PRUEBAS DE HACKING ETHICO POTENCIADAS CON INTELIGENCIA ARTIFICIAL

ITM

Medellín, 05 de mayo de 2026

Señor:

Carlos Alberto Cortes Lopez
Jefe de administracion de Red institucional
Oficina de Tecnologia e Informatica
ITM

PRUEBAS DE ETHICAL HACKING

Presentamos a continuación nuestra propuesta técnica para la ejecución de pruebas de ethical hacking, estructurada conforme a los requerimientos definidos en el proceso de evaluación.

Nuestro valor diferencial

El equipo de KRONUX SOLUTIONS integra inteligencia artificial avanzada con talento humano especializado en seguridad ofensiva. Este modelo híbrido nos permite ejecutar evaluaciones de seguridad con mayor cobertura, velocidad de análisis y precisión en la identificación de vulnerabilidades. Nuestras plataformas de IA ejecutan escaneos automatizados continuos, correlacionan indicadores de compromiso en tiempo real y detectan patrones de ataque emergentes; mientras nuestros especialistas aplican criterio técnico, contexto de negocio y metodologías reconocidas como **PTES** (Penetration Testing Execution Standard), **OWASP Testing Guide**, **OSSTMM** y **NIST SP 800-115**.

Nuestros profesionales cuentan con experiencia comprobada en proyectos de infraestructura, seguridad y virtualización, y operan bajo estándares de certificación como **OSCP**, **CEH**. Adicionalmente, KRONUX SOLUTIONS tiene presencia activa en la comunidad de ciberseguridad colombiana: hemos participado como ponentes y organizadores en eventos como **InfoSecurity Colombia**, **Barcamp Security** y **B-Sides Bogotá**, y colaboramos con comunidades técnicas especializadas en el país.

PERSONAL CETIFICADO

Cordialmente,

Carlos Arismendy
KRONUX SOLUTIONS S.A.S
carlos.arismendy@kronux.com.co
Cel: 313– 6007697

TABLA DE CONTENIDOS

1. KRONUX SOLUTIONS S.A.S

Kronux Solutions es una empresa de ciberseguridad especializada en seguridad ofensiva, análisis de vulnerabilidades y respuesta a incidentes, que integra inteligencia artificial avanzada con equipos humanos de alto perfil técnico. Nuestro modelo híbrido IA + Expertos permite ejecutar evaluaciones de seguridad con mayor cobertura y profundidad: las plataformas de IA automatizan el procesamiento de eventos, correlacionan indicadores de compromiso en tiempo real y aceleran la identificación de vectores de ataque; mientras nuestros especialistas, certificados en **OSCP** (Offensive Security), **CEH** (EC Council) y estándares de gestión como **ISO 27001**, aplican pensamiento crítico, creatividad ofensiva y juicio técnico que ningún sistema automatizado puede reemplazar. Esta combinación nos permite entregar resultados más precisos, en menor tiempo y con mayor contexto de negocio que los enfoques tradicionales.

PRODUCTOS DE SEGURIDAD

- Firewalls de nueva generación
- Prevención de intrusiones
- Protección amenazas avanzadas persistentes
- Firewalls de aplicaciones Web
- Filtrados de contenido web
- Filtrados de contenido email
- Accesos remotos seguros vpn
- Cifrado
- Gestión de vulnerabilidades
- Análisis web Owasp top 10
- Cumplimiento ISO 27001
- Advanced Ethical hacking
- Open source Intelligence
- Servicio de SOC
- Auditorías en ISO 27001
- Entrenamientos de Seguridad

NUESTROS CLIENTES

Por la misma de seguridad de nuestros clientes estos no son nombrados en nuestras propuestas ni divulgados en nuestros sitios web, debido a que en pruebas de Ethical hacking que hemos realizado, hemos visto como esta información puede ser utilizada por ciberdelincuentes para hacer daño a las empresas.

Podemos informar que nuestra empresa, desde su SOC (Security Operation Center) potenciado con Inteligencia Artificial, actualmente atiende diferentes entidades del sector público, privado y financiero. Nuestro SOC híbrido combina motores de IA para la detección automatizada de amenazas en tiempo real con analistas humanos expertos que validan, contextualizan y responden a cada incidente con criterio estratégico. Operamos en entornos desde 50 usuarios a 2.500 usuarios, garantizando una cobertura de seguridad continua y adaptativa.

2. ALCANCE DE LA PROPUESTA

A continuación, se detalla el alcance de la propuesta de acuerdo a la solicitud presentada

Pruebas de Ethical Hacking Externo:

Nro.	DESCRIPCION
1	5 sitios web transaccionales (Caja negra y caja gris con un perfil de usuario, basados en el top 10 de OWASP)
2	6 direcciones IP (Directorio Activo, firewalls, bases de datos) - Generación de información de pruebas acordes al tipo de infraestructura

Alcance pruebas Ethical hacking externo.

Se realizarán pruebas tipo caja negra y y caja gris con un usuario basado en un perfil, con el objetivo de validar que no se pueda acceder al sitio sin las autenticaciones necesarias, y a su vez si una vez autenticado puede comprometer algún tipo de información.

Se realizará una evaluación exhaustiva de los portales transaccionales utilizando nuestro enfoque híbrido de IA + Hackers Éticos. Nuestras herramientas de Inteligencia Artificial ejecutarán escaneos automatizados de alta velocidad para identificar vulnerabilidades conocidas, configuraciones inseguras y exposiciones de datos, mientras que nuestros hackers éticos expertos realizarán pruebas manuales avanzadas para descubrir vulnerabilidades de lógica de negocio y vectores de ataque complejos que solo el ingenio humano puede detectar. Esta combinación permite determinar con máxima precisión si el portal presenta riesgos de distribución de malware, redirección a sitios fraudulentos, robo de credenciales o compromiso de la integridad de los datos.

Se ejecutarán pruebas avanzadas de Caja Gris utilizando 1 perfil de acceso (usuario final) combinando escaneos automatizados con IA y técnicas manuales de explotación ejecutadas por nuestros hackers éticos. La IA analizará patrones de tráfico, detectará anomalías en los flujos de autenticación y realizará fuzzing inteligente sobre los endpoints, mientras nuestros expertos humanos validarán la robustez de los controles de autorización, simularán escalaciones de privilegios creativas, evaluarán la seguridad de las bases de datos frente a inyecciones avanzadas y verificarán que no existan rutas de acceso no autorizado a información confidencial de otros usuarios o funcionalidades administrativas críticas.

Todas las pruebas y análisis de vulnerabilidades se ejecutan siguiendo rigurosamente la metodología OWASP Top 10 (edición 2025), el estándar internacional más reconocido en seguridad de aplicaciones web, complementado con frameworks de pruebas como PTES (Penetration Testing Execution Standard) y NIST SP 800-115, garantizando una cobertura integral de los principales vectores de amenaza

3. ENTREGABLES

Entregables pruebas de Ethical hacking

- Informe De vulnerabilidades basado en el TOP 10 de OWASP
- Informe detallado del resultado de las pruebas de intrusión de los objetivos sin autenticación y con autenticación, con los hallazgos clasificados con su criticidad de acuerdo al impacto y Recomendaciones que ayuden a su remediación.
- Informe ejecutivo de los hallazgos y recomendación para mitigar los riesgos.
- Plataforma Ciberseguridad activa por 90 días con Inventario de activos evaluados de la prueba de Ethical Hacking , identificación de los riesgos clasificados por severidad , Matriz de calor, plan de tratamiento riesgos, utilizando buenas practicas como ISO 27005 e ISO 31000 y plan de respuesta a incidentes sobre los hallazgos de los objetivos evaluados.

Información Pruebas de Ethical Hacking

El servicio de Ethical Hacking de Kronux Solutions combina plataformas de inteligencia artificial con equipos humanos especializados en seguridad ofensiva para evaluar el nivel real de exposición de su organización ante amenazas cibernéticas. Nuestro modelo híbrido permite ejecutar simulaciones de ataque con mayor cobertura técnica que los enfoques exclusivamente manuales o automatizados: las plataformas de IA procesan y correlacionan indicadores de vulnerabilidad en tiempo real, mientras nuestros especialistas aplican técnicas de explotación avanzadas, pensamiento lateral y criterio técnico para descubrir vulnerabilidades que las herramientas automatizadas por sí solas no logran

identificar. Este enfoque permite a su organización anticiparse a las amenazas y fortalecer proactivamente su postura de seguridad con evidencia técnica accionable.

Contar con firewalls y sistemas de detección de intrusos no garantiza protección completa frente a un atacante determinado. Nuestro servicio integra análisis automatizado de configuraciones, reglas de red y patrones de tráfico para identificar brechas de seguridad no evidentes, con pruebas de penetración manuales que evalúan la capacidad de respuesta real de su infraestructura ante escenarios de ataque dirigidos. El resultado es una visión completa y documentada del nivel de exposición al riesgo cibernético de su organización, acompañada de una hoja de ruta priorizada para su remediación efectiva.

Nuestro servicio de Ethical Hacking está orientado a entregar resultados con impacto directo en la seguridad operativa de su negocio. La automatización nos permite acelerar la recolección y correlación de datos, identificar patrones de riesgo y priorizar hallazgos por criticidad; mientras nuestros especialistas validan cada vulnerabilidad mediante explotación manual controlada, interpretan los resultados con contexto de negocio y elaboran recomendaciones adaptadas a la realidad operativa de su organización. El entregable final es un plan de acción priorizado con métricas de riesgo cuantificadas y guías detalladas de remediación, diseñado para que su equipo de TI enfoque los recursos donde generan mayor impacto en la protección del negocio.

Los objetivos principales de los test de intrusión (Ethical Hacking) son:

- Identificar las vulnerabilidades en los servicios y aplicaciones que tiene la empresa.
- Clasificar el nivel de criticidad en las vulnerabilidades encontradas.
- Verificar que sean efectivos los controles en los dispositivos de seguridad. Verificar con las test de intrusión, cuáles de estas vulnerabilidades pueden ser explotadas y cuáles son los impactos para la empresa.
- Revisar qué información y servicios pueden quedar expuestos si el ataque se materializa.
- Si los ataques y pruebas de intrusión son exitosas, permite que el personal de sistemas pueda evaluar si un ataque de estos ya se pudo haber materializado en la red de la empresa.

Infraestructura tecnologías usadas y personal

Kronux Solutions opera con un ecosistema tecnológico de vanguardia que integra Inteligencia Artificial, herramientas propietarias y open source, y la experiencia de hackers éticos altamente capacitados. Nuestro enfoque híbrido IA + Humano utiliza plataformas de IA para automatizar la detección de vulnerabilidades, análisis de código fuente, correlación de amenazas y generación de reportes inteligentes, potenciando exponencialmente la

capacidad de nuestro equipo humano. Dependiendo de las necesidades y alcance de los clientes, complementamos con dispositivos especializados para ataques a redes inalámbricas, dispositivos físicos USB, Ethernet, entre otros. Adicionalmente, contamos con desarrollos propios impulsados con IA que han sido nuestro gran diferencial competitivo; hemos ido optimizando y automatizando nuestros algoritmos de machine learning para detectar y explotar vulnerabilidades en aplicativos desarrollados en Colombia (PQRS, Sucursales Virtuales, Gestión Documental), logrando tasas de detección superiores al combinar la velocidad de la IA con la intuición y creatividad de nuestros expertos humanos.

El personal que realizará las pruebas representa la fusión perfecta entre tecnología de IA y talento humano excepcional. Nuestros expertos, respaldados por herramientas de Inteligencia Artificial propias, cuentan con amplia experiencia en pruebas de Ethical Hacking avanzado y poseen certificaciones de Offensive Security (OSCP, OSCE). Han participado en el diseño de retos de Ethical Hacking en formato **CTF (Capture The Flag)** y tienen presencia activa en eventos de la comunidad de ciberseguridad colombiana como **InfoSecurity Colombia**, **Barcamp Security** y **B-Sides Bogotá**. Esta combinación de certificaciones técnicas, experiencia ofensiva práctica y conocimiento del entorno tecnológico colombiano permite ejecutar pruebas con mayor contexto, precisión y relevancia para la realidad operativa de su organización.

4. RESUMEN DE LA INVERSIÓN PROPUESTA

A continuación, presentamos nuestra oferta la cual esperamos que se ajuste a sus necesidades.

Item #	Descripción	Objetivos	Valor Unitario	Subtotal
1	Pentesting a sitios web transaccionales (Caja Negra y Caja Gris, 1 perfil de usuario, basado en OWASP Top 10)	5	$ 4.325.000	$ 21.625.000
2	Pentesting de Infraestructura (Directorio Activo, firewalls, bases de datos)	6	$ 3.220.000	$ 19.320.000
	TOTAL	11		$ 40.945.000 + IVA

Tiempo para la ejecución del proyecto.

El tiempo estimado aproximado para este proyecto es de 40 días, siempre y cuando se pueda seguir el cronograma de actividades acordado.

El proyecto puede iniciar aproximadamente 8 a 12 días después de firmar los documentos, esto con el objetivo de poder asignar el personal, y recursos tecnológicos necesarios para una buena ejecución del proyecto, lo anterior nos permite también preparar entornos de pruebas propios para ayudar a tener mejor efectividad en las pruebas de Ethical hacking.

5. TERMINOS Y CONDICIONES

- Antes de iniciar cualquier actividad se deben tener contratos firmados autorizando a Kronux Solutions a realizar las actividades objeto del contrato, con el objetivo de no incumplir ninguna ley como la ley 1273 del 2009 de delitos informáticos.

- Se debe acordar con el cliente mecanismos de protección para cifrar y proteger con clave la información para garantizar que desde el inicio hasta el final toda la información este protegida adecuadamente.

  Kronux Solutions solo entregará la información a las personas que defina ITM S.A.S como líderes a cargo del proyecto.

- Es importante que ITM tenga respaldo de la información y de las plataformas que van a hacer parte de las pruebas de Ethical hacking, con el fin de que, si una vulnerabilidad es explotada y puede dejar un servicio por fuera, puedan restaurarse fácilmente para no afectar el servicio.

- Este estimado tiene una validez de Treinta (30) días calendario a partir de la fecha de entrega

- A todos los valores se debe adicionar el IVA.

- Forma de pago: al finalizar la ejecución del contrato.

- Si se requieren pólizas se deben adicionar al valor de la propuesta

- Los valores aplican para la ciudad de Medellín.