HAWKTESTERS

PROPUESTA DE SERVICIOS DE SEGURIDAD WEB

HAWKTESTERS, S.L. & RAPICREDIT S.A.S

INFORMACIÓN DE CONTACTO

Email: sales@hawktesters.com
Número de celular: +57 317 6897494
Website: www.hawktesters.com

TABLA DE CONTENIDO

CLÁUSULA DE CONFIDENCIALIDAD

Este documento es propiedad de **HAWKTESTERS, S.L.**, y no podrá ser copiado, reproducido, distribuido ni comunicado, total o parcialmente, sin el consentimiento previo y por escrito de **HAWKTESTERS, S.L.**. En caso de utilizarse como fuente de información, deberá mencionarse la referencia correspondiente.

RAPICREDIT, S.A.S se compromete a no utilizar la información contenida en esta propuesta en caso de no formalizarse un acuerdo que derive en la aceptación del contrato correspondiente.

Este documento puede estar sujeto a modificaciones de común acuerdo entre **HAWKTESTERS, S.L.** y **RAPICREDIT, S.A.S**, las cuales se reflejarán en futuras versiones de esta propuesta.

HAWKTESTERS, S.L. se compromete a mantener la máxima confidencialidad e integridad de toda la información, datos y documentación proporcionados por **RAPICREDIT, S.A.S** a los que tenga acceso como parte de esta relación profesional. Toda la información recibida será tratada como reservada y confidencial, y su custodia y no divulgación será garantizada por parte del personal de **HAWKTESTERS, S.L.**.

En ningún momento, **HAWKTESTERS, S.L.** compartirá con terceros información relativa a esta propuesta sin contar con la autorización expresa y por escrito de **RAPICREDIT, S.A.S**.

1. RESUMEN EJECUTIVO

1.1 HAWKTESTERS, S.L.

HAWKTESTERS, S.L. es una empresa española altamente especializada en ciberseguridad, enfocada en ofrecer servicios de seguridad informática ofensiva.

Nuestro equipo, compuesto por ingenieros con más de 10 años de experiencia en el sector, cuenta con certificaciones de alto nivel, como OSCP, OSEP, OSCE, OSWE, OSCP+, OSWA, eWPTxv2 y PNPT.

1.2 IMPACTANDO VUESTRO MODELO DE NEGOCIO

En HAWKTESTERS, S.L. simulamos adversarios reales para fortalecer la resiliencia tecnológica de nuestros clientes, con un enfoque técnico profundo y adaptado al negocio. Nuestra operación combina capacidades ofensivas avanzadas con inteligencia de amenazas, permitiéndonos detectar brechas que pasan desapercibidas en enfoques convencionales.

Contamos con un stack exclusivo que incluye:

- **Equipo altamente certificado**
- **Infraestructura propia** para simulación de ataques, evadiendo mecanismos EDR/XDR/AV con agentes personalizados.
- **Instrumentación avanzada** y escenarios realistas de phishing, exfiltración, explotación y movimiento lateral.
- **Integración de Threat Intelligence** en nuestros servicios para aumentar la relevancia, calidad y realismo de cada simulación.

Trabajamos como un equipo rojo externo, pero alineado con vuestros objetivos internos de seguridad.

1.3 OBJETIVO PROPUESTA COMERCIAL

En esta ocasión, se propone la realización de una prueba de penetración sobre la aplicación web proporcionada por RAPICREDIT, S.A.S, con el objetivo de identificar vulnerabilidades críticas que puedan impactar directamente en el modelo de negocio. La evaluación se enfocará en detectar debilidades que, en caso de ser explotadas, comprometerían el funcionamiento integral de los procesos estratégicos y operativos de la organización, afectando tanto la continuidad como la competitividad del core business.

2. DESCRIPCIÓN DEL SERVICIO

El servicio propone un plan detallado para realizar una prueba de penetración orientada a identificar aquellas vulnerabilidades en las aplicaciones web de los activos en alcance que puedan impactar significativamente el modelo de negocio. La prueba adoptará metodologías estándar de la industria para asegurar una evaluación exhaustiva de la postura de seguridad, poniendo especial énfasis en analizar el impacto potencial de las vulnerabilidades detectadas sobre el funcionamiento y la continuidad operativa del core business.

2.1 OBJETIVO

Los principales objetivos de esta prueba de penetración son:

1. **Identificar vulnerabilidades** en la aplicación web que puedan comprometer el core business.
2. **Evaluar el** potencial **impacto** de estas vulnerabilidades sobre la operatividad y la continuidad del modelo de negocio.
3. **Proporcionar recomendaciones** viables para mejorar la seguridad de los activos.

2.2 METODOLOGÍA DE PRUEBAS

Para garantizar una evaluación completa, el test de penetración utilizará las siguientes metodologías:

1. **Metodologías OWASP:** Utilización de la guía de pruebas OWASP (Proyecto de Seguridad de Aplicaciones Web Abiertas) para identificar vulnerabilidades comunes en aplicaciones web.
2. **SANS Security**: Aplicación de las directrices del Instituto SANS (SysAdmin, Audit, Network, and Security) para un enfoque sistemático en las pruebas de seguridad.

2.3 EVALUACIÓN DE VULNERABILIDADES Y ANÁLISIS DE IMPACTO

Las vulnerabilidades identificadas durante el test de penetración serán evaluadas según los siguientes criterios:

1. **CVSS 3.0 (Common Vulnerability Scoring System)**:
   - Uso del marco CVSS 3.0 para asignar un puntaje de gravedad a cada vulnerabilidad, considerando factores como la explotabilidad, el impacto en la confidencialidad, integridad y disponibilidad, y la complejidad del ataque.
2. **Análisis de Impacto:**
   - Cada vulnerabilidad será evaluada en función de su potencial impacto en el modelo de negocio, analizando cómo podría comprometer las operaciones críticas, la seguridad de los datos y el cumplimiento de los estándares y regulaciones de la industria, además de su repercusión sobre la estabilidad y competitividad de la organización.

2.4 MODALIDAD DE EJECUCIÓN

Todos los servicios serán ejecutados de forma remota desde la red interna de HAWKTESTERS, S.L., sin necesidad de presencia física en las instalaciones del cliente. Nuestro equipo opera de manera distribuida y segura, desde ubicaciones autorizadas en Europa y Latinoamérica, utilizando una infraestructura propia diseñada para realizar auditorías ofensivas bajo los más altos estándares técnicos y éticos.

HAWKTESTERS, S.L. proporcionará los medios técnicos necesarios para la ejecución del servicio, incluyendo herramientas especializadas, entornos de análisis seguros y personal altamente cualificado en pruebas de seguridad ofensiva.

En caso de que el alcance requiera pruebas sobre entornos internos no expuestos a internet, el cliente deberá proporcionar acceso remoto controlado (VPN, jumpbox, etc.) o una alternativa viable que permita ejecutar las pruebas de manera segura y eficiente.

No se contemplan desplazamientos físicos ni ejecución en sitio, salvo acuerdo previo y justificado, en cuyo caso los gastos asociados deberán ser cubiertos por el cliente.

2.5 FASES DEL SERVICIO

El proyecto se desarrollará en tres fases principales:

1. **Fase de Investigación y Reconocimiento:**
    - Recopilación de información y definición de los activos a evaluar (aplicación web).
2. **Fase de Ejecución de Pruebas:**
    - Ejecución de pruebas de penetración en la aplicación web.
3. **Fase de Reporte y Presentación:**
    - Elaboración de dos informes:
        - **Informe Técnico:** Detallará las vulnerabilidades encontradas, su demostración, el impacto y recomendaciones de mitigación para cada área evaluada.
        - **Informe Ejecutivo:** Ofrecerá una visión estratégica del impacto y los riesgos asociados, y sugerirá acciones a nivel gerencial.
    - Reunión de cierre para explicar los hallazgos y resolver dudas.

2.6 CRONOGRAMA

ETAPA	ACTIVIDAD GENERAL	DÍAS CALENDARIO
Fase 1	**Aplicación Web**	**10**
Actividades	**Día 1 – Kickoff técnico y preparación** ● Reunión inicial con el equipo técnico. ● Revisión de documentación (arquitectura, endpoints, usuarios, roles, etc.). ● Acceso a ambientes de prueba, credenciales y repositorios (si aplica). **Día 2 – Mapeo de superficie de ataque y análisis contextual** ● Exploración ofensiva del entorno con foco en identificar vectores que puedan afectar procesos del negocio. ● Identificación de puntos de entrada internos y externos alineados con el funcionamiento del modelo operativo. ● Análisis de medidas defensivas activas y pasivas. **Día 3 – Control de acceso y autenticación** ● Pruebas de bypass y control de acceso (vertical y horizontal) enfocados en restricciones entre roles que protegen funciones sensibles del negocio. **Día 4 – Gestión de sesiones y vectores cliente** ● Pruebas del lado cliente (DOM XSS, manipulación de eventos, etc.) orientadas a detectar vectores que puedan ser aprovechados para desestabilizar procesos clave o manipular flujos transaccionales. **Día 5/6 – Validación de entradas y puntos menos comunes** ● Pruebas de sanitización en campos típicos y atípicos (headers, JSON, uploads...). ● Revisión de dependencias y librerías expuestas en el cliente. **Día 7/8 – Inyecciones y análisis profundo** ● Pruebas de inyección (SQL, SSTI, command injection, etc.). ● Uso de código fuente si está disponible para guiar ataques más precisos. ● Validación de técnicas de evasión para explorar persistencia y explotación realista. **Día 8 – Exposición de información sensible** ● Revisión de endpoints internos, logs, archivos temporales y configuraciones expuestas que puedan derivar en fugas de datos relevantes para la continuidad operativa o estratégica. **Día 9 – Abuso de lógica de negocio** ● Pruebas dirigidas a funcionalidades críticas del modelo de negocio: procesos de registro, pagos, validaciones, límites operativos, etc. ● Explotación de comportamientos no intencionados que permitan abusar del sistema sin necesidad de vulnerabilidades técnicas tradicionales. **Día 10 – Consolidación y reporte** ● Priorización de hallazgos por riesgo real. ● Redacción del reporte técnico y resumen ejecutivo. ● *Opcional*: reunión de cierre para presentación de resultados y dudas.	

Nota: La gama de pruebas mencionada en el cronograma tiene como propósito ilustrar el nivel de experticia del equipo. No obstante, dichas pruebas no se limitan únicamente a las allí descritas, ya que el equipo está conformado por profesionales con experiencia en los tipos de activos contemplados en la evaluación.

3. ALCANCE Y ENTREGABLES

3.1 ALCANCE DEFINIDO

El alcance detallado a realizar se describe a continuación:

Servicio	Activo	Descripción del Activo
Prueba de Penetración de Aplicación Web	Una (1) aplicación web	Página principal de Rapicredit **https://www.rapicredit.com/**

3.2 ENTREGABLES

Después de completar la fase de investigación, se iniciará la fase de generación de informes. Durante esta fase, se redactarán dos informes: un **informe técnico** se redactará para resaltar las vulnerabilidades y proponer soluciones correctivas. Paralelamente, el **informe ejecutivo** ofrecerá un análisis a nivel estratégico de las implicaciones y riesgos asociados con las vulnerabilidades identificadas.

- Informe Técnico
  - Descripción inicial de las metodologías
  - Descripción de las vulnerabilidades encontradas
  - Demostración de las vulnerabilidades
  - Impacto de los riesgos causados por las vulnerabilidades
  - Mitigación de las vulnerabilidades
- Informe Ejecutivo
  - Descripción del impacto y riesgo de las vulnerabilidades encontradas
  - Análisis de la madurez y postura de ciberseguridad de los activos
- Reunión de cierre del proyecto
  - Explicación técnica y ejecutiva de las vulnerabilidades encontradas
  - Posibilidad de aclarar dudas encontradas en el informe
  - Planificación de la fase de retest

3.3 FASE DE RETEST

HAWKTESTERS, S.L. incluye una ronda de re-test sin coste adicional, con el objetivo de validar la corrección de las vulnerabilidades identificadas durante la auditoría.

Este re-test debe ser solicitado **dentro de los 30 días posteriores a la entrega del informe final**, con el fin de asegurar una ventana razonable para la implementación de medidas de remediación por parte del cliente.

En caso de que el re-test se solicite **fuera de este período de 30 días**, se aplicará una tarifa adicional proporcional al esfuerzo requerido, la cual será previamente acordada con el cliente.

Durante el re-test, se evaluarán exclusivamente los hallazgos previamente reportados, verificando su mitigación o corrección efectiva sin incluir nuevas pruebas de seguridad.

4. PROPUESTA DE VALOR

4.1 VALOR DEL SERVICIO

A continuación, encontrará un esquema detallado de los precios propuestos por HAWKTESTERS, S.L:

Servicio	Alcance	Valor (COP)
Prueba de Penetración de Aplicación Web	Una (1) aplicación web	$ 8.499.000
Total	**1 Evaluación completa**	$ 8.499.000

4.2 DETALLES SOBRE LA FACTURACIÓN

Las condiciones de facturación se establecen de la siguiente forma:

- **50% del valor total** se factura por anticipado al momento de la aceptación de la propuesta, como condición para iniciar los trabajos.
- El **50% restante** se factura con la entrega del informe final de hallazgos, sin incluir el informe del re-test.
- En caso de solicitarse el re-test fuera del período de 30 días establecido, se generará una factura adicional correspondiente al esfuerzo requerido.

La forma de pago será de **treinta (30) días calendario** contados a partir de la emisión de la factura correspondiente.

Los pagos deben realizarse mediante transferencia bancaria a los datos proporcionados por HAWKTESTERS, S.L. En caso de requerir facturación con condiciones especiales (como split billing o uso de plataformas de pago), estas deberán ser acordadas previamente.

4.3 CONDICIONES ADICIONALES

A continuación se detallan los términos y condiciones aplicables a la presente propuesta:

- **Confidencialidad:** HAWKTESTERS, S.L. se compromete a mantener la confidencialidad de toda la información a la que tenga acceso durante la ejecución del servicio. Este compromiso es extensible a todo el personal involucrado en el proyecto. En caso de ser requerido, se podrá firmar un acuerdo de confidencialidad (NDA) específico.

- **Validez de la propuesta:** La presente propuesta tiene una validez de **treinta (30) días calendario** a partir de su emisión. Pasado este plazo, las condiciones técnicas y económicas podrían estar sujetas a revisión.

- **Costes adicionales:** Dado que HAWKTESTERS, S.L. opera 100% de forma remota, **no se incluyen** en esta propuesta gastos de desplazamiento ni hospedaje. En caso de que, de forma excepcional, se acuerde una ejecución presencial, estos costes deberán ser asumidos por el cliente y serán facturados por separado.

- **Inicio del servicio:** El inicio del servicio podrá programarse a partir de los **15 días hábiles** posteriores a la aceptación formal de la propuesta y el pago del anticipo (si está acordado), sujeto a disponibilidad de agenda del equipo técnico.

5. TÉRMINOS Y CONDICIONES

Este Contrato de Propuesta Comercial para Pruebas de Penetración establece los términos y condiciones que rigen el acuerdo contractual entre HAWKTESTERS, S.L. (en adelante, *el Proveedor*) y RAPICREDIT, S.A.S. (en adelante, *el Cliente*). Ambas partes acuerdan estar sujetas a los términos establecidos en el presente documento.

1. Introducción

Estos Términos y Condiciones regulan la prestación de servicios profesionales de pruebas de penetración y simulación ofensiva realizados por el Proveedor, orientados a detectar vulnerabilidades y evaluar la resiliencia de los activos del Cliente frente a amenazas reales.

2. Objetivo del Servicio

El Proveedor ejecutará una prueba de penetración avanzada sobre la aplicación web del Cliente, simulando escenarios realistas de ataque, con el objetivo de identificar, clasificar y reportar vulnerabilidades explotables, junto con recomendaciones específicas para su mitigación.

3. Modalidad de Ejecución

Todos los servicios se llevarán a cabo de forma remota desde la infraestructura interna de HAWKTESTERS, S.L. En caso de requerirse acceso a entornos internos no expuestos, el Cliente deberá proporcionar acceso controlado (VPN, jumpbox, etc.).
No se contemplan desplazamientos físicos ni ejecución in situ, salvo acuerdo expreso. En tal caso, los gastos de viaje, hospedaje y logística deberán ser cubiertos por el Cliente.

4. Condiciones de Facturación y Pago

- Anticipo del 50% al momento de aceptación de la propuesta, como condición para iniciar el servicio.
- 50% restante al momento de la entrega del informe técnico de hallazgos.
- El informe de *retest* no está incluido en esta segunda factura.
- El plazo de pago es de treinta (30) días calendario a partir de la emisión de cada factura.

En caso de requerirse facturación internacional o condiciones especiales, deberán ser acordadas por escrito antes del inicio del proyecto.

5. Re-Test

Se incluye una ronda de re-test sin coste adicional, siempre que sea solicitada dentro de los 30 días posteriores a la entrega del informe final. Este re-test se centrará exclusivamente en los hallazgos previamente reportados.
Si el re-test se solicita después de dicho período, se aplicará una tarifa adicional proporcional al esfuerzo requerido, que será acordada entre las partes.

6. Confidencialidad

- El Proveedor se compromete a mantener la más estricta confidencialidad sobre toda la información, acceso, documentación y datos a los que tenga acceso durante la prestación del servicio, extendiendo este compromiso a todo su equipo técnico.
- En caso de requerirse, se podrá firmar un Acuerdo de Confidencialidad (NDA) adicional entre las partes.
- El Cliente se compromete igualmente a mantener la confidencialidad sobre los métodos, herramientas y documentación proporcionada por el Proveedor.

7. Responsabilidad de las Partes

- Proveedor: Ejecutará el servicio con los más altos estándares técnicos, metodologías ofensivas actualizadas y prácticas alineadas con los marcos reconocidos del sector.
- Cliente: Proporcionará la información, accesos y autorizaciones necesarias para el desarrollo de la prueba. Será responsable de realizar respaldos de sus sistemas y datos antes del inicio de las pruebas.

El Proveedor no se hace responsable por pérdidas de datos, indisponibilidades o daños ocasionados durante la ejecución del servicio si se han respetado los límites de alcance establecidos.

8. Limitación de Responsabilidad

El Proveedor no será responsable de daños directos, indirectos o consecuenciales derivados del uso de los hallazgos o recomendaciones proporcionadas en el informe. Las pruebas se realizarán bajo autorización explícita del Cliente, quien asume los riesgos operativos correspondientes.

9. Validez de la Propuesta

La presente propuesta comercial tiene una validez de treinta (30) días calendario desde su emisión. Transcurrido este plazo, los términos técnicos y económicos podrán estar sujetos a revisión.

10. Modificaciones

Cualquier modificación a estos Términos y Condiciones deberá realizarse por escrito y ser aceptada expresamente por ambas partes.

11. Resolución de Controversias

Las partes se comprometen a resolver de forma amistosa cualquier diferencia que surja del presente contrato. Si no se llegara a un acuerdo, ambas partes se someterán a los tribunales de la ciudad de Madrid, España, sede del Proveedor.

12. Aceptación de los Términos

La aceptación de la propuesta por parte del Cliente implica la conformidad con todos los términos y condiciones aquí establecidos.