Taller: “Hackeando la Seguridad… para Proteger”

¿Qué es la Seguridad de los Sistemas de Información?

Es el conjunto de prácticas, políticas y tecnologías diseñadas para proteger los datos, la infraestructura tecnológica y los procesos organizacionales de accesos no autorizados, alteraciones o pérdidas. Su importancia radica en garantizar la confidencialidad, integridad y disponibilidad de la información. Va más allá del software: también incluye el factor humano. Hoy más que nunca, la seguridad es un activo estratégico en cualquier organización. Su implementación debe ser continua, preventiva y adaptable.

Confidencialidad: Protegiendo el Secreto

Este principio garantiza que la información solo sea accesible a personas autorizadas. Se aplican mecanismos como cifrado, control de accesos y políticas de privacidad. Es crucial en contextos como banca, salud o defensa. La filtración de datos sensibles puede afectar la reputación y causar pérdidas millonarias. Se relaciona directamente con el respeto por la privacidad de los usuarios.

Integridad: Información Sin Alteraciones

Busca asegurar que la información no sea modificada de forma no autorizada. Utiliza herramientas como firmas digitales, hashing y controles de versiones. Es vital para mantener la veracidad de los datos almacenados o transmitidos. Una base de datos alterada sin control puede llevar a decisiones equivocadas o fraudes. La integridad garantiza confianza en el sistema.

Disponibilidad: Acceso Cuando se Necesita

La disponibilidad implica que los sistemas y datos estén accesibles en el momento que se requieren. Para ello, se implementan redundancias, respaldos y planes de contingencia. Ataques como DDoS (denegación de servicio) buscan justamente comprometer este principio. Sin disponibilidad, incluso el sistema más seguro es inservible. Es el pilar que sostiene la continuidad operativa.

Autenticación y Control de Acceso

La autenticación permite verificar la identidad del usuario, mientras que el control de acceso define qué puede hacer dentro del sistema. Se utilizan contraseñas, biometría, tokens o autenticación multifactor (MFA). Es un filtro fundamental para prevenir accesos maliciosos. Sin una buena política de control, se abren puertas a vulnerabilidades internas y externas.

Principales Amenazas a los Sistemas de Información

Entre las amenazas más comunes están los virus, ransomware, phishing, ingeniería social y ataques internos. Estas amenazas evolucionan constantemente, exigiendo estrategias de

defensa actualizadas. Muchas veces, el eslabón más débil es el usuario final. La capacitación y conciencia del personal son tan importantes como el firewall más avanzado. Un enfoque preventivo es la mejor defensa.

Parte Práctica del Taller: "Hackeando la Seguridad… desde el Laboratorio"

Seleciona y desarrolla alguno de los siguientes laboratorios y entrega un informe del mismo. La actividad se puede entregar en grupo dedos estudiantes.

Laboratorio 1: Cifrado de Mensajes con Python

Objetivo: Aplicar técnicas básicas de cifrado simétrico para proteger datos.

Instrucciones:
1. Instala la librería `cryptography` en Python.
2. Escribe un script que cifre y descifre un mensaje usando la clave simétrica generada.
3. Simula el envío de un mensaje cifrado entre dos usuarios.
4. Modifica el mensaje cifrado y verifica cómo se rompe la integridad.
Refuerzo: Confidencialidad e integridad.

Laboratorio 2: Escaneo y Análisis de Red con Wireshark

Objetivo: Observar el tráfico de red y detectar posibles vulnerabilidades.

Instrucciones:
1. Instala y ejecuta Wireshark en un entorno de red controlado (por ejemplo, laboratorio virtual).
2. Filtra paquetes HTTP, DNS y ARP.
3. Identifica credenciales que viajan sin cifrado (en protocolos inseguros).
4. Reflexiona sobre la importancia de protocolos seguros como HTTPS.
Refuerzo: Confidencialidad y disponibilidad.

Laboratorio 3: Pruebas de Autenticación y Control de Accesos

Objetivo: Implementar autenticación básica y roles de acceso en una app web.

Instrucciones:
1. Usa un backend simple (por ejemplo, Spring Boot o Flask) con usuarios y contraseñas.
2. Implementa login con autenticación básica o JWT.
3. Crea dos roles: "admin" y "user" y controla las rutas accesibles para cada uno.
4. Realiza pruebas para intentar saltar el control de accesos.
Refuerzo: Autenticación y control de acceso.