



Energiza!

HACKING ÉTICO

HACKING ÉTICO

Anticiparse para proteger

Fundamentos, ética y marco legal del hacking ético



¿Qué es el Hacking Ético?

- Práctica autorizada para identificar vulnerabilidades.
- Protege activos digitales de organizaciones.
- Características:
 - Autorización previa
 - Confidencialidad total
 - Documentación técnica clara
 - Cumplimiento legal y ético



Principios Fundamentales

Los pilares del hacker ético:

- **Legalidad:** Solo con permiso.
- **Integridad:** Transparencia en los reportes.
- **Confidencialidad:** Resguardo de datos sensibles.
- **Proporcionalidad:** No dañar el sistema.



Historia del Hacking Ético

- Nace en los años 90 con el **Departamento de Defensa de EE.UU.**
- Formalización del “penetration testing”
- EC-Council y SANS Institute:
 - Certificaciones CEH, OSCP, GPEN
 - Manuales y códigos de buenas prácticas



Metodologías y Certificaciones

Metodologías:

- OSSTMM
- OWASP Testing Guide
- NIST SP 800-115


Certificaciones:

- CEH – EC-Council
- OSCP – Offensive Security
- GPEN – SANS Institute



Código Ético

EC-Council: Protección legal, transparencia, responsabilidad social.

SANS Institute: Conducta profesional, respeto a la ley.  Ética = Confianza + Credibilidad + Legitimidad



Marco Legal y Normativo

Legislaciones clave:

- CFAA (EE.UU.), RGPD (UE), Ley de Protección de Datos (LatAm)
- Convenio de Budapest sobre ciberdelincuencia


Normas técnicas:

- ISO/IEC 27001
- NIST SP 800-53
- OWASP Web Security Testing Guide



Conclusión

El hacking ético es una herramienta preventiva, legal y ética.

Requiere formación continua, principios firmes y conocimientos técnicos actualizados. 
Proteger es prevenir.





Energiza!