



PROPUESTA DE SERVICIOS DE SEGURIDAD MOBILE

HAWKTESTERS, S.L. & MURARTE GLOBAL, S.L.

INFORMACIÓN DE CONTACTO

Email: sales@hawktesters.com

Número de celular: +34 644 02 6557

Website: www.hawktesters.com

TABLA DE CONTENIDO

CLÁUSULA DE CONFIDENCIALIDAD.....	4
1. RESUMEN EJECUTIVO.....	5
1.1 HAWKTESTERS, S.L.....	5
1.2 IMPACTANDO VUESTRO MODELO DE NEGOCIO.....	5
1.3 OBJETIVO PROPUESTA COMERCIAL.....	5
2. DESCRIPCIÓN DEL SERVICIO.....	6
2.1 OBJETIVO.....	6
2.2 METODOLOGÍA DE PRUEBAS.....	6
2.3 EVALUACIÓN DE VULNERABILIDADES Y ANÁLISIS DE IMPACTO.....	6
2.4 MODALIDAD DE EJECUCIÓN.....	6
2.5 FASES DEL SERVICIO.....	7
2.6 CRONOGRAMA.....	8
3. ALCANCE Y ENTREGABLES.....	9
3.1 ALCANCE DEFINIDO.....	9
3.2 ENTREGABLES.....	9
3.3 FASE DE RETEST.....	9
4. PROPUESTA DE VALOR.....	11
4.1 VALOR DEL SERVICIO.....	11
4.2 DETALLES SOBRE LA FACTURACIÓN.....	11
4.3 CONDICIONES ADICIONALES.....	11
5. TÉRMINOS Y CONDICIONES.....	13



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.

MURARTE GLOBAL, S.L. 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 **MURARTE GLOBAL, S.L.**, 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 **MURARTE GLOBAL, S.L.** 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 **MURARTE GLOBAL, S.L.**

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+, OSPA, 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.
- **Registro ofensivo detallado**, con logs de cada ataque simulado para trazabilidad técnica y mejora continua.

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 móvil híbrida (Ionic React) para iOS y Android proporcionada por MURARTE GLOBAL, S.L., con el objetivo de identificar posibles vulnerabilidades de seguridad que pudieran ser explotadas por un atacante remoto.

2. DESCRIPCIÓN DEL SERVICIO

El servicio propone un plan detallado para realizar una prueba de penetración con el objetivo de identificar las vulnerabilidades en la aplicación móvil híbrida (Ionic React) para iOS y Android definida en el alcance. La prueba de penetración adoptará metodologías estándar de la industria para asegurar una evaluación exhaustiva de la postura de seguridad y el impacto potencial de las vulnerabilidades detectadas.

2.1 OBJETIVO

Los principales objetivos de esta prueba de penetración son:

1. **Identificar vulnerabilidades** en la aplicación móvil.
2. **Evaluar el** potencial **impacto** de estas vulnerabilidades.
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 MASVS y MSTG:** Utilización de la guía de pruebas OWASP para identificar vulnerabilidades comunes en aplicaciones móviles.
2. **SANS Security:** Aplicación de las directrices del Instituto SANS 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:**
 - Evaluación del potencial impacto de cada vulnerabilidad en las operaciones de la organización, la seguridad de los datos y el cumplimiento de estándares y regulaciones de la industria.

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.
2. **Fase de Ejecución de Pruebas:**
 - Análisis de la aplicación móvil enfocada en funcionalidades críticas.
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	JORNADAS LABORALES
Fase 1	Aplicación Móvil	7
Actividades	<p>Día 1: Preparación y análisis estático</p> <ul style="list-style-type: none">• Reunión técnica para repasar flujos críticos, roles, endpoints y restricciones.• Revisión del código fuente (si se entrega).• Análisis de buenas prácticas en almacenamiento de claves, secretos y tokens.• Identificación de librerías y versiones vulnerables.• Revisión de permisos solicitados por la app y análisis de manifiesto. <p>Día 2: Análisis de autenticación, sesiones y almacenamiento</p> <ul style="list-style-type: none">• Pruebas de login, registro, recuperación de cuenta, etc.• Validación de control de sesión: expiración, renovación, almacenamiento.• Validación de mecanismos de autenticación biométrica y fallback. <p>Día 3: Tráfico de red y pruebas de comunicación</p> <ul style="list-style-type: none">• Configuración de proxy para interceptar tráfico HTTPS.• Validación de certificados, pinning (si aplica) y técnicas de bypass.• Análisis de tráfico: endpoints, headers, tokens, fugas de datos. <p>Día 4/5: Pruebas de lógica de negocio y manipulación de app</p> <ul style="list-style-type: none">• Análisis de flujos vulnerables: pagos, validaciones locales, reuso de requests.• Pruebas de abuso de funciones: bypass de restricciones del cliente.• Validación de seguridad en WebViews.• Revisión de controles de acceso.• Pruebas en entornos rooted/emulados si corresponde. <p>Día 6/7: Consolidación de hallazgos</p> <ul style="list-style-type: none">• Redacción del reporte técnico: pasos de explotación, impacto y mitigación.• Generación del resumen ejecutivo	

Nota: Cada fase contará con su respectivo informe. Es decir, al tratarse de tres fases, independientemente de la modalidad elegida, se entregarán tres informes en total.

Adicionalmente, 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	Modalidad
Prueba de Penetración de Aplicación Móvil	Una (1) aplicación Móvil	<ul style="list-style-type: none">• Aplicación híbrida desarrollada en Ionic React• Disponible para iOS (v16) y Android (SDK mínimo 29).• Backend en NestJS y Express.• Tres roles a disposición• 45 endpoints expuestos mediante API.• La infraestructura se encuentra alojada en AWS.	Caja Gris

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:

Servicio	Alcance	Valor (EUR)	IVA (21%)
Prueba de Penetración de Aplicación Móvil	Una (1) aplicación Móvil	1350 EUR	283.5 EUR
Total	1 Evaluación completa	1350 EUR	1633.5 EUR

4.2 DETALLES SOBRE LA FACTURACIÓN

Las condiciones de facturación se establecen de la siguiente forma:

- **50% del valor total (816.75 EUR)** se factura por anticipado al momento de la aceptación de la propuesta, como condición para iniciar los trabajos.
- El **50% restante (816.75 EUR)** 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. En caso de requerir facturación internacional o 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 MURARTE GLOBAL, S.L. (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 móvil 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. 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.