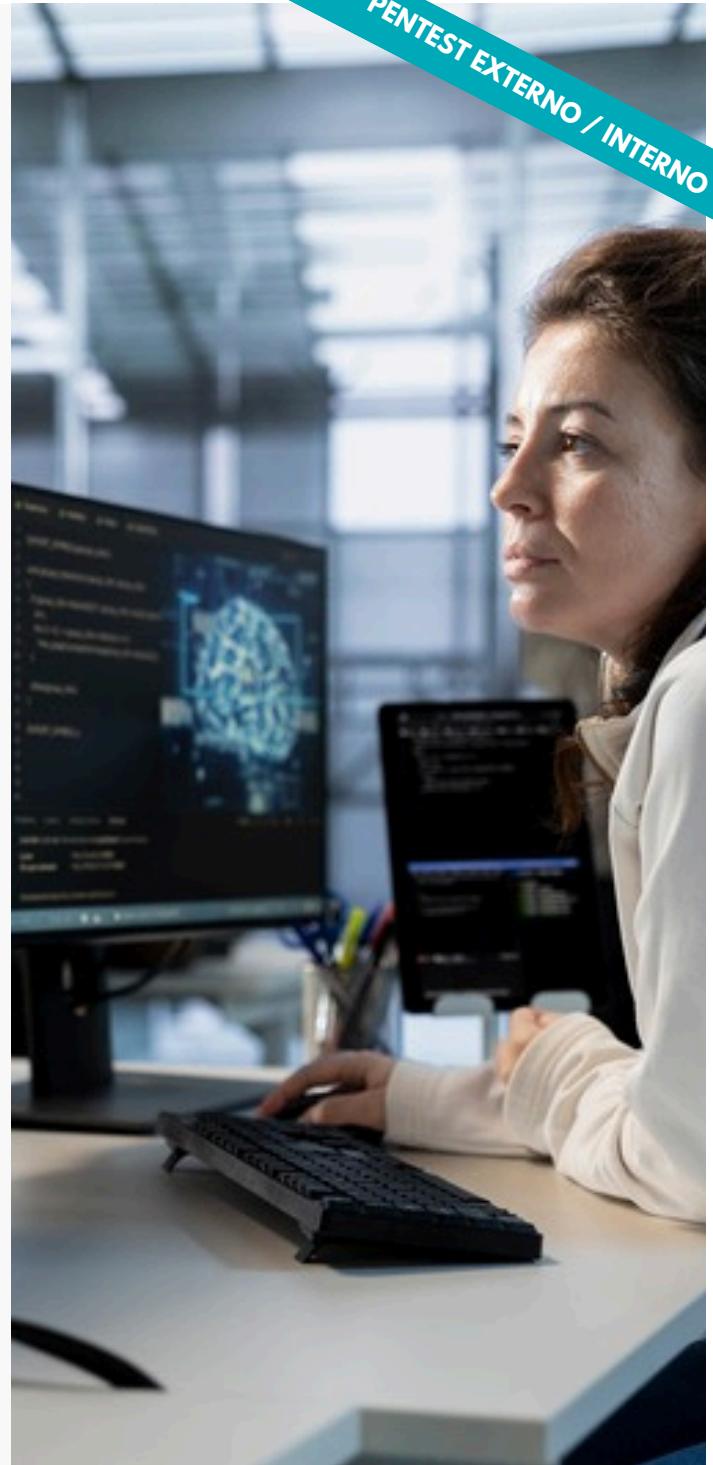


Pentest & Ethical Hacking

Los Servicios de auditoría de seguridad tratan de proporcionar información sobre el grado de la integridad de los sistemas de información con la finalidad de eliminar accesos ilegales, prevenir robos de información y pérdidas de productividad. El proceso de auditoría incluirá distintas pruebas de intrusión con el objetivo de identificar vulnerabilidades a través de una revisión de las técnicas de ataque actuales, realizando un hacking ético de las aplicaciones identificadas y reproduciendo estos ataques mediante un plan de pruebas.

Servicios de prevención de vulnerabilidades

- Pentesting
- Auditoría externa e interna
- Análisis de vulnerabilidades en código fuente
- Ingeniería inversa de malware
- OSINT e inteligencia de amenazas
- Campañas de phishing y malware
- Test de intrusión
- Auditoría aplicación web
- Auditoría wireless
- Auditoría de Redes: VoIP, WiFi, Citrix, accesos remotos.
- Auditoría de Base de Datos: SQL, Oracle
- Auditoría de Código estático y dinámico
- Auditoría de Móviles: aplicaciones y entorno
- Auditorías de Cumplimiento: PCI, ESSI, NIST
- Análisis Forense



PENTEST EXTERNO / INTERNO

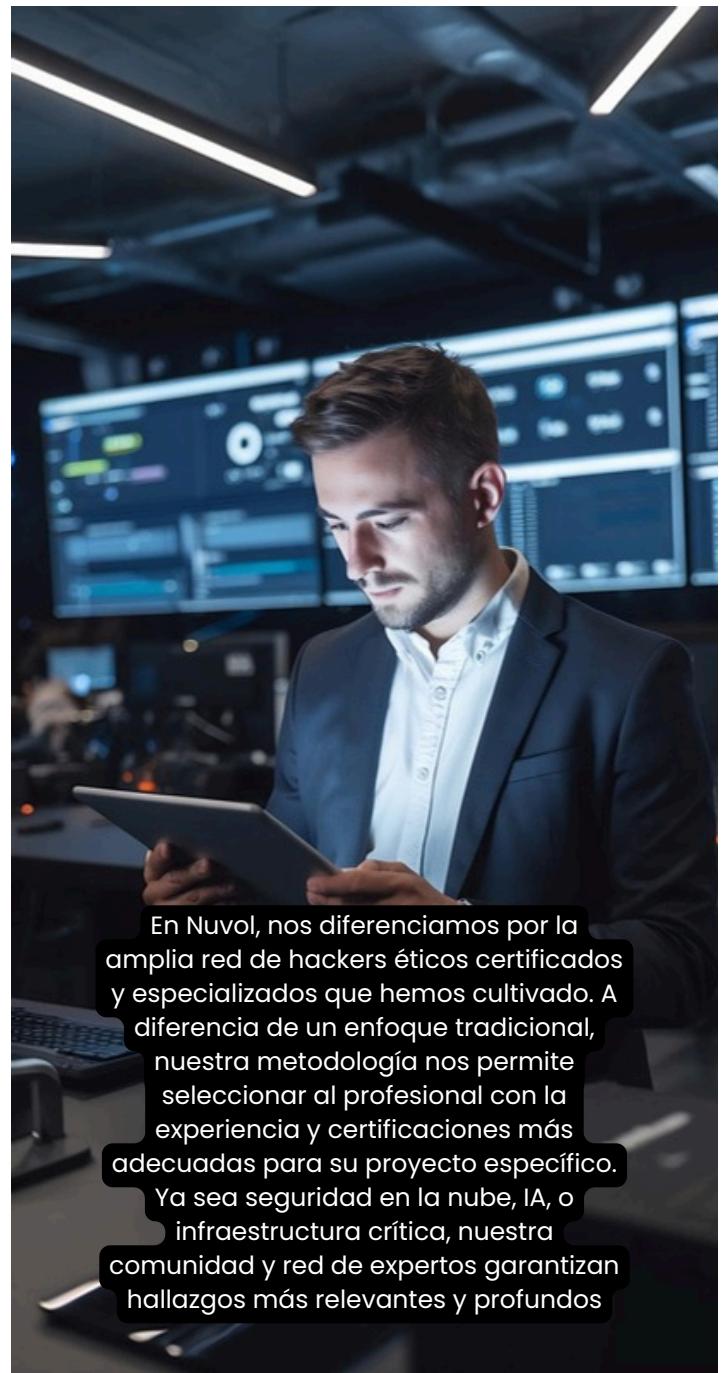
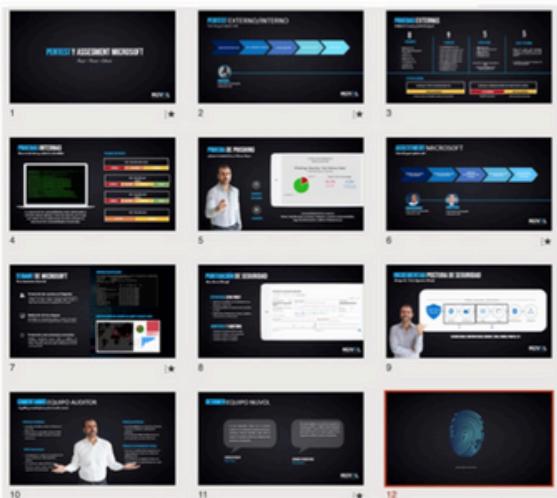
¿Porqué elegirnos?

- Auditorias personalizadas al entorno existente
- Mas allá de un escaneo de vulnerabilidades detectamos los riesgos de negocio de acuerdo a los servicios del cliente
- Reportes técnicos y ejecutivos enfocados a la dirección
- Realización de las tareas en sitio y en los horarios que nuestros clientes establezcan
- Siempre cumplimos con los tiempos de proyecto establecidos
- Servicios de ingeniería social incluidos, tanto físicos como por medios electrónicos, personalizados al ambiente de trabajo de los empleados de la organización.



Ejemplo reporte técnico y ejecutivo

Tabla de contenido	
Objetivos generales	4
Objetivos específicos	4
Descripción	4
Métricas en la clasificación de vulnerabilidades	5
Metodologías y estándar usado	6
Escenario de pruebas	7
Objetivos	8
Direcciones IP origen de las pruebas	9
Herramientas utilizadas	10
Resumen ejecutivo de vulnerabilidades	10
Vulnerabilidades de mayor riesgo	11
Activos y segmentos de mayor riesgo	12
Fortalezas identificadas	12
Debilidades identificadas y puntos de mejora	12
Resumen de riesgo	13
Reconocimiento inicial y análisis de información externa	14
Correos electrónicos identificados en fuentes externas	16
Código fuente público	18
Subdominios y registros DNS	18
Ciber Exposición del dominio principal del propietario	19
Verificación de firmas de correo - (SPF, DMARC)	21
Verificación de dominios similares	24
Ánalisis en buscadores	25
Ánalisis de objetivos	26
Vulnerabilidades identificadas	60
Recomendaciones generales	88
Referencias	90



En Nuvol, nos diferenciamos por la amplia red de hackers éticos certificados y especializados que hemos cultivado. A diferencia de un enfoque tradicional, nuestra metodología nos permite seleccionar al profesional con la experiencia y certificaciones más adecuadas para su proyecto específico.

Ya sea seguridad en la nube, IA, o infraestructura crítica, nuestra comunidad y red de expertos garantizan hallazgos más relevantes y profundos

Nuestro enfoque se centra en:

- **Impacto Empresarial Real:** Traducimos los hallazgos técnicos en riesgos concretos para el negocio, priorizando las vulnerabilidades críticas y ofreciendo planes de remediación accionables.
- **Adaptación Tecnológica:** Especializamos nuestras pruebas en tecnologías emergentes, como inteligencia artificial (IA), entornos de nube y la seguridad de la cadena de suministro, para protegerlo contra las amenazas más avanzadas.
- **Modelo de Servicio Continuo:** Ofrecemos Pentesting como Servicio (PTaaS) y simulaciones de adversarios (Red Teaming) para una vigilancia constante y una evaluación más precisa de sus defensas.
- **Fortalecimiento Colaborativo:** Trabajamos con sus equipos internos para fortalecer sus capacidades de ciberseguridad, validando sus controles existentes y proporcionando capacitación para cerrar brechas de conocimiento.

Nuestro objetivo es convertir el pentesting en una herramienta estratégica que demuestre un claro retorno de la inversión al mitigar riesgos financieros y operativos.