2. Fiabilidad, confidencialidad, integridad y disponibilidad.

2.1. Fiabilidad.

La fiabilidad se define como la probabilidad de que un bien funcione adecuadamente durante un período determinado bajo condiciones operativas específicas (por ejemplo, condiciones de presión, temperatura, velocidad, tensión o forma de una onda eléctrica, nivel de vibraciones, etc.).

Un sistema fiable debe tener entre otras: la capacidad de evitar fallos, tolerancia a defectos y capacidad de recuperación (tanto prestaciones como datos afectados).

2.2. Confidencialidad.

La confidencialidad es la cualidad que debe poseer un documento o archivo para que este solo se entienda de manera comprensible o sea leído por la persona o sistema que este autorizado.

De esta manera se dice que un documento (o archivo o mensaje) es confidencial si y solo si puede ser comprendido por la persona o entidad a quien va dirigida o esté autorizada. En el caso de un mensaje esto evita que exista una intercepción de este y que pueda ser leído por una persona no autorizada.

Por ejemplo: si queremos enviar un mensaje a una persona y queremos que sólo dicha persona pueda leer el mensaje, podemos cifrar este mensaje con una clave de tal forma que la persona a la cual va dirigida el mensaje sea la única que puede descifrarlo, así nos aseguramos de que nadie más pueda leer el mensaje.

2.3. Integridad.

La integridad es la cualidad que posee un documento o archivo que no ha sido alterado y que además permite comprobar que no se ha producido manipulación alguna en el documento original. Aplicado a las bases de datos seria la correspondencia entre los datos y los hechos que refleja.

2.4. Disponibilidad.

La disponibilidad es la característica, cualidad o condición de la información de encontrarse a disposición de quienes deben acceder a ella, ya sean personas, procesos o aplicaciones.

En el caso de los sistemas informáticos utilizados para almacenar y procesar la información, los controles de seguridad utilizados para protegerlo, y los canales de comunicación protegidos que se utilizan para acceder a ella deben estar funcionando correctamente. El objetivo de la La Alta Disponibilidad sistemas es que debe seguir estando disponible en todo momento, evitando interrupciones del servicio debido a cortes de energía, fallos de hardware, y actualizaciones del sistema.

3. Elementos vulnerables en el sistema informático: hardware, software y datos.

En seguridad informática, la palabra vulnerabilidad hace referencia a una debilidad en un sistema permitiendo a un atacante violar la confidencialidad, integridad, disponibilidad, control de acceso y consistencia del sistema o de sus datos y aplicaciones.

Las amenazas siempre están presentes, pero sin la identificación de una vulnerabilidad, no podrán causar ningún impacto.

3.1. Hardware.

Las vulnerabilidades de hardware representan la probabilidad de que las piezas físicas del sistema fallen (ya sea por mal uso, descuido, mal diseño etc.) dejando al sistema desprotegido o inoperable. También trata sobre las formas en que el hardware puede ser usado por personas para atacar la seguridad del sistema, por ejemplo el sabotaje de un sistema al sobrecargarlo deliberadamente con componentes de hardware que no han sido diseñados correctamente para funcionar en el sistema.

- **Mal diseño:** es cuando los componentes de hardware del sistema no son apropiados y no cumplen los requerimientos necesarios, en otras palabras, dicha pieza del módulo no fue diseñada correctamente para trabajar en el sistema.
- **Errores de fabricación:** es cuando las piezas de hardware son adquiridas con desperfectos de fabricación y posteriormente fallan al momento de intentar usarse. Aunque la calidad de los componentes de hardware es responsabilidad del fabricante, la organización que los adquiere es la más afectada por este tipo de amenaza.
- **Suministro de energía:** las variaciones de voltaje dañan los dispositivos, por ello es necesario verificar que las instalaciones de suministro de energía funcionen dentro de los parámetros requeridos. Dichas instalaciones también deben proporcionar el nivel de voltaje especificado por el fabricante para no acortar su vida útil.
- **Desgaste:** el uso constante del hardware produce un desgaste considerado, con el tiempo este desgaste reduce el funcionamiento optimo del dispositivo hasta dejarlo inutilizable.
- **Descuido y mal uso:** todos los componentes deben ser usados dentro de los parámetros establecidos por los fabricantes, esto incluye tiempos de uso, periodos y procedimientos adecuados de mantenimiento, así como un apropiado almacenamiento. No seguir estas prácticas provoca un desgaste mayor y la consiguiente reducción de la vida útil de los recursos.

3.2. Software.

Cada programa (ya sea de paquetería o de sistema operativo) puede ser usado como medio para atacar a un sistema más grande, esto se da debido a errores de programación, o porque en el diseño no fueron considerados ciertos aspectos (por ejemplo controles de acceso, seguridad, implantación, etc.).Ambos factores hacen susceptible al sistema a las amenazas de software.

- **Software de desarrollo:** es un tipo de software personalizado, puede ser creado con el fin de atacar un sistema completo o aprovechar alguna de sus características para violar su seguridad.
- **Software de aplicación**: este software no fue creado específicamente para realizar ataques, pero tiene características que pueden ser usadas de manera maliciosa para atacar un sistema.

5. Amenazas. Tipos: físicas y lógicas.

5.1. Amenazas Lógicas

Bajo la etiqueta de "amenazas lógicas" encontramos todo tipo de programas que de una forma u otra pueden dañar a nuestro sistema, creados de forma intencionada para ello (*software* malicioso, también conocido como *malware*) o simplemente por error (*bugs* o agujeros). Algunas de estas amenazas son:

a) *Software incorrecto.*

Las amenazas más habituales a un sistema provienen de errores cometidos de forma involuntaria por los programadores de sistemas o de aplicaciones. A estos errores de programación se les denomina bugs, y a los programas utilizados para aprovechar uno de estos fallos y atacar al sistema, exploits. Algunos ejemplos de software incorrecto son:

- Defectos de instalación o programación.
- Eliminación o sustitución de bibliotecas comunes a más de un programa o del sistema (DLL Hell).
- Reiniciar arbitrariamente la sesión de un usuario para que la instalación tenga efecto.
- Presuponer que el usuario tiene una conexión permanente a internet.

b) *Herramientas de seguridad*

Cualquier herramienta de seguridad representa un arma de doble filo: de la misma forma que un administrador las utiliza para detectar y solucionar fallos en sus sistemas o en la subred completa, un potencial intruso las puede utilizar para detectar esos mismos fallos y aprovecharlos para atacar los equipos. Herramientas como NESSUS, SAINT o SATAN pasan de ser útiles a ser peligrosas cuando las utilizan crackers que buscan información sobre las vulnerabilidades de un host o de una red completa.

El mal uso de estas herramientas puede concluir en situaciones de bloqueo, enlentecimiento e incluso denegación de servicio de las máquinas analizadas. Estas herramientas sólo deben ser lanzadas contra máquinas ajenas única y exclusivamente cuando sus responsables nos hayan autorizado a ello. Bajo ninguna circunstancia deben ser empleadas contra máquinas que no sean de nuestra propiedad sin consentimiento expreso por parte de sus propietarios, informando en cada caso de la actividad que vayamos a realizar.

c) *Puertas traseras.*

Software que permite el acceso al sistema y facilita la entrada a la información de un usuario sin su permiso o conocimiento.

Durante el desarrollo de aplicaciones grandes o de sistemas operativos es habitual entre los programadores insertar `atajos' en los sistemas habituales de autenticación del programa o del núcleo que se está diseñando. A estos atajos se les denomina puertas traseras, y con ellos se consigue mayor velocidad a la hora de detectar y depurar fallos: por ejemplo, los diseñadores de un software de gestión de bases de datos en el que para acceder a una tabla se necesiten cuatro claves diferentes de diez caracteres cada una pueden insertar una rutina para conseguir ese acceso mediante una única clave `especial', con el objetivo de perder menos tiempo al depurar el sistema.

Algunos programadores pueden dejar estos atajos en las versiones definitivas de su software para facilitar un mantenimiento posterior, para garantizar su propio acceso, o simplemente por descuido; la cuestión es que si un atacante descubre una de estas puertas traseras (no nos importa el método que utilice para hacerlo) va a tener un acceso global a datos que no debería poder leer, lo que obviamente supone un grave peligro para la integridad de nuestro sistema.

d) Bombas lógicas

Software que permanece oculto hasta que se cumplen unas condiciones preprogramadas (por ejemplo una fecha) momento en el que se ejecuta, en ese punto, la función que realizan no es la original del programa, sino que generalmente se trata de una acción perjudicial.

Ejemplos de acciones que puede realizar una bomba lógica:

- Borrar información del disco duro
- Mostrar un mensaje
- Reproducir una canción
- Enviar un correo electrónico
- Apagar el Monitor

e) Canales cubiertos

Son canales de comunicación que permiten a un proceso transferir información de forma que viole la política de seguridad del sistema; dicho de otra forma, un proceso transmite información a otros (locales o remotos) que no están autorizados a leer dicha información. Los canales cubiertos no son una amenaza demasiado habitual en redes de I+D.

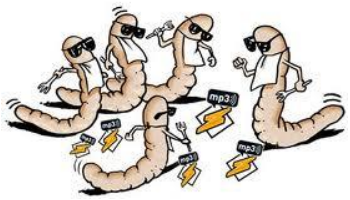
f) Virus

Un virus es una secuencia de código que se inserta en un fichero ejecutable (denominado huésped), de forma que cuando el archivo se ejecuta, el virus también lo hace, insertándose a sí mismo en otros programas.

Algunas acciones que puede realizar un virus son:

- Mostrar en la pantalla mensajes o imágenes humorísticas, generalmente molestas.
- Ralentizar o bloquear el ordenador.
- Destruir la información almacenada en el disco, en algunos casos vital para el sistema, que impedirá el funcionamiento del equipo.
- Reducir el espacio en el disco.
- Molestar al usuario cerrando ventanas, moviendo el ratón.

g) gusanos



Un gusano es un tipo de malware que tiene la capacidad de copiarse a sí mismo para infectar otros sistemas utilizando servicios del propio sistema operativo que normalmente son invisibles al usuario. En ocasiones porta virus o aprovecha los bugs de los sistemas a los que se conecta para dañarlos.

Al ser difíciles de programar su número no es muy elevado, pero el daño que pueden causar es muy grande.

h) Caballos de Troya

Los troyanos o caballos de Troya son instrucciones escondidas en un programa de forma que éste parezca realizar las tareas que un usuario espera de él, pero que realmente ejecute funciones ocultas (generalmente en detrimento de la seguridad) sin el conocimiento del usuario.

Evitar la infección de un troyano es difícil, algunas de las formas más comunes de infectarse son:

- Descarga de programas de redes p2p y sitios web que no son de confianza.
- Páginas web que contienen contenido ejecutable (por ejemplo controles ActiveX o aplicaciones Java).
- Exploits para aplicaciones no actualizadas (navegadores, reproductores multimedia, clientes de mensajería instantánea).
- Ingeniería social (por ejemplo un cracker manda directamente el troyano a la víctima a través de la mensajería instantánea).
- Archivos adjuntos en correos electrónicos y archivos enviados por mensajería instantánea.

i) Programa conejo o bacteria

Bajo este nombre se conoce a los programas que no hacen nada útil, sino que simplemente se dedican a reproducirse hasta que el número de copias acaba con los recursos del sistema (memoria, procesador, disco...), produciendo una negación de servicio. Por sí mismos no hacen ningún daño, sino que lo que realmente perjudica es el gran número de copias suyas en el sistema, que en algunas situaciones pueden llegar a provocar la parada total de la máquina.

j) Técnicas salami

Por técnica salami se conoce al robo automatizado de pequeñas cantidades de bienes (generalmente dinero) de una gran cantidad origen. El hecho de que la cantidad inicial sea grande y la robada pequeña hace extremadamente difícil su detección: si de una cuenta con varios millones de pesetas se roban unos céntimos, nadie va a darse cuenta de ello. Las técnicas salami no se suelen utilizar para atacar sistemas normales, sino que su uso más habitual es en sistemas bancarios.

5.2. Amenazas Físicas.

Es muy importante ser consciente que por más que nuestra empresa sea la más segura desde el punto de vista de ataques externos (hackers, virus, ataques de DoS, etc.); la seguridad de la misma será nula si no se ha previsto como combatir un incendio o cualquier otro tipo de desastre natural y no tener presente políticas claras de recuperación.

La seguridad física es uno de los aspectos más olvidados a la hora del diseño de un sistema informático. Si bien algunos de los aspectos de seguridad física básicos se prevén, otros, como la detección de un atacante interno a la empresa que intenta acceder físicamente a una sala de cómputo de la misma, no. Esto puede derivar en que para un atacante sea más fácil lograr tomar y copiar una cinta de backup de la sala de cómputo, que intentar acceder vía lógica a la misma. Así, la Seguridad Física consiste en la **"aplicación de barreras físicas y procedimientos de control, como medidas de prevención y contramedidas ante amenazas a los recursos e información confidencial"**. Se refiere a los controles y mecanismos de seguridad dentro y alrededor del centro de cómputo, así como los medios de acceso remoto al y desde el mismo; implementados para proteger el hardware y medios de almacenamiento de datos.

- **Las principales amenazas que se prevén en Seguridad Física son:**

  1. Desastres naturales, incendios accidentales, tormentas e inundaciones
  2. Amenazas ocasionadas por el hombre
  3. Disturbios, sabotajes internos y externos deliberados.

- **Evaluar y controlar permanentemente la seguridad física de las instalaciones de cómputo y del edificio es la base para comenzar a integrar la seguridad como una función primordial dentro de cualquier organismo.**

- **Tener controlado el ambiente y acceso físico permite:**

a) Disminuir sinistros
b) Trabajar mejor manteniendo la sensación de seguridad
c) Descartar falsas hipótesis si se produjeran incidentes
d) Tener los medios para luchar contra accidentes

6. Seguridad física y ambiental.

La Seguridad Física consiste en la **"*aplicación de barreras físicas y procedimientos de control, como medidas de prevención y contramedidas ante amenazas a los recursos e información confidencial*".** Se refiere a los controles y mecanismos de seguridad dentro y alrededor del Centro de Cómputo así como los medios de acceso remoto al y desde el mismo; implementados para proteger el hardware y medios de almacenamiento de datos. Como por ejemplo: cámaras de vídeo en la sala del controlador de procesamiento de datos (CPD) y puertas de acceso al CPD con cerraduras electrónicas activadas por tarjetas.

Las principales amenazas que se prevén en la seguridad física son:

1. Desastres naturales, incendios accidentales tormentas e inundaciones.
2. Amenazas ocasionadas por el hombre.
3. Disturbios, sabotajes internos y externos deliberados.

Los peligros más importantes que se corren en un centro de procesamiento son:

1) Incendios.

Los incendios son causados por el uso inadecuado de combustibles, fallas de instalaciones eléctricas defectuosas y el inadecuado almacenamiento y traslado de sustancias peligrosas.

El fuego es una de las principales amenazas contra la seguridad. Es considerado el enemigo número uno de las computadoras ya que puede destruir fácilmente los archivos de información y programas.

2) Inundaciones

Se las define como la invasión de agua por exceso de escurrimientos superficiales o por acumulación en terrenos planos, ocasionada por falta de drenaje ya sea natural o artificial. Esta es una de las causas de mayores desastres en centros de cómputos. Además de las causas naturales de inundaciones, puede existir la posibilidad de una inundación provocada por la necesidad de apagar un incendio en un piso superior. Para evitar este inconveniente se pueden tomar las siguientes medidas: construir un techo impermeable para evitar el paso de agua desde un nivel superior y acondicionar las puertas para contener el agua que bajase por las escaleras.

3) Condiciones Climatológicas

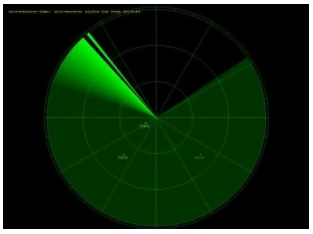
Normalmente se reciben por anticipado los avisos de tormentas, tempestades, tifones y catástrofes sísmicas similares. Las condiciones atmosféricas severas se asocian a ciertas partes del mundo y la probabilidad de que ocurran está documentada.

La frecuencia y severidad de su ocurrencia deben ser tenidas en cuenta al decidir la construcción de un edificio.

Existe otra condición meteorológica que son los terremotos, estos fenómenos sísmicos pueden ser tan poco intensos que sólo pueden ser detectados por instrumentos muy sensibles ó tan intensos que causan la destrucción de edificios y hasta la pérdida de vidas humanas. En la actualidad estos fenómenos están ocurriendo en lugares donde no se los asociaba.

4) Señales de Radar

La influencia de las señales o rayos de radar sobre el funcionamiento de un ordenador ha sido exhaustivamente estudiado desde hace varios años.



Los resultados de las investigaciones más recientes son que las señales muy fuertes de radar pueden inferir en el procesamiento electrónico de la información, pero únicamente si la señal que alcanza el equipo es de 5 Volts/Metro, o mayor. Ello podría ocurrir sólo si la antena respectiva fuera visible desde una ventana del centro de procesamiento respectivo y, en algún momento, estuviera apuntando directamente hacia dicha ventana.

5) Instalaciones Eléctricas

Las subidas (picos) y caídas de tensión no son el único problema eléctrico al que se han de enfrentar los usuarios. También está el tema del ruido que interfiere en el funcionamiento de los componentes electrónicos. El ruido interfiere en los datos, además de favorecer la escucha electrónica.

En el cableado podemos sufrir el riesgo de interferencias, cortes de cable o daños en el cable que pueden provocar pérdida de la integridad de los datos.

Además se debe proveer de un sistema de calefacción, ventilación y aire acondicionado que se dedique exclusivamente al cuarto de los pc y equipos de proceso de datos ya que son causa potencial de incendios.

6) Ergonometría

Los fines de la aplicación de objetos ergonómicos son fundamentalmente la protección de los trabajadores tales como agotamiento, las sobrecargas y el envejecimiento prematuro.

El lugar de trabajo debe estar diseñado de manera que el usuario se coloque en la posición más natural posible. Cada posición variará de acuerdo a los distintos usuarios, por ello lo fundamental es que el puesto de trabajo se ajustable.

El monitor debe tener una posición adecuada y debe ser antirreflejante para evitar los problemas en la visión de los usuarios.

Se debe evitar el estrés informático, haciendo las tareas lo menos monótonas y rutinarias posibles.

Para que la productividad no se vea afectada la luminosidad y la temperatura así como la humedad deben ser las adecuadas.

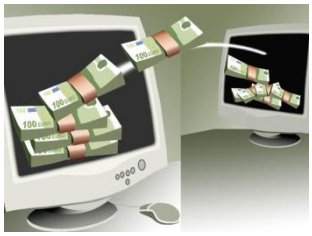
7) Acciones Hostiles

a) **Robo**

Las computadoras son posesiones valiosas de las empresas y están expuestas, de la misma forma que lo están las piezas de stock e incluso el dinero. La información importante o confidencial puede ser fácilmente copiada. Muchas empresas invierten millones de dólares en programas y archivos de información, a los que dan menor protección que la que otorgan a una máquina de escribir o una calculadora. El software, es una propiedad muy fácilmente sustraíble y las cintas y discos son fácilmente copiados sin dejar ningún rastro.

b) **Fraude**

Cada año, millones de dólares son sustraídos de empresas y, en muchas ocasiones, los ordenadores han sido utilizadas como instrumento para dichos fines.



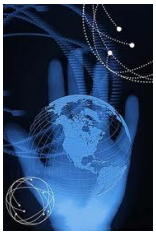
c) **Sabotaje**

El peligro más temido en los centros de procesamiento de datos, es el sabotaje. Empresas que han intentado implementar programas de seguridad de alto nivel, han encontrado que la protección contra el saboteador es uno de los retos más duros. Este puede ser un empleado o un sujeto ajeno a la propia empresa.Físicamente, los imanes son las herramientas a las que se recurre, ya que con una ligera pasada la información desaparece, aunque las cintas estén almacenadas en el interior de su funda de protección. Una habitación llena de cintas puede ser destruida en pocos minutos y los centros de procesamiento de datos pueden ser destruidos sin entrar en ellos. Además, suciedad, partículas de metal o gasolina pueden ser introducidos por los conductos de aire acondicionado. Las líneas de comunicaciones y eléctricas pueden ser cortadas, etc.

8) Control de Accesos

El control de acceso no sólo requiere la capacidad de identificación, sino también asociarla a la apertura o cerramiento de puertas, permitir o negar acceso basado en restricciones de tiempo, área o sector dentro de una empresa o institución. Algunos de los controles que podemos realizar son:

1. Utilización de Guardias
2. Utilización de Detectores de Metales
3. Utilización de Sistemas Biométricos
4. Verificación Automática de Firmas (VAF)
5. Seguridad con Animales
6. Protección Electrónica



Evaluar y controlar permanentemente la seguridad física del edificio es la base para o comenzar a integrar la seguridad como una función primordial dentro de cualquier organismo.

Tener controlado el ambiente y acceso físico permite:

- disminuir siniestros
- trabajar mejor manteniendo la sensación de seguridad
- descartar falsas hipótesis si se produjeran incidentes
- tener los medios para luchar contra accidentes

6.1. Ubicación y protección física de los equipos y servidores.

Para minimizar el impacto de un posible problema físico tendremos que imponer condiciones de seguridad para los equipos y sistemas de la organización. Por otra lado para que los equipos informáticos funcionen correctamente deben de encontrarse en bajo ciertas condiciones.

Los **servidores** dado que su funcionamiento ha de ser continuo deben de situarse en un lugar que cumpla las condiciones óptimas para el funcionamiento de estos, además debe estar bajo llave en un armario rack y estar en un lugar con acceso restringido al cual sólo acceda personal autorizado.

Para asegurar los sistemas y equipos que han de mantenerse siempre operativos se crean lugares que se conocen como "Centro de Procesamiento de Datos" o por sus siglas CPD. En estos CPD se deben de cumplir una serie de requisitos para protegerlos de posibles desastres:

- Se debe evitar el polvo y la electricidad estática.
- La temperatura debe ser continua las 24 horas los 365 días al año.
- Se debe evitar el uso de techos falsos.
- Deben estar libres de cualquier amenaza contra inundación.
- Se deben mantener bajo llave, las cuales serán asignadas solo al personal autorizado.

Para poder asegurar un CPD lo primero que debemos hacer es asegurar el recinto con medidas de seguridad física, como por ejemplo:

Sistemas contra incendios:

Existen varios sistemas de extinción de incendios como: extracción de oxígeno, inserción de gases nobles o extintores especiales que eviten el riesgo de electrocución.

Sistemas de control de acceso:

- Llaves tradicionales
- Contraseñas: con su correspondiente política de contraseñas.
- Tarjetas magnéticas.
- Sistemas de identificación por radiofrecuencia:
- Sistemas de token: se compone de un elemento móvil que genera claves aleatorias.
- Sistemas biométricos.
- Sistemas de control de temperatura.

Dependiendo del entorno y los sistemas a proteger la seguridad física será más o menos importante y restrictiva, aunque siempre deberemos tenerla en cuenta.

A continuación mencionaremos algunos de los problemas de seguridad física con los que nos podemos enfrentar y las medidas que podemos tomar para evitarlos o al menos minimizar su impacto:

➢ Protección del hardware

El hardware es frecuentemente el elemento más caro de todo sistema informático y por tanto las medidas encaminadas a asegurar su integridad son una parte importante de la seguridad física de cualquier organización.

Problemas a los que nos enfrentamos:

- **Acceso físico**

Si alguien que desee atacar un sistema tiene acceso físico al mismo todo el resto de medidas de seguridad implantadas se convierten en inútiles.

Para problemas deberemos implantar mecanismos de prevención (control de acceso a los recursos) y de detección (si un mecanismo de prevención falla o no existe debemos al menos detectar los accesos no autorizados cuanto antes).

Para la prevención soluciones variadas:
- analizadores de retina
- tarjetas inteligentes
- videocámaras
- vigilantes jurados

En muchos casos es suficiente con controlar el acceso a las salas y cerrar siempre con llave los despachos o salas donde hay equipos informáticos y no tener cableadas las tomas de red que estén accesibles.

- **Desastres naturales**

Además de los posibles problemas causados por ataques realizados por personas, es importante tener en cuenta que también los *desastres naturales* pueden tener muy graves consecuencias, sobre todo si no los contemplamos en nuestra política de seguridad y su implantación.

Algunos desastres naturales a tener en cuenta:
- Terremotos y vibraciones
- Tormentas eléctricas
- Inundaciones y humedad
- Incendios y humos

Los **terremotos** son el desastre natural menos probable en la mayoría de organismos ubicados en España, por lo que no se harán grandes inversiones en prevenirlos, aunque hay varias cosas que se pueden hacer sin un desembolso elevado y que son útiles para prevenir problemas causados por pequeñas vibraciones:

- No situar equipos en sitios altos para evitar caídas.
- No colocar elementos móviles sobre los equipos para evitar que caigan sobre ellos.
- Separar los equipos de las ventanas para evitar que caigan por ellas o qué objetos lanzados desde el exterior los dañen.
- Utilizar fijaciones para elementos críticos.
- Colocar los equipos sobre plataformas de goma para que esta absorba las vibraciones.

Otro desastre natural importante son las **tormentas con aparato eléctrico**, especialmente frecuentes en verano, que generan subidas súbitas de tensión muy superiores a las que pueda generar un problema en la red eléctrica. A parte de la protección mediante el uso de pararrayos, la única solución a este tipo de problemas es desconectar los equipos antes de una tormenta (qué por fortuna suelen ser fácilmente predecibles).

En entornos normales es recomendable que haya un cierto grado de **humedad**, ya que en si el ambiente es extremadamente seco hay mucha electricidad estática. No obstante, tampoco interesa tener un nivel de humedad demasiado elevado, ya que puede producirse condensación en los circuitos integrados que den origen a un cortocircuito. En general no es necesario emplear ningún tipo de aparato para controlar la humedad, pero no está de más disponer de alarmas que nos avisen cuando haya niveles anómalos.

Otro tema distinto son las **inundaciones**, ya que casi cualquier medio (máquinas, cintas, routers ...) que entre en contacto con el agua queda automáticamente inutilizado, bien por el propio líquido o bien por los cortocircuitos que genera en los sistemas electrónicos. Contra ellas podemos instalar sistemas de detección que apaguen los sistemas si se detecta agua y corten la corriente en cuanto estén apagados.

Por último **el fuego y los humos**, que en general provendrán del incendio de equipos por sobrecarga eléctrica. Contra ellos emplearemos sistemas de extinción, que aunque pueden dañar los equipos que apaguemos (aunque actualmente son más o menos inocuos), nos evitarán males mayores. Además del fuego, también el humo es perjudicial para los equipos (incluso el del tabaco), al ser un abrasivo que ataca a todos los componentes, por lo que es recomendable mantenerlo lo más alejado posible de los equipos.

- **<u>Alteraciones del entorno</u>**

Deberemos contemplar problemas que pueden afectar el régimen de funcionamiento habitual de las máquinas como la alimentación eléctrica, el ruido eléctrico producido por los equipos o los cambios bruscos de temperatura.

Electricidad

Quizás los problemas derivados del entorno de trabajo más frecuentes son los relacionados con el sistema eléctrico que alimenta nuestros equipos; cortocircuitos, picos de tensión, cortes de flujo, etc.

Para corregir los problemas con las subidas de tensión podremos instalar tomas de tierra o filtros reguladores de tensión.

Para los cortes podemos emplear *Sistemas de Alimentación Ininterrumpida* (SAI), que además de proteger ante cortes mantienen el flujo de corriente constante, evitando las subidas y bajadas de tensión.

Por último indicar que además de los problemas del sistema eléctrico también debemos preocuparnos de la corriente estática, que puede dañar los equipos. Para evitar problemas se pueden emplear esprais antiestáticos o ionizadores y tener cuidado de no tocar componentes metálicos, evitar que el ambiente esté excesivamente seco, etc.

Ruido eléctrico

El ruido eléctrico suele ser generado por motores o por maquinaria pesada, pero también puede serlo por otros ordenadores o por multitud de aparatos, y se transmite a través del espacio o de líneas eléctricas cercanas a nuestra instalación.

Para prevenir los problemas que puede causar el ruido eléctrico lo más barato es intentar no situar el *hardware* cerca de los elementos que pueden causar el ruido. En caso de que fuese necesario hacerlo siempre podemos instalar filtos o apantallar las cajas de los equipos.

Temperaturas extremas

Las temperaturas extremas, ya sea un calor excesivo o un frio intenso, perjudican gravemente a todos los equipos. En general es recomendable que los equipos operen entre 10 y 32 grados Celsius. Para controlar la temperatura emplearemos aparatos de aire acondicionado.

➢ Protección de los datos

Además proteger el *hardware* se debe incluir medidas de protección de los **datos**, ya que en realidad la mayoría de ataques tienen como objetivo la obtención de información, no la destrucción del medio físico que la contiene.

A continuación los problemas de seguridad que afectan a la transmisión y almacenamiento de datos:

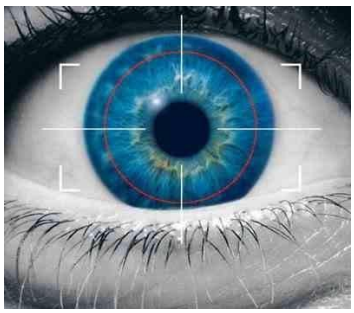
- **Eavesdropping**

La *interceptación* o *eavesdropping*, también conocida por ''passive wiretapping'' es un proceso mediante el cual un agente capta información que va dirigida a él; esta captación puede realizarse por muchísimos medios: *sniffing* en redes ethernet o inalámbricas, capturando radiaciones electromagnéticas.

6.3. Sistemas Biométricos: Funcionamiento. Estándares

La biometría es el estudio de métodos automáticos para el reconocimiento único de humanos basados en uno o más rasgos conductuales o físicos intrínsecos. El término se deriva de las palabras griegas "bios" de vida y "metron" de medida.

La **"biometría informática"** es la aplicación de técnicas matemáticas y estadísticas sobre los rasgos físicos o de conducta de un individuo, para "verificar" identidades o para "identificar" individuos.



En las tecnologías de la información (TI), la autentificación biométrica se refiere a las tecnologías para medir y analizar las características físicas y del comportamiento humanas con propósito de autentificación.

Las huellas dactilares, las retinas, el iris, los patrones faciales, de venas de la mano o la geometría de la palma de la mano, representan ejemplos de características físicas (estáticas), mientras que entre los ejemplos de características del comportamiento se incluye la firma, el paso y el tecleo (dinámicas). La voz se considera una mezcla de características físicas y del comportamiento, pero todos los rasgos biométricos comparten aspectos físicos y del comportamiento.

Es decir, un sistema que fundamenta sus decisiones de reconocimiento mediante una característica personal que puede ser reconocida o verificada de manera automatizada.

FUNCIONAMIENTO

En un sistema de Biometría típico, la persona se registra con el sistema cuando una o más de sus características físicas y de conducta es obtenida, procesada por un algoritmo numérico, e introducida en una base de datos. Idealmente, cuando entra, casi todas sus características concuerdan; entonces cuando alguna otra persona intenta identificarse, no empareja completamente, por lo que el sistema no le permite el acceso. Las tecnologías actuales tienen tasas de error que varían ampliamente (desde valores bajos como el 60%, hasta altos como el 99,9%).

El rendimiento de una medida biométrica se define generalmente en términos de tasa de **falso positivo** (False Acceptance Rate o FAR), la **tasa de falso negativo** (False NonMatch Rate o FNMR, también False Rejection Rate o FRR), y el **fallo de tasa de alistamiento** (Failure-to-enroll Rate, FTR o FER).

7. Seguridad Lógica.

La **seguridad lógica** se refiere a la seguridad en el uso de software y los sistemas, la protección de los datos, procesos y programas, así como la del acceso ordenado y autorizado de los usuarios a la información. La "seguridad lógica" involucra todas aquellas medidas establecidas por la administración -usuarios y administradores de recursos de tecnología de información- para minimizar los riesgos de seguridad asociados con sus operaciones cotidianas llevadas a cabo utilizando la tecnología de información. Los principales objetivos que persigue la seguridad lógica son:

- Restringir el acceso a los programas y archivos
- Asegurar que se estén utilizando los datos, archivos y programas correctos en y por el procedimiento correcto.

7.1. Copias de seguridad.

Una **copia de seguridad** o **backup** (su nombre en inglés) en tecnología de la información o informática es una copia de seguridad - o el proceso de copia de seguridad - con el fin de que estas copias adicionales puedan utilizarse para restaurar el original después de una eventual pérdida de datos. Esta Copia de Seguridad también se denomina Copia de Respaldo e incluso, podremos encontrarnos con la denominación Backup en términos ingleses.

Fundamentalmente son útiles para dos cosas. Primero, recuperarse de una catástrofe informática. Segundo recuperar una pequeña cantidad de archivos que pueden haberse eliminado accidentalmente o corrompido. La pérdida de datos es muy común: El 66% de los usuarios de internet han sufrido una seria pérdida de datos.

Ya que los sistemas de respaldo contienen por lo menos una copia de todos los datos que vale la pena salvar, deben de tenerse en cuenta los requerimientos de almacenamiento. La organización del espacio de almacenamiento y la administración del proceso de efectuar la copia de seguridad son tareas complicadas.

Podemos **perder nuestra información** o cuando menos **no poder acceder a ella** por motivos muy diversos, desde infecciones del sistema por virus y malware, fallos de hardware (cortes de corriente y picos de tensión, excesos de temperatura y daños en los dispositivos), apagados incorrectos del equipo, problemas motivados por algún programa, daños del usuario al borrar archivos por error, etc.

A la hora de **seleccionar que contenido guardar en esas copias**, debemos pensar siempre en el nivel de importancia de la información, es decir, que archivos personales importantes tenemos ordenador y cuales podría suponer un gran problema perderlos, como fotografías, documentos del trabajo, documentación personal, etc., esos, evidentemente son los que debemos **asegurar siempre**.

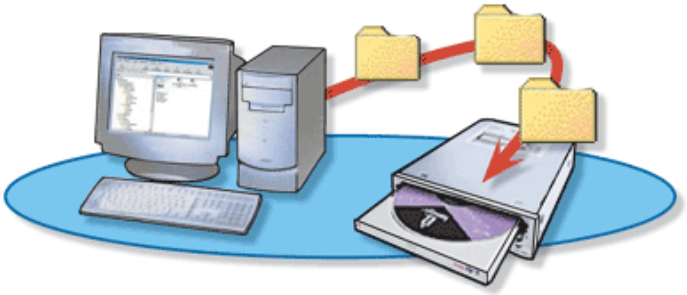
La periodicidad para realizar las copias de seguridad de nuestros datos, dependerá del mayor o menor movimiento de información que realicemos en nuestro equipo.

Las copias de seguridad garantizan dos objetivos: **integridad y disponibilidad.**

7.1.1. Tipos de copias de seguridad.

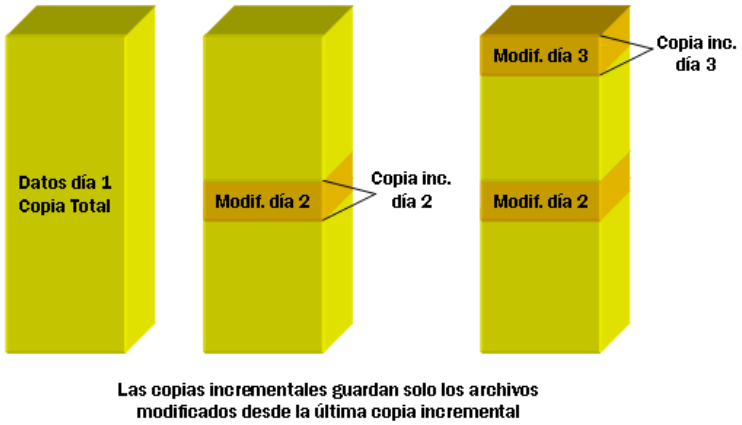
Existen varios tipos de copias de seguridad según los datos que respaldemos en ellas:

TOTAL Ó COMPLETA: realiza una copia de todos los archivos seleccionados por el usuario, normalmente carpetas enteras de datos. Cada vez que se realiza una copia de este tipo se copian otra vez "todos" los archivos seleccionados aunque no hayan sido modificados desde la última copia realizada. Borra el bit de modificado de cada archivo que copia.



INCREMENTAL: En un proceso de copia de seguridad incremental, el programa examina el bit de modificado y hace una copia de seguridad sólo de los archivos que han cambiado desde la última copia de seguridad incremental o normal. Al igual que en la copia de seguridad normal, esta tarea borra el bit de modificado de cada archivo que copia. Este tipo de copia minimiza el tiempo y el espacio necesario para salvar los datos al almacenar únicamente los archivos que han cambiado, pero si tenemos que realizar una restauración de archivos ante un desastre debemos disponer de todas las copias incrementales anteriores hasta llegar a la última copia normal.

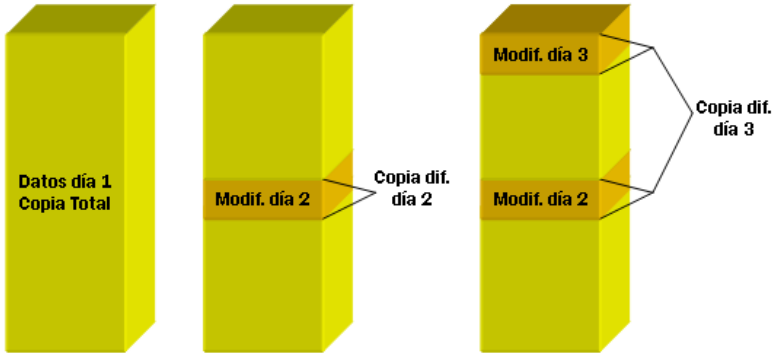
Ejemplo, si hacemos copia de seguridad total el día 1 de cada mes y copia de seguridad incremental el resto de los días, cada copia incremental solo guardará los archivos que se hayan modificado ese día. Si tenemos que realizar la restauración de archivos ante un desastre, debemos disponer de la copia total y de todas las copias incrementales que hayamos realizado desde la copia total.



Las copias incrementales guardan solo los archivos modificados desde la última copia incremental

DIFERENCIAL: Realiza el mismo proceso que la copia incremental salvo por el hecho de que el programa no elimina el bit de modificado de los archivos que copia, lo que equivale a decir que durante una copia de seguridad diferencial se copian todos los archivos que han cambiado desde la última copia de seguridad normal o incremental. Sus ventajas son que se requiere menos espacio que en el copia normal y que en el proceso de restauración únicamente necesitaremos la última copia normal y la última copia diferencial, pero por el contrario se consume más tiempo en realizar la copia y también más espacio que en la incremental.

Ejemplo, si hacemos copia de seguridad total el día 1 de cada mes y copia de seguridad diferencial el resto de los días, cada copia diferencial guardará los archivos que se hayan modificado desde el día 1. La ventaja es que se requiere menos espacio que la copia total y que en el proceso de restauración únicamente necesitaremos la última copia total y la última copia diferencial. Una copia diferencial anula a la copia diferencial anterior. Por el contrario, se consume más tiempo en realizar la copia y también más espacio que en el caso de copia incremental.



Las copias diferenciales guardan solo los archivos modificados desde la última copia total

Recomendación sobre el tipo de copia a efectuar

Si el volumen de datos de nuestra copia de seguridad no es muy elevado (menos de 4 GB), lo más práctico es realizar siempre **copias totales** ya que en caso de desastre, tan solo debemos recuperar la última copia.

Si el volumen de datos de nuestra copia de seguridad es muy elevado (mayor de 50 GB) pero el volumen de datos que se modifican no es elevado (sobre 4 GB), lo más práctico es realizar una **primera copia total y posteriormente realizar siempre copias diferenciales**. Así, en caso de desastre, tan solo debemos recuperar la copia total y la última diferencial. Periódicamente debemos realizar una copia total y así empezar de nuevo.

Si el volumen de datos de nuestra copia de seguridad es muy elevado (mayor de 50 GB) y el volumen de datos que se modifican también lo es, las copias diferenciales ocuparán mucho espacio, por lo tanto en este caso lo más práctico será realizar una **primera copia total y posteriormente realizar siempre copias incrementales** ya que son las que menos espacio ocupan. El problema es que en caso de desastre debemos recuperar la última copia total y todas las incrementales realizadas desde que se hizo la última copia total. En estos casos, conviene hacer copias totales más a menudo para no tener que mantener un número muy elevado de copias incrementales.

b) Centros de Respaldo.

Un centro de respaldo es un centro de procesamiento de datos (CPD) específicamente diseñado para tomar el control de otro CPD principal en caso de contingencia.

Grandes organizaciones, tales como bancos o Administraciones Públicas, no pueden permitirse la pérdida de información ni el cese de operaciones ante un desastre en su centro de proceso de datos. Terremotos, incendios o atentados en estas instalaciones son infrecuentes, pero no improbables. Por este motivo, se suele habilitar un centro de respaldo para absorber las operaciones del CPD principal en caso de emergencia.

Un centro de respaldo se diseña bajo los mismos principios que cualquier CPD, pero bajo algunas consideraciones más. En primer lugar, debe elegirse una localización totalmente distinta a la del CPD principal con el objeto de que no se vean ambos afectados simultáneamente por la misma contingencia. Es habitual situarlos entre 20 y 40 kilómetros del CPD principal. La distancia está limitada por las necesidades de telecomunicaciones entre ambos centros.

En segundo lugar, el equipamiento electrónico e informático del centro de respaldo debe ser absolutamente compatible con el existente en el CPD principal. Esto no implica que el equipamiento deba ser exactamente igual. Normalmente, no todos los procesos del CPD principal son críticos. Por este motivo no es necesario duplicar todo el equipamiento. Por otra parte, tampoco se requiere el mismo nivel de servicio en caso de emergencia. En consecuencia, es posible utilizar hardware menos potente. La pecera de un centro de respaldo recibe estas denominaciones en función de su equipamiento:

- *Sala blanca*: cuando el equipamiento es *exactamente* igual al existente en el CPD principal.
- *Sala de back-up:* cuando el equipamiento es similar pero no exactamente igual.

En tercer lugar, el equipamiento software debe ser idéntico al existente en el CPD principal. Esto implica exactamente las mismas versiones y parches del software de base y de las aplicaciones corporativas que estén en explotación en el CPD principal. De otra manera, no se podría garantizar totalmente la continuidad de operación.

Por último, pero no menos importante, es necesario contar con una réplica de los mismos datos con los que se trabaja en el CPD original. Este es el problema principal de los centros de respaldo.

Existen dos políticas o aproximaciones a este problema:

- *Copia síncrona de datos*: Se asegura que todo dato escrito en el CPD principal también se escribe en el centro de respaldo antes de continuar con cualquier otra operación.
- *Copia asíncrona de datos:* No se asegura que todos los datos escritos en el CPD principal se escriban inmediatamente en el centro de respaldo, por lo que puede existir un desfase temporal entre unos y otros.

La copia asíncrona puede tener lugar fuera de línea. En este caso, el centro de respaldo utiliza la última copia de seguridad existente del CPD principal. Esto lleva a la pérdida de los datos de operaciones de varias horas (como mínimo) hasta días (lo habitual). Esta opción es viable para negocios no demasiado críticos, donde es más importante la continuidad del negocio que la pérdida de datos. Por ejemplo, en cadenas de supermercados o pequeños negocios. No obstante, es inviable en negocios como la banca, donde es impensable la pérdida de una sola transacción económica.

En los demás casos, la política de copia suele descansar sobre la infraestructura de almacenamiento corporativo. Generalmente, se trata de redes SAN y cabinas de discos con suficiente inteligencia como para implementar dichas políticas.

Tanto para la copia síncrona como asíncrona, es necesaria una extensión de la red de almacenamiento entre ambos centros. Es decir, un enlace de telecomunicaciones entre el CPD y el centro de respaldo. En caso de copia asíncrona es imprescindible que dicho enlace goce de baja latencia. Motivo por el que se suele emplear un enlace de fibra óptica, que limita la distancia máxima a decenas de kilómetros. Existen dos tecnologías factibles para la copia de datos en centros de respaldo:

- iSCSI.
- Fibre Channel.

Un centro de respaldo por sí sólo no basta para hacer frente a una contingencia grave. Es necesario disponer de un Plan de Contingencias corporativo. Este plan contiene tres subplanes que indican las medidas técnicas, humanas y organizativas necesarias en tres momentos clave:

- **Plan de respaldo:** Contempla las actuaciones necesarias *antes* de que se produzca un incidente. Esencialmente, mantenimiento y prueba de las medidas preventivas.
- **Plan de emergencia:** Contempla las actuaciones necesarias *durante* un incidente.
- **Plan de recuperación:** Contempla las actuaciones necesarias *después* de un incidente. Básicamente, indica cómo volver a la operación normal.

7.3.3. Almacenamiento remoto: SAN, NAS y almacenamietno clouding.

a) SAN.

Una red de área de almacenamiento, en inglés SAN (storage area network), es una red concebida para conectar servidores, matrices (arrays) de discos y librerías de soporte. Principalmente, está basada en tecnología fibre channel y más recientemente en iSCSI. Su función es la de conectar de manera rápida, segura y fiable los distintos elementos que la conforman.

Una red SAN se distingue de otros modos de almacenamiento en red por el modo de acceso a bajo nivel. El tipo de tráfico en una SAN es muy similar al de los discos duros como ATA,SATA y SCSI. La mayoría de las SAN actuales usan el protocolo SCSI para acceder a los datos de la SAN, aunque no usen interfaces físicas SCSI. Este tipo de redes de datos se han utilizado y se utilizan tradicionalmente en grandes main frames como en IBM, SUN o HP. Aunque recientemente con la incorporación de Microsoft se ha empezado a utilizar en máquinas con sistemas operativos Microsoft.

Una SAN es una red de almacenamiento dedicada que proporciona acceso de nivel de bloque a LUNs. Un LUN, o número de unidad lógica, es un disco virtual proporcionado por la SAN. El administrador del sistema tiene el mismo acceso y los derechos a la LUN como si fuera un disco directamente conectado a la misma. El administrador puede particionar y formatear el disco en cualquier medio que él elija.

Dos protocolos de red utilizados en una SAN son Fibre Channel e iSCSI.

Es de vital importancia que el sitio dónde se encuentre la Red de almacenamiento, se encuentre en un área geográfica distinta a dónde se ubican los servidores que contienen la información crítica; además se trata de un modelo centralizado fácil de administrar, puede tener un bajo costo de

expansión y administración, lo que la hace una red fácilmente escalable; fiabilidad, debido a que se hace más sencillo aplicar ciertas políticas para proteger a la red.

Las SAN se componen de tres capas:

- **Capa Host**. Esta capa consiste principalmente en Servidores, dispositivos ó componentes (HBA, GBIC, GLM) y software (sistemas operativos).
- **Capa Fibra**. Esta capa la conforman los cables (Fibra óptica) así como los SAN Hubs y los SAN switches como punto central de conexión para la SAN.
- **Capa Almacenamiento**. Esta capa la componen las formaciones de discos (Disk Arrays, Memoria Caché, RAIDs) y cintas empleados para almacenar datos.

La red de almacenamiento puede ser de dos tipos:

- **Red Fibre Channel**. La red Fibre Channel es la red física de dispositivos Fibre Channel que emplea Fibre Channel Switches y Directores y el protocolo Fibre Channel Protocol (FCP) para transporte (SCSI-3 serial sobre Fibre Channel).
- **Red IP**. Emplea la infraestructura del estándar LAN con hubs y/o switches Ethernet interconectados. Una SAN IP emplea iSCSI para transporte (SCSI-3 serial sobre IP)

a) NAS.

NAS (del inglés Network Attached Storage) es el nombre dado a una tecnología de almacenamiento dedicada a compartir la capacidad de almacenamiento de un ordenador (Servidor) con ordenadores personales o servidores clientes a través de una red (normalmente TCP/IP), haciendo uso de un Sistema Operativo optimizado para dar acceso con los protocolos CIFS, NFS, FTP o TFTP.

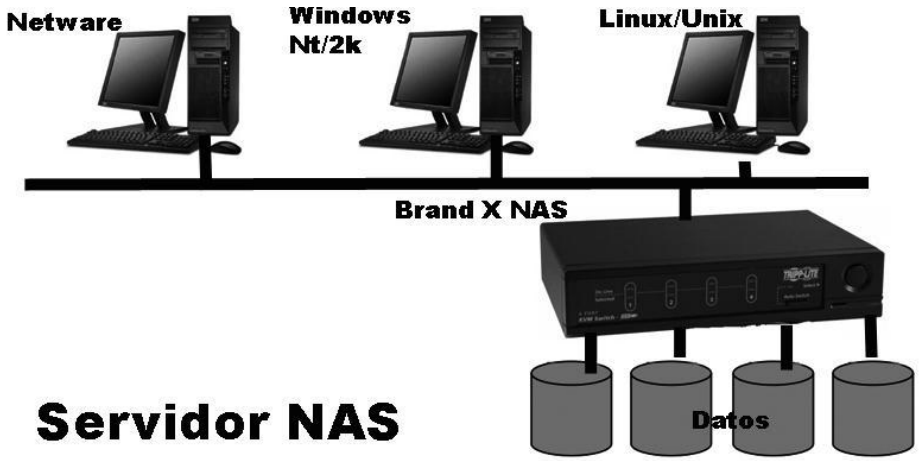
Generalmente, los sistemas NAS son dispositivos de almacenamiento específicos a los que se accede desde los equipos a través de protocolos de red (normalmente TCP/IP). También se podría considerar un sistema NAS a un servidor (Linux, Windows,...) que comparte sus unidades por red, pero la definición suele aplicarse a sistemas específicos.

Los protocolos de comunicaciones NAS están basados en ficheros por lo que el cliente solicita el fichero completo al servidor y lo maneja localmente, están por ello orientados a información almacenada en ficheros de **pequeño tamaño y gran cantidad**. Los protocolos usados son protocolos de compartición de ficheros como NFS, Microsoft Common Internet File System (CIFS).

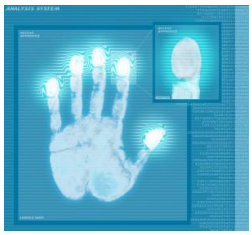
Muchos sistemas NAS cuentan con uno o más dispositivos de almacenamiento para incrementar su capacidad total. Normalmente, estos dispositivos están dispuestos en RAID (Redundant Arrays of Independent Disks) o contenedores de almacenamiento redundante.

NAS es muy útil para proporcionar el almacenamiento centralizado a ordenadores clientes en entornos con grandes cantidades de datos. NAS puede habilitar sistemas fácilmente y con bajo costo con balance de carga, tolerancia a fallos y servidor web para proveer servicios de almacenamiento. El crecimiento del mercado potencial para NAS es el mercado de consumo donde existen grandes cantidades de datos multimedia.

El precio de las aplicaciones NAS ha bajado en los últimos años, ofreciendo redes de almacenamiento flexibles para el consumidor doméstico con costos menores de lo normal, con discos externos USB o FireWire.



7.4. Control de Acceso Lógico.



Los controles de acceso lógico son mecanismos que protegen los sistemas informativos, aplicaciones y datos informáticos. Las contraseñas son un importante control de acceso.

El control de acceso implica quién tiene acceso a sistemas informáticos específicos y recursos en un momento dado. El concepto de control de acceso consta de tres pasos. Estos pasos son la identificación, autenticación y autorización. Con el uso de estos tres principios un administrador del sistema puede controlar que recursos están disponibles para los usuarios de un sistema.

7.4.1. Identificación, autentificación y autorización.

La identificación se refiere las cosas como nombres de usuario y tarjetas de identificación. Es el medio por el cual un usuario del sistema identifica quiénes son. Este paso se realiza generalmente al iniciar sesión.

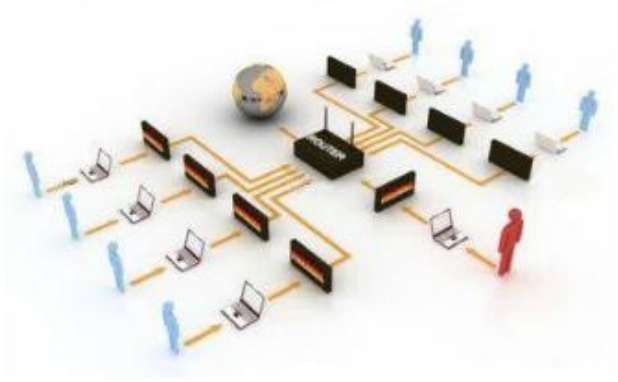
La autenticación es el segundo paso del proceso de control de acceso. Contraseñas, reconocimiento de voz, y escáneres biométricos son métodos comunes de autenticación. El objetivo de la autenticación es para verificar la identidad del usuario del sistema.

La autorización se produce después de que un usuario del sistema se autentica y luego es autorizado a utilizar el sistema. El usuario esta generalmente sólo autorizado a usar una porción de los recursos del sistema en función de su papel en la organización. Por ejemplo, el personal de ingeniería tiene acceso a diferentes aplicaciones y archivos que el personal de finanzas, o recursos humanos no.

Hay más maneras de hacer cumplir el control de acceso además de usar software. El control de acceso se puede mantener por algo tan simple como una puerta cerrada. Sólo los usuarios con la clave correcta o con el uso de una tarjeta se les permitiría entrar.

7.5. Auditorias de Seguridad Informática.

Una **auditoría de seguridad informática** o auditoría de seguridad de sistemas de información (SI) es el estudio que comprende el análisis y gestión de sistemas llevado a cabo por profesionales generalmente por Ingenieros o Ingenieros Técnicos en Informática para identificar, enumerar y posteriormente describir las diversas vulnerabilidades que pudieran presentarse en una revisión exhaustiva de las estaciones de trabajo, redes de comunicaciones o servidores.



Una vez obtenidos los resultados, se detallan, archivan y reportan a los responsables quienes deberán establecer medidas preventivas de refuerzo y/o corrección siguiendo siempre un proceso secuencial que permita a los administradores mejorar la seguridad de sus sistemas aprendiendo de los errores cometidos con anterioridad.

Las auditorías de seguridad de SI permiten conocer en el momento de su realización cuál es la situación exacta de sus activos de información en cuanto a protección, control y medidas de seguridad.

7.5.1. Tipos de auditorías.

Los servicios de auditoría pueden ser de distinta índole:

- **Auditoría de seguridad interna.** En este tipo de auditoría se contrasta el nivel de seguridad y privacidad de las redes locales y corporativas de carácter interno
- **Auditoría de seguridad perimetral.** En este tipo de análisis, el perímetro de la red local o corporativa es estudiado y se analiza el grado de seguridad que ofrece en las entradas exteriores
- **Test de intrusión.** El test de intrusión es un método de auditoría mediante el cual se intenta acceder a los sistemas, para comprobar el nivel de resistencia a la intrusión no deseada. Es un complemento fundamental para la auditoría perimetral.
- **Análisis forense.** El análisis forense es una metodología de estudio ideal para el análisis posterior de incidentes, mediante el cual se trata de reconstruir cómo se ha penetrado en el sistema, a la par que se valoran los daños ocasionados. Si los daños han provocado la inoperabilidad del sistema, el análisis se denomina análisis *postmortem.*
- **Auditoría de páginas web.** Entendida como el análisis externo de la web, comprobando vulnerabilidades como la inyección de código sql, Verificación de existencia y anulación de posibilidades de Cross Site Scripting (XSS), etc.
- **Auditoría de código de aplicaciones.** Análisis del código tanto de aplicaciones páginas Web como de cualquier tipo de aplicación, independientemente del lenguaje empleado

7.6. Criptografía.

La **criptografía** (del griego κρύπτω *krypto*, «oculto», y γράφω *graphos*, «escribir», literalmente «escritura oculta») es el arte o ciencia de cifrar y descifrar información mediante técnicas especiales y es empleada frecuentemente para permitir un intercambio de mensajes que sólo puedan ser leídos por personas a las que van dirigidos y que poseen los medios para descifrarlos.

7.6.1. Objetivos, conceptos, historia.

La finalidad de la criptografía es, en primer lugar, garantizar el secreto en la comunicación entre dos entidades (personas, organizaciones, etc.) y, en segundo lugar, asegurar que la información que se envía es auténtica en un doble sentido: que el remitente sea realmente quien dice ser y que el contenido del mensaje enviado, habitualmente denominado criptograma, no haya sido modificado en su tránsito.

En la actualidad, la criptografía no sólo se utiliza para comunicar información de forma segura ocultando su contenido a posibles "fisgones". Una de las ramas de la criptografía que más ha revolucionado el panorama actual de las tecnologías informáticas es el de la firma digital: tecnología que busca asociar al emisor de un mensaje con su contenido de forma que aquel no pueda posteriormente repudiarlo.

La palabra criptografía es un término genérico que describe todas las técnicas que permiten cifrar mensajes o hacerlos ininteligibles sin recurrir a una acción específica.

La criptografía se basa en la aritmética: En el caso de un texto, consiste en transformar las letras que conforman el mensaje en una serie de números (en forma de bits ya que los equipos informáticos usan el sistema binario) y luego realizar cálculos con estos números para:

- **Modificarlos y hacerlos incomprensibles.** El resultado de esta modificación (el mensaje cifrado) se llama texto cifrado, en contraste con el mensaje inicial, llamado texto simple.
- **Asegurarse de que el receptor pueda descifrarlos.** El hecho de codificar un mensaje para que sea secreto se llama cifrado. El método inverso, que consiste en recuperar el mensaje original, se llama descifrado.

El cifrado normalmente se realiza mediante una clave de cifrado y el descifrado requiere una clave de descifrado. Las claves generalmente se dividen en dos tipos:

- **Las claves simétricas:** son las claves que se usan tanto para el cifrado como para el descifrado. En este caso hablamos de cifrado simétrico o cifrado con clave secreta.
- **Las claves asimétricas:** son las claves que se usan en el caso del cifrado asimétrico (también llamado cifrado con clave pública). En este caso, se usa una clave para el cifrado y otra para el descifrado.

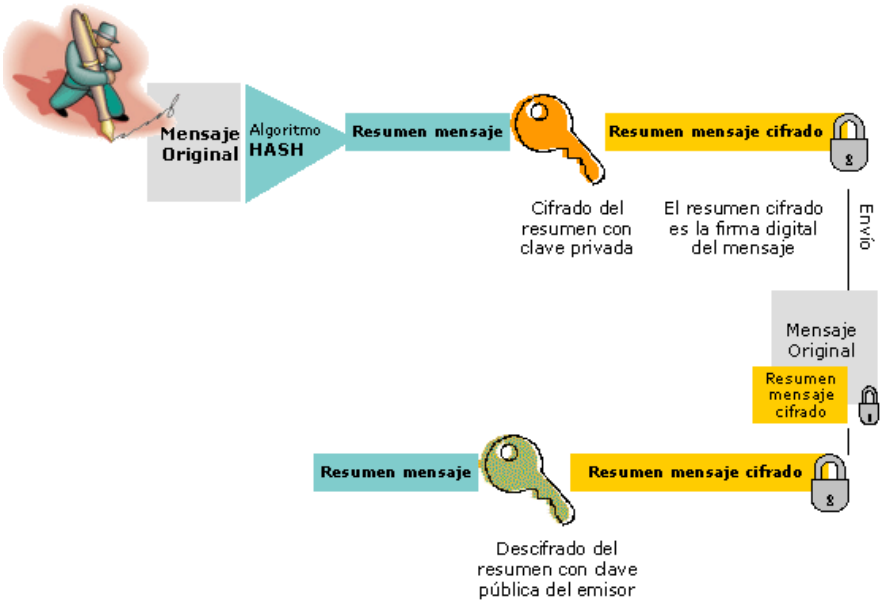
7.6.2. Cifrado y descifrado.

En la jerga de la criptografía, la información original que debe protegerse se denomina texto en claro o texto plano.

El cifrado es el proceso de convertir el texto plano en un galimatías ilegible, denominado texto cifrado o criptograma. Por lo general, la aplicación concreta del algoritmo de cifrado (también llamado cifra) se basa en la existencia de una clave: información secreta que adapta el algoritmo de cifrado para cada uso distinto.

Las dos técnicas más sencillas de cifrado, en la criptografía clásica, son la **sustitución** (que supone el cambio de significado de los elementos básicos del mensaje -las letras, los dígitos o los símbolos-) y la **transposición** (que supone una reordenación de los mismos); la gran mayoría de las cifras clásicas son combinaciones de estas dos operaciones básicas.

El descifrado es el proceso inverso que recupera el texto plano a partir del criptograma y la clave. El protocolo criptográfico especifica los detalles de cómo se utilizan los algoritmos y las claves (y otras operaciones primitivas) para conseguir el efecto deseado. El conjunto de protocolos, algoritmos de cifrado, procesos de gestión de claves y actuaciones de los usuarios, es lo que constituyen en conjunto un criptosistema, que es con lo que el usuario final trabaja e interactúa.

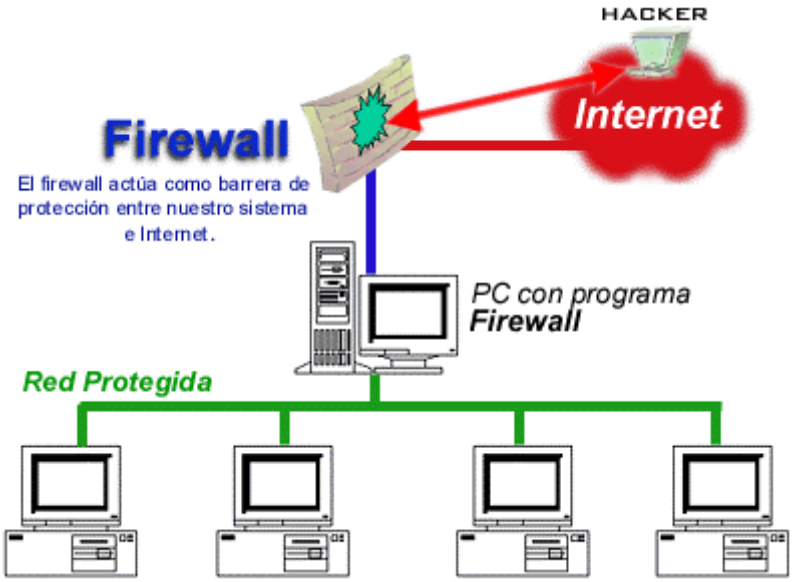


Existen dos grandes grupos de cifras: los algoritmos que usan una única clave tanto en el proceso de cifrado como en el de descifrado, y los que emplean una clave para cifrar mensajes y una clave distinta para descifrarlos. Los primeros se denominan **cifras simétricas**, de clave simétrica o de clave privada, y son la base de los algoritmos de cifrado clásico. Los segundos se denominan **cifras asimétricas**, de clave asimétrica o de clave pública y *forman el núcleo de las técnicas de cifrado modernas.*

8.2. Seguridad Activa y Seguridad Pasiva.

Seguridad activa: Tiene como objetivo proteger y evitar posibles daños en los sistemas informáticos. Podemos encontrar diferentes recursos para evitarlos como:

- Una de esas técnicas que podemos utilizar es el uso adecuado de contraseñas, que podemos añadirles números, mayúsculas, etc.
- También el uso de software de seguridad informática: como por ejemplo ModSecurity, que es una herramienta para la detección y prevención de intrusiones para aplicaciones web, lo que podríamos denominar como "firewall web".
- Y la encriptación de los datos.



Seguridad pasiva: Su fin es minimizar los efectos causados por un accidente, un usuario o malware. Las prácticas de seguridad pasiva más frecuentes y más utilizadas hoy en día son:

- El uso de hardware adecuado contra accidentes y averías.
- También podemos utilizar copias de seguridad de los datos y del sistema operativo.