17 - Seguridad Informática

domingo, 9 de mayo de 2021 16:10

SEGURIDAD: consiste en todas las acciones que llevamos adelante para proteger la integridad y seguirdad de los datos de un sistema informático. Hay de dos tipos:

ACTIVA: los elementos activos contienen información (servidores, celulares, bases de datos, etc.) que alguien quiere vulnerar (obtener, destruir, etc.) a través de una vulnerabilidad. La seguridad activa protégé y evita daños en los sistemas informáticos.

- Usar contraseñas adecuadamente.
- Usar software de seguridad (antivirus, cortafuegos).
- Encriptar datos importantes (algoritmo de cifrado).

PASIVA: es un conjunto de acciones o técnicas de seguridad que entran en acción para minimizar los daños al sistema informático. Se activan cuando una amenaza ha sido introducida al sistema.

- Realizar copias de seguridad distribuidas.
- Escanear y limpiar equipos continuamente.
- Crear particiones en el disco duro.
- Frente a un ataque, desconectar el equipo de la red.
- Frente a un virus, verificar que el antivirus funcione.

SEGURIDAD **FÍSICA**: permite resguardar de daños a los equipos que almacenan los activos (datos) de la organización.

- Dispositivos físicos de protección: pararrayos, extintores, detectores de humo, etc.
- UPS (Uninterrumptable Power Supply): anti apagones (tiene una mini batería para no perder energía de una).
- Respaldo de datos: copias de los activos más importantes.
- Sistemas redundantes: si un sistema falla, la información se recupera del otro lugar donde se encuentra.

SEGURIDAD **LÓGICA**: software que impide el ingreso a nuestra computadoras de malware o hackers.

- Control de acceso: impide el acceso a personas no autorizadas mediante el uso de usuarios y contraseñas.
- Cifrado de datos: consiste en la aplicación de un algoritmo de cifrado acompañado de una clave, para solo ser leido por el destinatario.
- Antivirus: permite escanear, detectar y eliminar malware.
- Firewalls: impide que malware o hackers pueda ingresar a nuestra computadora a través de internet o una red.

MEDIDAS DE SEGURIDAD:

PROACTIVAS:

- Directivas: dicen qué podemos o no hacer.
- Disuasivas: desviar uso indebido (advertencias).
- Preventivas: informar y prevenir acción indebida.

REACTIVAS:

- Detectivas: búsqueda de potenciales peligros.
- Correctivas: solucionar el sistema luego del desvío. Se activan después de encontrar el riesgo/incidente.

AUDITORIA: es la acción de analizar de manera exhaustiva y profunda las distintas características y áreas de una organización.

- **EFICIENCIA**: la información recabada debe ser útil para la toma de decisiones. Se necesita experiencia en gestión de proyectos.
- **NORMATIVA**: se deben cumplir las normativas determinadas para certificar que la empresa trabaja bajo normas estándares. Se necesita conocimiento de softwares y normativas.
- **GESTIÓN DE RECURSOS**: recursos utilizados de manera correcta. Se necesita conocimiento de infraestructura.

El auditor es el encargado de analizar y determinar que toda la informática de la organización trabaje de manera eficiente. La mayoría trabajan en grupos de hasta 4 personas y plasmarán en un informe final todas las debilidades, oportunidades de mejora y recomendaciones (no obligatorias). Suelen usar las siguientes herramientas:

- Entrevistas: determinar si el personal utiliza normas.
- Encuestas: panorama general del estado de la empresa.
- Análisis de los procesos: revisar documentación.
- Análisis del código de software: verifica pautas cumplidas.

DoS (Ataque de Denegación de Servicio):
"Dimensión de disponibilidad" refiere a que la persona debe tener acceso a la información en tiempo y forma. La DoS consiste en interrumpir el acceso a los servicios por parte de usuarios legítimos. Sucede una gran cantidad de peticiones desde una sola dirección IP al servicio, saturando los puertos hasta que el servidor no tiene capacidad de respuesta y comienza a rechazar peticiones.

DDoS (Ataque de Denegación de Servicio Distribuido):
A diferencia de un DoS, se lleva a cabo desde varias direcciones IP. Se pueden usar *bots* (aplicación de software que realiza tareas simples y repetitivas) y *botnets* (conjunto de bots que quedan a espera de una señal para comenzar el ataque DDoS).

HACKER: experto en ramas técnicas de la tecnología de información de las comunicaciones (programación, redes, SO, software, etc). Le apasiona indagar sobre cosas nuevas, y logra encontrar vulnerabilidades de un sistema. Hay tipos:

White hats: utilizan los conocimientos con el fin de defender los sistemas de información.
Gray hats: tienen conocimiento tanto de la parte defensiva como de la parte ofensiva.
Black hats: son los "crackers" (quienes violan la seguridad de un sistema informático con fines ilícitos o no éticos), recurren a hacer actividades maliciosas o ilegales.