Seguridad Informática

1. Confidencialidad: Es la protección de la información sensible, y solo las personas autorizadas pueden acceder a ella.

2. Integridad: Es garantizar que los datos no sean modificados de manera no autorizada.

3. Disponibilidad: Significa la accesibilidad y disponibilidad de los sistemas y los datos en cuando sean solicitados.

4. Autenticación: Es la forma de verificar y confirmar la identidad de un usuario.

5. Menciona las 3 formas de autenticar a un usuario: biometría, contraseña, certificados digitales, preguntas de seguridad

6. Autorización: Es el proceso para acceder a recursos o datos específicos dentro de un sistema, esta evalúa las condiciones o permisos.

7. Auditoria: No poder negar mi participación, ya que se registra en los logs.

8. Diferencia entre autenticación y autorización: La autenticación esta encargada de la identidad mientras que la autorización define que puede hacer la entidad

9. Activo: Es todo lo que tiene de valor para la empresa

10. Vulnerabilidad: Algo que puede ser usado para poder entrar

11. Ataque: Es cualquier acción hecha por una persona, grupo o software con el objetivo de comprometer la seguridad de un sistema.

12. Impacto: Es la materialización de una amenaza

13. Evento: Es cuando los servicios, la seguridad, o la infraestructura ha sido comprometida o vulnerado.

14. Riesgo: Posibilidad de que se produzca un contratiempo o una desgracia, de que alguien sufra un prejuicio o daño.

15. Amenaza: Puede ser un atacante, un malware, personal no capacitado

16. Exploit: Es el software que automatiza o técnica que se utiliza para aprovechar una vulnerabilidad en un sistema

17. Payload: Código que aprovecha la vulnerabilidad

18. Desarrollo seguro de software: Explica brevemente cada categoría.
    a. Principio de privilegio mínimo: Significa que los usuarios deben de tener el mínimo nivel de acceso y privilegios para hacer las tareas.
    b. Defensa en profundidad: Es cuando implementas múltiples capas de seguridad en una aplicación o sistema.
    c. Enlace más débil: Es cuando un sistema puede ser comprometido si un elemento es vulnerable
    d. Fallar a lo seguro: Cuando después de una vulnerabilidad puedes contener el ataque
    e. Economía de mecanismos: Es cuando un sistema de seguridad es claro y simple este tendrá los más mínimos errores o vulnerabilidades.

19. OWASP Top Ten 2021: Explica brevemente cada categoría.

1.- Broken Access Control: Permite que un atacante pueda obtener acceso a las cuentas de los usuarios por medio de una debilidad.

2.- Cryptographic Failures: Cuando llegas a comprometer datos confidenciales que son importantes los cuales están almacenados o transmitidos.

3.- Injection: Es cuando puedes inyectar código no autorizado a una aplicación web y esta hará algo que no ha sido contemplado.

4.- Insecure Design: Se enfoca en los riesgos de los malos diseños.

5.- Security misconfiguration: Son debilidades que están ahí por una mala o error de configuración y esto surge por un mal diseño.

6.- Vulnerable and Outdated Components: Esto de refiere a que hay componentes obsoletos y estos deben de evaluarse para determinar su viabilidad y ver si pueden presentar un riesgo o no.

7.- Identification and Authentication Failures: Cuando se implementa una mala autenticación o administración de sesión, se pueden llegar a comprometer las contraseñas, sesiones, claves y esto puede llevar al robo de identidad

8.- Software and data Integrity Failures: Esta está basada en el fallo de deserialización y permite que un atacante pueda ejecutar código de manera remota.

- Falla en la integridad del Software
- Falta de autenticación de datos
- Componentes o software desactualizado

9.- Security Loggin and Monitoring Failures: Es cuando no se hace la debida supervisión a los sitios web, esto ocasiona que el sitio web sea vulnerable a actividades comprometedoras.

- Cuando hay errores en los registros y pueden existir brechas de seguridad
- Vulne: log4shell

10.- Server Side Request Forgery: Es cuando un atacante hace que una aplicación envíe una solicitud a otra aplicación de manera inesperada y manipulad.

- Una red no segmentada y puedan mapear los puertos abiertos en los servicios internos
- XXE