

SEGURIDAD INFORMÁTICA

Seguridad de la información → Todas las acciones para proteger la integridad, la privacidad de los datos y toda la información que se encuentre alojada en un sistema informático

Seguridad Activa: protege y evita daños en los sistemas informáticos

Seguridad Pasiva: acciones o técnicas de seguridad que entran en acción para minimizar los daños a los sistemas informáticos.

Medidas de seguridad

1) **Proactivas:**

- a. Directivas → qué podemos o no hacer
- b. Disuasivas → desvían la intención del atacante potencial al sistema o el uso indebido por parte del personal
- c. Preventivas → Informar y prevenir una acción indebida

2) **Reactivas:**

- a. Detectivas → búsqueda de potenciales ataques
- b. Correctivas → solucionar el sistema luego del incidente

Auditoria

Analizar y determinar que toda la informática de la organización trabaje de manera eficiente.

El auditor informático plasmará en un informe final todas las debilidades, oportunidades de mejora y recomendaciones para que la organización sin carácter obligatorio decida si aceptarlas o no.

Seguridad física

Establecimiento de técnicas que permiten resguardar de cualquier tipo de daños a los equipos en los cuales se almacena los activos de una organización —sus datos—.

- a) Dispositivos físicos de protección
- b) UPS (Uninterruptable Power Supply)
- c) Respaldo de datos
- d) Sistemas redundantes

Seguridad lógica

Es un tipo de software que impide que malware o hackers puedan ingresar a nuestra computadora a través de Internet o de una red. Está conformada por un conjunto de procesos que se encargan de garantizar la seguridad de los datos y sistemas, además controlan el acceso a los mismos.

- a) Control de acceso
- b) Cifrado de datos
- c) Antivirus
- d) Firewalls

Ataques de denegación de servicios

Dimensión de disponibilidad de la información: la persona debe tener acceso a la información en el momento en que la necesite, en tiempo y forma.

Denegación de servicio: consiste en la interrupción del acceso a los servicios (computadoras y redes) por parte de los usuarios legítimos.

Ataque de denegación de servicio (DoS): Es un ataque a un sistemas de computadoras o red que provoca que un servicio o recurso de esta computadora sea inaccesible para su usuario.

Se produce una gran cantidad de peticiones desde solamente una máquina o una dirección IP al servicio, produciendo una saturación de los puertos, hasta que llega un momento en que el servidor no tiene capacidad de respuesta a todos los servicios solicitados y comienza a rechazar peticiones, es aquí donde se produce la denegación del servicio.

Por otro lado, un DoS no solo puede ocurrir desde la red. El incremento del uso de recursos de manera sintética o forzada (como CPU o memoria) también puede producir un DoS.

Ataque de denegación de servicio distribuido (DDoS): se produce una gran cantidad de peticiones al servicio, pero en este tipo se lleva a cabo desde varios puntos o direcciones IPs de conexión produciendo la saturación del puerto de destino, hasta que llega un momento en que el servidor no tiene capacidad de respuesta a todos los servicios solicitados y comienza a rechazar peticiones.

Métodos de ataque:

- Consumen el ancho de banda.
- Alteran las tablas de enrutamiento —la ruta por donde debe ir la información—. Por tal motivo, la información que se envía no llega a destino.

- Fallas en los componentes físicos de una red.

Hacking y Cracking

Un hacker es una persona a la cual le apasiona el conocimiento, descubrir o aprender nuevas cosas e indagar más sobre ellas. Toda aquella persona que hackea cualquier tipo de sistema descubre sus vulnerabilidades.

Tipos de hacker

- Sombrero blanco (white hats): utilizan los conocimientos en informática y seguridad informática con el fin de defender los sistemas de información.
- Sombrero gris (gray hats): tienen conocimientos tanto de la parte defensiva como ofensiva y pueden trabajar en cualquiera de los ámbitos.
- Sombrero negro (black hats): tienen conocimientos informáticos y recurren a hacer actividades maliciosas o ilegales. También conocidos como crackers.