Seguridad Informática

1. Confidencialidad: Aegurar que el acceso a la información se realice únicamente con los datos correctos
2. Integridad: Asegurar que la información sea libre de alteraciones o modificaciones por personas, procesos o entidades no autorizadas
3. Disponibilidad: Asegurar que la información esté disponible para quienes lo necesiten en el momento en que lo necesiten
4. Autenticación: Confirmar que alguien es quien dice ser
5. Menciona las 3 formas de autenticar a un usuario: Conocimiento, Propiedad y Característica
6. Autorización: Debe cumplir con la matriz de accesos, roles y funcionalidades, no debe ser capaz de escalar privilegios, privilegio mínimo
7. Auditoria: Que quede siempre rastro y registro de las acciones, bitácoras
8. Diferencia entre autenticación y autorización: Autenticación tiene que ver con la identidad de la persona y su demostración, Autorización tiene que ver con los privilegios y roles de un usuario
9. Activo: Cualquier elemento de la empresa que tenga valor para la misma
10. Vulnerabilidad: Debilidad, fallo o error presentado en un sistema
11. Ataque: Intento de aprovechar una vulnerabilidad
12. Impacto: Materialización de una amenaza en un sistema
13. Evento: Cualquier cambio en un sistema, generalmente negativo
14. Riesgo: Probabilidad de que se ejecute o materialice una amenaza
15. Amenaza: La entidad que puede poner en peligro los activos
16. Exploit: Software que automatiza la explotación de una vulnerabilidad
17. Payload: Un código que aprovecha una vulnerabilidad
18. Desarrollo seguro de software: Explica brevemente cada categoría.
19. Principio de privilegio mínimo: Que cada usuario cuente únicamente con los privilegios mínimos necesarios para ejecutar sus acciones, sin nada extra que no necesite
20. Defensa en profundidad: Incorporación de una serie de capas de medidas de seguridad y mitigación de riesgos
21. Enlace más débil: Que un sistema o una aplicación es tan segura como lo sea su componente más débil
22. Fallar a lo seguro: Mantener la confidencialidad, integridad y disponibilidad por defecto en un estado seguro ante una falla
23. Economía de mecanismos: Mantenerlo simple. Mantener el diseño de software y detalles de implementación simples para reducir la superficie de ataque
24. OWASP Top Ten 2021: Explica brevemente cada categoría.

A01:2021 – Pérdida de control de acceso: Esta categoría ocurre cuando los usuarios son capaces de actuar fuera de los permisos que les fueron asignados, ya sea eludiendo las comprobaciones de control o elevando sus privilegios, entre otros.

A02:2021 - Fallas Criptográficas: Ocurre cuando los datos no se encuentran cifrados o protegidos de manera adecuada, lo que puede provocar la exposición de datos sensibles/confidenciales o hasta el compromiso total del sistema

A03:2021 – Inyección: Cuando se inserta un código maliciosos en un campo no sanitizado correctamente

A04:2021 - Diseño Inseguro: Esta categoría se aplica cuando no se tuvo cuidado en el diseño de la aplicación y se dejaron vulnerabilidades básicas, sin tener en cuenta

A05:2021 - Configuración de Seguridad Incorrecta: La aplicación no tiene un proceso de configuración de seguridad de aplicaciones coordinado y repetible, lo que la hace correr un mayor riesgo

A06:2021 - Componentes Vulnerables y Desactualizados: Los componentes no tienen la última versión de seguridad, lo que provoca que sean más vulnerables a los ataques

A07:2021 - Fallas de Identificación y Autenticación: El proceso de identificación y autenticación del sistema es débil, y no tiene las protecciones mínimas necesarias, como permitir contraseñas por defecto, autenticación de doble factor, entre otras cosas, lo que lo vuelve susceptible por ejemplo a ataques por fuerza bruta

A08:2021 - Fallas en el Software y en la Integridad de los Datos: Esta categoría se aplica cuando se permite hacer actualizaciones de software y datos críticos sin verificación de integridad en los mismos.

A09:2021 - Fallas en el Registro y Monitoreo: Los sistemas no se monitorean correctamente, lo que afecta directamente la visibilidad, las alertas de incidentes y los análisis forenses

A10:2021 - Falsificación de Solicitudes del Lado del Servidor: Ocurre cuando una aplicación web obtiene un recurso remoto sin hacer validación de URL del usuario, permitiendo que el atacante envíe una solicitud falsa.