PROPUESTA TECNICA DE SERVICIO “ETHICAL HACKING”

PENTARAMA S.A.

27 de octubre de 2025

Lima, 27 de octubre de 2025

PENTARAMA S.A.
Lima, Perú

Estimados Sr(es).

Me es muy grato saludarles y por medio de la presente hacerles llegar nuestra propuesta técnica relacionada al servicio ***"Ethical Hacking"*** para **PENTARAMA S.A.** (en adelante, **"CLIENTE", "ORGANIZACIÓN"** o **"COMPAÑIA"**).

Nuestra propuesta técnica se basa en la amplia experiencia de nuestros profesionales en auditorías, consultorías, desarrollos e implementaciones de soluciones en TI, riesgo y seguridad de la información.

La presente propuesta busca contribuir con la seguridad en la infraestructura tecnológica de su COMPAÑIA, mediante una evaluación exhaustiva y recomendaciones específicas de seguridad, que facilitarán la implementación de controles requeridos por las mejores prácticas de la industria.

Sin otro particular, quedamos a su disposición para cualquier consulta.

Atentamente,

Raúl Díaz
Socio Líder de Consultoría
Strategos Consulting Services
+51-1-307-0604 +51–994521461
raul.diaz@strategoscs.com

INDICE

1. NUESTRA EMPRESA

Strategos Consulting Services, es una compañía de capital peruano que brinda servicios de consultoría, auditoría y capacitación en la industria Financiera, Tarjetas de Pago, Energía, Salud, Militar y Gobierno. Está conformada por especialista de sobresaliente trayectoria profesional en las áreas de Estrategia de Negocios, Tecnologías de la Información, Seguridad de la Información y Riesgos.

Nuestros profesionales trabajan con los marcos de conocimiento mundialmente reconocidos publicados por las marcas:

Nuestros Diferenciadores:

- Nuestros servicios son integrales y personalizados a las necesidades de nuestros clientes.
- Nuestros resultados buscan estar alineados a los objetivos estratégicos de negocio, no solo a resultados técnicos.

- Buscamos contribuir con la innovación del modelo de negocio, productos y servicios.
- Contamos con servicios posventa sobre reevaluación del servicio de acuerdo a nuestras recomendaciones.
- Todos nuestros consultores cuentan con experiencia académica.
- Todos nuestros consultores cuentan con certificaciones internacionales de acuerdo a su campo de experiencia.
- Todos nuestros consultores están dispuestos a ayudar al cliente sobre consultas adicionales relacionadas o complementarias al servicio brindado en cualquier momento.
- Somos Centro Autorizado de Capacitación de EC-Council y EXIN.

2. OBJETIVOS DEL SERVICIO

- Validar el nivel de seguridad en cuanto a vulnerabilidades técnicas a nivel de red, segmentación y aplicaciones web.
- Brindar recomendaciones de solución para remediar las vulnerabilidades identificadas.

3. ALCANCE DEL SERVICIO

El alcance del servicio consiste en realizar un Ethical Hacking al siguiente activo**.**

N°	Activo de información	Cantidad
1	Aplicación que se conectará a NIUBIZ	1

En caso exista un cambio en el alcance, se procederá actualizar la propuesta.

4. PRUEBAS DE SEGURIDAD

Las actividades de evaluación se definen a continuación siguientes:

4.1. Evaluación de Seguridad Web OWASP WSTG

Las **pruebas de penetración externa a nivel de aplicación** web On Premise o Cloud incluirán las **89 evaluaciones** del **"Web Security Testing Guide V4.2"**.

Estas pruebas se realizarán de manera manual para no activar controles perimetrales:

Tabla 1 – WSTG

N°	ID Prueba (OWASP)	Descripción de Prueba
Obtención de Información		
1	WSTG-INFO-001	Realizar el descubrimiento y reconocimiento de divulgación de información basados en motores de búsqueda
2	WSTG-INFO-002	Identificar el software de aplicación
3	WSTG-INFO-003	Revisar archivos con metadatos en búsqueda de divulgación de información
4	WSTG-INFO-004	Enumerar las aplicaciones en el servidor web
5	WSTG-INFO-005	Revisar los comentarios y metadatos de las páginas web buscando divulgación de información
6	WSTG-INFO-006	Identificar los puntos de entrada de las aplicaciones
7	WSTG-INFO-007	Mapear las rutas de ejecución a través de las aplicaciones
8	WSTG-INFO-008	Identificar el Framework usado por las aplicaciones
9	WSTG-INFO-009	Identificar la aplicación
10	WSTG-INFO-010	Mapear la arquitectura de las aplicaciones
Evaluación de la Gestión de Configuración y Despliegue		
11	WSTG-CONFIG-001	Evaluar la configuración de la red e infraestructura
12	WSTG-CONFIG-002	Evaluar la configuración de la plataforma de las aplicaciones
13	WSTG-CONFIG-003	Evaluar el manejo de las extensiones de nombres de archivos en búsqueda de información sensible
14	WSTG-CONFIG-004	Buscar información sensible en archivos de copia de seguridad y no referenciados
15	WSTG-CONFIG-005	Enumerar las interfaces de administración de infraestructura y de las aplicaciones
16	WSTG-CONFIG-006	Evaluar los métodos HTTP
17	WSTG-CONFIG-007	Evaluar la seguridad estricta en el transporte vía HTTP
18	WSTG-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	WSTG-IDENT-001	Evaluar las definiciones de roles
20	WSTG-IDENT-002	Evaluar los procesos de registro de usuarios
21	WSTG-IDENT-003	Evaluar el proceso de aprovisionamiento de las cuentas de usuario
22	WSTG-IDENT-004	Evaluar la enumeración de cuentas de usuario y las "cuentas que se puedan adivinar"
23	WSTG-IDENT-005	Evaluar las políticas débiles o no forzadas para nombres de usuarios
24	WSTG-IDENT-006	Evaluar los permisos de cuentas tipo Invitado/Practicante
25	WSTG-IDENT-007	Evaluar el proceso de suspensión/reactivación de cuentas

N°	ID Prueba (OWASP)	Descripción de Prueba
Evaluación de la Autenticación		
26	WSTG-AUTHN-001	Evaluación de credenciales transportadas sobre un canal no encriptado
27	WSTG-AUTHN-002	Evaluar las credenciales default
28	WSTG-AUTHN-003	Evaluar los mecanismos débiles de bloqueo de cuentas
29	WSTG-AUTHN-004	Evaluar la evasión del esquema de autenticación
30	WSTG-AUTHN-005	Evaluar la funcionalidad de recordar contraseña
31	WSTG-AUTHN-006	Evaluar las debilidades del caché del browser
32	WSTG-AUTHN-007	Evaluar las políticas de contraseña débiles
33	WSTG-AUTHN-008	Evaluar los mecanismos débiles de recuperación de acceso mediante pregunta/respuesta
34	WSTG-AUTHN-009	Evaluar funcionalidades débiles de cambio de contraseña o reinicio
35	WSTG-AUTHN-010	Evaluar autenticaciones débiles mediante canales alternos
Evaluación de Autorización		
36	WSTG-AUTHZ-001	Evaluar el recorrido de directorios/inclusión de archivos
37	WSTG-AUTHZ-002	Evaluar la evasión del esquema de autorización
38	WSTG-AUTHZ-003	Evaluar el escalamiento de privilegios
39	WSTG-AUTHZ-004	Evaluar las referencias inseguras a objetos de forma directa
Evaluar el Manejo de Sesiones		
40	WSTG-SESS-001	Evaluar la evasión del esquema de manejo de sesiones
41	WSTG-SESS-002	Evaluar los atributos de las cookies
42	WSTG-SESS-003	Evaluar la "fijación" de sesiones
43	WSTG-SESS-004	Evaluar variables de sesión expuestas
44	WSTG-SESS-005	Evaluar la ocurrencia de falsificación de requerimientos cruzados (Cross Site Request Forgery)
45	WSTG-SESS-006	Evaluar la funcionalidad de termino de sesión (logout)
46	WSTG-SESS-007	Evaluar el tiempo máximo de inactividad por sesión
47	WSTG-SESS-008	Evaluar el uso inapropiado de variables de sesión (Session puzzling)
Evaluar la Validación de Datos		
48	WSTG-INPVAL-001	Evaluar Cross Site Scripting Reflejado
49	WSTG-INPVAL-002	Evaluar Cross Site Scripting Almacenado
50	WSTG-INPVAL-003	Evaluar la manipulación de verbos HTTP
51	WSTG-INPVAL-004	Evaluar la "contaminación" de parámetros HTTP
52	WSTG-INPVAL-005	Evaluar inyecciones de SQL
53	WSTG-INPVAL-006	Evaluar inyecciones de LDAP
54	WSTG-INPVAL-007	Evaluar inyecciones en datos generados por una herramienta ORM (Object Relational Mapping)
55	WSTG-INPVAL-008	Evaluar inyecciones de XML
56	WSTG-INPVAL-009	Evaluar inyecciones de SSI
57	WSTG-INPVAL-010	Evaluar inyecciones de XPath
58	WSTG-INPVAL-011	Evaluar inyecciones IMAP/SMTP
59	WSTG-INPVAL-012	Evaluar inyecciones de código
60	WSTG-INPVAL-013	Evaluar inyecciones de comandos

N°	ID Prueba (OWASP)	Descripción de Prueba
61	WSTG-INPVAL-014	Evaluar desbordamiento de buffer
62	WSTG-INPVAL-015	Evaluar vulnerabilidades incubadas
63	WSTG-INPVAL-016	Evaluar la división y/o encubrimiento de tráfico HTTP
Manejo de Errores		
64	WSTG-ERR-001	Análisis de códigos de error
65	WSTG-ERR-002	Análisis de trazados de pila
Criptografía		
66	WSTG-CRYPST-001	Evaluar cifrados débiles de SSL/TSL, protección protecciones insuficientes en el transporte
67	WSTG-CRYPST-002	Evaluar ataques del tipo "Padding Oracle"
68	WSTG-CRYPST-003	Evaluar información sensible enviada por canales no encriptados
Evaluación de la Lógica de Negocio		
69	WSTG-BUSLOGIC-001	Evaluar la validación de datos de la lógica negocio
70	WSTG-BUSLOGIC-002	Evaluar la posibilidad de falsificar peticiones
71	WSTG-BUSLOGIC-003	Evaluar los controles de integridad
72	WSTG-BUSLOGIC-004	Evaluar el tiempo de procesamiento
73	WSTG-BUSLOGIC-005	Evaluar la cantidad de veces que una función puede ser usada sin límites
74	WSTG-BUSLOGIC-006	Evaluar las desviaciones en flujos de trabajo
75	WSTG-BUSLOGIC-007	Evaluar las defensas ante malos usos de las aplicaciones
76	WSTG-BUSLOGIC-008	Evaluar la carga de archios de tipos no esperados
77	WSTG-BUSLOGIC-009	Evaluar la carga de archivos con contenido malicioso
Evaluación del Lado Cliente		
78	WSTG-CLIENT-001	Evaluar Cross Site Scripting basados en DOM (Document Object Model)
79	WSTG-CLIENT-002	Evaluar la ejecución de JavaScript
80	WSTG-CLIENT-003	Evaluar inyecciones de HTML
81	WSTG-CLIENT-004	Evaluar redirecciones de URL en el Lado Cliente
82	WSTG-CLIENT-005	Evaluar inyecciones de CSS
83	WSTG-CLIENT-006	Evaluar la manipulación de recursos del Lado Cliente
84	WSTG-CLIENT-007	Evaluar "Cross Origin Resource Sharing"
85	WSTG-CLIENT-008	Evaluar "Cross Site Flashing"
86	WSTG-CLIENT-009	Evaluar "Clickjacking"
87	WSTG-CLIENT-010	Evaluar WebSockets
88	WSTG-CLIENT-011	Evaluar "Web Messaging" (Cross Document Messaging)
89	WSTG-CLIENT-012	Evaluar almacenamiento local

4.2. Evaluación de Application Programming Interface (API)

Las pruebas de penetración externa incluirán la evaluación de APIs en servidores On Premise o CLOUD donde se realizarán las siguientes 10 pruebas determinadas por OWASP:

Tabla 2 – API Testing

Id de prueba	Prueba	Descripción de riesgo
API1-2023	Evaluación de autorización de nivel de objeto débil	Las APIs tienden a exponer puntos finales que manejan identificadores de objetos, creando un problema de control de acceso. Las verificaciones de autorización a nivel de objeto deben considerarse en cada función que accede a una fuente de datos utilizando una entrada del usuario.
API2-2023	Evaluación de autenticación de usuario débil	Los mecanismos de autenticación a menudo se implementan incorrectamente, lo que permite a los atacantes comprometer los tokens de autenticación o explotar fallas de implementación para asumir las identidades de otros usuarios de manera temporal o permanente. La capacidad de comprometer el sistema para identificar al usuario compromete la seguridad de la API en general.
API3-2023	Evaluación de exposición excesiva de datos	Los desarrolladores tienden a exponer todas las propiedades de los objetos sin tener en cuenta la sensibilidad de los datos, confiando en el filtrado de datos de la misma página cliente.
API4-2023	Evaluación de falta de recursos y limitación de velocidad	Las APIs, normalmente, no imponen ninguna restricción sobre el tamaño o la cantidad de recursos que puede solicitar el usuario. Esto no solo puede afectar el rendimiento del servidor API, lo que conlleva una denegación de servicio (DoS), también deja la puerta abierta para ataques de fuerza bruta en la de autenticación.
API5-2023	Evaluación de autorización de nivel de función débil	Las políticas de control de acceso complejas con diferentes jerarquías, grupos y roles, y una separación poco clara entre las funciones administrativas y normales, tienden a generar fallas de autorización. Al explotar estas debilidades, los atacantes obtienen acceso a los recursos y / o funciones administrativas de otros usuarios.
API6-2023	Evaluación de asignación masiva	El envió de datos del cliente (por ejemplo, JSON) a modelos de datos en el servidor, sin un filtrado de propiedades adecuado basado en una lista blanca, generalmente conduce a la asignación masiva. Adivinar las propiedades de los objetos, explorar otros puntos finales de la API, leer la documentación o proporcionar propiedades de objetos adicionales en las cargas útiles de solicitud, permite a los atacantes modificar las propiedades de los objetos que no deberían hacerlo.
API7-2023	Evaluación de configuración incorrecta de seguridad	La configuración incorrecta de seguridad suele ser el resultado de configuraciones predeterminadas no seguras, configuraciones incompletas o ad-hoc, almacenamiento en la nube abierta, encabezados HTTP mal configuradas, métodos HTTP innecesarios, uso

Id de prueba	Prueba	Descripción de riesgo
		compartido de permisos de recursos de origen cruzado (CORS) y mensajes de error detallados que contienen información confidencial.
API8-2023	Evaluación de inyección	Los defectos de inyección, como SQL, NoSQL, Inyección de comandos, etc., ocurren cuando se envían datos no confiables a un intérprete como parte de un comando o consulta. Los datos maliciosos del atacante pueden engañar al intérprete para que ejecute comandos no deseados o acceda a los datos sin la autorización adecuada.
API9-2023	Evaluación de gestión de activos impropia	Las API tienden a exponer más puntos finales que las aplicaciones web tradicionales, lo que hace que la documentación adecuada y actualizada sea muy importante. Los hosts adecuados y el inventario de versiones de API implementadas también juegan un papel importante para mitigar problemas como versiones de API obsoletas y puntos finales de depuración expuestos.
API10-2023	Insuficiente registro y monitoreo	El registro y la supervisión insuficientes o respuesta a incidentes ineficaz, permite a los atacantes comprometer aún más los sistemas, mantener la persistencia, saltar a más sistemas, extraer o destruir datos. La mayoría de los estudios de incumplimiento demuestran que el tiempo para detectar un incumplimiento es superior a 200 días, generalmente detectado por partes externas en lugar de procesos internos o monitoreo.

4.3. Evaluación de Aplicaciones Móviles OWASP MSTG

Las pruebas de penetración de móvil incluirán la evaluación las siguientes evaluaciones de acuerdo con el tipo de aplicación móvil y su funcionalidad:

Tabla 3 – Mobile Security Testing Guide

Architecture, Design and Threat Modeling Requirements	
MASVS-ID	**Detailed Verification Requirement**
MSTG-ARCH-1	Todos los componentes se encuentran identificados y asegurar que son necesarios.
MSTG-ARCH-2	Los controles de seguridad nunca se aplican sólo en el cliente, sino que también en los respectivos servidores.
MSTG-ARCH-3	Se definió una arquitectura de alto nivel para la aplicación y los servicios y se incluyeron controles de seguridad en la misma.
MSTG-ARCH-4	Se identificó claramente la información considerada sensible en el contexto de la aplicación móvil.

MSTG-ARCH-5	Todos los componentes de la aplicación están definidos en términos de la lógica de negocio o las funciones de seguridad que proveen.
MSTG-ARCH-6	Se realizó un modelado de amenazas para la aplicación móvil y los servicios en el que se definieron las mismas y sus contramedidas.
MSTG-ARCH-7	Todos los controles de seguridad poseen una implementados centralizada.
MSTG-ARCH-8	Existe una política explícita sobre el uso de claves criptográficas (si se usan) a través de todo su ciclo de vida. Idealmente siguiendo un estándar de gestión de claves como el NIST SP 800-57.
MSTG-ARCH-9	Existe un mecanismo para forzar las actualizaciones de la aplicación móvil.
MSTG-ARCH-10	La implementación de medidas de seguridad es una parte esencial durante todo el ciclo de vida del desarrollo de software de la aplicación.
MSTG-ARCH-11	Existe una política de divulgación responsable y es llevada a cabo adecuadamente.
MSTG-ARCH-12	La aplicación debería de cumplir con las leyes y regulaciones de privacidad.
Data Storage and Privacy Requirements	
MASVS-ID	**Detailed Verification Requirement**
MSTG-STORAGE-1	Las funcionalidades de almacenamiento de credenciales del sistema deben de ser utilizadas para almacenar información sensible, tal como información personal, credenciales de usuario o claves criptográficas.
MSTG-STORAGE-2	No se debe almacenar información sensible fuera del contenedor de la aplicación o del almacenamiento de credenciales del sistema.
MSTG-STORAGE-3	No se escribe información sensible en los registros (logs) de la aplicación.
MSTG-STORAGE-4	No se comparte información sensible con servicios externos salvo que sea una necesidad de la arquitectura.
MSTG-STORAGE-5	Se desactiva la caché del teclado en los campos de texto que contienen información sensible.
MSTG-STORAGE-6	No se expone información sensible mediante mecanismos de comunicación entre procesos (IPC).
MSTG-STORAGE-7	No se expone información sensible como contraseñas y números de tarjetas de crédito a través de la interfaz o capturas de pantalla.
MSTG-STORAGE-8	No se incluye información sensible en las copias de seguridad generadas por el sistema operativo.

MSTG-STORAGE-9	La aplicación elimina toda información sensible de la vista cuando la aplicación pasa a un segundo plano.
MSTG-STORAGE-10	La aplicación no conserva ninguna información sensible en memoria más de lo necesario y la memoria se limpia tras su uso.
MSTG-STORAGE-11	La aplicación obliga a que exista una política mínima de seguridad en el dispositivo, como que el usuario deba configurar un código de acceso.
MSTG-STORAGE-12	La aplicación educa al usuario acerca de los tipos de información personal que procesa y de las mejores prácticas en seguridad que el usuario debería seguir al utilizar la aplicación.
MSTG-STORAGE-13	No se guarda ningún tipo de información sensible de forma local en el dispositivo móvil. En su lugar, esa información debería ser obtenida desde un sistema remoto sólo cuando es necesario y únicamente residir en memoria.
MSTG-STORAGE-14	En caso de ser necesario guardar información sensible de forma local, ésta debe de ser cifrada usando una clave derivada del hardware de almacenamiento seguro, el cual debe requerir autenticación previa.
MSTG-STORAGE-15	El almacenamiento local de la aplicación debe de ser borrado tras un número excesivo de intentos fallidos de autenticación.
Cryptography Requirements	
MASVS-ID	**Detailed Verification Requirement**
MSTG-CRYPTO-1	La aplicación no depende únicamente de criptografía simétrica cuyas claves se encuentran directamente en el código fuente de la misma.
MSTG-CRYPTO-2	La aplicación utiliza implementaciones de criptografía probadas.
MSTG-CRYPTO-3	La aplicación utiliza primitivas de seguridad que son apropiadas para el caso particular y su configuración y parámetros siguen las mejores prácticas de la industria.
MSTG-CRYPTO-4	La aplicación no utiliza protocolos o algoritmos criptográficos ampliamente considerados obsoletos para su uso en seguridad.
MSTG-CRYPTO-5	La aplicación no reutiliza una misma clave criptográfica para varios propósitos.
MSTG-CRYPTO-6	Los valores aleatorios son generados utilizando un generador de números aleatorios suficientemente seguro.
Authentication and Session Management Requirements	
MASVS-ID	Detailed Verification Requirement

MSTG-AUTH-1	Si la aplicación provee acceso a un servicio remoto, un mecanismo aceptable de autenticación como usuario y contraseña es realizado en el servidor remoto.
MSTG-AUTH-2	Si se utiliza la gestión de sesión por estado, el servidor remoto usa tokens de acceso aleatorios para autenticar los pedidos del cliente sin requerir el envío de las credenciales del usuario en cada uno.
MSTG-AUTH-3	Si se utiliza la autenticación basada en tokens sin estado, el servidor proporciona un token que se ha firmado utilizando un algoritmo seguro.
MSTG-AUTH-4	Cuando el usuario cierra sesión se termina la sesión también en el servidor.
MSTG-AUTH-5	Existe una política de contraseñas y es aplicada en el servidor.
MSTG-AUTH-6	El servidor implementa mecanismos, cuando credenciales de autenticación son ingresadas una cantidad excesiva de veces.
MSTG-AUTH-7	Las sesiones y los tokens de acceso expiran luego de un tiempo predefinido de inactividad.
MSTG-AUTH-8	La autenticación biométrica, si la hay, no está asociada a eventos (p. ej. usando una API que simplemente retorna "true" o "false"), sino basada en el desbloqueo del keychain/keystore (almacenamiento seguro).
MSTG-AUTH-9	El sistema remoto implementa un mecanismo de segundo factor de autenticación (2FA) y lo impone consistentemente.
MSTG-AUTH-10	Para realizar transacciones críticas se requiere una autenticación adicional (step-up).
MSTG-AUTH-11	La aplicación informa al usuario acerca de todas las actividades sensibles en su cuenta. El usuario es capaz de ver una lista de los dispositivos conectados, información contextual (dirección IP, localización, etc.), y es capaz de bloquear ciertos dispositivos.
MSTG-AUTH-12	Los modelos de autorización deberían de ser definidos e impuestos por el sistema remoto.
Network Communication Requirements	
MASVS-ID	**Detailed Verification Requirement**
MSTG-NETWORK-1	La información es enviada cifrada utilizando TLS. El canal seguro es usado consistentemente en la aplicación.
MSTG-NETWORK-2	Las configuraciones del protocolo TLS siguen las mejores prácticas de la industria, o lo hacen lo mejor posible en caso de que el sistema operativo del dispositivo no soporte los estándares recomendados.

MSTG-NETWORK-3	La aplicación verifica el certificado X.509 del sistema remoto al establecer el canal seguro y sólo se aceptan certificados firmados por una CA de confianza.
MSTG-NETWORK-4	La aplicación utiliza su propio almacén de certificados o realiza _pinning_ del certificado o la clave pública del servidor. Bajo ningún concepto establecerá conexiones con servidores que ofrecen otros certificados o claves, incluso si están firmados por una CA de confianza.
MSTG-NETWORK-5	La aplicación no depende de un único canal de comunicaciones inseguro (email o SMS) para operaciones críticas como registro de usuarios o recuperación de cuentas.
MSTG-NETWORK-6	La aplicación sólo depende de bibliotecas de conectividad y seguridad actualizadas.
Platform Interaction Requirements	
MASVS-ID	**Detailed Verification Requirement**
MSTG-PLATFORM-1	La aplicación requiere la cantidad de permisos mínimamente necesaria.
MSTG-PLATFORM-2	Todo dato ingresado por el usuario o cualquier fuente externa debe ser validado y, si es necesario, saneado. Esto incluye información recibida por la UI o mecanismos IPC como los Intents, URLs y datos provenientes de la red.
MSTG-PLATFORM-3	La aplicación no expone ninguna funcionalidad sensible a través esquemas de URL salvo que dichos mecanismos estén debidamente protegidos.
MSTG-PLATFORM-4	La aplicación no expone ninguna funcionalidad sensible a través de mecanismos IPC salvo que dichos mecanismos estén debidamente protegidos.
MSTG-PLATFORM-5	JavaScript se encuentra deshabilitado en los WebViews salvo que sea necesario.
MSTG-PLATFORM-6	Las WebViews se configuran para permitir el mínimo de los esquemas (idealmente, sólo https). Esquemas peligrosos como file, tel y app-id están deshabilitados.
MSTG-PLATFORM-7	Si objetos nativos son expuestos en WebViews, debe verificarse que cualquier componente JavaScript se carga exclusivamente desde el contenedor de la aplicación.
MSTG-PLATFORM-8	La serialización de objetos, si se realiza, debe implementarse utilizando API seguras.
MSTG-PLATFORM-9	La aplicación se protege contra ataques de tipo screen overlay. (sólo Android)
MSTG-PLATFORM-10	La caché, el almacenamiento y los recursos cargados (JavaScript, etc.) de las WebViews deben de borrarse antes de destruir la WebView.

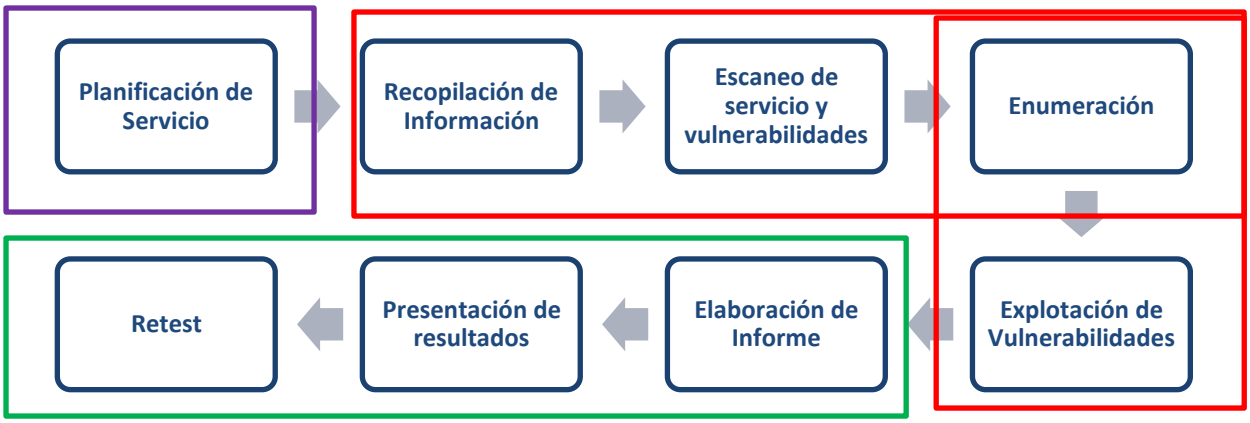
MSTG-PLATFORM-11	Verificar que la aplicación impide el uso de teclados de terceros siempre que se introduzca información sensible. (sólo iOS)
Code Quality and Build Setting Requirements	
MASVS-ID	**Detailed Verification Requirement**
MSTG-CODE-1	La aplicación es firmada y provista con un certificado válido, cuya clave privada está debidamente protegida.
MSTG-CODE-2	La aplicación fue publicada en modo release y con las configuraciones apropiadas para el mismo (por ejemplo, non-debuggable).
MSTG-CODE-3	Los símbolos de depuración fueron eliminados de los binarios nativos.
MSTG-CODE-4	Cualquier código de depuración y/o de asistencia al desarrollador (p. ej. código de test, backdoors, configuraciones ocultas) debe ser eliminado. La aplicación no hace logs detallados de errores ni de mensajes de depuración.
MSTG-CODE-5	Todos los componentes de terceros se encuentran identificados y revisados en cuanto a vulnerabilidades conocidas.
MSTG-CODE-6	La aplicación captura y gestiona debidamente las posibles excepciones.
MSTG-CODE-7	Los controles de seguridad deniegan el acceso por defecto.
MSTG-CODE-8	En código no administrado, la memoria es solicitada, utilizada y liberada de manera correcta.
MSTG-CODE-9	Las funcionalidades de seguridad gratuitas de las herramientas, tales como minificación del byte-code, protección de la pila, soporte PIE y conteo automático de referencias, se encuentran activadas.
Resilience Requirements	
MASVS-ID	**Detailed Verification Requirement**
MSTG-RESILIENCE-1	La aplicación detecta y responde a la presencia de un dispositivo rooteado, ya sea alertando al usuario o finalizando la ejecución de la aplicación.
MSTG-RESILIENCE-2	La aplicación impide la depuración o detecta y responde a la misma. Se deben cubrir todos los protocolos de depuración.
MSTG-RESILIENCE-3	La aplicación detecta y responde a cualquier modificación de ejecutables y datos críticos de la propia aplicación.
MSTG-RESILIENCE-4	La aplicación detecta la presencia de herramientas de ingeniería inversa o frameworks comunmente utilizados.
MSTG-RESILIENCE-5	La aplicación detecta y responde a ser ejecutada en un emulador.

MSTG-RESILIENCE-6	La aplicación detecta y responde ante modificaciones de código o datos en su propio espacio de memoria.
MSTG-RESILIENCE-7	La aplicación implementa múltiples mecanismos de detección para los puntos del 8.1 al 8.6. Nótese que, a mayor cantidad y diversidad de mecanismos usados, mayor será la resistencia.
MSTG-RESILIENCE-8	Los mecanismos de detección provocan distintos tipos de respuestas, incluyendo respuestas retardadas y silenciosas.
MSTG-RESILIENCE-9	La ofuscación se aplica a las defensas del programa, lo que a su vez impide la desofuscación mediante análisis dinámico.
MSTG-RESILIENCE-10	La aplicación implementa un “enlace al dispositivo” utilizando una huella del dispositivo derivado de varias propiedades únicas al mismo.
MSTG-RESILIENCE-11	Todos los archivos ejecutables y bibliotecas correspondientes a la aplicación se encuentran cifrados, o bien los segmentos importantes de código se encuentran cifrados o "empaquetados" (packed). De este modo cualquier análisis estático trivial no revelará código o datos importantes.
MSTG-RESILIENCE-12	Si el objetivo de la ofuscación es proteger código propietario, debe utilizarse un esquema de ofuscación apropiado para la tarea particular y robusto contra métodos de deofuscación manual y automatizada, considerando la investigación actual publicada. La eficacia del esquema de ofuscación debe verificarse mediante pruebas manuales. Nótese que, siempre que sea posible, las características de aislamiento basadas en hardware son preferibles a la ofuscación.
MSTG-RESILIENCE-13	A modo de defensa en profundidad, además de incluir un refuerzo (hardening) sólido de la comunicación, puede implementarse el cifrado de datos (payloads) a nivel de aplicación como medida adicional contra ataques de eavesdropping.

5. NUESTRA METODOLOGIA

Nuestra metodología de pruebas de seguridad se basa en las mejores prácticas como *OWASP, NIST SP 800-115 y PCI DSS v4.0 requisito 11.4* incluyen las siguientes actividades:

Pre-Engagement Engagement



Post-Engagement

Planificación: En esta etapa se firman los acuerdo de confidencialidad, se entregan las direcciones IP del alcance, criterios de éxito, revisión de informes de vulnerabilidades pasadas y modelo de amenazas, revisión de la documentación PCI DSS como matriz CDE, flujo de datos de tarjeta y arquitectura de red que incluya segmentación, lista de controles compensatorios aplicados y ultimo informe ROC.

Recopilación de Información o reconocimiento: En esta etapa se recopila información vital como nombre de usuarios, protocolos hasta contar con la información suficiente para explotar alguna debilidad o vulnerabilidad que permita acceso a las máquinas comprometidas.

Escaneo de servicios y vulnerabilidades: En esta etapa se realiza el escaneo de puertos y servicios. Luego se analizan las vulnerabilidades en los servicios encontrados.

Enumeración: Se hace un inventario de los puertos y servicios abiertos, así como las vulnerabilidades encontradas.

Explotación: Se realiza la identificación y diseño de exploits para las vulnerabilidades encontradas. En la prueba de externa e interna se tratarán de enviar inyecciones de código a las aplicaciones Web o correos electrónicos maliciosos para obtener acceso a la organización. A nivel de aplicación se evaluarán las siguientes debilidades según el TOP TEN OWASP 2021:

- A1. Control de Acceso Débil
- A2. Fallas Criptográficas
- A3. Inyección
- A4. Diseño Inseguro
- A5. Inadecuada Configuración de Seguridad
- A6. Componentes vulnerables y fuera de vigencia
- A7. Fallas de Identificación y Autenticación
- A8. Fallas de Integridad de Datos y Software
- A9. Fallas de monitoreo y logging de seguridad
- A10. Server-Side Request Forgery (SSRF)

Elaboración de Informe: Se redacta todos los resultados y hallazgos obtenidos de las pruebas de penetración. Se incluyen todas las evidencias por cada vulnerabilidad encontrada. Para cada vulnerabilidad se analiza la desviación contra las normas o estándares de seguridad aceptada por la industria como ISO 27001, ISO 27002, SBS 504, NIST SP 800-115, OWASP y PCI DSS v4.0. Se utilizará la calificación CVSS v3.1 o v4.0 según corresponda.

6. TIEMPO DEL SERVICIO

El tiempo de servicio es de 8 días útiles.

7. HONORARIOS

Nuestros honorarios ascienden a S/.12,000 (soles). No incluye IGV.

Forma de pago: 70% adelanto y 30% al final.

8. ENTREGABLES

Nuestros entregables son:

- Informe ejecutivo y técnico que detalla las vulnerabilidades identificadas y eventos de riesgos y recomendaciones de mejora. En el informe se incluye las pruebas no exitosas.
- Informe del Re-test (Hasta 1 año después de la ejecución del servicio cuando subsane las vulnerabilidades el CLIENTE)

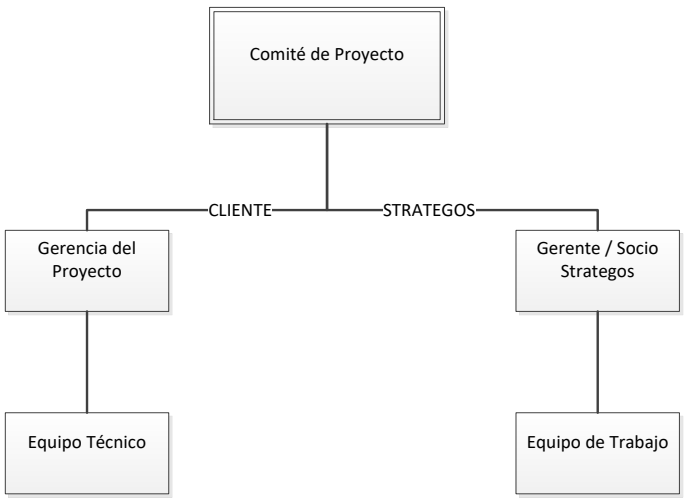
Los informes incluyen lo siguiente:

- Metodología de trabajo
- Evidencia de las vulnerabilidades.
- Recomendaciones de remediación de vulnerabilidades.

9. EQUIPO DEL PROYECTO

Se conformarán equipos mixtos de trabajo tanto de la COMPAÑIA como de *Strategos Consulting Services.*

El proyecto se organizará con tres niveles de gestión, tal como se muestra a continuación:



Comité de Dirección del Proyecto

Este comité es el máximo organismo de dirección del Proyecto, y estaría conformado por el Gerente General de la COMPAÑIA y/o los Directores y/o Gerentes asignados por la Compañía, y por el Socio o Gerente de *Strategos Consulting Services*.

Gerencia del Proyecto

La Gerencia del Proyecto estará conformada por el Gerente asignado por la COMPAÑIA y por el Director o Gerente de *Strategos Consulting Services*.

Equipo de Trabajo

Equipo de trabajo mixto el cual estará conformado por el personal técnico asignado por la COMPAÑIA y los consultores de *Strategos Consulting Services*.

Nota: *Si hubiera cambio de nuestros consultores por fuerza mayor, el reemplazo sería por uno de igual o de mayor trayectoria en seguridad informática. Los CVs se adjuntan en el ANEXO I – Equipo de Trabajo*

Consultor	Grado académico	Certificaciones	Rol
Raul Díaz	Ingeniero de sistemas, Magister en Administración de Negocios y Candidato a Doctor en Gestión Estratégica	CEH, CEH PRACTICAL, CEH MASTER, EWPT, EJPT, CPTE, ECSA, CASE JAVA	Pentester Externo e Interno
Juan Ruiz	Bachiller en Ingeniería de sistemas	CEH, CEH PRACTICAL, CEH MASTER, CPTE, EJPT, EWPT, CSWAE y ECCPT	Pentester Interno y Segmentación
Fredy Tito Chura	Ingeniero Electrónico y Magister en Seguridad Informática	CEH, CPTE, CASE JAVA, ISO 27001 LA, ISO 27001 LI, ISO 31000 Risk Manager, ISO 22301 LI, COBIT-F, ITIL y Lead Cybersecurity Professional Certificate (LCSPC)	Pentester externo e interno
German Martínez	Bachiller en Ingeniería Electrónica	EJPT	Pentester Externo
Carlos Larrabure	Bachiller en Ingeniería de Sistemas	CASE JAVA	Pentester Externo

10. CLIENTES QUE RECIBIERON SERVICIOS SIMILARES

N°	Empresas	Servicio Ejecutado	Año
1	Financiera Confianza	Ethical Hacking	2021-Al presente
2	Banco Alfin	Ethical Hacking	2023-Al presente
3	Niubiz	Pruebas de Intrusión de aplicaciones especificas	2019-Al presente
4	La Positiva	Ethical Hacking	2019-2023
5	Banco Falabella	Ethical Hacking	2017-2018
6	IZIPAY	Ethical Hacking	2023

N°	Empresas	Servicio Ejecutado	Año
	Grupo Konecta	Ethical Hacking	2022-Al presente
7	Compartamos Financiera	Evaluación Independiente ASVS y MASVS (incluye Ethical Hacking)	2022
8	Banco Interamericano de Finanzas (BANBIF)	Ethical Hacking	2023-Al presente
9	Tu Sueldo Ya	Ethical Hacking	2022
10	Pasa la Posta	Ethical Hacking	2021
11	Oficina de Normalización Previsional (ONP)	Ethical Hacking	2023
12	Electrosur	Ethical Hacking	2020-2023
13	Oficina Nacional de Procesos Electorales (ONPE)	Ethical Hacking	2021-2023
14	Caja Sullana	Evaluación Independiente ASVS y MASVS (incluye Ethical Hacking)	2024
15	Fondo de Inclusión Social Energético (FISE)	Ethical Hacking	2023
16	Superintendencia de Banca, Seguros y AFP (SBS)	Ethical Hacking	2015
17	Organismo Supervisor de Inversión Privada en Telecomunicaciones (OSIPTEL)	Ethical Hacking	2022
18	Fondo MIVIVIENDA	Ethical Hacking	2023
17	Autoridad Portuaria Nacional	Ethical Hacking	2023
18	Ministerio de Comercio Exterior - VUCE	Ethical Hacking	2023
19	Contraloría General de la Republica	Ethical Hacking	2023
20	Superintendencia Nacional de Aduanas y de Administración Tributaria (SUNAT)	Ethical Hacking	2024

11. DATOS COMERCIALES

- La propuesta tiene una validez de 30 días calendario.
- RAZON SOCIAL: Strategos y Asociados S.A.C. | RUC: 20562742787
- Contacto: Raúl Díaz | +51-994521461 o Jessica Díaz | +51-967701087
- Forma de pago, al finalizar el proyecto contra entrega de Factura.
- En caso se acepte la propuesta, el proyecto daría inicio 7 días después de recibida la O/C o se coordinara con el CLIENTE.

ANEXO I – EQUIPO DE TRABAJO DE PENTESTING

Raúl Díaz, Gestor de Proyecto

Es Socio Líder de Consultoría de Strategos Consulting Services. Asesor en Gestión de Riesgos en Leasing Total. Ingeniero de Sistemas de la Universidad de Lima, estudios de Posgrado en Gerencia de Tecnologías de la Información, Posgrado en Implantación de Sistemas Gestión de Seguridad Información según ISO/IEC 27001. Magister en Administración de Negocios en ESAN. Estudiante de doctorado en Gestión Estratégica por la PUCP. Cuenta con más de 13 años de experiencia en consultoría de servicios de Tecnologías de la Información, Seguridad de la Información y Gestión de Riesgos en la industria de tarjetas de pago, banca, energía y salud. Ha realizado proyectos de Ethical Hacking en importantes empresas como Bancolombia, Visa Argentina, Transbank, Banco Itau, Banco Mercantil de Santa Cruz, Procesos de Medios de Pago (Mastercard), Interbank, Banco Falabella, Presidencia de Consejo de Ministros, Superintendencia de Administración Tributaria, Endesa Perú, Endesa Colombia, Electrosur, Red de Energía del Perú, ISA Medellin, Banco de la Nación, Banco Azteca, Peru Rails E-Commerce, Fonafe, AFP Integra, Instituto Apoyo, EdPyme Raiz, Proempresa, Dirección General de Medicamentos, Insumos y Drogas, Caja Municipal de Tacna, Caja Municipal de Trujillo, Leasing Total, TAWA, Jurado Nacional de Elecciones entre otros. Docente de TI y Ciberseguridad en la Universidad de Lima y ESAN. Instructor Internacional para EC-COUNCIL, EXIN y PECB Latinoamérica.

Raúl cuenta con las siguientes certificaciones internacionales:

- ***ISO 37001 Senior Lead Implementer por PECB***
- ***ISO 37001 Senior Lead Auditor por PECB***
- ***ISO 27032 Lead Cybersecurity Manager por PECB***
- ***ISO 31000 Risk Manager por PECB***
- ***Certified BlockChain Professional***
- ***Certified in Risk and Information Systems Control(CRISC) por ISACA***
- ***Certified Information Security Manager (CISM) por ISACA***
- ***Certified Information System Auditor (CISA) por ISACA***
- ***Certified Penetration Testing Engineer (CPTE) por MILE2***
- ***Certified Ethical Hacker (C\|EH)***
- ***Certified Ethical Hacker Practical (C\|EH PRACTICAL)***
- ***Certified Ethical Hacker Master (C\|EH MASTER)***
- ***Elearnsecurity Junior Penetration Tester (EJPT)***
- ***Elearnsecurity Web Application Penetration Testing (EWPT)***

- ***EC-Council Certified Security Specialist (ECSS)***
- ***Certified Application Security Engineer (CASE) Java***
- ***Certified Eccouncil Instructor (C\|EI)***
- ***Certified Hacking Forensic Investigator (C\|HFI)***
- ***EC-Council Security Analyst (E\|CSA)***
- ***EC-Council Certified Secure Programmer (E\|CSP)***
- ***ISF ISO/IEC 27002 por Exin***
- ***ITIL Foundations por Exin***

Su experiencia profesional se basa en consultoría y auditoría a empresas nacionales e internacionales en diversos proyectos, tales como:

- Implementación de Sistemas de Gestión de Seguridad de la Información. ISO 27001.
- Implementación de Sistemas de Gestión de Continuidad de Negocio. ISO 22301
- Implementación de Metodología de Gestión de Riesgo. ISO 27005, Coso y Cobit.
- Implementación de Metodología del Ciclo de Vida del Software con controles de seguridad de la información según OWASP.
- Rediseño de procesos de negocio e innovación.
- Ejecución de Programas de Concientización en Seguridad de la Información.
- Evaluación de Transacciones Financieras.
- Análisis Gap y Cumplimiento PCI DSS y PA DSS.
- Cumplimiento G-140, G-139 y reglamento de tarjetas
- Auditoría de Sistemas basada en riesgos y controles internos.
- Evaluación de Madurez de Controles Internos.
- Gestión de Proyecto de Desarrollo de Software Cliente / Servidor, Web, Componentes y WebServices.
- Generación de Procedimientos de primera respuesta, cadena de custodia,
- Detección del Fraude mediante técnicas de informática forense.
- Implementación de Metodología de Gestión de Vulnerabilidades Técnicas.
- Ethical Hacking Interno y Externo a diversas tecnologías e Ingeniería social.
- Revisión de Código Fuente de JAVA, C#, VISUAL BASIC, Python y Perl.
- Diagnósticos de Seguridad Informática según ISO 27001, ISO 20000, ISO 22301
- Gestión de Proyectos de Hardening de Sistemas.

Juan Ruiz, Consultor Senior

Consultor Senior de Strategos Consulting Services. Ingeniero de Redes y Comunicaciones por la Universidad Tecnológica del Perú, con experiencia de 9 años en seguridad de redes y aplicaciones. Ha sido especialista de seguridad en MC Procesos y Jefe de Tecnologías de la Información del Instituto de la Producción

(ITP). Ha ejecutado proyectos de consultoría en el sector financiero y público sobre ciberseguridad y pentesting. Juan es certificado en **Certified Ethical Hacker (CEH), Certified Ethical Hacker Practical (CEH PRACTICAL), Certified Ethical Hacker Master (CEH MASTER) de EC-Council, ElearnSecurity Junior Penetration Tester (EJPT), Elearnsecurity Web Application Penetration Testing (EWPT), Certified Secure Web Application Engineer (CSWAE) y Certified Penetration Testing Engineer (CPTE) de Mile2**, **Certified Professional Penetration Tester (ECPPT)**, **ISO 27001 Internal Auditor y Lead Cybersecurity Professional Certificate (LCSPC).**

Virgilio Fredy Tito Chura, Consultor Senior

Consultor senior de Strategos Consulting Services con 12 años de experiencia en pruebas de penetración y seguridad de la información. Ingeniero Electrónico y Magister en Seguridad Informática en la UTP. **Cuenta con certificaciones Certified Ethical Hacker (CEH), Certified Penetration Testing Engineer (CPTE), Certified Application Security Engineer (CASE JAVA), ISO 27001 LI, ISO 27001 LA, ISO 22301 LI, ISO 31000 Risk Manager, COBIT-F, ITIL y Lead Cybersecurity Professional Certificate (LCSPC).** Ha participado en proyectos en pentesting a clientes de Strategos como Electrosur, Proempresa, Leasing Total, Rutas de Lima, La Positiva Seguros, Banco Falabella y Gildemeister.

German Martinez, Consultor Junior de Pentesting

Consultor senior de Strategos Consulting Services. Bachiller en Ingeniería de Electrónica de la UPC. Cuenta con dos años de experiencia en servicios de Ethical Hacking, Cumplimiento PCI DSS e Implementación de Sistemas de Gestión de Seguridad de la Información. **Cuenta con certificación eJPT (eLearnSecurity Junior Penetration Tester).** Cuenta con el curso Certified Application Security Engineer JAVA (CASE).

Carlos Larrabure, Consultor Junior de Pentesting

Consultor Junior de Strategos Consulting Services. Bachiller en Ingeniería de Sistemas de la Universidad de Lima. Cuenta con dos años de experiencia en servicios de Ethical Hacking, Cumplimiento PCI DSS e Implementación de Sistemas de Gestión de Seguridad de la Información. Cuenta con la **certificación Certified Application Security Engineer JAVA (CASE).**