UNIVERSIDAD AUTONOMA

DEL ESTADO DE MEXICO

KARLA ZARET VAZQUEZ LEDO

CUESTIONARIO DE CIBERSEGURIDAD

SISTEMAS OPERATIVOS

7MO SEMESTRE

27/11/2025

1. ¿Qué es un pirata informático?
   Individuo que accede ilegalmente a sistemas con fines delictivos (robo, sabotaje, extorsión).

2. ¿Qué es un hacker?
   Experto que busca vulnerabilidades; puede ser ético (white hat), malicioso (black hat) o intermedio (grey hat).

3. ¿Qué es un gusano?
   Malware autónomo que se replica y propaga por redes sin necesidad de un anfitrión.

4. ¿Qué es un ataque DoS?
   Inunda un servidor/tráfico para hacerlo inaccesible a usuarios legítimos (Denegación de Servicio).

5. ¿Qué es una botnet?
   Red de dispositivos infectados controlados remotamente para ataques coordinados.

6. ¿Cuáles son los medios de ataque?
   Redes (Internet, WiFi), dispositivos infectados, phishing, exploits, ingeniería social.

7. ¿Cómo se comporta un troyano?
   Simula software legítimo, permanece oculto y da acceso remoto al atacante.

8. ¿Qué es el espionaje industrial?
   Robo ilegal de información empresarial confidencial para ventaja competitiva.

9. ¿Qué es la ciberdelincuencia?
   Delitos cometidos con medios informáticos: fraude, robo de datos, extorsión, sabotaje.

10. ¿Cuáles son las armas de los ciberdelincuentes?
    Malware, ransomware, exploits, phishing, keyloggers, botnets, puertas traseras.

11. ¿Dónde se centran los primeros ataques?
    En usuarios (phishing), sistemas desactualizados, dispositivos IoT, redes inseguras.

12. ¿Para qué sirve una puerta trasera?
    Acceso oculto que burla autenticación para entrada no detectada.

13 ¿Qué es un keylogger?
Software/hardware que registra pulsaciones de teclado para robar credenciales.

14 ¿Cómo acceder a cámaras vulnerables?
Mediante malware, contraseñas débiles/default, exploits de firmware o servicios mal configurados.

15 ¿Objetivo de la ingeniería social en ciberespionaje?
Manipular personas para que revelen información o comprometan seguridad.

16 ¿Qué hacen los ISAC's?
Centros de intercambio de información sobre amenazas cibernéticas entre organizaciones.

17 ¿Cyberwar Playbook?
Estrategias militares de guerra cibernética: tácticas de ataque/defensa.

18 ¿Pasos al detectar un ataque?
Aislar, preservar evidencias, analizar, eliminar amenaza, restaurar, fortalecer y reportar.