# HACKING ÉTICO

El hacking ético constituye la práctica sistemática y autorizada de evaluar la seguridad de sistemas informáticos mediante técnicas invasivas controladas. Su objetivo principal radica en anticipar y mitigar riesgos, garantizando la confidencialidad, integridad y disponibilidad de la información sin vulnerar el marco jurídico.

**Características, principios, metodologías y certificaciones**

Los agentes de hacking ético se distinguen por su imparcialidad, transparencia y responsabilidad. Actúan bajo autorización expresa, definiendo alcances y límites en un acuerdo legal (scope agreement). Entre sus principios destacan:

- *Consentimiento informado*: todas las acciones requieren aprobación previa de la organización.
- *Divulgación completa*: cualquier hallazgo se reporta de manera integral, incluyendo vulnerabilidades y pasos de remediación.
- *Confidencialidad*: la información a la que acceden se mantiene bajo estricta discreción.

Las metodologías seguidas suelen derivar de marcos reconocidos, como:

- OSSTMM (Open Source Security Testing Methodology Manual).
- PTES (Penetration Testing Execution Standard).
- NIST SP 800-115 (Technical Guide to Information Security Testing and Assessment).

Para acreditar competencias, existen certificaciones de prestigio:

- **CEH (Certified Ethical Hacker, EC–Council)**: valida conocimientos en técnicas de intrusión y contramedidas.
- **OSCP (Offensive Security Certified Professional)**: enfatiza la explotación práctica de vulnerabilidades.

**Marco legal y ético: leyes de protección de datos**

Las actividades de evaluación de seguridad se hallan circunscritas por normativas nacionales e internacionales. Entre las leyes contra el acceso no autorizado destacan:

- **Ley de Delitos Informáticos** (adaptada en múltiples jurisdicciones), que sanciona cualquier intrusión sin permiso.

- **Reglamento General de Protección de Datos (RGPD, Unión Europea)**: impone obligaciones sobre el tratamiento de datos personales y notificación de brechas.

- **Ley de Protección de Datos Personales (ej. Chile, Ley 19.628)**: regula el uso, almacenamiento y cesión de información sensible.

En el ámbito de propiedad intelectual, la **Ley de Derechos de Autor** protege el software y las bases de datos, restringiendo la copia y distribución no autorizadas. A nivel internacional, tratados como el **Convenio de Budapest** facilitan la cooperación frente a delitos cibernéticos.

**2.3 Normas y estándares de la industria**

La uniformidad en controles de seguridad se logra mediante marcos de referencia:

- **ISO/IEC 27001**: especifica requisitos para un Sistema de Gestión de Seguridad de la Información (SGSI), integrando controles técnicos, organizativos y físicos.

- **NIST SP 800-53**: catálogo exhaustivo de controles para sistemas federales de EE. UU., ampliamente adoptado por el sector privado.

- **OWASP Testing Guide (TG)**: orienta pruebas específicas a aplicaciones web, identificando vectores de ataque comunes y buenas prácticas de defensa.

Estos estándares definen procesos de gestión de riesgos, ciclos de mejora continua (PDCA) y criterios de auditoría, asegurando coherencia entre pruebas de intrusión y políticas corporativas.

**Debates éticos y legales**

La práctica del hacking ético suscita discusiones en torno a la ambigüedad de ciertos escenarios. Por ejemplo, la delimitación exacta del alcance puede afectar la validez jurídica de pruebas forenses. Asimismo, el equilibrio entre transparencia y confidencialidad a menudo genera tensiones cuando se negocia el reporte público de vulnerabilidades.

En conclusión, el hacking ético emerge como disciplina profesional indispensable. Al combinar rigor metodológico, respeto al marco legal y adhesión a códigos de ética, los especialistas contribuyen a fortalecer las defensas informáticas sin sacrificar principios fundamentales de privacidad y protección de datos.