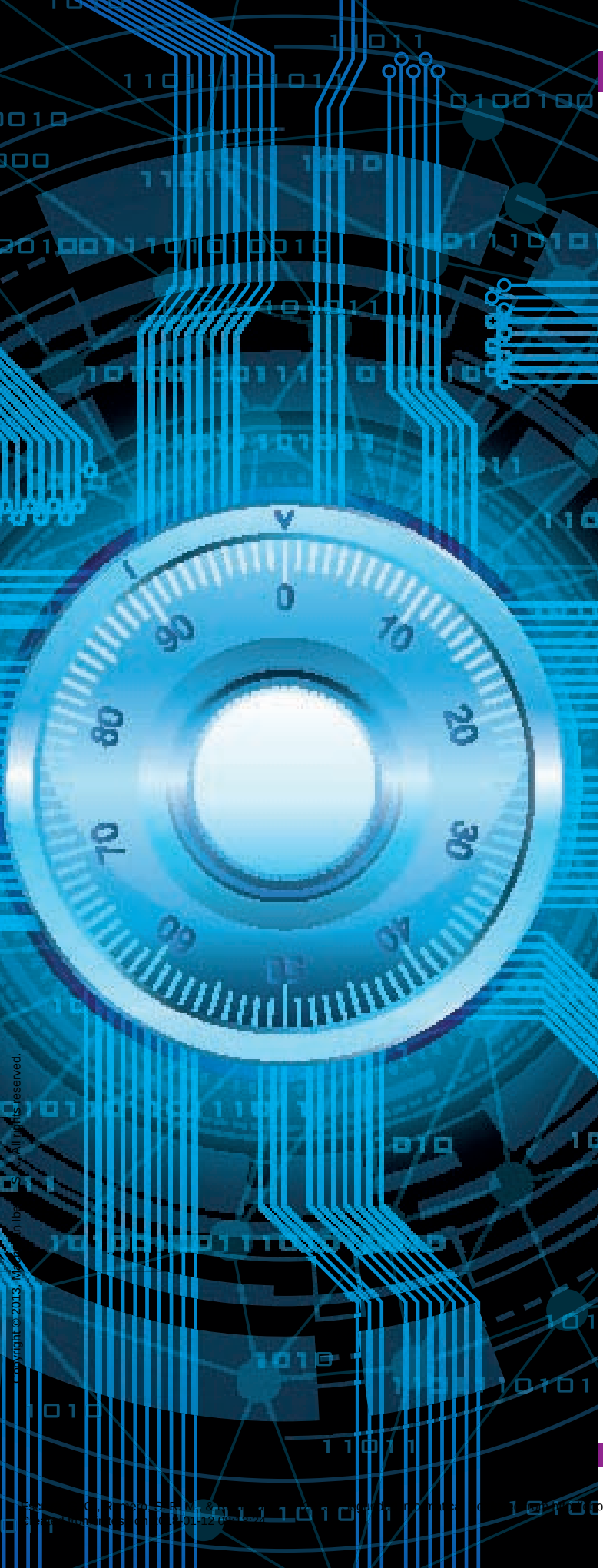


unidad 1

Introducción a la seguridad informática

SUMARIO

- Seguridad de la información y seguridad informática
- Conceptos básicos relacionados con la seguridad informática
- Principios básicos de la seguridad informática
- Políticas de seguridad
- Planes de contingencia

OBJETIVOS

- Conocer las diferencias entre seguridad de la información y seguridad informática.
- Aprender los conceptos básicos relacionados con el mundo de la seguridad informática.
- Describir cuáles son los principios básicos de la seguridad.
- Conocer qué son y qué utilidad tienen las políticas de seguridad.
- Aprender en qué consisten los planes de contingencia.

1 >> Seguridad informática y seguridad de la información

Uno de los activos más valiosos para cualquier empresa es la información que maneja. La información es el conjunto de datos que da sentido a una empresa, datos que la definen, datos con los que trabaja y datos que, en manos inadecuadas, pueden llevar a la misma a la ruina. Extendiendo este concepto de seguridad al mundo de las telecomunicaciones y la informática, puede entenderse desde dos puntos de vista: **seguridad de la información y seguridad informática.**

La **seguridad de la información** es el conjunto de medidas y procedimientos, tanto humanos como técnicos, que permiten proteger la integridad, confidencialidad y disponibilidad de la información:

- **Integridad:** certificando que tanto la información como sus métodos de proceso son exactos y completos.
- **Confidencialidad:** asegurando que únicamente pueden acceder a la información y modificarla los usuarios autorizados.
- **Disponibilidad:** permitiendo que la información esté disponible cuando los usuarios la necesiten.

Este término, por tanto, es un concepto amplio que engloba medidas de seguridad que afectan a la información independientemente del tipo de esta, soporte en el que se almacene, forma en que se transmita, etc.

La **seguridad informática,** por su parte, es una rama de la seguridad de la información que trata de proteger la información que utiliza una infraestructura informática y de telecomunicaciones para ser almacenada o transmitida. Podemos distinguir los siguientes tipos:

- En función de lo que se quiere proteger:
  - **Seguridad física:** se asocia a la protección física del sistema ante amenazas como inundaciones, incendios, robos, etc.
  - **Seguridad lógica:** mecanismos que protegen la parte lógica de un sistema informático (datos, aplicaciones y sistemas operativos). Uno de los medios más utilizados es la criptografía.
- En función del momento en que tiene lugar la protección:
  - **Seguridad activa:** se encarga de prevenir, detectar y evitar cualquier incidente en los sistemas informáticos antes de que se produzca (medidas preventivas). Por ejemplo, utilización de contraseñas.
  - **Seguridad pasiva:** comprende todas aquellas técnicas o procedimientos necesarios para minimizar las consecuencias de un incidente de seguridad (medidas correctoras). Por ejemplo, las copias de seguridad.

Normas ISO/IEC 27000

Para gestionar de forma adecuada la seguridad de la información se han desarrollado un conjunto de estándares que se han convertido en el marco para establecer, implantar, gestionar y mejorar un Sistema de Gestión de la Seguridad de la Información (SGSI). Son las normas ISO/IEC 27000, desarrolladas por ISO *(International Organization for Standarization)* e IEC *(International Electrotechnical Commission)*.

Web

http://pwnies.com: página web de los premios Pwnies, distinción que reconoce lo mejor y lo peor de la seguridad informática durante el último año.

Actividades propuestas

1·· Debate con tus compañeros de clase: ¿a qué crees que se deben la mayoría de los fallos de seguridad?

2·· Realiza una tabla comparando ejemplos de seguridad pasiva y activa del campo de la informática y del campo de los vehículos.

2 >> Conceptos básicos en materia de seguridad

En el mundo de la seguridad de la información e informática, es habitual manejar una terminología específica (activos, vulnerabilidades, amenazas, ataques, riesgos, impacto, desastre, contingencias, etc.) que explicaremos a lo largo de este epígrafe.

2.1 > Activos

Un activo se define como aquel recurso del sistema (informático o no) necesario para que la organización alcance los objetivos propuestos; es decir, todo aquello que tenga valor y que deba ser protegido frente a un eventual percance, ya sea intencionado o no. Según esta definición, consideraremos como activos: los trabajadores, el software, los datos, los archivos, el hardware, las comunicaciones, etc.

La seguridad informática tiene como objetivo proteger dichos activos, por lo que la primera labor será identificarlos para establecer los mecanismos necesarios para su protección y analizar la relevancia de los mismos en el proceso de negocio de la organización. No tiene sentido gastar miles de euros en proteger activos no importantes para el negocio o que no tengan un valor que justifique ese gasto.

Desde el punto de vista de la informática, los principales activos de una empresa son los siguientes:

- **Información:** todo aquel elemento que contenga datos almacenados en cualquier tipo de soporte. Como por ejemplo, documentos, libros, patentes, correspondencia, estudios de mercado, datos de los empleados, manuales de usuario, etc.
- **Software:** programas o aplicaciones que utiliza la organización para su buen funcionamiento o para automatizar los procesos de su negocio. Entre estos se pueden encontrar las aplicaciones comerciales, los sistemas operativos, etc.
- **Físicos:** toda la infraestructura tecnológica utilizada para almacenar, procesar, gestionar o transmitir toda la información necesaria para el buen funcionamiento de la organización. También estaría incluida en esta categoría la estructura física de la organización, tal como la sala de servidores, los armarios, etc.
- **Personal de la organización** que utilice la estructura tecnológica y de comunicación para el manejo de la información.

2.2 > Vulnerabilidades

En el campo de la seguridad informática se considera como vulnerabilidad a cualquier debilidad de un activo que pueda repercutir de alguna forma sobre el correcto funcionamiento del sistema informático. Estas debilidades, también conocidas como “agujeros de seguridad”, pueden estar asociadas a fallos en la implementación de las aplicaciones o en la configuración del sistema operativo, a descuidos en la utilización de los sistemas, etc. Por ejemplo, no utilizar ningún tipo de protección frente a fallos eléctricos o carecer de mecanismos de protección frente a ataques informáticos, como antivirus o cortafuegos.

MAGERIT v. 3

MAGERIT es la metodología de análisis y gestión de riesgos desarrollada por el Consejo Superior de Administración Electrónica. Es un método formal adoptado por las Administraciones Públicas para investigar los riesgos que soportan los sistemas de información y recomendar las medidas adecuadas que deberán adoptarse para poder controlar dichos riesgos.

Es muy importante corregir cualquier vulnerabilidad detectada o descubierta, porque constituye un peligro potencial para la estabilidad y seguridad del sistema en general.

Las vulnerabilidades de algunas aplicaciones pueden permitir una escalada de privilegios, con lo que un atacante podría conseguir más privilegios de los previstos. Esto podría implicar que en algunos casos llegaran a tener los mismos que los administradores, pudiendo controlar el sistema. Un ejemplo sería cuando una vulnerabilidad produce un fallo en un servidor web que permite que un atacante acabe accediendo al sistema como si se tratara de un administrador, con lo que podría realizar acciones reservadas a estos.

Para minimizarlas, los administradores de los sistemas informáticos deben actualizar periódicamente el sistema operativo y las aplicaciones y mantenerse actualizados en temas relacionados con la seguridad informática. Para ello pueden visitar páginas web especializadas en materia de seguridad informática, como los equipos de respuesta a incidentes de seguridad de la información (CERT o CSIRT) o páginas web de seguridad, como www.hispasec.com, etc.

2.3 > Amenazas

Una amenaza es cualquier entidad o circunstancia que atente contra el buen funcionamiento de un sistema informático. Aunque hay amenazas que afectan a los sistemas de forma involuntaria, como, por ejemplo, un desastre natural, en la mayoría de casos es necesaria una intención de producir daño.

Las amenazas se suelen dividir en pasivas y activas, en función de las acciones realizadas por parte del atacante:

- **Amenazas pasivas**, también conocidas como "escuchas". Su objetivo es obtener información relativa a una comunicación. Por ejemplo, los equipos informáticos portátiles que utilizan programas especializados para monitorizar el tráfico de una red WiFi.
- **Amenazas activas**, que tratan de realizar algún cambio no autorizado en el estado del sistema, por lo que son más peligrosas que las anteriores. Como ejemplos se encuentran la inserción de mensajes ilegítimos, la usurpación de identidad, etc.

Otra posible clasificación, en función de su ámbito de acción, sería diferenciar entre amenazas sobre la seguridad física, lógica, las comunicaciones o los usuarios de la organización.

MAGERIT presenta la siguiente clasificación de amenazas:

Grupos de amenazas	Ejemplos
Desastres naturales	Fuego, daños por agua, desastres naturales.
Desastres industriales	Fuego, daños por agua, desastres industriales, contaminación mecánica, contaminación electromagnética, etc.
Errores y fallos no intencionados	Errores de usuarios, errores de configuración, etc.
Ataques deliberados	Manipulación de la configuración, suplantación de la identidad del usuario, Difusión de software dañino, etc.

2.4 > Ataques

Un ataque es una acción que trata de aprovechar una vulnerabilidad de un sistema informático para provocar un impacto sobre él e incluso tomar el control del mismo. Se trata de acciones tanto intencionadas como fortuitas que pueden llegar a poner en riesgo un sistema. De hecho, en alguna metodología como MAGERIT se distingue entre ataques (acciones intencionadas) y errores (acciones fortuitas).

Como ejemplos de ataques, que desarrollaremos a lo largo de este libro, podemos citar la utilización de programas para conseguir acceso al servidor de forma ilegítima o la realización de ataques de denegación de servicio para colapsar el servidor.

Normalmente un ataque informático pasa por las siguientes fases:

- **Reconocimiento.** Consiste en obtener toda la información necesaria de la víctima, que puede ser una persona o una organización.
- **Exploración.** Se trata de conseguir información sobre el sistema a atacar, como por ejemplo, direcciones IP, nombres de *host,* datos de autenticación, etc.
- **Obtención de acceso.** A partir de la información descubierta en la fase anterior, se intenta explotar alguna vulnerabilidad detectada en la víctima para llevar a cabo el ataque.
- **Mantener el acceso.** Después de acceder al sistema, se buscará la forma de implantar herramientas que permitan el acceso de nuevo al sistema en futuras ocasiones.
- **Borrar las huellas.** Finalmente, se intentarán borrar las huellas que se hayan podido dejar durante la intrusión para evitar ser detectado.

En el mercado existen una gran variedad de herramientas de seguridad que permiten conseguir un nivel óptimo de seguridad, pero hay estrategias de ataque que hacen ineficaces a estas herramientas, como las orientadas a explotar las debilidades del factor humano.

Es el caso de la **ingeniería social**, que consiste en la obtención de información confidencial y/o sensible de un usuario mediante métodos que son propios de la condición humana. El ataque más simple sería el de engañar al usuario haciéndose pasar por el administrador del sistema de su organización para obtener alguna información de relevancia.

Ejemplos

Ataque de ingeniería social

Un usuario malicioso haciéndose pasar por el administrador de la organización envía un correo electrónico a los usuarios para obtener información, en este caso la contraseña, de manera fraudulenta.

```
From: Administrador <admin@organizacion.com>

To: Usuario <user@organizacion.com>

Se está llevando a cabo un mantenimiento del sistema con el objetivo de
conseguir un óptimo funcionamiento. Para poder conseguirlo, es necesario
que se cambie la contraseña, para ello pinche en el siguiente enlace.

http://mantenimiento.organizacion.com

Gracias por su colaboración,
```

Casos prácticos 1

Análisis de vulnerabilidades, ataques y amenazas a un sistema

•• Lee el siguiente artículo y responde a las preguntas que se hacen a continuación del mismo.

> La compañía de seguridad para Internet BitDefender ha localizado un nuevo fraude en la red social Facebook que utiliza para propagarse el etiquetado en las fotos que permite dicha red social.
>
> El método utilizado es el siguiente: un usuario es etiquetado en una foto de una chica joven y vestida de manera provocativa. Junto a esa foto, se incluye un mensaje que dice: "Descubre quiénes son tus principales seguidores", junto con un *link* para utilizar una aplicación que permitiría conocer esa información.
>
> Si el usuario pincha en el *link*, será redirigido a una aplicación que, por un lado, le pedirá su nombre de usuario y contraseña y, por otro, le pedirá permisos para publicar mensajes en su muro y para acceder a su lista de contactos en Facebook. Una vez haya introducido los datos y dado permiso a la aplicación, esta mostrará un mensaje de error, señalando que no está disponible en ese momento.
>
> Sin embargo, inmediatamente, comenzarán a publicarse nuevas fotos en la galería del usuario en la que serán etiquetados todos sus amigos. Además, en el muro de estos aparecerá que alguien les ha etiquetado en esa foto, junto con el comentario inicial ("Descubre quiénes son tus principales seguidores") más el *link* que conduce a la aplicación falsa.
>
> En el momento en que uno de esos amigos pinche en el *link* e instale la aplicación creyendo que su amigo ya la ha aprobado y que se la está recomendando, el proceso volverá a comenzar. De esta manera, la aplicación consigue un efecto viral, propagándose por la red social.
>
> Fuente: Europa Press. Madrid. 13/04/11

a) ¿De qué tipo de ataque se trata?
b) Analiza las vulnerabilidades y amenazas a ese sistema.
c) ¿Qué recomendaciones darías para evitar esta situación?

Solución ••

a) Se trata de un ataque basado en ingeniería social, realizado con la finalidad de conseguir los datos del usuario para propagarse.
b) La **vulnerabilidad** es el elemento personal, encarnado por la confianza del usuario en los contenidos recibidos, que le lleva a conceder privilegios totales al atacante. La **amenaza** existente es un tipo de amenaza pasiva, consistente en suplantar la identidad del usuario para permitir al atacante conseguir sus fines.
c) Se recomienda desconfiar tanto de las fotos como de los mensajes de este tipo, que pretenden llamar la atención ante situaciones curiosas. Al mismo tiempo, se debe desconfiar de las aplicaciones que supuestamente realizan acciones que en realidad no pueden llevarse a cabo, como por ejemplo saber cuántas veces han visitado tu perfil.

Actividades propuestas

3•• ¿Cuál es el activo más valioso para una empresa?

a) ¿Qué vulnerabilidades podrían afectarle?
b) ¿Qué amenazas son las que podrían afectarle? Clasifícalas.

2.5 > Riesgos

Existen diversas definiciones para definir el término riesgo; entre todas ellas destacamos las siguientes:

- Según la UNE-71504:2008, un riesgo es la estimación del grado de exposición a que una amenaza se materialice sobre uno o más activos causando daños o perjuicios a la organización.
- El Centro Criptológico Nacional define el riesgo como la probabilidad de que una amenaza se materialice aprovechando una vulnerabilidad y causando daño (impacto) en un proceso o sistema.

El riesgo es, por tanto, una medida de la probabilidad de que se materialice una amenaza. Por ejemplo, si la instalación eléctrica del edificio es antigua, existirá un riesgo elevado de sufrir una interrupción del servicio en caso de producirse una subida de tensión.

El coste asociado a la reducción de esa cifra aumenta de manera exponencial frente a la necesidad de minimizar el riesgo, por lo que se debe tratar de obtener un factor coste/riesgo que sea asumible por la organización. Ningún sistema de seguridad debería tener un coste superior al del sistema en conjunto o al de la información que protege.

Para poder establecer unos procedimientos de seguridad adecuados, será necesario realizar una clasificación de los datos y un análisis de riegos, con el fin de establecer prioridades y realizar una administración más eficiente de los recursos de la organización.

En el **análisis de riesgos** hay que tener en cuenta qué activos hay que proteger, sus vulnerabilidades y amenazas, así como la probabilidad de que estas se produzcan junto con el impacto de las mismas. Además, habrá que tener también en cuenta durante cuánto tiempo y qué esfuerzo y dinero se está dispuesto a invertir.

Los resultados del análisis de riesgos permiten recomendar qué medidas se deberán tomar para conocer, prevenir, impedir, reducir o controlar los riesgos previamente identificados y así poder reducir al mínimo su potencialidad o sus posibles daños.

Existen diferentes niveles de riesgo a los que puede estar expuesto un activo. El nivel dependerá de la probabilidad de que se materialice una amenaza y al grado de impacto producido. Por ejemplo:

Nivel	Tipo de riesgo
Alto	Robo de información Robo de hardware
Medio	Accesos no autorizados
Muy bajo	Inundaciones

Hay que tener en cuenta que el riesgo cero no existe, ya que no es posible prever y evitar todas las posibles situaciones que podrían afectar a nuestros sistemas.

PILAR

Es una aplicación implementada por la metodología MAGERIT, para el análisis y gestión de riesgos de un sistema de información. Ha sido desarrollada por el Centro Criptológico Nacional (CCN) y es de amplia utilización en la Administración Pública española.

2.6 > Impacto

Una organización se ve afectada cuando se produce una situación que atenta contra su funcionamiento normal; estas consecuencias para la empresa reciben el nombre de impacto. Dicho de otra forma, el impacto sería el alcance producido o daño causado en caso de que una amenaza se materialice.

Dos organizaciones pueden verse afectadas en diferente medida ante la materialización de la misma amenaza si han adoptado estrategias diferentes para solucionarla. Así, el impacto del borrado del disco duro ocasionado por un virus informático será muy escaso en una empresa que realiza periódicamente copias de seguridad de la información importante, pero será bastante grave en una empresa que no lleva a cabo copias de seguridad regularmente.

Un impacto leve no afecta prácticamente al funcionamiento de la empresa y se produce en organizaciones que han identificado las amenazas y han establecido las pautas a seguir en el caso de que se materialicen. Por otro lado, un impacto grave afecta seriamente a la empresa pudiendo ocasionar su quiebra y se produce en organizaciones que no han considerado las consecuencias que supone para ellas la materialización de esa amenaza.

Las empresas deben, por tanto, identificar los impactos para la organización en el caso de que las posibles amenazas se produzcan. Esta tarea es uno de los objetivos del análisis de riesgos que debe realizar toda organización.

2.7 > Desastres

Según ISO 27001, un desastre es cualquier evento accidental, natural o malintencionado que interrumpe las operaciones o servicios habituales de una organización. Por ejemplo, la caída de un servidor como consecuencia de una subida de tensión o un ataque.

Un evento de este tipo puede destruir los activos de la empresa. Tradicionalmente se planteaba únicamente la destrucción de recursos físicos, como sillas, edificios, etc. pero hoy día las organizaciones se enfrentan a una nueva forma de desastre que afecta a los recursos lógicos, que constituye uno de sus principales activos: la información. Un desastre de este tipo podría ocasionar grandes pérdidas e incluso el cese de la actividad económica.

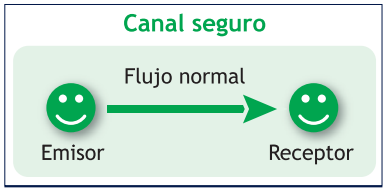
Las organizaciones deben estar preparadas ante cualquier tipo de desastre de manera que se reduzca el impacto que pueda ocasionar. Para ello, desarrollan e implantan planes de contingencia que permiten la prevención y recuperación de desastres informáticos.

Actividades propuestas

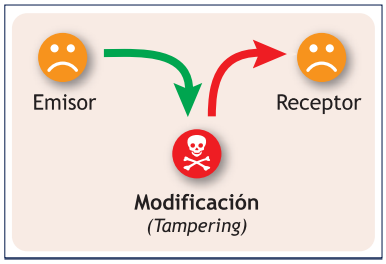
4·· ¿Crees que la evaluación de riesgos será igual para todas las empresas? ¿Por qué?

5·· Enumera posibles preguntas que podrían hacerse en la realización de una evaluación de riesgos.

6·· Busca en Internet aplicaciones comerciales que permitan realizar una evaluación de riesgos.



1.1. Flujo normal de la información.

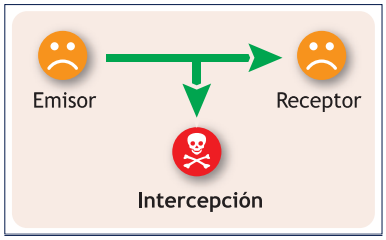


1.2. Violación de la integridad.

Sniffers

Sniffer es una palabra inglesa que significa "husmeo".

Un *sniffer* es un tipo de herramienta utilizada por atacantes para capturar información que circula por la red y no ha sido enviada para ellos. También se denomina así a los usuarios que husmean la información transmitida en una red.



1.3. Violación de la confidencialidad.

3 >> Principios de seguridad informática

Aunque la mayoría de expertos coinciden en que no existe ningún sistema totalmente seguro e infalible al 100%, se debe tratar de proteger la información y el sistema que la utiliza para ofrecer un nivel de seguridad razonable a los usuarios.

Para que un sistema se pueda considerar razonablemente seguro se debe garantizar que se cumplen los principios básicos de la seguridad informática: integridad, confidencialidad y disponibilidad.

3.1 > Integridad

La integridad es un principio básico de la seguridad informática que consiste en garantizar que la información solo pueda ser alterada por las personas autorizadas o usuarios legítimos, independientemente de si esa modificación se produce de forma intencionada o no. Así, por ejemplo, no se viola la integridad cuando usuarios autorizados modifican un registro de una base de datos o cuando un usuario que trabaja con la base de datos borra un registro que no debería por error.

La vulneración de la integridad tiene distinto significado según se produzca en un equipo o en una red de comunicaciones:

- **Equipo de trabajo.** Se produce violación de la integridad cuando un usuario no legítimo modifica información del sistema sin tener autorización para ello.
- **Red de comunicaciones.** Existe violación de la integridad cuando un atacante actúa como intermediario en una comunicación, recibe los datos enviados por un usuario, los modifica y se los envía al receptor (ataques *man-in-the-middle*). Un mecanismo que nos protege frente a este tipo de ataques es la firma electrónica, que se estudiará con más detalle en unidades posteriores.

3.2 > Confidencialidad

La confidencialidad es otro de los principios básicos de la seguridad informática que garantiza que la información solo es accesible e interpretada por personas o sistemas autorizados.

La vulneración de la confidencialidad también afecta de forma diferente a equipos y redes:

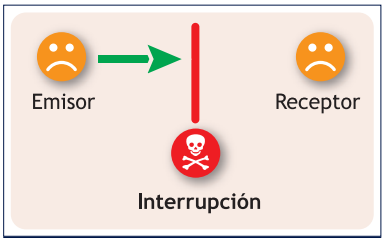
- **Equipo de trabajo.** Se produce una violación de la confidencialidad cuando un atacante consigue acceso a un equipo sin autorización, controlando sus recursos. Un ejemplo sería la obtención de las claves de acceso. Otro ejemplo, mucho más simple, se produce cuando un usuario abandona momentáneamente su puesto de trabajo, dejando su equipo sin bloquear y con información mostrándose en la pantalla.
- **Red de comunicaciones.** Se vulnera la confidencialidad de una red cuando un atacante accede a los mensajes que circulan por ella sin tener autorización para ello. Existen mecanismos que permiten protegerse frente este tipo de ataques, como el cifrado de la información o el uso de protocolos de comunicación.

3.3 > Disponibilidad

El tercer pilar básico de un sistema seguro es la disponibilidad, esto es, asegurar que la información es accesible en el momento adecuado para los usuarios legítimos.

La violación de la disponibilidad también se da de forma distinta en equipos y redes:

– **Equipos informáticos.** Se vulnera la disponibilidad de un equipo cuando los usuarios que tienen acceso a él no pueden utilizarlo. Por ejemplo, podría ser un virus que ha paralizado el sistema.
– **Redes de comunicaciones.** Se produce un ataque contra la disponibilidad cuando se consigue que un recurso deje de estar disponible para otros usuarios que acceden a él a través de la red. Existen una gran variedad de ataques que atentan contra la disponibilidad de un recurso en una red, como los ataques de denegación de servicio. Estos ataques, así como las técnicas que podemos utilizar para proteger las redes, se estudiarán en la unidad dedicada a la seguridad en redes.

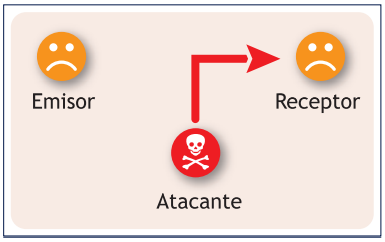


1.4. Violación de la disponibilidad.

3.4 > Otras características deseables en un sistema seguro

Además de los principios básicos que acabamos de ver, existen otros principios de seguridad que se consideran como deseables en todo sistema informático. Estos principios son los siguientes:

– **No repudio.** Este principio consiste en probar la participación de ambas partes en una comunicación. Por ejemplo, cuando se entrega la declaración de la renta telemáticamente, se firma con un certificado digital que solo puede poseer la persona que la presenta. La firma digital es una prueba irrefutable, de forma que impide que el ciudadano pueda negar o repudiar el trámite realizado. Este principio está estandarizado en la ISO-7498-2. Existen dos clases:
  • **No repudio de origen:** protege al destinatario del envío, ya que este recibe una prueba de que el emisor es quien dice ser.
  • **No repudio de destino:** protege al emisor del envío, ya que el destinatario no puede negar haber recibido el mensaje del emisor.
– **Autenticación.** Permite comprobar la identidad de los participantes en una comunicación y garantizar que son quienes dicen ser. Esta característica asegura el origen de la información. Existen ataques que atentan contra este principio, como la suplantación de la identidad o los de robos de contraseñas.



1.5. Violación de la autenticación.

Actividades propuestas

7·· A partir de los principios expresados en este epígrafe:

a) Plantea un posible ataque contra cada uno de estos principios.
b) Indica una posible solución para cada uno de los ataques planteados.

8·· Busca más información sobre los *sniffers* en Internet. ¿Qué son? ¿Qué utilidad tienen?

4 >> Políticas de seguridad

La RFC 1244 define la política de seguridad como:

> **Una declaración de intenciones de alto nivel que cubre la seguridad de los sistemas informáticos y que proporciona las bases para definir y delimitar responsabilidades para las diversas actuaciones técnicas y organizativas que se requieran.**

En otras palabras, las políticas de seguridad informática detallan una serie de normas y protocolos a seguir donde se definen las medidas a tomar para la protección de la seguridad del sistema, así como la definición de los mecanismos para controlar su correcto funcionamiento.

Tienen como objetivo concienciar a los miembros de una organización sobre la importancia y sensibilidad de la información y servicios críticos. Se puede decir que son una descripción de todo aquello que se quiere proteger.

Las políticas de seguridad deben cubrir aspectos relacionados con la protección física, lógica, humana y de comunicación, tener en cuenta todos los componentes de la organización y no dejar de lado el entorno del sistema.

¿Qué aspectos se deben tener en cuenta a la hora de elaborar las políticas de seguridad?

- Elaborar las reglas y procedimientos para los servicios críticos.
- Definir las acciones que habrá que ejecutar y el personal que deberá estar involucrado.
- Sensibilizar al personal del departamento encargado de la administración del sistema informático de los posibles problemas relacionados con la seguridad que pueden producirse.
- Establecer una clasificación de los activos a proteger en función de su nivel de criticidad, de forma que los sistemas vitales sean los más protegidos y no se gasten recursos en proteger aquellos activos con menor importancia.

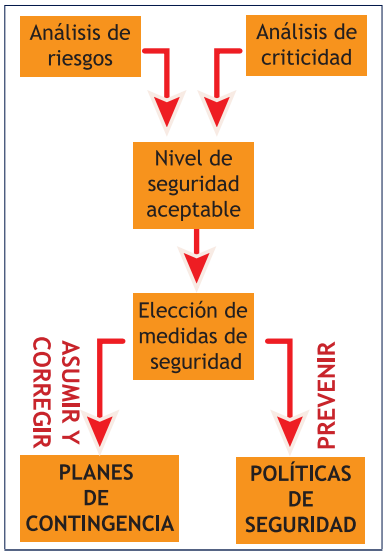
Las medidas de control deben ser efectivas, fáciles de usar, actualizadas periódicamente y, por supuesto, apropiadas a la situación. No hay que olvidar que deben funcionar en el momento adecuado.

Numerosas organizaciones internacionales han desarrollado documentos, directrices y recomendaciones con información relacionada con el uso adecuado de las nuevas tecnologías para sacarle el máximo provecho y evitar el uso inadecuado de las mismas.

RFC

Son las siglas de *Request For Comments* (petición de comentarios). Son unas notas emitidas por una organización de normalización (la IETF, *Internet Engineering Task Force*), con la intención de establecer estándares en Internet.

Cada RFC tiene un título y un número asignado.



1.6. Control de riesgos.

Actividades propuestas

9·· ¿Crees que establecer normas a los usuarios de una organización para que tengan una contraseña de acceso segura es una buena política de seguridad?

10·· Indica qué políticas de seguridad establecerías para evitar la caída de los servidores de la organización.