SAD - U1 Seguridad Física

Descargar estos apuntes

Índice

1. Importancia de la seguridad física

Desgraciadamente todos los días nos llegan noticias sobre sustracción de bienes materiales: dinero, joyas, etc. Una vez producido el delito, se puede intentar detener al culpable y recuperar los bienes robados; pero es mucho más útil e importante tomar medidas para que estos hechos no se produzcan instalando sistemas de seguridad preventivos: alarmas, rejas en ventanas, puertas de seguridad, etc. Del mismo modo, habitualmente se producen situaciones catastróficas ocasionadas por causas naturales como inundaciones, incendios, etc. Estas situaciones no pueden evitarse, pero sí disminuir sus consecuencias para las personas o bienes, mediante la adopción de medidas preventivas.

Si todas estas situaciones son desagradables en un entorno personal, en el ámbito de la empresa revisten especial gravedad, puesto que afectan a su patrimonio, necesario para llevar a cabo su actividad. En primer término se puede pensar que este patrimonio está integrado por los bienes tangibles de la empresa (mobiliario, ordenadores, etc.), pero aún más importantes que estos son los bienes intangibles (los datos). En efecto, una pérdida de un equipo físico puede ser reemplazada fácilmente; en cambio, es muy posible que la pérdida de los datos de la empresa sea irreemplazable. Además, hay que tener en cuenta que esos datos pueden ser utilizados por otras personas con fines ilícitos (para estafar a la empresa, para averiguar sus secretos industriales, etc.).

Es por ello que la seguridad física adquiere una importancia vital a la hora de preservar tanto los datos que poseen las empresas, como los equipos y dispositivos encargados de su tratamiento y almacenamiento. Podemos, por tanto, definir la seguridad física como:

> El conjunto de medidas de prevención y detección destinadas a evitar los daños físicos a los sistemas informáticos y proteger los datos almacenados en ellos.

Los riesgos externos a los que están sujetos los sistemas informáticos y las medidas preventivas que se pueden adoptar son los siguientes:

- Fenómenos naturales, como inundaciones, tormentas, terremotos, etc.
  Se pueden adoptar medidas preventivas como la instalación de los equipos en ubicaciones adecuadas dotadas de las oportunas medidas de protección (ubicaciones seguras, pararrayos, etc.).

- Riesgos humanos, como actos involuntarios, actos vandálicos y sabotajes.
  Entre las medidas preventivas estarían: control de acceso a recintos, elaboración de perfiles psicológicos de empleados con acceso a datos confidenciales, formación a usuarios en materia de seguridad, etc.

Riesgos

Actividad U1.1: Indica varios ejemplos de fenómenos naturales y de riesgos humanos que pueden poner en peligro la seguridad física de los equipos informáticos de tu aula.
Indica, respecto a cada uno, si puede evitarse o no y, en su caso, cómo podría evitarse.

2. Protección física de los equipos

En este epígrafe nos ocuparemos de las medidas de protección para los sistemas informáticos, centrándonos en los equipos de usuario. Dejaremos el estudio de la protección de los servidores para el siguiente apartado, ya que suelen estar situados en salas especiales y cuentan con medidas de protección especiales.

2.1. Entorno físico del equipo

Uno de los elementos más importantes a la hora de fijar las medidas preventivas para la seguridad física de los equipos informáticos es el lugar donde estos están situados. Las condiciones físicas de esta ubicación determinan los riesgos a que están sujetos los equipos. Así:

Factor de riesgo	Medidas preventivas
Espacio	Los ordenadores deben tener una buena ventilación; por ello, se debe procurar que exista espacio suficiente alrededor de la carcasa para permitir la correcta circulación del aire caliente proveniente de su interior. Igualmente, se debe evitar colocar objetos sobre la carcasa para no obstruir las salidas de ventilación.
Humedad	La humedad relativa aconsejable es del 50% aproximadamente: una humedad excesiva provoca corrosión en los componentes. Una humedad muy escasa (por debajo del 30%) favorece la existencia de electricidad estática. Por ello, hay que tener cuidado con la calefacción y con el aire acondicionado, pues secan mucho el ambiente.
Luz solar	La luz solar directa debe ser evitada pues puede producir un sobrecalentamiento del equipo. Para evitar la incidencia de los rayos solares sobre el equipo, pueden instalarse persianas y cortinas o cambiar la ubicación del mismo.
Temperatura ambiente	Los ordenadores están formados por componentes electrónicos y magnéticos sensibles a la temperatura. La temperatura ideal para los equipos informáticos se sitúa entre 15 y 25 ºC. Si la temperatura ambiente no está dentro del rango óptimo, es aconsejable la instalación de un aparato de refrigeración o climatización.
Partículas de polvo	El polvo y la suciedad afectan al buen funcionamiento del equipo informático. Por ejemplo, pueden disminuir la refrigeración de los componentes debido a la obstrucción de los ventiladores, etc. Por ello, los equipos deben situarse en zonas de mínimo impacto de partículas adversas y, periódicamente, se debe llevar a cabo una limpieza general del equipo.

Factor de riesgo	Medidas preventivas
Campos magnéticos	Los imanes y electroimanes alteran los campos magnéticos y pueden provocar la pérdida de datos en dispositivos de almacenamiento como el disco duro. Algunos de los dispositivos susceptibles de causar averías de este tipo son: destornilladores imantados, altavoces, motores eléct ricos, etc.
Vibraciones y golpes	Pueden provocar averías en el equipo informático, sobre todo en los discos duros. Por ello, se debe colocar el equipo lejos de aparatos que produzcan vibraciones y en lugares resguardados que no sean de paso, fijar bien los componentes y utilizar carcasas de alta calidad.
Suelos	Determinados tipos de suelo (como los laminados), debido a su mala conductividad eléctrica, acumulan electricidad estática. Por ello, se debe poner especial cuidado respecto a la superficie donde se ubica el ordenador. Si se usan alfombras, debe cuidarse de que sean antiestáticas.

2.2. Instalaciones

Además de las condiciones ambientales, hay otras circunstancias derivadas de la ubicación de los equipos y de su propio funcionamiento que pueden ocasionar riesgos para los mismos:

- **Instalación eléctrica adecuada**: los equipos informáticos funcionan gracias a la energía eléctrica que les llega a través de sus conexiones. Una instalación eléctrica defectuosa es susceptible de causar graves daños. Se pueden adoptar las siguientes medidas preventivas:
  - *Protecciones eléctricas adecuadas*. Los enchufes deben contar con tomas de tierra y la corriente suministrada debe ser lo más estable posible para evitar picos de tensión.
  - *Mantenimiento del suministro eléctrico*. La corriente eléctrica está sometida a anomalías, como apagones, caídas de tensión, etc. Hay que tomar las medidas necesarias para minimizar el riesgo de estas anomalías, así como para disminuir sus consecuencias negativas. Para prevenir las averías que estas anomalías pudieran producir a los equipos
    informáticos se desarrollaron los sistemas de alimentación ininterrumpida (SAI). Un SAI es un dispositivo que tiene por finalidad proporcionar alimentación a los equipos conectados a él cuando se produce un corte en la corriente eléctrica, dando tiempo a que los equipos se apaguen de forma adecuada y no se produzca ninguna pérdida de información.
- **Instalación de red adecuada**. Los equipos estarán conectados a una red de datos y esta a su vez a una red general. En primer término, hay que proteger esta red de accesos físicos no deseados. Además, normalmente la red está configurada por cable, por lo que habrá que vigilar que el tipo de cable es el correcto, así como que su estado de conservación es el adecuado al entorno (los cables pueden estar expuestos a la humedad, afectados por radiaciones electromagnéticas, etc.).
- **Control de acceso**. Tanto si el ordenador está en una oficina, como si está en una sala especialmente destinada a su uso, habrá que controlar el acceso a ese lugar. Además, deberá asegurarse la entrada en el equipo en sí mediante el establecimiento de claves.
- **Protección frente a incendios**. Se deben utilizar tanto sistemas de prevención como sistemas de protección:
  - *Sistemas de prevención*: son los más eficaces, pues van encaminados a que no se produzca el incendio. Por ejemplo, instalación de detectores de humo y alarmas, mantenimiento del orden y la limpieza para evitar la acumulación de materiales combustibles, etc.
  - *Sistemas de protección*: son los que se ponen en marcha en caso de que se haya producido un incendio. Los más comunes son la colocación de barreras para aislar el incendio, la delimitación clara de las vías de evacuación y salidas de emergencia y la instalación de sistemas de extinción. En el caso de los incendios que se pueden producir en una oficina con equipos informáticos, los extintores apropiados son los de clase C (o ABC), de polvo

seco polivalente o CO_2. Nunca se debe intentar apagar uno de estos incendios con agua a chorro debido al riesgo de sufrir una descarga eléctrica.

Agua nebulizada como agente extintor

Si bien en los incendios de líquidos inflamables, equipos eléctricos y electrónicos el uso del agua a chorro está totalmente contraindicado, en los últimos tiempos se está extendiendo el empleo del agua nebulizada como agente extintor válido para este tipo de incendios.

Como veremos en el epígrafe dedicado a los CPD, en caso de incendio de componentes electrónicos, este sistema es muy recomendable, pues no solo extingue el fuego, sino que combate uno de los mayores enemigos de los sistemas electrónicos, como es el humo.

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.

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, grupos de Telegram, 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.

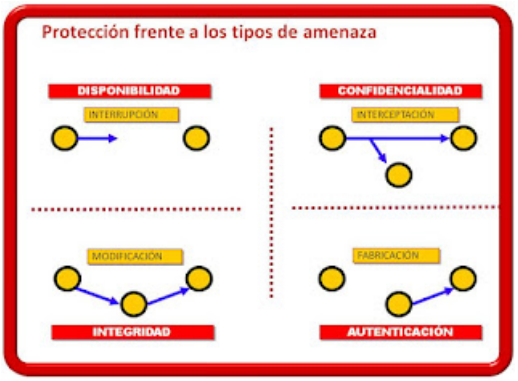
MAGERIT presenta la siguiente clasificación de amenazas:

Grupo 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 del curso, 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.

Ataques, vulnerabilidades, amenazas

Actividad U1.3: Lee el siguiente artículo Etiquetas en fotos de Facebook y responde a las preguntas

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

Actividad U1.4: 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.

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.

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.

Evaluación de riesgos

Actividad U1.5: ¿Crees que la evaluación de riesgos será igual para todas las empresas? ¿Por qué?
Actividad U1.6: Enumera posibles preguntas que podrían hacerse en la realización de una evaluación de riesgos.
Actividad U1.7: Busca en Internet aplicaciones comerciales que permitan realizar una evaluación de riesgos (de seguridad informática). Indica si son software libre o de pago y busca el precio de las licencias.

Premios Pwnies

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

3. Principios de la 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.

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.

Actividades propuestas

Actividad U1.8: 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.
c) 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.

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.

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.

Políticas de seguridad

Actividad U1.10: ¿Crees que establecer normas a los usuarios de una organización para que tengan una contraseña de acceso segura es una buena política de seguridad?
Actividad U1.11·· Indica qué políticas de seguridad establecerías para evitar la caída de los servidores de la organización.

5. Planes de contingencia

Las políticas de seguridad contemplan la parte de prevención de un sistema, pero no hay que desechar la posibilidad de que, aun a pesar de las medidas tomadas, pueda ocasionarse un desastre. Hay que recordar que ningún sistema es completamente seguro. Es en este caso cuando entran en juego los planes de contingencia.

El plan de contingencia contiene medidas detalladas para conseguir la recuperación del sistema, es decir, creadas para ser utilizadas cuando el sistema falle, no con la intención de que no falle.

La creación de un plan de contingencia debe abarcar las siguientes fases:

- **Evaluación**: en esta etapa hay que crear el grupo que desarrollará el plan. Se deberán identificar los elementos considerados como críticos para la organización, analizar el impacto que pueda producirse ante un desastre y definir cuáles deberán ser las soluciones alternativas a cada uno de los problemas que se puedan producir.

- **Planificación**: en esta fase se deberá documentar y validar el plan de contingencia por parte de los responsables de las áreas involucradas de la organización.
- **Realización de pruebas** para comprobar la viabilidad del plan.
- **Ejecución del plan** para comprobar que efectivamente asegurará la continuidad de las tareas críticas de la organización en caso de posible catástrofe.
- Recuperación: tras el incidente o ataque, deberá restablecerse el orden en la organización.

El plan de contingencia deberá ser revisado periódicamente para que siempre pueda estar de acuerdo con las necesidades de la organización. Entre las numerosas medidas que debe recoger, podemos indicar las siguientes:

- Tener **redundancia**: es decir, tener duplicado el hardware para el almacenamiento de la información, de forma que quede asegurada la continuidad de la actividad diaria en caso de problemas con dicho hardware.
- Tener la **información almacenada de manera distribuida**, es decir, no tener almacenada en el mismo lugar toda la información considerada como crítica para la organización.
- Tener un **plan de recuperación** que contemple las medidas necesarias para restaurar el estado de los recursos tal y como estaban antes de la materialización de la amenaza. Por ejemplo, tener un buen plan para la realización de copias de seguridad.
- Tener a todo el **personal de la organización formado y preparado** ante cualquier situación de emergencia.

Soluciones de alta disponibilidad

Una solución de alta disponibilidad permite que los sistemas de información de la organización estén disponibles las 24 horas de los 7 días de la semana. Con esta solución las empresas pueden tener la posibilidad de no perder información debido a fallos en los sistemas.

La **alta disponibilidad o redundancia** es importante cuando nos encontramos con un `punto único de fallo`.
El punto único de fallo o SPOF (Single Point of Failure) puede ser un componente hardware, software o electrónico. Un fallo en él puede ocasionar un fallo general en el sistema. Para evitarlo, se utiliza la redundancia de elementos para evitar la caída del sistema si uno de ellos falla.

Planes de contingencia

Actividad U1.12: ¿Qué medidas de contingencia se podrían tomar para evitar la pérdida de información en un sistema informático?
Actividad U1.13: ¿Qué medidas de contingencia se podrían tomar para evitar la caída de un servidor de una organización?
Avtividad U1.11: ¿Quiénes crees que deben elaborar el plan de contingencia para una empresa?
Actividad U1.12: ¿Crees que un plan de contingencia, una vez creado, es ya para toda la vida?