Seguridad activa y pasiva

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.

**¿Qué es la seguridad activa?**

Los elementos denominados activos contienen información, pueden tener muchas formas: servidores, dispositivos móviles, bases de datos, entre otros. 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:

* Uso y empleo adecuado de contraseñas. Una de las técnicas para que una contraseña sea segura consiste en la combinación entre letras, números, mayúsculas y otros caracteres. No se debe usar nombre de mascotas o fechas de nacimiento, entre otros datos que pueden ser de conocimiento público.
* Uso de software de seguridad informática, como antivirus, anti-espías y cortafuegos.
* Encriptar los datos importantes: La encriptación consiste en cifrar los datos o la información mediante un algoritmo de cifrado con una clave para que el dato/información solo pueda ser leído si se conoce la clave de cifrado.

**¿Qué es la 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:

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

Clases de medidas de seguridad:  
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.

AUDITORIA:   
Auditar: 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.

Objetivos de la auditoria de sistemas de información:  
\*Eficiencia: Se debe trabajar de manera tal que la información recabada sea útil para la toma de decisiones.  
\*Normativa: Se deben cumplir las normativas determinadas para certificar que la empresa trabaja bajo las normas estándares.  
\*Gestión de recursos: Recursos utilizados de manera correcta.

Conocimiento del auditor informatico: Para cumplir con los objetivos mencionados anteriormente, es necesario:  
\*Eficiencia: Experiencia en gestión de proyectos.  
\*Normativa: Conocimiento de softwares y normativas  
\*Gestion de recursos: Conocimiento de infraestructura.

Auditor:  
La mayoría de los auditores trabajan en pequeños grupos de hasta 4 personas y son el nexo directo con los distintos departamentos y dirección. El auditor informática plasmara en un informe final todas las debilidades, oportunidades de mejora y recomendaciones para que la organización sin carácter obligatorio decida si aceptarlas o no.

![Tabla

Descripción generada automáticamente]()

**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—.  
\*Dispositivos físicos de protección: Pararrayos, extintores, detectores de humo, alarma contra intrusos, entre otros.  
\*UPS (uninterruptable Power Supply): Es un dispositivo electrónico que almacena energía por medio de una batería interna. Esto le permite a los dispositivos que están conectados al mismo, frente a un apagón eléctrico, seguir almacenando la información por un determinado tiempo.  
\*Respaldo de datos: Es importante saber que los datos son los activos más importantes dentro de una organización, por tal motivo, es de suma importancia el manejo y cuidado de los mismos ya que pueden estar expuestos a muchos factores como hurto, alteración, virus, entre otros. Por tal motivo, se deben realizar copias de seguridad o backups de los datos completos e incrementales. El backup es un proceso por el cual se realiza la copia de los datos originales con el fin de prevenir cualquier tipo de pérdida de los mismos.  
\*Sistemas redundantes: Son la copia de datos de mayor importancia. Cuando uno de los sistemas falla, no se pierde la información, sino que se recupera del otro lugar donde se encuentra.

**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:

![Imagen que contiene Texto

Descripción generada automáticamente]()

ATAQUES DE DENEGACION DE SERVICIOS:  
\*Ataque de denegación de servicios (DoS): Cuando hablamos de la dimensión de disponibilidad nos referimos a que la persona debe tener acceso a la información en el momento en que la necesite, en tiempo y forma. La denegación de servicio consiste en la interrupción del acceso a los servicios(computadoras y redes) por parte de los usuarios legítimos. Puede ser producida por una gran cantidad de peticiones desde solamente una maquina o una dirección IP al servicio, produciendo una saturación de los puertos, hasta que el servidor no tiene capacidad de respuesta a todos los servicios solicitados y comienza a rechazar peticiones. Denegacion de servicio. Pero también 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): En un DDoS lo que sucede es que 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.

Bot-botones  
Computadora-Zombie

Hacking y Cracking

Un sistema de información es un conjunto de elementos que están orientados al tratamiento y la administración de los datos para obtener información en base a ellos.

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.   
Y por qué no nombrar a aquellas personas que han sido hackers, por ejemplo, Rene Favaloro, un hacker en medicina, al descubrir una vulnerabilidad en el sistema cardiaco y realizar el primer bypass cardiaco.

**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.

**Las diferencias entre hacker y cracker**

El **hacker** es un experto en varias ramas técnicas relacionadas con las tecnología 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.