
# UNIVERSIDAD AUTÓNOMA DE ZACATECAS

## PROGRAMA ACADÉMICO DE INGENIERÍA DE SOFTWARE

MAYELA SARRIA SALAZAR

MATERIA: SEGURIDAD EN REDES Y SISTEMAS DE SOFTWARE

MAESTRO: CARLOS CASTAÑEDA

FECHA: 09/09/2025 Matricula: 37184124

# Actividad 1

**1. ¿Qué es la seguridad en su forma más simple?**

En su forma más simple, la seguridad implica la protección de los activos.

**2. ¿A qué se refiere el concepto de ciberseguridad?**

La ciberseguridad es la aplicación de tecnologías, procesos y controles para proteger sistemas, redes, programas, dispositivos y datos de ciberataques.

**3. ¿Cuál es el objetivo principal de la ciberseguridad?**

Su objetivo es reducir el riesgo de ciberataques y proteger contra la explotación no autorizada de sistemas, redes y tecnologías.

**4. ¿Por qué es vital preocuparse por la ciberseguridad?**

Es vital porque gran parte del valor de un negocio se concentra en el valor de su información.

**5. ¿Qué elementos componen la triada de la ciberseguridad?**

La triada de la ciberseguridad se compone de Confidencialidad, Integridad y Disponibilidad (CID).

**6. ¿Cómo se garantiza la Confidencialidad de la información?**

Se garantiza a través de la autenticación y autorización, encriptación, borrado remoto y capacitación de usuarios.

**7. ¿Qué se entiende por Integridad en la triada de la ciberseguridad?**

La integridad se refiere a salvaguardar la exactitud y totalidad de la información y los métodos de procesamiento y transmisión.

**8. ¿Cómo se logra la Disponibilidad de la información y los recursos?**

Se logra mediante la redundancia de servidores y sus componentes, así como las actualizaciones de software.

**9. Define qué es una Amenaza en el contexto de ciberseguridad.**

Una amenaza es cualquier cosa que pueda explotar una vulnerabilidad para comprometer un activo.

**10. ¿Qué es una Vulnerabilidad?**

Es una debilidad o brecha en los controles de seguridad.

**11. ¿Qué es el Malware y cómo se instala en un sistema?**

El Malware es cualquier código que se utiliza para robar datos, evitar controles de acceso o causar daños. Se instala cuando el usuario hace clic en un enlace malicioso, visita sitios web engañosos o descarga archivos sin analizar.

**12. ¿Cuál es la principal característica del Ransomware?**

El Ransomware es un tipo de malware que restringe el acceso a partes o archivos del sistema y exige un rescate a cambio de quitar esta restricción.

**13. ¿Qué es la Ingeniería Social?**

Es un intento de manipular a las personas para que realicen acciones, cometan errores de seguridad o divulguen información confidencial.

**14. ¿Qué es el Phishing?**

El Phishing son correos electrónicos maliciosos que se disfrazan como legítimos para engañar al usuario y hacer que comparta información personal, haga clic en un enlace que instala malware, o capture credenciales de acceso.

**15. ¿A qué se refiere un ataque "Zero-day Exploit"?**

Un ataque de este tipo explota una vulnerabilidad recién descubierta o no reportada para la cual aún no existe un parche de seguridad por parte del fabricante o desarrollador.

**16. ¿Cuál es el objetivo de un ataque de Denegación de Servicio (DoS)?**

Inundar los sistemas, redes o servidores con tráfico masivo para que no puedan atender las solicitudes legítimas.

**17. ¿Qué caracteriza a los "Black Hat Hackers"?**

Operan en el anonimato y están motivados por el beneficio personal o económico, la venganza, el acecho o el activismo político.

**18. ¿Quiénes son los "White Hat Hackers"?**

Son personas que operan bajo el permiso expreso del dueño de una red o sistema para reportar sus hallazgos, también conocidos como hackers éticos o analistas de seguridad.

**19. ¿Quién fue Kevin Mitnick y por qué es conocido?**

Kevin Mitnick fue llamado el "criminal informático más buscado en la historia de EE. UU." por el Departamento de Justicia. Tras cumplir su condena, se convirtió en consultor y orador en materia de seguridad informática.

**20. ¿Qué hizo Jonathan James para ser considerado un hacker famoso?**

Jonathan James, conocido como "c0mrade", hackeó la red de la NASA y descargó el código fuente de la Estación Espacial Internacional, lo que obligó a la NASA a cerrar su red por tres semanas, con un costo de $41,000