Tarea 01 Cuestionario

Licenciatura en Software, Universidad Autónoma de Zacatecas

Seguridad en Redes y Sistemas de Software

Autor:

Jonathan Alexis Martínez Reyes

Profesor: Carlos Héctor Castañeda Ramírez

30/Enero/2025

1. ¿Qué es la ciberseguridad?
Es lo que nos permite tomar medidas de precaución para proteger los sistemas, aplicaciones, datos de usuarios,etc. cuando nos quieran atacar de forma digital.

2. ¿Cuáles son los objetivos de la ciberseguridad?
Su objetivo es disminuir los riesgos y detectar posibles amenazas a los sistemas digitales.

3. ¿Qué es un malware?
Es un Software malicioso diseñado para dañar o infiltrarse en sistemas.

4.¿Cuáles son algunos tipos de malware?
Virus: Infecta archivos y se propaga a otros sistemas.
Gusano: Se replica a sí mismo y se propaga por redes.
Spyware: Recopila información sin el consentimiento del usuario.

5. ¿Qué es un firewall y cómo funciona?
Un firewall es un sistema de seguridad que filtra el tráfico de la red. Funciona estableciendo reglas para dar o bloquear conexiones basadas en la dirección IP protegiendo la red de accesos no autorizados.

6. ¿Qué es un ataque de phishing?
Un ataque de phishing es un intento de engañar a las personas para que revelen información confidencial, como contraseñas o números de tarjetas de crédito, mediante correos electrónicos, mensajes o sitios web falsos.

7. ¿Cómo se puede prevenir un ataque phishing?
Verificar la autenticidad de los correos y enlaces.
No proporcionar información personal sin confirmar la identidad del solicitante.
Mantener el software actualizado.
No utilizar una misma contraseña para todas las cuentas de correo electrónico, cuentas de bancos, etc.

8. ¿Qué es un ataque DoS?
Un ataque de denegación de servicio (DoS) es un intento de sobrecargar un sistema, servidor o red con tráfico falso, haciendo que no esté disponible para los usuarios o sea provocar interrupciones en un servicio.

9. ¿Qué es el cifrado de datos?
El cifrado de datos es el proceso de convertir información en un formato ilegible (cifrado) para protegerla de accesos no autorizados.

10.¿Por qué es importante en ciberseguridad cifrar datos?
Es importante porque garantiza la confidencialidad de los datos, incluso si son interceptados.

11. ¿Qué es un parche de seguridad?
Un parche de seguridad es una actualización de software que corrige vulnerabilidades o errores en un sistema

12. ¿por qué es necesario aplicarlo?
Porque los atacantes suelen explotar estas vulnerabilidades para infiltrarse en los sistemas y los parches ayudan a prevenir estos ataques.

13. ¿Cuál es la diferencia entre un virus y un gusano?
Un virus necesita un archivo anfitrión para propagarse y depende de la interacción del usuario para ejecutarse, mientras que un gusano puede replicarse y propagarse por sí mismo a través de redes sin necesidad de un archivo anfitrión o interacción del usuario.

14. ¿Qué es un hacker ético?
Es un profesional que utiliza sus habilidades para identificar y corregir vulnerabilidades en sistemas, redes, aplicaciones, etc.

15. ¿Cuál es su papel en la ciberseguridad?
Su papel es simular ataques cibernéticos con el permiso del propietario del sistema con el fin de mejorar la seguridad y prevenir ataques reales.

16. ¿Qué es la autenticación de dos factores (2FA)?
Es un método de seguridad que requiere dos formas diferentes de verificar la identidad del usuario, como una contraseña y un código enviado al teléfono.

17. ¿Es recomendable usar una 2FA?
Sí, ya que añade una capa adicional de seguridad, haciendo más difícil que los atacantes accedan a las cuentas.

18. ¿Qué es un "backup"?
Un backup es una copia de seguridad de los datos importantes.

19. ¿Por qué es importante en la ciberseguridad un backup?
Porque permite recuperar la información en caso de pérdida, daño o ataque cibernético.

20. ¿Qué es la "confidencialidad" en ciberseguridad y cómo se garantiza?
La confidencialidad es la protección de la información para que no sea accedida por personas no autorizadas. Se garantiza mediante técnicas como el cifrado de datos, el control de acceso y el uso de contraseñas seguras.