Experiencia específica:

Experiencia específica de cuatro (04) años desempeñándose en proyectos de evaluación de Ethical Hacking, análisis de vulnerabilidades, seguridad de aplicaciones, pruebas de penetración o gestión de proyectos de ciberseguridad y seguridad de la información.





Debe de acreditar como mínimo dos (02) servicios relacionados con la ejecución de este tipo de proyectos de ciberseguridad (análisis de vulnerabilidades y/o Ethical Hacking o similares) en empresas públicas y/o privadas, lo cual será validado mediante cartas y/o constancias.

IV. DESCRIPCIÓN DEL SERVICIO

- El servicio no debe de afectar el funcionamiento de los sistemas o el desempeño de la red. Esta actividad será coordinada entre la UIT y el proveedor para buscar la mejor hora de ejecución en aras de minimizar riesgos de rendimiento y pérdida de disponibilidad del servicio.
- El proveedor deberá contemplar el escaneo de puertos y servicios TCP/IP.
- El proveedor deberá identificar las vulnerabilidades en la infraestructura tecnológica de la organización. Este análisis comprende servidores, aplicaciones críticas definidas por ProInnovate y Firewalls.
- Se deben identificar vulnerabilidades asociadas con malas prácticas de desarrollo de los sistemas de información basado en la metodología OWASP.
- Se debe realizar un análisis de direcciones IPs públicas para identificar vulnerabilidades.
- Verificación de fallas conocidas a nivel de protocolos (TLS, HTTPS, POP, SMTP, IMAP, MAPI, SMB, NFS, FTP) y TCP/IP en general.
- Detectar las vulnerabilidades en el servicio de base de datos y ataques de SQL Injection, XSS, XSRF, etc.
- Escaneo de las vulnerabilidades de los servidores en general (correo, base de datos, aplicaciones, archivos, etc).
- Descubrir los activos de información publicados en internet.
- Evaluar las vulnerabilidades de estos activos definiendo su criticidad e impacto usando el score base CVSS.
- Ejecutar las pruebas que sean necesarias realizar para descartar los falsos positivos (detección de amenazas que no son reales) en las vulnerabilidades detectadas.
- Hacer uso de las herramientas de Ethical Hacking para demostrar la veracidad de los resultados.
- Realizar el retest (refrendo) de las vulnerabilidades una vez que la organización haya realizado la corrección respectiva. Este refrendo no debe exceder los 9 meses calendario.
- Bajo ninguna circunstancia y en ningún momento se generará algún tipo de cambio sobre los sistemas y/o información a las que se logre acceso.

Para el presente servicio, la entidad brindará información sobre los sistemas/aplicaciones y servicios informáticos al proveedor. Esta información estará compuesta por direcciones IP, puertos, usuarios y credenciales de acceso (perfiles de acceso al sistema Ingenius, etc), URLs, nombres de dominio, diagramas de red, etc.

El objetivo es que el escenario sea el más real posible considerando a un atacante con conocimiento y acceso a la infraestructura tecnológica de ProInnovate y se determine cuál es el nivel de riesgo al que está expuesta la organización. Esta coordinación será realizada por la Unidad de Tecnología de la Información con el proveedor contratado.

El proveedor deberá brindar una charla de concientización de por lo menos 2 horas dirigida al personal de UIT sobre los siguientes temas:

- Fuga de Información.
- Ciberseguridad.





PERÚ

Ministerio
de la Producción



"Decenio de la Igualdad de Oportunidades para mujeres y hombres"
"Año de la unidad, la paz y el desarrollo"

V. PRODUCTOS

Se presentará un único producto que deberá contener lo siguiente:

- ✓ Cronograma y planificación de actividades del proyecto.
- ✓ Acta de Inicio del Proyecto.
- ✓ Informe detallado que contemple una matriz con el resumen de las vulnerabilidades detectadas durante la ejecución del servicio. El proveedor deberá incluir las conclusiones y recomendaciones para minimizar la ocurrencia de futuros ataques, mitigar los riesgos y mejorar la postura de la seguridad y ciberseguridad de la organización.
- ✓ El postor deberá indicar en su informe el detalle de las herramientas y/o productos que utilizará durante la ejecución del servicio.

VI. PLAZO DE EJECUCIÓN DEL SERVICIO

El plazo de ejecución del servicio no podrá ser mayor a 45 días calendario contabilizados a partir del día siguiente de notificada la orden de servicio, la Unidad de Tecnologías de la Información coordinará de forma directa con el proveedor la ejecución del servicio.

VII. FORMA Y CONDICIONES DE PAGO

El pago del servicio se realizará en una sola armada por S/ 37,800 (treinta y siete mil ochocientos con 00/100 Soles), e incluye los impuestos de ley.

VIII. LUGAR DE LA PRESTACIÓN DEL SERVICIO

En la sede central de ProInnovate, Jr. Juan Bielovucich N° 1325 – Lince, Lima. Para el presente servicio, la ejecución por parte del proveedor será en modalidad remota. Sin embargo, queda a discreción de la Unidad de Tecnologías de la Información si el proveedor deberá sustentar con alguna prueba los hallazgos detectados de forma presencial en la sede central de ProInnovate.

IX. COORDINACIÓN Y SUPERVISIÓN

La coordinación y supervisión de la prestación del servicio, estará a cargo del Jefe de la Unidad de Tecnología de la Información de Proinnovate

X. CONFORMIDAD DE LA PRESTACIÓN DE SERVICIO

La conformidad del servicio será emitida por el jefe de la Unidad de Tecnología de la Información de Proinnovate. Si hubiera observaciones a los productos entregados, estas serán notificadas por el área usuaria, y el consultor deberá subsanarlas en un plazo no mayor de 05 días calendarios de su notificación.

XI. SISTEMA DE CONTRATACIÓN

El sistema de contratación a suma alzada.

XII. PENALIDAD

En caso de retraso injustificado del contratista en la ejecución de las prestaciones objeto del contrato, la Entidad le aplica automáticamente una penalidad por mora por cada día de atraso, de conformidad con en el artículo 162 del Reglamento de la Ley de Contrataciones del Estado.



BICENTENARIO
DEL PERÚ
2021 - 2024



**PERÚ**Ministerio
de la Producción

"Decenio de la Igualdad de Oportunidades para mujeres y hombres"
"Año de la unidad, la paz y el desarrollo"

XIII. CONFIDENCIALIDAD

El proveedor queda expresamente obligado a mantener absoluta confidencialidad y reserva sobre la información fruto de la compra, servicio, implementación, o cualquier otro aspecto relacionado con la entidad, no pudiendo difundir, aplicar, ni comunicar a terceros información a la que haya tenido acceso durante ejecución del servicio, no pudiendo copiar o utilizar esta información con fin distinto a su objeto ni tampoco ceder a otros ni siquiera a efectos de conservación. Esta obligación se mantendrá incluso después de la firma de conformidad del servicio

XIV. ANTISOBORNO

Los participantes se obligan a conducirse en todo momento, durante la postulación al concurso, 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, integrantes de los órganos de administración, apoderados, representantes legales, funcionarios, asesores y personas vinculadas.

Además, los participantes se comprometen a i) comunicar a las autoridades competentes, de manera directa y oportuna, cualquier acto o conducta ilícita o corrupta de la que tuviera conocimiento; y ii) adoptar medidas técnicas, organizativas y/o de personal apropiadas para evitar los referidos actos o prácticas

XV. GARANTÍA

El período de garantía será durante todo el tiempo del servicio y acabado este se extenderá por seis (06) meses.

Firma del responsable



BICENTENARIO
DEL PERÚ
2021 - 2024

