Clase 17“Seguridad informática”

- ✓ La seguridad de la información consiste en todas las acciones que llevamos adelante para proteger la integridad, la privacidad de los datos y toda la información que se encuentre alojada en un sistema informático. Para poder proteger a nuestra computadora tenemos dos tipos de seguridad: seguridad activa y seguridad pasiva.

Seguridad activa y pasiva

Seguridad activa:

- → Los elementos denominados activos contienen información, pueden tener muchas formas: servidores, dispositivos móviles, bases de datos, etc.
- → Esos activos contienen información que alguien quiere vulnerar, obtener, destruir, etcétera. Como su intención es acceder a una información, lo va a hacer a través de una vulnerabilidad (problema que tienen los sistemas que contienen información). La amenaza aprovecha esa vulnerabilidad para ingresar de forma indebida a la información y hacer lo que quería hacer.
- → La seguridad activa protege y evita daños en los sistemas informáticos.
- → Buenas prácticas:

1. Uso y empleo adecuado de contraseñas.
2. Uso de software de seguridad informática, como antivirus, antiespías y cortafuegos.
3. Encriptar los datos importantes: Mediante un algoritmo de cifrado con una clave para que el dato/información solo pueda ser leído si se conoce la clave de cifrado.

Seguridad pasiva:

- → Es un conjunto de acciones o técnicas de seguridad que entran en acción para minimizar los daños a los sistemas informáticos.
- → Estas acciones se activan cuando se ha introducido un malware o cualquier otra amenaza en los sistemas.
- → Buenas prácticas:

1. La realización de copias de seguridad de los datos en más de un dispositivo y/o en distintas ubicaciones físicas.
2. Escanear y limpiar continuamente los equipos para controlar y evitar ataques de malware.
3. Crear particiones en el disco duro para almacenar archivos y backups/copia de seguridad en una unidad distinta a donde tenemos nuestro sistema operativo.
4. Frente a un ataque, desconectar el equipo de la red hasta que se pueda solucionar.
5. Es importante que cuando haya una infección por un virus, comprobar que el antivirus funcione correctamente.
6.

Medidas de protección

Proactivas

- ✓ Directivas: Nos dicen qué podemos o no hacer. Intentan que las actividades de los sistemas se realicen de una manera específica con el fin de que se produzcan ciertos resultados esperados.
- ✓ Disuasivas: Pueden desviar la intención del atacante potencial a un sistema o el uso indebido por parte del personal. Se diferencian con las directivas en que estas no nos restringen directamente,

sino que nos hacen una advertencia, la cual se puede o no tener en cuenta a la hora de ejecutar la acción indebida.

- ✓ Preventivas: Buscan que no se produzca un accidente o cualquier tipo de acción indebida en los sistemas. La diferencia con las disuasivas es que estas buscan informar y prevenir una acción indebida.

Reactivas

- ✓ Detectivas: Se basan en la búsqueda de potenciales ataques o peligros a los que puede estar expuesto un sistema informático.
- ✓ Correctivas: Una vez se ha encontrado el riesgo o ha sucedido un incidente que ha puesto en peligro a los datos o información, se activan estas medidas de seguridad. Su objetivo es solucionar el sistema luego que ha sucedido el desvío.

Auditorias

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

→ En informática, el auditor es el encargado de 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.

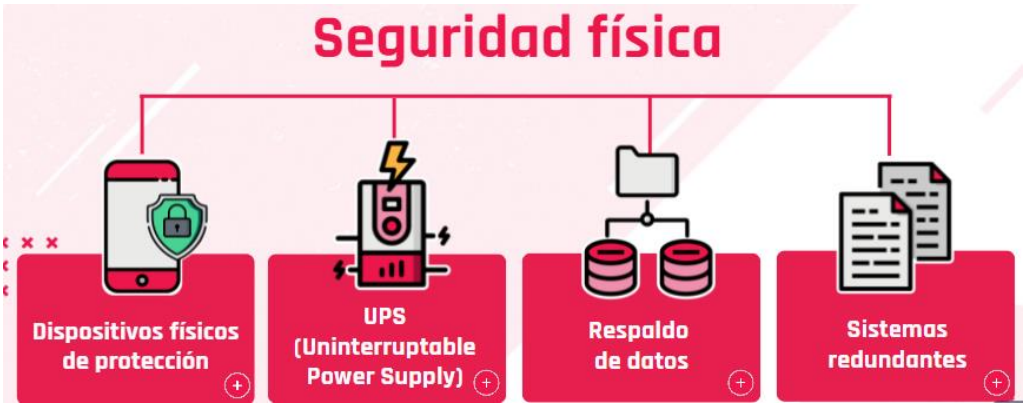
Conocimientos	Descripción
Entrevistas	A través de entrevistas al personal determinar si son conscientes y utilizan las normas establecidas por la empresa en su día a día.
Encuestas	Sirven para tener un panorama general del estado de la empresa.
Análisis de los procesos	Las empresas deberían tener documentado sus distintos procesos para que el auditor revise que cumplan los estándares pautados.
Analisis del codigo de software	Mediante distintas pruebas o análisis de la sintaxis los auditores aseguran que las pautas para el desarrollo de software sean cumplidas.

Objetivos de la auditoría de sistemas de información

1. EFICIENCIA: Se debe trabajar de manera tal que la información recabada sea útil para la toma de decisiones.
2. NORMATIVA: Se deben cumplir las normativas determinadas para certificar que la empresa trabaja bajo las normas estándares.
3. GESTIÓN DE RECURSOS: Recursos utilizados de manera correcta.

Seguridad física

→ Consiste en el 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).



Seguridad lógica

→ La 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.

→ Incluye aspectos como: Control de acceso, cifrado de datos, antivirus, firewalls.

Control de acceso 	Impide el acceso a las personas no autorizadas mediante el uso de usuarios y contraseñas.
Cifrado de datos 	El cifrado es la acción de transformar un mensaje de tal forma que no pueda ser comprendido por otra persona distinta al receptor. Por lo tanto, el cifrado de datos consiste en la aplicación de un algoritmo de cifrado acompañado de una clave, con el objetivo de transformar el mensaje, para que únicamente pueda ser leído por el destinatario.
Antivirus 	Permite escanear, detectar y eliminar malware en un sistema informático.
Firewalls 	Impide que malware o hackers puedan ingresar a nuestra computadora a través de Internet o de una red.

Ataque de denegación de servicio (DoS)

La 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 distribuido (DDoS)

Es cuando 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, es aquí donde se produce el ataque de denegación de servicio distribuido.

Diferencia entre ambas

En DoS las peticiones se realizan desde solo una máquina o una dirección IP, como también puede ser desde algún agente instalado programado para tal fin. En DDoS las peticiones se realizan desde varios puntos o direcciones IPs.

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 con el objetivo de poder encontrar alguna herramienta que la minimice o suprima —en el caso de un white hat— o utilizar esta vulnerabilidad a su favor —en el caso de un black hat— y esto lo logra en base a su conocimiento.

Tipos de hacker

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

Las diferencias entre hacker y cracker

→ El hacker es un experto en varias ramas técnicas relacionadas con las tecnologías de información de las comunicaciones, como son: programación, redes, sistemas operativos e ingeniería de software.

→ El cracker es también un experto, pero además es quien viola la seguridad de un sistema informático con fines ilícitos o con un objetivo deshonesto y no ético.