📘 Glosario: Fundamentos de Ciberseguridad y Hacking Ético

---

1. Ciberseguridad

Conjunto de prácticas, metodologías, tecnologías y políticas diseñadas para proteger la confidencialidad, integridad y disponibilidad de los sistemas de información, redes, aplicaciones y datos frente a accesos no autorizados, amenazas, ataques o interrupciones.

---

2. Hacking Ético

Disciplina dentro de la ciberseguridad que utiliza técnicas ofensivas de análisis y explotación de vulnerabilidades con autorización previa, con el fin de detectar debilidades antes de que sean aprovechadas por actores maliciosos.

---

3. Confidencialidad

Pilar fundamental de la seguridad de la información que asegura que los datos solo sean accesibles por personas o sistemas autorizados.

---

4. Integridad

Garantía de que la información no ha sido alterada o manipulada de forma no autorizada desde su creación, transmisión o almacenamiento.

---

5. Disponibilidad

Asegurar que los sistemas, servicios y datos estén accesibles y operativos cuando se necesiten, minimizando interrupciones en la continuidad operativa.

---

6. Malware

Software malicioso desarrollado con el objetivo de dañar, explotar o interrumpir sistemas informáticos. Incluye virus, troyanos, gusanos, ransomware y spyware.

---

7. Phishing

Técnica de ingeniería social que busca engañar a los usuarios para que revelen información confidencial (como contraseñas o datos bancarios) simulando una fuente confiable.

---

8. Ataques DDoS (Denegación de Servicio Distribuida)

Ataque cibernético que intenta saturar los recursos de un sistema o red, provocando su indisponibilidad para los usuarios legítimos.

---

9. Inyección SQL (SQL Injection)

Vulnerabilidad de seguridad en aplicaciones web que permite a los atacantes inyectar comandos SQL maliciosos en formularios de entrada, comprometiendo bases de datos.

---

10. XSS (Cross-Site Scripting)

Técnica que consiste en inyectar scripts maliciosos en páginas web vistas por otros usuarios, con el objetivo de robar información, secuestrar sesiones o manipular contenido.

---

11. Gestión de Identidades y Accesos (IAM)

Conjunto de procesos y tecnologías utilizados para gestionar de forma segura las identidades digitales y los permisos de acceso a los recursos corporativos.

---

12. Hacker de Sombrero Negro (Black Hat)

Individuo que explota vulnerabilidades con fines maliciosos o lucrativos, actuando de forma ilegal y no ética.

---

13. Hacker de Sombrero Blanco (White Hat)

Especialista en ciberseguridad que realiza pruebas de intrusión con autorización, con el objetivo de detectar vulnerabilidades antes que los atacantes.

---

14. Hacker de Sombrero Gris (Grey Hat)

Actor que explora vulnerabilidades sin autorización explícita, pero sin una intención claramente maliciosa; su accionar suele estar en un terreno ético difuso.

---

15. Ciberguerra

Conflicto entre estados o grupos a través de medios digitales, con fines militares, políticos o económicos, que implica ciberataques contra infraestructuras críticas, espionaje o sabotaje.

---

16. Cyber Kill Chain

Modelo de análisis de amenazas desarrollado por Lockheed Martin que descompone un ciberataque en fases (reconocimiento, entrega, explotación, instalación, etc.) para entenderlo y detenerlo eficazmente.

---

17. CVE (Common Vulnerabilities and Exposures)

Estándar global que identifica y cataloga vulnerabilidades conocidas en software, facilitando su gestión y mitigación. Ejemplo: CVE-2021-44228 (Log4Shell).

---

18. Seguridad Operacional

Disciplina que se encarga de los controles, políticas y procedimientos para proteger la información durante su procesamiento y manejo cotidiano.

---

19. Ingeniería Social

Manipulación psicológica de personas para que revelen información confidencial o realicen acciones que comprometan la seguridad de un sistema.

---

20. Respuesta ante Incidentes

Conjunto estructurado de procesos técnicos y organizacionales orientados a detectar, contener, erradicar y recuperar ante un incidente de seguridad informática.

---

21. Ransomware

Tipo de malware que cifra los archivos de un sistema y exige un rescate económico a cambio de la clave de descifrado.

---

22. OWASP Top 10

Lista publicada por la OWASP Foundation que presenta las 10 principales vulnerabilidades de seguridad en aplicaciones web, actualizada periódicamente y adoptada como estándar global.

---

23. NIST Cybersecurity Framework

Marco de referencia desarrollado por el National Institute of Standards and Technology (EE.UU.) que proporciona directrices para identificar, proteger, detectar, responder y recuperarse ante amenazas cibernéticas.

---

24. Spoofing

Técnica que consiste en suplantar la identidad de un dispositivo o usuario para obtener acceso no autorizado a recursos o información.

---

25. Man-in-the-Middle (MitM)

Tipo de ataque donde un tercero intercepta, modifica o suplanta la comunicación entre dos partes sin que estas lo perciban.
