TÉRMINOS DE REFERENCIA

SERVICIO DE ETHICAL HACKING DE SEGURIDAD DE LA INFORMACIÓN

1. **OBJETO:**

   Contratar una empresa especializada para realizar un servicio de Ethical Hacking y Seguridad Informática para evaluar el nivel de vulnerabilidades a la que está expuesta la infraestructura de T.I. de San Gabán S.A.

2. **FINALIDAD PÚBLICA:**

   Analizar la infraestructura tecnológica de TI de San Gabán S.A., que soportan los sistemas de información y poder determinar el nivel de exposición y las vulnerabilidades potenciales que pueden ser alcanzados o identificadas por un intruso que intente acceder de manera NO autorizada y/o realizar modificaciones de información de los sistemas de la organización comprometiendo la confidencialidad, integridad y disponibilidad de la información perjudicando la continuidad del servicio.

3. **ANTECEDENTES DE LA CONTRATACIÓN:**

   San Gabán S.A. a través de la División de TI, requiere contar con una evaluación de las vulnerabilidades de la infraestructura de TI especialmente en este escenario de pandemia en donde los servicios de TI se vienen accediendo de forma remota, para que en función a ellos se pueda iniciar un plan de acción de fortalecimiento de las vulnerabilidades identificadas.

4. **OBJETIVO GENERAL Y ESPECÍFICOS:**

   4.1. Objetivo General

   El objetivo del servicio consiste en que se realice un TEST de INTRUSIÓN interno/externo a la infraestructura de red, aplicaciones y dispositivos de seguridad perimetral utilizando un enfoque de PENTESTING con el propósito de identificar las posibles vulnerabilidades a las que podría estar expuesta la infraestructura de TI de San Gabán S.A. y definir los planes de acción para mitigar las mismas.

   4.1. Objetivos Específicos

   - Identificar vulnerabilidades en la infraestructura tecnológica conectada y expuesta a Internet.
   - Identificar vulnerabilidades en servidores, equipos de seguridad y equipos de comunicaciones de la red LAN de la organización.
   - Identificar vulnerabilidades asociadas a malas prácticas de desarrollo en los sistemas de información, las mismas que se encuentran descritas en la metodología OWASP.
   - Brindar recomendaciones específicas que mejor se ajusten a la infraestructura tecnológica del cliente y que le permitan mitigar los riesgos identificados en el proceso de Ethical Hacking

5. **SISTEMA DE CONTRATACIÓN:**

   El presente procedimiento se rige por el sistema de Suma Alzada.

6. **ADELANTOS:**
   No se otorgarán adelantos.
7. **SUBCONTRATACIÓN:**
   No es procedente la subcontratación para el presente procedimiento de contratación.
8. **NORMAS OBLIGATORIAS Y/O VOLUNTARIAS:**
   No se incluyen normas obligatorias y/o voluntarias.
9. **DESCRIPCIÓN TÉCNICA DEL SERVICIO:**

9.1 Ethical Hacking

Dentro del alcance del presente servicio se evaluarán los siguientes componentes de la Infraestructura de T.I.:

- Correo Electrónico
- VPN
- Mesa de partes
- Web services
- Portal Web
- 15 direcciones IP internas de servidores
- 10 direcciones IP públicas

Para el cumplimiento del servicio se debe cumplir con las siguientes fases mínimamente:

Fase 01: Preparativos

Actividades:

1. Firma de acuerdos de confidencialidad y contrato entre la organización y el proveedor a fin de garantizar la confidencialidad de la información.
2. Establecer el cronograma y planificación de actividades del proyecto.
3. Determinar los requisitos del proveedor y cliente para la realización de actividades.
4. Determinar ventanas de tiempo para la realización de actividades.
5. Establecer los riesgos y controles del Proyecto.
6. Establecer plan de comunicaciones.
7. Reunión de inicio (Kick Off) del Proyecto.

Entregables:

Los entregables de esta Fase son:

1. Acuerdo de confidencialidad entre el cliente y proveedor
2. Plan de Gestión del Proyecto

Fase 02: Ejecución del Servicio

Actividades:

1. Reconocimiento de información.
2. Escaneo e identificación de segmentos de red.
3. Escaneo de puertos y servicios sobre el protocolo TCP/UDP.
4. Escaneo e Identificación de vulnerabilidades en los activos informáticos
5. Explotación de vulnerabilidades y accesos.

6. Realización de técnicas de Post Explotación
7. Toma de evidencias y accesos.

Entregables:

1. Matriz de identificación de vulnerabilidades.

Fase 03: Trabajo de Escritorio

Actividades:

1. Desarrollo de informe técnico sobre infraestructura tecnológica.
2. Desarrollo de informe técnico sobre aplicaciones web.
3. Validación del nivel de riesgo de Seguridad de información asociada a las vulnerabilidades identificadas, se empleará el estándar CVSS v3 para determinar el nivel de riesgo.
4. Desarrollo del informe ejecutivo y resultados generales del Proyecto.
5. Presentación de resultados ante los involucrados del Proyecto.

Entregables:

1. Informes técnicos detallados por cada revisión con recomendaciones ad-hoc
2. Resumen ejecutivo al finalizar el servicio

9.2 Entregables del Proyecto Final

1. Plan de Gestión del Proyecto
2. Informe Técnico Detallado de Vulnerabilidades
3. Informe Ejecutivo de Resultados
4. Informe de Resolución de Vulnerabilidades

9.3 Metodología a Utilizar

- OSSTMM (Open Source Security Testing Methodology Manual)
- NIST SP 800-115 –Technical Guide to Information Security Testing and Assessment
- ISSAFF, (Information Systems Security Assessment Framework)
- OWASP Testing Guide v4.0
- CVSS (Common Vulnerability Scoring System)

9.4 Reevaluación de vulnerabilidad.

Se debe realizar un RETEST de vulnerabilidades sin costo, dicho RETEST debe realizarse después de 06 meses de concluido el servicio.

9.5 Condiciones Generales del Servicio

- El servicio se realizará de forma remota desde las instalaciones del proveedor, según sea necesario; el horario que se efectuarán las pruebas se coordinará al inicio del proyecto.

- La ejecución del servicio no debe causar daño alguno en el funcionamiento de los sistemas o en el desempeño de la red de la institución.
- San Gabán S.A. designará a una persona responsable del proyecto, la cual tendrá la responsabilidad de coordinar y facilitar el acceso al equipo del postor a los recursos, servicios e información necesarios al interior de la organización para la ejecución del servicio.
- El postor en coordinación con el personal técnico de San Gabán S.A., elaborarán los cronogramas para la ejecución de la evaluación de seguridad y pruebas de penetración al inicio del servicio.
- Se deberá firmar un acuerdo de CONFIDENCIALIDAD entre el postor y San Gabán S.A., en el cual se estipulará la información que la institución deberá brindar al proveedor, para los análisis de las pruebas y las penalidades para el proveedor en caso de la difusión del resultado de las pruebas o de la información brindada por parte de la Institución, las cuales no haya autorizado.
- 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.
- El postor deberá indicar las herramientas, equipos y/o productos que utilizará durante la ejecución de la evaluación de seguridad y pruebas de penetración, en caso se utilice herramientas gratuitas, el postor las entregará a la Institución.
- La metodología utilizada para la ejecución del Ethical Hacking, 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 para San Gabán S.A. surgidas en el análisis efectuado a la seguridad y pruebas de penetración, deben ser aplicables y ejecutados para subsanar las vulnerabilidades sin afectar los servicios revisados.
- Los informes y recomendaciones entregados a San Gabán S.A., como parte de la evaluación de seguridad y pruebas de penetración, deben ser completamente en español, a excepción de los reportes técnicos emitidos directamente por las herramientas utilizadas, las cuales servirán como anexos a los informes finales presentados**.**
- Todos los entregables serán proporcionados en medio digital.

9.6 Actividades técnicas de evaluación.

Prueba sobre Infraestructura tecnológica y sistemas operativos.

Reconocimiento de información:

- Búsqueda de información en Internet a través de Google, Bing, SHODAN, etc
- Exposición de información sensible a buscadores: archivos de registros (logs), archivos de configuración, etc.
- Búsqueda de información a través de consultas a los servidores DNS
- Búsqueda de información de segmentos de red a través de consultas WHOIS
- Búsqueda de información sensible de empleados a través de METADATA, correos

electrónicos, subdominios, redes sociales, etc.

Escaneo de puertos y servicios:

- Exploración de protocolos que se ejecutan sobre IP.
- Exploración de puertos: syn scan, ack scan, UDP scan, xmas scan, fin scan, null scan, RPC scan, idle scan.
- Identificación de servicios y obtención de banners.
- Evasión de mecanismos de defensa perimetral (Firewall, IPS) mediante técnicas de fragmentación y codificación.

Análisis de Vulnerabilidades:

- Identificación de servicios mediante captura de banners (FTP, HTTP, HTTPs, SMB, NFS, DNS, LDAP, SSH)
- Identificación de servicios mediante huellas digitales.
- Identificación de servidores HTTP.
- Enumeración de recursos de sistemas operativos Windows mediante NULL SESSIONS.
- Identificación de vulnerabilidades mediante NMAP SCRIPT ENGINE (NSE)
- Identificación de acceso anónimos a directorios LDAP.
- Enumeración de servicios SNMP.
- Verificación de configuraciones inseguras o por defecto.
- Identificación de parches no aplicados.
- Identificación y eliminación de FALSOS POSITIVOS.

Explotación de vulnerabilidades:

- Explotación y pruebas controladas de ingreso no autorizado a Sistemas Operativos
- Explotación y pruebas controladas de ingreso no autorizado a Bases de Datos
- Desarrollo de scripts en Python personalizados que permitan la explotación específica de vulnerabilidades identificadas.
- Pruebas de acceso a través de patrones de contraseñas identificadas.
- Toma de evidencias de acceso

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 serán del tipo CAJA GRIS (Gray Box), para esto se proporcionará credenciales de acceso al sistema de información. Las pruebas deberán incluir las siguientes actividades:

Nro. Control	CODIGO OWASP	PRUEBA A REALIZAR
Obtención de Información		
1	OTG-INFO-001	Realizar el descubrimiento y reconocimiento de divulgación de información basados en motores de búsqueda
2	OTG-INFO-002	Identificar el software de Web

3	OTG-INFO-003	Revisar archivos con metadata en búsqueda de divulgación de información
4	OTG-INFO-004	Enumerar las aplicaciones en el servidor web
5	OTG-INFO-005	Revisar los comentarios y metadata de las páginas web buscando divulgación de información
6	OTG-INFO-006	Identificar los puntos de entrada de las aplicaciones
7	OTG-INFO-007	Mapear las rutas de ejecución a través de las aplicaciones
8	OTG-INFO-008	Identificar el Framework usado por las aplicaciones
9	OTG-INFO-009	Identificar la aplicación
10	OTG-INFO-010	Mapear la arquitectura de las aplicaciones
Evaluación de la Gestión de Configuración y Despliegue		
11	OTG-CONFIG-001	Evaluar la configuración de la red/infraestructura
12	OTG-CONFIG-002	Evaluar la configuración de la plataforma de las aplicaciones
13	OTG-CONFIG-003	Evaluar el manejo de las extensiones de nombres de archivos en búsqueda de información sensible
14	OTG-CONFIG-004	Buscar información sensible en archivos de copia de seguridad y no referenciados
15	OTG-CONFIG-005	Enumerar las interfaces de administración de infraestructura y de las aplicaciones
16	OTG-CONFIG-006	Evaluar los métodos HTTP
17	OTG-CONFIG-007	Evaluar la seguridad estricta en el transporte vía HTTP
18	OTG-CONFIG-008	Evaluar el cumplimiento de las políticas de "dominio s cruzados" para las aplicaciones tipo RIA (aplicaciones de Internet enriquecidas)
Evaluar la Gestión de Identidades		
19	OTG-IDENT-001	Evaluar las deficiones de roles
20	OTG-IDENT-002	Evaluar los procesos de registro de usuarios
21	OTG-IDENT-003	Evaluar el proceso de provisionamiento de las cuentas de usuario
22	OTG-IDENT-004	Evaluar la enumeración de cuentas de usuario y las "cuentas adivinables"
23	OTG-IDENT-005	Evaluar las políticas débiles o no forzadas para nombres de usuarios
24	OTG-IDENT-006	Evaluar los permisos de cuentas tipo Invitado/Practicante
25	OTG-IDENT-007	Evaluar el proceso de suspensión/reactivación de cuentas
26	OTG-AUTHN-001	Evaluación de credenciales transportadas sobre un canal no encriptado
27	OTG-AUTHN-002	Evaluar las credenciales default
28	OTG-AUTHN-003	Evaluar los mecanismos débiles de bloqueo de cuentas
29	OTG-AUTHN-004	Evaluar la evasión del esquema de autenticación
30	OTG-AUTHN-005	Evaluar la funcionalidad de recordar contraseña
31	OTG-AUTHN-006	Evaluar las debilidades del caché del browser
32	OTG-AUTHN-007	Evaluar las políticas de contraseña débiles
33	OTG-AUTHN-008	Evaluar los mecanismos débiles de recuperación de acceso mediante pregunta/respuesta
34	OTG-AUTHN-009	Evaluar funcionalidades débiles de cambio de contraseña o reinicialización
35	OTG-AUTHN-010	Evaluar autenticaciones débiles mediante canales alternos

Evaluación de Autorización		
36	OTG-AUTHZ-001	Evaluar el recorrido de directorios/inclusión de archivos
37	OTG-AUTHZ-002	Evaluar la evasión del esquema de autorización
38	OTG-AUTHZ-003	Evaluar el escalamiento de privilegios
39	OTG-AUTHZ-004	Evaluar las referencias inseguras a objetos de forma directa
Evaluar el Manejo de Sesiones		
40	OTG-SESS-001	Evaluar la evasión del esquema de manejo de sesiones
41	OTG-SESS-002	Evaluar los atributos de las cookies
42	OTG-SESS-003	Evaluar la "fijación" de sesiones
43	OTG-SESS-004	Evaluar variables de sesión expuestas
44	OTG-SESS-005	Evaluar la ocurrencia de falsificación de requerimientos cruzados (Cross Site Request Forgery)
45	OTG-SESS-006	Evaluar la funcionalidad de termino de sesión (logout)
46	OTG-SESS-007	Evaluar el tiempo máximo de inactividad por sesión
47	OTG-SESS-008	Evaluar el uso inapropiado de variables de sesión (Session puzzling).
Evaluar la Validación de Datos		
48	OTG-INPVAL-001	Evaluar Cross Site Scripting Reflejado
49	OTG-INPVAL-002	Evaluar Cross Site Scripting Almacenado
50	OTG-INPVAL-003	Evaluar la manipulación de verbos HTTP
51	OTG-INPVAL-004	Evaluar la "contaminación" de parámetros HTTP
52	OTG-INPVAL-005	Evaluar inyecciones de SQL
53	OTG-INPVAL-006	Evaluar inyecciones de LDAP
54	OTG-INPVAL-007	Evaluar inyecciones en datos generados por una herramienta ORM (Object Relational Mapping)
55	OTG-INPVAL-008	Evaluar inyecciones de XML
56	OTG-INPVAL-009	Evaluar inyecciones de SSI
57	OTG-INPVAL-010	Evaluar inyecciones de XPath
58	OTG-INPVAL-011	Evaluar inyecciones IMAP/SMTP
59	OTG-INPVAL-012	Evaluar inyecciones de código
60	OTG-INPVAL-013	Evaluar inyecciones de commandos
61	OTG-INPVAL-014	Evaluar desbordamiento de buffer
62	OTG-INPVAL-015	Evaluar vulnerabilidades incubadas
63	OTG-INPVAL-016	Evaluar la división y/o encubrimiento de tráfico HTTP
64	OTG-ERR-001	Análisis de códigos de error
65	OTG-ERR-002	Análisis de trazados de pila
Criptografía		
66	OTG-CRYPST-001	Evaluar cifrados débiles de SSL/TSL, protección protecciones insuficientes en el transporte

67	OTG-CRYPST-002	Evaluar ataques del tipo "Padding Oracle"
68	OTG-CRYPST-003	Evaluar información sensible enviada por canales no encriptados.
Evaluación de la Lógica de Negocio		
69	OTG-BUSLOGIC-001	Evaluar la validación de datos de la lógica negocio
70	OTG-BUSLOGIC-002	Evaluar la posibilidad de falsificar peticiones
71	OTG-BUSLOGIC-003	Evaluar los controles de integridad
72	OTG-BUSLOGIC-004	Evaluar el tiempo de procesamiento
73	OTG-BUSLOGIC-005	Evaluar la cantidad de veces que una función puede ser usada sin límites
74	OTG-BUSLOGIC-006	Evaluar las desviaciones en flujos de trabajo
75	OTG-BUSLOGIC-007	Evaluar las defensas ante malos usos de las aplicaciones
76	OTG-BUSLOGIC-008	Evaluar la carga de archivos de tipos no esperados
77	OTG-BUSLOGIC-009	Evaluar la carga de archivos con contenido malicioso
Evaluación del Lado Cliente		
78	OTG-CLIENT-001	Evaluar Cross Site Scripting basados en DOM (Document Object Model)
79	OTG-CLIENT-002	Evaluar la ejecución de JavaScript
80	OTG-CLIENT-003	Evaluar inyecciones de HTML
81	OTG-CLIENT-004	Evaluar redirecciones de URL en el Lado Cliente
82	OTG-CLIENT-005	Evaluar inyecciones de CSS
83	OTG-CLIENT-006	Evaluar la manipulación de recursos del Lado Cliente
84	OTG-CLIENT-007	Evaluar "Cross Origin Resource Sharing"
85	OTG-CLIENT-008	Evaluar "Cross Site Flashing"
86	OTG-CLIENT-009	Evaluar "Clickjacking"
87	OTG-CLIENT-010	Evaluar WebSockets
88	OTG-CLIENT-011	Evaluar "Web Messaging" (Cross Document Messaging)
89	OTG-CLIENT-012	Evaluar almacenamiento local

Pruebas de seguridad que se realizaran sobre los Web Services y APIS.

- Confidencialidad del Transporte
- Autenticación del Servidor
- Mecanismos de autenticación del usuario
- Evaluación de los mecanismos de Encoding
- Integridad de los mensajes

- Confidencialidad de los mensajes
- Autorización
- Esquemas de validación
- Validación del contenido
- Pruebas de tamaño de los mensajes para evaluar ataques DOS
- Perfiles de seguridad en el punto final del sistema que consume el web Service

9.7 Herramientas a utilizar.

Fase de Ethical Hacking	Herramientas	Descripción de funcionalidad
Reconocimiento	Sublist3r - https://github.com/aboul3la/Sublist3r Theharvester - https://github.com/laramies/theHarvester Dnsdumpster - https://dnsdumpster.com/ Findsubdomains - https://findsubdomains.com/	Herramientas utilizadas para identificar las direcciones IP asociadas a la organización, identificación de segmentos de red, identificación de subdominios e identificación de servicios principales.
	Nslookup – Comando nativo del sistema operativo Whois – Comando nativo del sistema operativo Consulta en repositorios públicos (Google, Bing, Shodan) - https://www.shodan.io/	Herramientas utilizadas para la identificación de registros a nivel de los servidores DNS, identificación de controles SPF y búsqueda de información sensible en Internet y Redes Sociales.
Escaneo	Escaneo de Puertos y Servicios: Nmap - https://nmap.org Zenmap GUI - https://nmap.org SoftPerfect Network Scanner - https://www.softperfect.com/products/networkscanner/	Herramienta para identificación de puertos a través del protocolo TCP/UDP, escaneo de servicios e identificación de sistemas operativos. Se utiliza la herramienta y sus técnicas de escaneo (syn, tcp, xmas, fin, ack, etc) para identificar puertos y/o backdoors a nivel del sistema operativo.
	Escaneo de Vulnerabilidades: NSE – NMAP (Nmap Scan Engine) - https://nmap.org Nessus Professional - https://www.tenable.com/products/nessus/nessus-professional Metasploit Auxiliary Scan - https://www.metasploit.com	Herramientas utilizadas para identificar vulnerabilidades sobre puertos del protocolo TCP/UDP identificados sobre el sistema operativos. Detalle de herramientas: - NSE – Nmap: El uso de NMAP Script Engine permite la identificación de múltiples vulnerabilidades sobre servicios del sistema operativo. - Nessus Professional: La herramienta cuenta con scripts y templates para la identificación de vulnerabilidades asociadas a servicios y el sistema

Fase de Ethical Hacking	Herramientas	Descripción de funcionalidad
		operativo de la organización. - Metasploit: El framework METASPLOIT cuenta con un módulo auxiliar para la identificación de vulnerabilidades a nivel de diversos protocolos y servicios del sistema operativo.
Escaneo	Escaneo de vulnerabilidades en Base de Datos: A continuación, se detallan las herramientas a utilizar la identificación de vulnerabilidades en base de datos: Hydra - https://sectools.org/tool/hydra/ Metasploit Auxiliary Module - https://www.metasploit.com Metasploit Post Explotation Module - https://www.metasploit.com Nessus Plugins Base de Datos - https://www.tenable.com/products/nessus/nessus- professional	Gestión de contraseñas: La herramienta HYDRA permite realizar un análisis de la gestión de contraseñas del sistema de base de datos. Gestión de configuración: El módulo auxiliar de METASPLOIT permite identificar las configuraciones débiles a nivel de bases de datos, las mismas que consideran PROCEDURES, funciones y configuraciones débiles que permiten ESCALAR privilegios. Gestión de actualizaciones y/o parches: Nessus Plugins cuenta con quinientos noventa y un (591) plugins para la detección de vulnerabilidades a nivel de motores de Bases de Datos.
	Escaneo de vulnerabilidades en Aplicaciones Web Acunetix - https://www.acunetix.com/ ZAP OWASP - https://www.owasp.org/index.php/OWASP_Zed_Attack_Proxy_Project BurpSuite Professional - https://portswigger.net/burp	Herramientas automatizadas: Acunetix y OWASP ZAP Estas herramientas permiten la identificación de vulnerabilidades conocidas a través de la modificación de parámetros en el sistema de información. Las herramientas permiten identificar vulnerabilidades asociadas a: SQL injection, Cross Site Scripting (XSS), CSRF (Cross Site Request Forgery, LFI (Local File Inclusion), RFI (Remote File inclusión). Herramientas de análisis manual: BurpSuite Professional Esta herramienta permite identificar los REQUEST y RESPONSE del sistema de información evaluado. Ideal para identificar vulnerabilidades a nivel del flujo de información, gestión de privilegios, identificación de roles y perfiles, identificación de exposición de información

Fase de Ethical Hacking	Herramientas	Descripción de funcionalidad
		innecesaria, así como la explotación manual de vulnerabilidades.
Explotación de Vulnerabilidades	A continuación, se detallan las herramientas para la explotación de vulnerabilidades: METASPLOIT Framework: ▪ Módulo Exploit ▪ Módulo Payload ▪ Módulo Post-Explotación John the Ripper RainbowCrack OPHCrack Systernals Microsoft: ▪ Procdump ▪ PsExec ▪ ProcessExplorer Mimikatz Pass The Hash (PTH) AIRCRACK-NG Vistumbler SQLMAP BurpSuite Firefox - HackBar	<u>Herramientas de explotación de vulnerabilidades</u>: Metasploit Framework es un entorno que contiene EXPLOITS y Payloads, los mismos que permiten el acceso a computadores/servidores a través de vulnerabilidades identificadas en la fase de "Escaneo de Vulnerabilidades". La herramienta Metasploit Framework contiene un número importante de exploits para acceder a sistemas operativos Microsoft Windows y Unix (Linux entre otros), una vez obtenido el acceso es posible ELEVAR PRIVILEGIOS a través de exploits locales. <u>Herramientas de POST – Explotación</u>: Las herramientas de POST – Explotación, permiten evaluar desde la perspectiva un atacante real los riesgos reales a los cuales se encuentran expuestos las organizaciones después de la explotación de vulnerabilidades. Las actividades y herramientas a utilizar son: - John the Ripper, RainbowCrack y OPCrack: Herramientas para hacer CRACKING de contraseñas a nivel del sistema operativo y Bases de Datos. - Mimikatz: Herramienta para procesar los DUMP de memoria y obtener contraseñas en texto claro.

Fase de Ethical Hacking	Herramientas	Descripción de funcionalidad
		Herramientas para análisis Wireless: Aicrack-NG y Vistumbler: Herramientas para realizar WARDRIVING y CRACKING de contraseñas Wireless.

9.8 Entregables

A efectos de cumplir con las actividades encomendadas, el proveedor deberá presentar los siguientes entregables.

ENTREGABLE	NOMBRE	DESCRIPCIÓN	ENTREGA
Entregable 1	Plan de Gestión del Proyecto	Informe Gestión del Proyecto.	A los 4 días de la firma o recepción de la orden de compra.
Entregable 2	Informe técnico detallado	Informe Técnico de Vulnerabilidades	A los 30 días de la firma o recepción de la orden de compra.
Entregable 3	Resumen ejecutivo	Informe Final.	A los 33 días de la firma o recepción de la orden de compra.

10. REQUISITOS DE CALIFICACIÓN:

10.1. CAPACIDAD LEGAL

10.1.1 Representación

El postor deberá acreditar la vigencia de los poderes del Representante Legal o Apoderado, con copia simple de la vigencia de poderes expedida por Registros Público, con una antigüedad no mayor a treinta (30) días a la presentación de la oferta.

De ser el caso, presentará la promesa formal de consorcio con firmas legalizadas de todos los integrantes del consorcio, en la que se consigne los datos de los integrantes, el representante común, el domicilio común y las obligaciones a las que se compromete cada uno de los integrantes del consorcio, así como el porcentaje equivalente a dichas obligaciones.

10.2. CAPACIDAD TÉCNICA Y PROFESIONAL

10.2.1 Equipamiento

El proveedor deberá acreditar que cuenta con el equipamiento y recursos mínimos necesarios para garantizar un eficiente y oportuno servicio, con la presentación de una Declaración Jurada.

10.2.2 Experiencia del Personal

El Proveedor deberá asegurar la participación de tres (03) consultores de seguridad de la información, los cuales deben cumplir con los siguientes requisitos mínimos:

10.2.2.1 Gerente o Jefe del Proyecto:

Cantidad: Un (1) Profesional.

Experiencia: Con experiencia profesional mínima de 8 años en TI, y haber participado como líder en proyectos relacionado a: Ethical Hacking y Análisis de Vulnerabilidades; Implementación de SGSI basado en ISO27001, Políticas y Procedimientos; Auditoría de Sistemas y Consultoría en Seguridad de la Información. Haber participado en 10 proyectos de Ethical Hacking.

Estudios Profesionales: Ingeniero Informático o de Sistemas, titulado.

Certificaciones: El gerente del proyecto deberá poseer por lo menos 3 certificaciones de los siguientes:

- ISO 27001 Lead Implementer, ISO 27001 Lead Auditor, C) ISSO (Certified Information Systems Security Officer), CISA (Certified Information Systems Auditor), CRISC (Certified in Risk and Information Systems Control)
- Certificación PMP (gestión de proyectos).

10.2.2.2 Consultor Sénior en Seguridad de la Información:

Cantidad: Un (1) Profesional.

Experiencia: Con experiencia profesional mínima de 06 años como Consultor Senior en Seguridad de la Información, enfocado en servicios de Análisis y Vulnerabilidades, Hacking Ético, Pentesting y Gestión de Riesgos de TI e ISO27001. Haber participado en 10 proyectos de Ethical Hacking.

Estudios Profesionales: Ingeniero Informático o de Sistemas, titulado.

Certificaciones: Deberá poseer por lo menos 4 certificaciones de los siguientes: ISO 27001 Lead Auditor, C|EH (Certified Ethical Hacker), CPTE (Certified Penetration Testing Engineer) , Security+, ITIL v3, CSWAE (Certified Secure Web Application Engineer), CPEH (Certified Professional Ethical Hacker), CISM (Certified Information Security Manager) o CPTC (Certified Penetrationt Testing Consultant).

10.2.2.3 Consultor Apoyo en Seguridad de la Información:

Cantidad: Un (01) Profesional

Experiencia: Con experiencia profesional mínima de 04 años como Consultor en Seguridad de la Información, en el campo de las Tecnologías de la Información, enfocado en servicios

de Análisis y Vulnerabilidades, Hacking Ético, Pentesting. Haber participado en 05 proyectos de Ethical Hacking.

Estudios Profesionales: Egresado de una carrera técnica de sistemas, informática, redes.

Certificaciones: Deberá poseer por lo menos 3 certificaciones de los siguientes: C|EH (Certified Ethical Hacker), CPTE (Certified Penetration Testing Engineer), CSWAE (Certified Secure Web Application Engineer), CPEH (Certified Professional Ethical Hacker) o CPTC (Certified Penetrationt Testing Consultant).

Respecto a la presentación de la documentación que acredite la experiencia, estudios y certificaciones del personal propuesto.

- En al caso de las certificaciones requeridas, se debe acreditar presentando mediante copia simple certificaciones, constancias o documentos, según corresponda.
- La experiencia se acreditará con cualquiera de los siguientes documentos: i) Copia simple de contratos y su respectiva conformidad. ii) Constancias, o iii) Certificados, o iv) Cualquier otra documentación que de manera fehaciente demuestre La experiencia del personal propuesto.
- El profesional, acreditará mediante copia simple del grado de bachiller o título profesional que corresponda.

10.3. EXPERIENCIA DEL POSTOR

El servicio será desarrollado por una empresa con un mínimo de antigüedad de cinco (05) años, brindando servicios de consultoría en Seguridad Informática en instituciones del sector público, sector banca y finanzas y sector privado en general.

El proveedor deberá acreditar un mínimo de 10 proyectos de Ethical Hacking, Análisis de Vulnerabilidad, Pentesting, Penetración de Sistemas Informáticos, las mismas que deberán ser acreditadas mediante copia simple de: i) contratos u órdenes de servicio, y su respectiva conformidad por la prestación efectuada; o ii) comprobantes de pago cuya cancelación se acredite documental y fehacientemente, con Voucher de depósito, reporte de estado de cuenta bancario, cancelación en el documento, u otro documento que acredite la cancelación.

11. PLAZO DE EJECUCIÓN:

El plazo de ejecución del presente servicio se estima en 20 días, el mismo que se computa desde el día siguiente de la firma del contrato.

12. LUGAR DE PRESTACIÓN DEL SERVICIO

Las actividades citadas en el punto “9.4 plan de trabajo básico”, se realizarán en forma remota o virtual, a través de una herramienta de conexión segura proporcionada por San Gabán S.A.

13. OTRAS PENALIDADES:

No se aplicarán otras penalidades.

14. PRESTACIONES ACCESORIAS:

No aplica para la presente contratación.

15. REAJUSTES:

No aplica para la presente contratación.

16. VICIOS OCULTOS:

La recepción conforme de la prestación por parte de LA ENTIDAD no enerva su derecho a reclamar posteriormente por defectos o vicios ocultos, conforme a lo dispuesto por los artículos 40 de la Ley de Contrataciones del Estado y 173 de su Reglamento.

El plazo máximo de responsabilidad del contratista es de un (1) año contado a partir de la conformidad otorgada por San Gabán S.A.

17. CONFORMIDAD:

La conformidad de la prestación del servicio se regula por lo dispuesto en el artículo 168° del Reglamento de la Ley de Contrataciones del Estado. La conformidad será otorgada por la División de Tecnologías de la Información.

18. FORMA DE PAGO:

La entidad realizará el pago total de la contraprestación pactada a favor del contratista a la entrega del informe final y a conformidad de San Gabán S.A.:

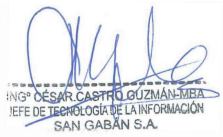
Para efectos del pago de las contraprestaciones ejecutadas por el contratista, San Gabán S.A. deberá contar con la siguiente documentación:

- Informe del funcionario responsable de la División de Tecnologías de la Información emitiendo la conformidad de la prestación efectuada.
- Comprobante de pago.
- Entregable por cada una de las fases de acuerdo al punto 11.

Dicha documentación se debe presentar en mesa de partes de San Gabán S.A., sito en Av. Floral 245, Barrio Bellavista, Puno o en su defecto en la mesa de partes virtual: mesadepartes@sangaban.com.pe. Los documentos de pago, para las valorizaciones se presentarán en la cuenta facturalogistica@sangaban.com.pe.

19. DOMICILIO PARA LA NOTIFICACIÓN EN EJECUCIÓN CONTRACTUAL:

El postor ganador de la buena pro, consignará un correo electrónico, a donde se le notificará todos los actos y actuaciones recaídos durante la ejecución contractual, como es el caso, entre otros, de ampliación de plazo. Asimismo, señalará un domicilio legal a donde se le notificará los actos que tienen un procedimiento preestablecido de notificación, como es el caso de resolución o nulidad de contrato.



Firmado digitalmente por CASTRO GUZMAN Cesar Humberto FAU 20262221335 hard
Ubicación: DNI: 06801396
Fecha: 2020.11.26 20:57:20 -05'00'

Por Área Usuaria

DECLARACION JURADA DE NO ESTAR IMPEDIDO DE CONTRATAR CON EL ESTADO

"SERVICIO DE ETHICAL HACKING DE SEGURIDAD DE LA INFORMACIÓN"

Señores.

EMPRESA DE GENERACION ELECTRICA SAN GABAN S.A.

Presente. -

De nuestra consideración:

El que suscribe……., identificado con DNI N° ……., Representante legal de la empresa …….. con RUC ……., domiciliada ……., declaro bajo juramento:

i. No haber incurrido y me obligo a no incurrir en actos de corrupción, así como a respetar el principio de integridad.

ii. No tener impedimento para postular en el procedimiento de contratación ni para contratar con el Estado, conforme al artículo 11 de la Ley de Contrataciones del Estado.

iii. Que mi información (en caso que el postor sea persona natural) o la información de la persona jurídica que represento, registrada en el RNP se encuentra actualizada.

iv. Conocer las sanciones contenidas en la Ley de Contrataciones del Estado y su Reglamento, así como las disposiciones aplicables del TUO de la Ley N° 27444, Ley del Procedimiento Administrativo General.

v. Participar en el presente proceso de contratación en forma independiente sin mediar consulta, comunicación, acuerdo, arreglo o convenio con ningún proveedor; y, conocer las disposiciones del Decreto Legislativo Nº 1034, Decreto Legislativo que aprueba la Ley de Represión de Conductas Anticompetitivas.

vi. Conocer, aceptar y someterme al requerimiento, condiciones y reglas del procedimiento de contratación

vii. Ser responsable de la veracidad de los documentos e información que presento en el presente procedimiento de contratación

viii. Comprometerme a mantener la oferta presentada durante el procedimiento de contratación y a la emisión de la Orden de Servicio y/o Orden de Compra, en caso de resultar favorecido con la buena pro.

Puno, ……de ……del 2020

EMPRESA DE GENERACION ELECTRICA SAN GABAN S.A.

Av. Floral Nº 245 - Bellavista Puno
Telefono : (051) 36-4401 Fax: (051) 36-5782
RUC: 20262221335

SOLICITUD DE COTIZACION E-ASP 213

DIA	MES	AÑO
		2020

SEÑORES / RAZON SOCIAL : .....

DIRECCION : ..... **RUC:** .....

TELEFONO : ..... **E-MAIL** .....

MARCAR : **BOLETA :** ☐ **FACTURA :** ☐ **GUIA DE REMISION :** ☐ **RECIBO X HONORARIOS :** ☐

INCLUYE : **IGV :** ☐

De nuestra consideración, sírvase cotizar a nombre de EMPRESA DE GENERACION ELECTRICA SAN GABAN S.A. lo solicitado a continuación, remitiendonos la presente solicitud a mas tardar el dia / / .

Entregar esta solicitud en las oficinas de San Gaban S.A:, mediante FAX: (051) 36-5782 o al correo electronico : **logistica@sangaban.com.pe.**

ITEM	CANT.	UNIDAD	DESCRIPCION BIEN / SERVICIO	PRECIO UNITARIO	TOTAL
				S/.	S/.
1	1	SERVICIO	SERVICIO DE ETHICAL HACKING DE SEGURIDAD DE LA INFORMACIÓN		
			Según Terminos de Referencia.		
			Incluye IGV		
			TOTAL		S/.

CPC. ALEX PHOL CALATAYUD QUISPE

Jefe de Logistica y Servicios
Empresa de Generacion Electrica San Gaban S.A.

FIRMA AUTORIZADA Y SELLO DEL PROVEEDOR

Se pide por favor que la cotizacion sea:	**Observaciones:**
a) Sin borrones ni emmendaduras casi contrario quedara sin validez.	.....
b) Especificar precio unitario con dos decimales, incluir impuestos y costos de envio.	.....
c) Indicar Plazo de Entrega	.....
d) Forma de Pago: 10 días de recepcionado y/o entregado en Bien/Servicio	
e) El Lugar de Entrega : Almacenes Av. Floral N° 245 - Ciudad de Puno	