Conceptos básicos de seguridad

Tabla de Contenidos

1.- Conceptos básicos de seguridad general

Se define la **seguridad** como la disciplina que se encarga de detectar, evaluar y gestionar los riesgos a los que se encuentra sometido algo.

Como se puede ver es un término muy ambiguo, lo cual es la razón de que habitualmente se trate de forma más concreta la seguridad en un campo o ámbito más concreto (seguridad ciudadana, seguridad informática, seguridad alimentaria, seguridad vial, etc.).

A su vez, un **riesgo** es una medida de la magnitud o del alcance de los daños que puede provocar una situación peligrosa.

Los riesgos se miden asumiendo que cualquier sistema tiene una o más vulnerabilidades que son susceptibles de ataque, ya sea de forma accidental o intencional.

Conocemos como **vulnerabilidad** a la probabilidad de que ocurran daños cuando se presente un peligro. No hay que confundir con **peligrosidad**, que se define como la probabilidad de que ocurra un peligro. La diferencia es que puede haber peligros que ocurran fácilmente (y por lo tanto la peligrosidad es muy grande) pero tienen poco impacto (vulnerabilidad baja) y viceversa. Por ejemplo los pilotos de Fórmula 1 tienen una alta probabilidad de verse envueltos en algún tipo de choque (peligrosidad alta). Sin embargo la probabilidad de que cuando ocurra un choque sufran daños es baja (vulnerabilidad baja). Este es el caso más habitual y buscado. El caso contrario (peligrosidad baja y vulnerabilidad alta) significa que hay un peligro que es poco probable que ocurra pero cuando lo haga el daño será probablemente grande.

La seguridad puede intervenir para intentar reducir la peligrosidad y/o la vulnerabilidad. La forma de hacerlo es mediante las medidas de seguridad.

Una **medida de seguridad** es una acción que se toma para prevenir o reducir la peligrosidad o vulnerabilidad de un sistema.

Las medidas de seguridad se implementan en cuatro pasos:

1. **Identificación de riesgos.** Se identifican los posibles riesgos o amenazas para el sistema.
2. **Análisis de riesgos.** Se analizan los riesgos para determinar las circunstancias en que se puede producir (peligrosidad) y el impacto que puede tener sobre el sistema (vulnerabilidad).
3. **Toma de medidas.** Determinación de las medidas necesarias para protegerse del riesgo e implementación de las mismas.
4. **Evaluación de las medidas tomadas.** Determinar la eficacia de las medidas tomadas y si cumplen las expectativas. Si se determina que la eficacia es baja o son incluso contraproducentes, se debe considerar la retirada de las nuevas medidas.

Esto significa que sólo cuando seamos conscientes de los potenciales riesgos que existen contra nuestro sistema podemos tomar las medidas de protección adecuadas.

Es muy importante reseñar que a la hora de analizar los riesgos y las medidas siempre debe haber un balance entre el coste que tendría la ocurrencia de un peligro y el coste que tiene la medida o medidas destinadas a

prevenirlo o a paliarlo. Por ejemplo, no parece una medida de seguridad muy razonable comprar una caja fuerte de un millón de euros para proteger unas joyas que valen 500 euros. Entre los costes de las medidas también es importante tener en cuenta los costes a largo plazo (mantenimientos) de las medidas así como el impacto de las medidas en la usabilidad del sistema. Por ejemplo, una medida puede ser barata de implementar pero tener un coste mensual, el cual suma continuamente al coste de la misma y puede hacer subir mucho el coste de la misma a largo plazo. El otro problema es que si una medida es muy efectiva pero dificulta mucho el uso o aprovechamiento normal del sistema al final provoque más costes porque los usuarios abandonan el uso.

2.- Seguridad informática

La seguridad informática es la seguridad orientada a los sistemas informáticos y telecomunicaciones. Tiene los siguientes objetivos:

- **Fiabilidad.** El sistema debe funcionar correctamente y realizar las funciones para las que se ha diseñado. Dicho de otra manera, el sistema no debe cometer errores. Se considera un error que, aunque el sistema funcione, no haga lo que estaba previsto que hiciera. Por ejemplo, si un programa de cálculo de precios no aplica correctamente los descuentos, el programa no es fiable aunque aparentemente esté funcionando y no se caiga.
- **Confidencialidad.** Se debe asegurar que los usuarios sólo tienen acceso a los recursos a los que están autorizados a acceder y a ninguno más. En otras palabras un usuario sólo debe poder acceder a la información a la que está autorizado y a ninguna más. Si un usuario puede acceder a información para la que no está autorizado se puede decir que no se cumple la confidencialidad del sistema y ni que decir tiene si un extraño puede acceder a cualquier información no pública.
- **Integridad.** Los datos tienen que ser veraces y completos, esto es, no se deben poder falsear los datos ni eliminar datos que no deben perderse. Los datos siempre deben estar completos y reflejar la situación real. Si se pueden "trucar" los datos o eliminar datos a voluntad, el sistema no es integro. Esto debe ser verdad aunque los cambios en los datos los realicen usuarios autorizados.
- **Disponibilidad.** Cualquier usuario legítimo debe poder utilizar el sistema en el momento que lo necesite. Si un usuario no puede acceder en un momento determinado al sistema porque, por ejemplo, está apagado o en mantenimiento, la disponibilidad es baja.
- **Verificabilidad (No Repudio).** Cuando se realicen modificaciones a la información se debe conocer quien, cuando y qué información se ha modificado. Este objetivo persigue el conocer, si hay algún problema con los datos, quién ha sido responsable de las modificaciones que causaron el problema.

La definición formal define la seguridad informática o ciberseguridad como el área de la informática que se enfoca en la infraestructura informática y todo lo relacionado con ésta, especialmente la seguridad de los datos almacenados o que se comunican al exterior.

No debe confundirse la seguridad informática con la seguridad de la información. La seguridad de la información se encarga de asegurar la información esté en el soporte que esté, informático o no.

3.- Tipos de seguridad informática

Existen distintos clasificaciones de la seguridad informática, atendiendo al punto de vista que se tome. En esta sección describiremos algunas de ellas.

3.1.- Según el momento en que se actúa

Según el momento en que actúan se pueden distinguir entre medidas de seguridad activa o pasiva.

3.1.1.- Seguridad activa

Son medidas que intentan **prevenir** los problemas de forma que estos no lleguen a ocurrir. Entre las medidas más comunes de seguridad activa podemos encontrar:

- Utilizar contraseñas fuertes.
- Utilizar y tener actualizados sistemas anti-malware.
- Sistema operativo actualizado.
- Educación de los usuarios.
- Cortafuegos.
- Prohibición de los medios extraíbles.
- Configuración del sistema operativo.

3.1.2.- Seguridad Pasiva

La seguridad pasiva consiste en las medidas destinadas a reparar o minimizar los daños producidos por un ataque o un accidente. Estas medidas se aplican cuando el ataque o el accidente **ya se han producido** y van destinadas a reparar o paliar los efectos. Entre las medidas más utilizadas de seguridad pasiva podemos encontrar:

- Política de copia de seguridad.
- Sistemas redundantes.

3.2.- Según lo que se proteja

Según el recurso que proteja cada medida de seguridad, estas se pueden clasificar en medidas de seguridad física o lógica.

3.2.1.- Seguridad Física

La seguridad física consiste en el conjunto de medidas destinadas a asegurar la integridad física de los equipos y las comunicaciones que forman el sistema. Dicho de otro modo se ocupan de proteger los elementos tangibles

del sistema, tales como ordenadores, servidores, unidades de disco, cables de comunicaciones, routers, antenas de comunicaciones, etc.

Las principales amenazas que se pueden presentar, junto con las medidas destinadas a defenderse de ellas se resumen en la siguiente tabla:

Amenaza	Mecanismo de defensa
Incendios	• Utilizar sólo elementos ignífugos (que no arden por si mismos) en las habitaciones donde están colocados los equipos. • Alejar las zonas donde están los sistemas infomáticos de zonas donde se utilicen materiales inflamables. • Sistemas de detección y extinción de incendios: Detectores de humo, aspersores, extintores, etc. para sofocar el incendio lo antes posible evitar en lo posible los daños.
Inundaciones	• Evitar la instalación de equipos en los sótanos o plantas bajas. • Impermeabilización y sellado de las puertas.
Robos	• Medidas de seguridad antirrobo: ◦ Puertas con cerraduras seguras (PIN, identificación biométrica, tarjeta criptográfica, etc.) ◦ Cámaras de seguridad ◦ Sistemas de detección de presencia y de intrusión ◦ Personal de vigilancia
Señales Electromagnéticas	• Evitar la instalación de los centros informáticos cerca de fuentes potentes de señales electromagnéticas como estaciones de radio, radares, comisarías, industrias, etc. • Protecciones como apantallamiento del cableado y de los equipos, uso de cable de fibra óptica que es resistente a estas señales o incluso apantallado completo de las habitaciones o edificios.
Fallos en la red eléctrica	• Utilizar sistemas de alimentación ininterrumpida (SAIs) que almacenan energía y alimentan los equipos en caso de interrupción breve del suministro eléctrico. • En caso de fallos de mayor duración uso de sistemas de generación autónomos (generadores eléctricos). • Existen empresas que proporcionan generadores móviles (en camiones) y que pueden alimentar un edificio ininterrumpidamente el tiempo que sea necesario • Otro tipo de fallos son las sobrecargas o sobretensiones. En estos casos hay que utilizar filtros de alimentación que estabilizan la corriente eléctrica que entra desde la suministradora y proporciona una corriente estable a los equipos.

3.2.2.- Seguridad lógica

La seguridad lógica consiste en el conjunto de medidas destinadas a proteger a los datos que contiene un sistema informático o que circulan por el mismo. En otras palabras, se encargan de proteger la parte no tangible del sistema, en oposición a la seguridad física. Ciertamente es el aspecto más importante de la seguridad puesto que la información de la una organización es su activo más importante. Si se pierde información la actividad de la organización se resiente más que si se estropea o compromete un equipos. Por lo tanto la seguridad lógica es fundamental.

Las amenazas a las que se enfrenta la seguridad lógica y las medidas para enfrentarlas se pueden consultar en la siguiente tabla:

Amenaza(s)	Medida(s)
Modificaciones no autorizadas a los datos o programas	• Restringir el acceso mediante identificación de los usuarios (Contraseñas, sistemas biométricos, autentificación en dos pasos, etc.) • Limitar el acceso de cada usuario de forma que sólo pueda acceder a los datos y programas que estrictamente necesita para desarrollar sus actividad y a ninguno más. • Registros de modificaciones que anoten cada modificación, cuando se hizo y quién la hizo de forma que se puedan seguir las causas de los problemas cuando estos se produzcan.
Ataques a través de la red (Internet o la red interna de la organización)	• Cortafuegos para evitar accesos desde Internet. • Sistemas de monitorización de red y detección de intrusiones. • Registros de acceso. Registran los accesos desde la red.
Pérdidas de información	• Copias de seguridad. • Sistemas tolerantes a fallos. Son sistemas que permiten algún nivel de fallo en sus componentes, funcionando de forma degradada hasta que se consiga arreglar el componente fallido. • Discos redundantes. La información se mantiene en dos o más discos que son copias idénticas. Si uno de los discos falla se siguen utilizando los otros hasta que se sustituya el fallido.
Malware	• Sistemas de detección y neutralización de malware (los conocidos popularmente como antivirus)
Suplantación de identidad	• Sistemas de autentificación avanzados como sistemas biométricos o de 2 pasos.

4.- Amenazas y fraudes a la seguridad informática

En esta sección discutiremos las amenazas que puede sufrir un sistema de información. Este paso es fundamental para poder determinar las medidas a tomar y la eficacia de las mismas.

4.1.- Amenazas

Las amenazas que puede sufrir un sistema informático se pueden clasificar de varias formas. En esta sección examinaremos tres de ellas.

4.1.1.- Según el tipo de atacante

Según el tipo de atacante, las amenazas se pueden clasificar en:

- Hackers. Son expertos informáticos que investigan la seguridad de los sistemas pero sin ánimo de dañar u obtener beneficio económico.
- Crackers. Hackers maliciosos, esto es, que tienen intención de dañar u obtener un beneficio económico.

- Phreakers. Crackers especializados en las redes de telefonía.
- Sniffers. Expertos en analizar el tráfico de las redes para obtener información.
- Ciberterrorista. Hackers que trabajan para gobiernos u organizaciones como espías o saboteadores.
- Carders. Se dedican al ataque a los sistemas de pago, especialmente tarjetas de crédito o cajeros automáticos.

4.1.2.- Según el resultado del ataque

Según el resultado del ataque, se pueden clasificar en:

- Interrupción. Se dificultan gravemente o interrumpen uno o más servicios prestados por el sistema.
- Intercepción. Se intercepta la información en camino, normalmente en una red.
- Modificación. La información del sistema se modifica sin autorización, por lo que deja de ser válida o consistente.
- Fabricación. Se crea una construcción informática que suplanta a la original y que puede utilizarse para acceder a información confidencial de los usuarios.

4.1.3.- Según la forma de actuación del ataque

Según la forma en que se realice el ataque, estos se pueden clasificar en:

- Spoofing. Suplanta la identidad de un equipo en la red.
- Sniffing. Monitoriza el tráfico en la red y lo analiza para extraer información.
- Exploit. Se localiza un fallo de seguridad en algún programa del equipo y se explota para conseguir acceso no autorizados.
- Malware. Se introducen programas malintencionados (malware) en el equipo. Estos realizan tareas variadas, desde daños hasta captura y envío de información sobre el equipo o la red.
- Denegación de Servicio. Consiste en realizar peticiones a un servicio de forma masiva de forma que se sobrecargue y no pueda proporcionar servicio adecuado a los clientes legítimos. Se puede realizar por un sólo equipo o de forma coordinada entre varios. A estos últimos se les denomina ataques distribuidos de denegación de servicio.
- Ingeniería social. Utiliza engaños para obtener información confidencial de las personas y utilizarlas para fines maliciosos.
- Phising. Se engaña al usuario para que proporcione información confidencial suplantando un sitio legítimo de Internet. Se denomina phishing (algo así como pesca) porque se enganchan a los usuarios mediante mensajes de correo o redes sociales. De estos solo unos pocos “pican” y acceden al sitio falso.

5.- Malware

Se denomina malware (MALicious softWARE – Software o programa malicioso) a aquellos programas creados expresamente para realizar acciones no deseadas por el propietario del equipo donde se van a ejecutar, a diferencia del software "normal" que realiza tareas que el usuario desea ver realizadas en su equipo.

Según su forma de funcionar o transmitirse, el malware se puede dividir en muchos tipos:

- **Virus**. Programa que se instala sin permiso con el objetivo de hacer copias de si mismo e instalarse en más equipos. Además puede hacer otras operaciones como borrar archivos, consumir recursos, desactivar dispositivos, etc.
- **Troyano**. Es un programa que aparenta ser una aplicación útil. El usuario la instala voluntariamente y la utiliza por la funcionalidad que ofrece. Pero además realiza otras tareas que el usuario no conoce y que le perjudican como robar información, eliminar archivos, etc. Existen varios tipos de troyanos, según la labor que realicen:
  - **Keylogger**. Es un programa que se instala sin consentimiento del usuario y registra todas las pulsaciones de teclas que se realizan en el ordenador. Periódicamente envía la información recolectada a su creador.
  - **Backdoor**. Crea un servidor al que se puede conectar el creador del malware desde Internet y tomar el control del sistema para que realice las tareas que el pirata quiera realizar.
- **Adware**. Muestran publicidad no deseada por el usuario, habitualmente interrumpiendo su labor u ocupando áreas de la pantalla que no le corresponden.
- **Ransomware**. Estos programas realizan un "secuestro" de los datos. Para ello realizan un cifrado de los archivos. Si se quieren recuperar hay que pagar un rescate (ransom) para obtener la clave de descifrado. La mejor manera de prevenir este tipo de malware es disponer de una buena política de copias de seguridad.
- **Falsos antivirus**. Estas aplicaciones se hacen pasar por antivirus y engañan al usuario informando de la presencia de varios de ellos en el sistema y solicitando una cantidad para liberar al sistema de ellos.

6.- Resumen

En este tema hemos iniciado la descripción de la seguridad informática, las amenazas que enfrentan los sistemas informáticos actuales y los métodos que se utilizan para contrarrestar estas amenazas. El tópico de la seguridad es largo y extenso por lo que en este tema hemos intentado dar una descripción que es necesariamente somera.