Seguridad y Alta Disponibilidad

Gema Díaz-Malaguilla Moreno

ÍNDICE

TEMA 1

ADOPCIÓN DE PAUTAS DE SEGURIDAD INFORMÁTICA

1. *Seguridad informática.*

La Seguridad Informática es la disciplina que involucra técnicas, aplicaciones y dispositivos que aseguran la autenticidad, integridad y privacidad de la información contenida dentro de un sistema informático, así como su transmisión.

Técnicamente resulta muy difícil desarrollar un sistema informático que garantice la completa seguridad de la información, sin embargo, el avance de la tecnología ha posibilitado la disposición de mejores medidas de seguridad para evitar daños y problemas que puedan ser aprovechados por los intrusos. Dentro de la seguridad informática se pueden mencionar dos tipos:

- **Seguridad lógica:** Conjunto de medidas de seguridad y herramientas informáticas de control de acceso a los sistemas informáticos.

- **Seguridad física:** Controles externos al ordenador, que tratan de protegerlo contra amenazas de naturaleza física como incendios, inundaciones, etc.

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.

- **Código malicioso:** es cualquier software que entra en un sistema de cómputo sin ser invitado e intenta romper las reglas, esto incluye caballos de Troya, virus, gusanos informáticos, bombas lógicas y otras amenazas programadas.

- **Virus:** este tipo de código malicioso tiene como principal característica la capacidad de duplicarse a si mismo usando recursos del sistema infectado, propagando su infección rápidamente.

- **Troyanos:** este tipo de código se presenta escondido en otros programas de aplicación aparentemente inofensivos, para posteriormente activarse de manera discreta cumpliendo su propósito nocivo.

- **Gusanos:** es muy similar a los virus, con la diferencia de que éstos aprovechan más los recursos de los sistemas infectados, atacando diferentes programas y posteriormente duplicándose para redistribuirse.

- **Errores de programación y diseño**: el software creado para cumplir alguna función dentro de la organización (Por ejemplo un sistema de transacciones financieras, sistema de nomina, sistemas operativos, etc.) también pueden causar perdida o modificación de la información. Esto ocurre cuando el software en cuestión no cumple con los estándares de seguridad requeridos pues nunca fue diseñado para dar soporte a una organización. Los errores de programación y fallas generales que puede tener un software de aplicación también representan una amenaza.

3.3. Datos

Las redes pueden llegar a ser lugares muy vulnerables para los datos, al tratarse de una serie de equipos conectados entre sí compartiendo recursos, es posible atacar a toda la red para atacar la información que se comparte en la misma, penetrando primero en uno de los equipos y posteriormente expandirse al resto.

En una red la prioridad es la transmisión de la información, así que todas las vulnerabilidades están relacionadas directamente con la posible intercepción de la información por personas no autorizadas y con fallas en la disponibilidad del servicio, así como la pérdida de privacidad ó robo de información.

La información es el elemento más sensible de todo el sistema informático, por lo que conlleva el riesgo de accesos no autorizados, que utilicen esa información o que la modifiquen, lo que puede ser mucho más grave.

4. Análisis de las principales vulnerabilidades del sistema informático.

Existen diferentes vulnerabilidades que, dependiendo de sus características, las podemos clasificar e identificar en los siguientes tipos:

De configuración

Si la gestión administrable por el usuario es tal que hace que el sistema sea vulnerable, la vulnerabilidad no es debida al diseño del mismo si no a cómo el usuario final configura el sistema. También se considera error de este tipo cuando la configuración por defecto del sistema es insegura, por ejemplo una aplicación recién instalada que cuenta de base con usuarios por defecto.

Validación de entrada

Este tipo de vulnerabilidad se produce cuando la entrada que procesa un sistema no es comprobada adecuadamente de forma que una vulnerabilidad puede ser aprovechada por una cierta secuencia de entrada.

Salto de directorio

Ésta aprovecha la falta de seguridad de un servicio de red para desplazarse por el árbol de directorios hasta la raíz del volumen del sistema. El atacante podrá entonces desplazarse a través de las carpetas de archivos del sistema operativo para ejecutar una utilidad de forma remota.

Seguimiento de enlaces

Se producen cuando no existe una protección lo suficientemente robusta que evite el acceso a un directorio o archivo desde un enlace simbólico o acceso directo.

Secuencias de comandos en sitios cruzados (XSS)

Este tipo de vulnerabilidad abarca cualquier ataque que permita ejecutar código de "scripting", comoVBScript o javascript, en el contexto de otro dominio. Estos errores se pueden encontrar en cualquier aplicación HTML, no se limita a sitios web, ya que puede haber aplicaciones locales vulnerables aXSS, o incluso el navegador en si. El problema esta en que normalmente no se validan correctamente los datos de entrada que son usados en cierta aplicación. Hay dos tipos:

Indirecta: consiste en modificar valores que la aplicación web utiliza para pasar variables entre dos páginas, sin usar sesiones.

Directa: consiste en localizar puntos débiles en la programación de los filtros.

Inyección de comandos en el sistema operativo

Hablamos de este tipo de vulnerabilidad para referirnos a la capacidad de un usuario, que controla la entrada de comandos (bien a través de un terminal de Unix/Linux o del interfaz de comando deWindows), para ejecutar instrucciones que puedan comprometer la integridad del sistema.

Inyección SQL

Inyección SQL es una vulnerabilidad informática en el nivel de base de datos de una aplicación. El origen es el filtrado incorrecto de las variables utilizadas en las partes del programa con código SQL.

Una inyección de código SQL sucede cuando se inserta un trozo de código SQL dentro de otro código SQL con el fin de modificar su comportamiento, haciendo que ejecute el código malicioso en la base de datos.

El hecho de que un servidor pueda verse afectado por las inyecciones SQL se debe a la falta de medidas de seguridad por parte de sus diseñadores/programadores, especialmente por una mala filtración de las entradas (por formularios, cookies o parámetros).

Inyección de código

Aquí encontramos distintos sub-tipos dentro de esta clase de vulnerabilidad:

Inyección directa de código estático: el software permite que las entradas sean introducidas directamente en un archivo de salida que se procese más adelante como código, un archivo de la biblioteca o una plantilla. En una inyección de código de tipo estático o también llamada permanente, una vez inyectado el código en una determinada parte de la aplicación web, este código queda almacenado en una base de datos. Una de las soluciones más apropiadas es asumir que toda la entrada es malévola. También es posible utilizar una combinación apropiada de listas negras y listas blancas para asegurar que solamente las entradas válidas y previstas son procesadas por el sistema.

Evaluación directa de código dinámico: el software permite que las entradas sean introducidas directamente en una función que evalúa y ejecuta dinámicamente la entrada como código, generalmente en la misma lengua que usa el producto. En una inyección de código de tipo dinámico o no permanente la inyección tiene un tiempo de vida limitado y no se almacena, al menos permanentemente, en ningún sitio. Las soluciones más apropiadas son las mismas que para la inyección directa de código estático.

Inclusión remota de archivo PHP: vulnerabilidad existente únicamente en paginas dinámicas escritas en PHP está debida a la inclusión de la función include() la cual permite el enlace de archivos situados en otros servidores, mediante los cuales se puede ejecutar código PHP en el servidor.

Formato de cadena

Nos referimos a este tipo de vulnerabilidad cuando se produce a través de cadenas de formato controladas externamente, como el tipo de funciones "printf" en el lenguaje "C" que pueden conducir a provocar desbordamientos de búfer o problemas en la representación de los datos.

Revelación/Filtrado de información

Un filtrado o escape de información puede ser intencionado o no intencionado. En este aspecto los atacantes pueden aprovechar esta vulnerabilidad para descubrir el directorio de instalación de una aplicación, la visualización de mensajes privados, etc. La severidad de esta vulnerabilidad depende del tipo de información que se puede filtrar.

Gestión de credenciales

Este tipo de vulnerabilidad tiene que ver con la gestión de usuarios, contraseñas y los ficheros que almacenan este tipo de información. Cualquier debilidad en estos elementos es considerado como una vulnerabilidad que puede ser explotada por un atacante.

Permisos, privilegios y/o control de acceso

Se produce cuando el mecanismo de control de acceso o asignación de permisos es defectuoso. Hay que tener en cuenta que se trata del sistema en sí y no se debe confundir con una mala gestión por parte del administrador.

Fallo de autenticación

Esta vulnerabilidad se produce cuando la aplicación o el sistema no es capaz de autenticar al usuario, proceso, etc. correctamente.

Carácter criptográfico

La generación de números aleatorios para generar secuencias criptográficas, la debilidad o distintos fallos en los algoritmos de encriptación así como defectos en su implementación estarían ubicados dentro de este tipo de vulnerabilidad.

Falsificación de petición en sitios cruzados (CSRF)

Este tipo de vulnerabilidad afecta a las aplicaciones web con una estructura de invocación predecible. El agresor puede colocar en la página cualquier código, el cual posteriormente puede servir para la ejecución de operaciones no planificadas por el creador del sitio web, por ejemplo, capturar archivos cookies sin que el usuario se percate.

El tipo de ataque CSRF más popular se basa en el uso del marcador HTML <img>, el cual sirve para la visualización de gráficos. En vez del marcador con la URL del archivo gráfico, el agresor pone un tag que lleva a un código JavaScript que es ejecutado en el navegador de la víctima.

Condición de carrera

Una condición de carrera se produce cuando varios procesos tratan de acceder y manipular los mismos datos simultáneamente. Los resultados de la ejecución dependerán del orden particular en que el acceso se lleva a cabo. Una condición de carrera puede ser interesante para un atacante cuando ésta puede ser utilizada para obtener acceso al sistema.

Error de búfer

Un búfer es una ubicación de la memoria en una computadora o en un instrumento digital reservada para el almacenamiento temporal de información digital, mientras que está esperando ser procesada.

El desbordamiento del búfer: un búfer se desborda cuando, de forma incontrolada, al intentar meter en él más datos de los que caben, ese exceso se vierte en zonas del sistema causando daños.

El agotamiento del búfer: es un estado que ocurre cuando un búfer usado para comunicarse entre dos dispositivos o procesos se alimenta con datos a una velocidad más baja que los datos se están leyendo en ellos.

Errores numéricos

El desbordamiento de entero (integer overflow): un desbordamiento del número entero ocurre cuando una operación aritmética procura crear un valor numérico que sea más grande del que se puede representar dentro del espacio de almacenaje disponible. Por ejemplo, la adición de 1 al valor más grande que puede ser representado constituye un desbordamiento del número entero.

El agotamiento de entero (integer underflow): consiste en que un valor se resta de otro, que es menor que el valor mínimo del número entero, y que produce un valor que no es igual que el resultado correcto.

Error en la gestión de recursos

El sistema o software que adolece de este tipo de vulnerabilidad permite al atacante provocar un consumo excesivo en los recursos del sistema (disco, memoria y CPU). Esto puede causar que el sistema deje de responder y provocar denegaciones de servicio.

Error de diseño

En ocasiones los programadores bien por culpa de los entornos de trabajo o bien por su metodología de programación, cometen errores en el diseño de las aplicaciones. Esto provoca que puedan aparecer fallos de seguridad y la consiguiente vulnerabilidad. También se puede aplicar el "error de diseño" si no hay fallos en la implementación ni en la configuración de un sistema, si no que el diseño inicial es erróneo.

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.

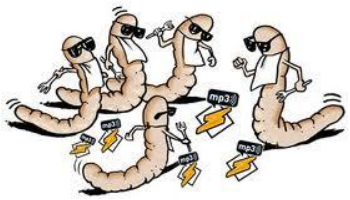
f) Virus

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

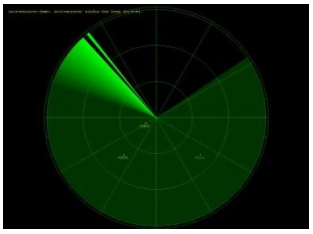
Normalmente se reciben por anticipado los avisos de tormentas, tempestades, tifones y catástrofes sísmicas similares. Las condiciones atmosféricas severas se asocian a ciertas partes del mundo y la probabilidad de que ocurran está documentada.

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.

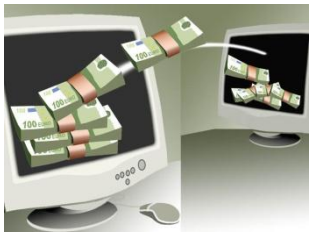
7) Acciones Hostiles

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.



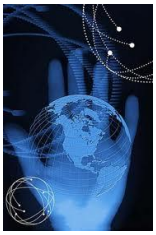
c) **Sabotaje**

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.

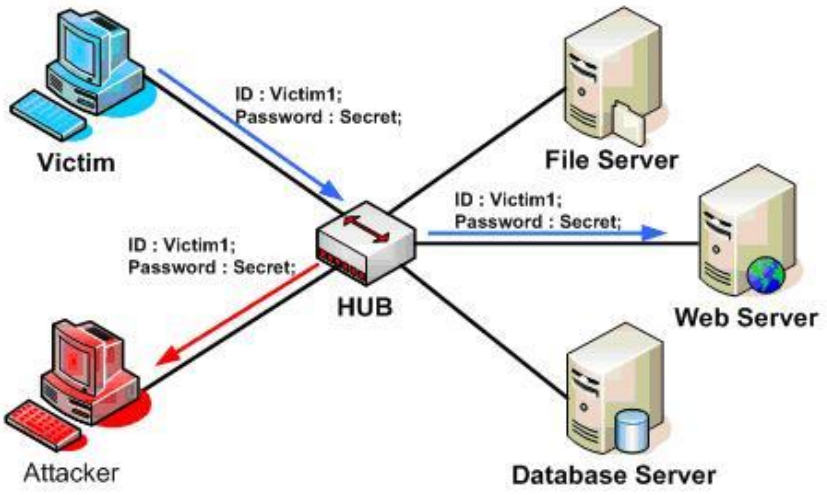
➢ Protección de los datos

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.



El problema de este tipo de ataque es que en principio es completamente pasivo y en general difícil de detectar mientras se produce.

Para evitar que funcionen los *sniffer* existen diversas soluciones, aunque al final la única realmente útil es cifrar toda la información que viaja por la red.

- **Copias de seguridad**

Los medios donde residen estas copias tendrán que estar protegidos físicamente; de hecho quizás deberíamos de emplear medidas más fuertes, ya que en realidad es fácil que en una sola cinta haya copias de la información contenida en varios servidores.

Lo más recomendable es guardar las copias en una zona alejada de la sala de operaciones; lo que se suele recomendar es disponer de varios niveles de copia, una que se almacena en una caja de seguridad en un lugar alejado y que se renueva con una periodicidad alta y otras de uso frecuente que se almacenan en lugares más próximos.

Para proteger más aun la información copiada se pueden emplear mecanismos de cifrado.

- **Soportes no electrónicos**

Otro elemento importante en la protección de la información son los elementos no electrónicos que se emplean para transmitirla, fundamentalmente el papel.

Cualquier dispositivo por el que pueda salir información de nuestro sistema ha de estar situado en un lugar de acceso restringido; también es conveniente que sea de acceso restringido el lugar donde los usuarios recogen los documentos que lanzan a estos dispositivos.

Además de esto es recomendable disponer de trituradoras de papel para destruir todos los papeles o documentos que se quieran destruir, ya que evitaremos que un posible atacante pueda obtener información rebuscando en nuestra basura.

6.2. Sistemas de alimentación ininterrumpida.

Un **sistema de alimentación ininterrumpida**, **SAI** (en inglés *Uninterruptible Power Supply*, ***UPS***), es un dispositivo que gracias a sus baterías, puede proporcionar energía eléctrica tras un apagón a todos los dispositivos que tenga conectados. Otra de las funciones de los UPS es la de mejorar la calidad de la energía eléctrica que llega a las cargas, filtrando subidas y bajadas de tensión y eliminando armónicos de la red en el caso de usar corriente alterna.

Los UPS dan energía eléctrica a equipos llamados cargas críticas, como pueden ser aparatos médicos, industriales o informáticos, incluso se utilizan en servidores y ordenadores de casi cualquier oficina o empresa, que requieren tener siempre alimentación y que ésta sea de calidad, debido a la necesidad de estar en todo momento operativos y sin fallos (picos o caídas de tensión).

Los cortes en el suministro eléctrico, pueden producir en nuestro sistema informático:

- Destrucción de la información.
- Daño en las infraestructuras (ordenadores, servidores…).
- Estrés y desmotivación de las personas que lo utilizan.
- Afecta a la productividad.
- Genera pérdidas.

Un SAI está formado por una o varias baterías y un convertidor de corriente que transforma la energía continua en alterna, y la eleva hasta obtener una tensión de 220V. Los SAI disponen de unos conectores que se enchufan a los equipos a alimentar.

Los SAI normalmente tienen una autonomía de unos 10 minutos, aunque existen modelos de gran autonomía de servicios. Esta autonomía está directamente relacionada con el consumo que tengan los dispositivos conectados al SAI.

A la hora de elegir un SAI debemos tener en cuenta la potencia que necesitamos para alimentar los dispositivos que queremos proteger, en función de eso compraremos un SAI de una potencia algo superior a la que necesitamos.

Fallos comunes en el suministro de energía eléctrica

El papel del UPS es suministrar potencia eléctrica en ocasiones de fallo de suministro, en un intervalo de tiempo "corto". (Si es un fallo en el suministro de la red, hasta que comiencen a funcionar los sistemas aislados de emergencia). Sin embargo, muchos sistemas de alimentación ininterrumpida son capaces de corregir otros fallos de suministro:

- Corte de energía: pérdida total de tensión de entrada.
- Sobretensión: tiene lugar cuando la tensión supera el 110% del valor nominal.
- Caída de tensión: cuando la tensión es inferior al 85-80% de la nominal.
- Picos de tensión.
- Ruido eléctrico.
- Inestabilidad en la frecuencia.
- Distorsión armónica, cuando la onda sinusoidal suministrada no tiene esa forma.

6.2.1. Tipos de sai.

Podemos distinguir tres tipos de SAI según su tipo de alimentación:

- **Off-line:** la alimentación viene de la **red eléctrica** y en caso de fallo de suministro el dispositivo empieza a generar su propia alimentación. Debido a que *no son activos*, hay un pequeño tiempo en el que no hay suministro eléctrico. Típicamente generan una forma de onda que no es sinusoidal, por lo que *no son adecuados para proteger dispositivos delicados o sensibles a la forma de onda de su alimentación.* Su uso más común es en la protección de dispositivos domésticos como ordenadores, monitores, televisores, etc.

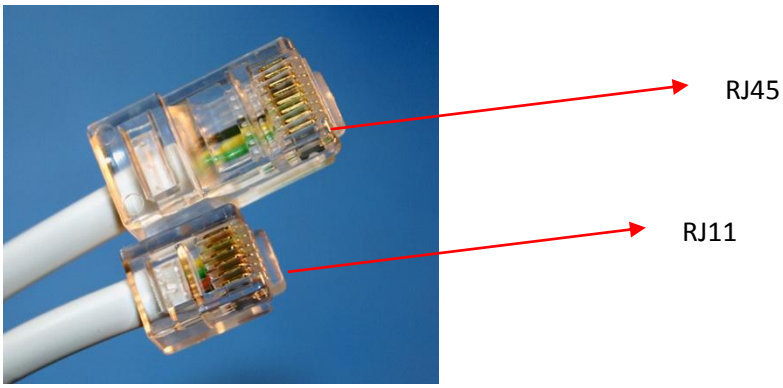
- **In-line:** también conocido como de "línea interactiva". Es similar al off-line, pero dispone de filtros activos que estabilizan la tensión de entrada. *Sólo en caso de fallo de tensión o anomalía grave empiezan a generar su propia alimentación.* Al igual que los SAI de tipo off-line tienen un pequeño tiempo de conmutación en el que no hay suministro eléctrico. Típicamente generan una forma de onda pseudo-sinusoidal o sinusoidal de mayor calidad que los SAI off-line. **Su uso más común es en la protección de dispositivos en pequeños comercios o empresas,** tales como ordenadores, monitores, servidores, cámaras de seguridad y videograbadores, etc.

- **On-line:** el más sofisticado de todos. **El dispositivo genera una alimentación limpia con una onda sinusoidal perfecta en todo momento a partir de sus baterías.** Para evitar que se descarguen las carga al mismo tiempo que genera la alimentación. Por tanto, en caso de fallo o anomalía en el suministro los dispositivos protegidos no se ven afectados en ningún momento porque no hay un tiempo de conmutación. Su principal inconveniente es que las baterías están constantemente trabajando, por lo que deben sustituirse con más frecuencia. **Su uso más común es**

en la protección de dispositivos delicados o de mucho valor en empresas, tales como servidores, electrónica de red, ordenadores de monitorización, videograbadores y cámaras de seguridad, etc.

6.2.2. Tipos de conexiones SAI.

- La mayoría de los SAI tienen **dos conectores RJ11** para proteger los equipos conectados a una línea telefónica, en caso de que la línea reciba una sobretensión. En uno se conecta la línea de entrada y al otro se conectan los dispositivos a proteger. A veces se proporciona un conector RJ45, que es compatible con el RJ11 y permite proteger líneas de datos también.



- Del mismo modo, la mayoría de los SAI tienen una salida **RS-232** y/o USB para conectarlos a un ordenador. Mediante el software adecuado, el ordenador es capaz de conocer el estado del SAI y de autoapagarse en caso de que tras un fallo de suministro prolongado, el ordenador vaya a quedarse sin alimentación. *Esto es adecuado si cada ordenador se protege con un SAI, pero insuficiente si un SAI protege varios ordenadores al mismo tiempo.*

RS-232

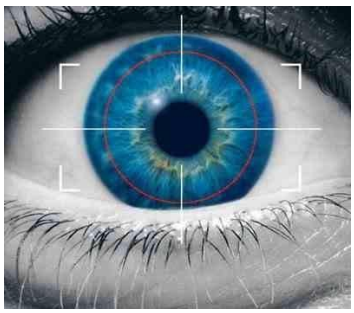
USB

- Algunos SAI permiten la conexión de una tarjeta de red que permite extender la función anterior a los ordenadores de toda una red. De este modo, si un SAI protege varios ordenadores, todos ellos pueden conocer su estado y apagarse ordenadamente antes de quedarse sin suministro eléctrico. Esto es especialmente importante en servidores empresariales donde un fallo eléctrico podría ocasionar la pérdida de información.

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.

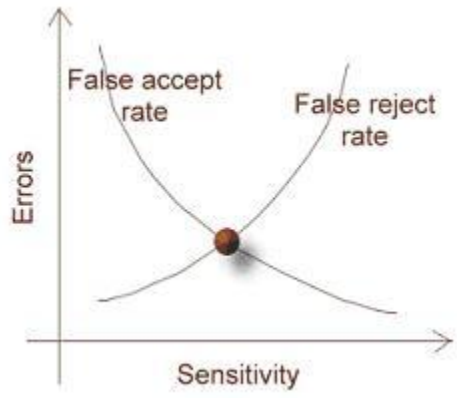
Las huellas dactilares, las retinas, el iris, los patrones faciales, de venas de la mano o la geometría de la palma de la mano, representan ejemplos de características físicas (estáticas), mientras que entre los ejemplos de características del comportamiento se incluye la firma, el paso y el tecleo (dinámicas). 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).



En los sistemas biométricos reales el FAR y el FRR pueden transformarse en los demás cambiando cierto parámetro. Una de las medidas más comunes de los sistemas biométricos reales es la tasa en la que el ajuste en el cual acepta y rechaza los errores es igual: la tasa de error igual (*Equal Error Rate* o EER), también conocida como la tasa de error de cruce (*Cross-over Error Rate* o CER). Cuanto más bajo es el EER o el CER, se considera que el sistema es más exacto.

Las tasas de error anunciadas implican a veces elementos idiosincrásicos o subjetivos. Por ejemplo, un fabricante de sistemas biométricos fijó el umbral de aceptación alto, para reducir al mínimo las falsas aceptaciones; en la práctica, se permitían tres intentos, por lo que un falso rechazo se contaba sólo si los tres intentos resultaban fallidos (por ejemplo escritura, habla, etc.), las opiniones pueden variar sobre qué constituye un falso rechazo. Si entro a un sistema de verificación de firmas usando mi inicial y apellido, ¿puedo decir legítimamente que se trata de un falso rechazo cuando rechace mi nombre y apellido? A pesar de estas dudas, los sistemas biométricos tienen un potencial para identificar a individuos con un grado de certeza muy alto. La prueba forense del ADN goza de un grado particularmente alto de confianza pública actualmente y la tecnología está orientándose al reconocimiento del iris, que tiene la capacidad de diferenciar entre dos individuos con un ADN idéntico.

ESTANDARES

En los últimos años se ha notado una preocupación creciente por las organizaciones regulatorias respecto a elaborar estándares relativos al uso de técnicas biométricas en el ambiente informático. Esta preocupación es reflejo del creciente interés industrial por este ámbito tecnológico, y a los múltiples beneficios que su uso aporta. No obstante ello, aún la estandarización continua siendo deficiente y como resultado de ello, los proveedores de soluciones biométricas continúan suministrando interfaces de software propietarios para sus productos, lo que dificulta a las empresas el cambio de producto o vendedor.

A nivel mundial el principal organismo que coordina las actividades de estandarización biométrica es el Sub-Comité 17 (SC17) del Joint Technical Committee on Information Technology (ISO/IEC JTC1), del International Organization for Standardization (ISO) y el International Electrotechnical Commission (IEC).

En Estados Unidos desempeñan un papel similar el Comité Técnico M1 del INCITS (InterNational Committee for Information Technology Standards), el National Institute of Standards and Technology (NIST) y el American National Standards Institute (ANSI).

Existen además otros organismos no gubernamentales impulsando iniciativas en materias biométricas tales como: Biometrics Consortium, International Biometrics Groups y BioAPI. Este último se estableció en Estados Unidos en 1998 compuesto por las empresas Bioscrypt, Compaq, Iridiam, Infineon, NIST, Saflink y Unisis. El Consorcio BioAPI desarrolló conjuntamente con otros

consorcios y asociaciones, un estándar que promoviera la conexión entre los dispositivos biométricos y los diferentes tipos de programas de aplicación, además de promover el crecimiento de los mercados biométricos.

Algunos de los estándares más importantes son:

- **Estándar ANSI X.9.84**: creado en 2001, por la ANSI (American National Standards Institute) y actualizado en 2003, define las condiciones de los sistemas biométricos para la industria de servicios financieros haciendo referencia a la transmisión y almacenamiento seguro de información biométrica, y a la seguridad del hardware asociado.

- **Estándar ANSI / INCITS 358:** creado en 2002 por ANSI y BioApi Consortium, presenta una interfaz de programación de aplicación que garantiza que los productos y sistemas que cumplen este estándar son interoperables entre sí.

- **Estándar NISTIR 6529:** también conocido como CBEFF (Common Biometric Exchange File Format) es un estándar creado en 1999 por NIST y Biometrics Consortium que propone un formato estandarizado (estructura lógica de archivos de datos) para el intercambio de información biométrica.

- **Estándar ANSI 378:** creado en 2004 por la ANSI, establece criterios para representar e intercambiar la información de las *huellas dactilares* a través del uso de minucias. El propósito de esta norma es que un sistema biométrico dactilar pueda realizar procesos de verificación de identidad e identificación, empleando información biométrica proveniente de otros sistemas.

- **Estándar ISO 19794-2:** creado en 2005 por la ISO/IEC con propósitos similares a la norma ANSI 378, respecto a la que guarda mucha similitud.

- **Estándar PIV-071006:** creado en 2006 por el NIST y el FBI en el contexto de la norma FIPS 201 del gobierno de EE.UU, establece los criterios de calidad de imagen que deben cumplir los lectores de huellas dactilares para poder ser usados en procesos de verificación de identidad en agencias federales.

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**.

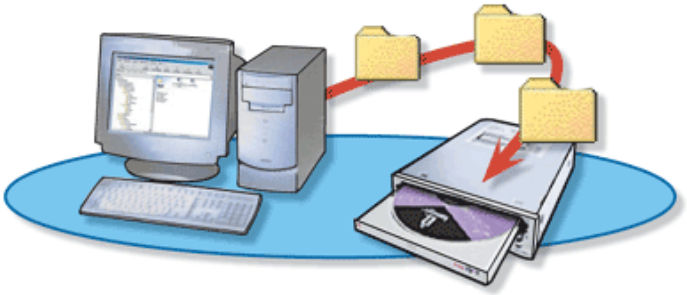
La periodicidad para realizar las copias de seguridad de nuestros datos, dependerá del mayor o menor movimiento de información que realicemos en nuestro equipo.

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

7.1.1. Tipos de copias de seguridad.

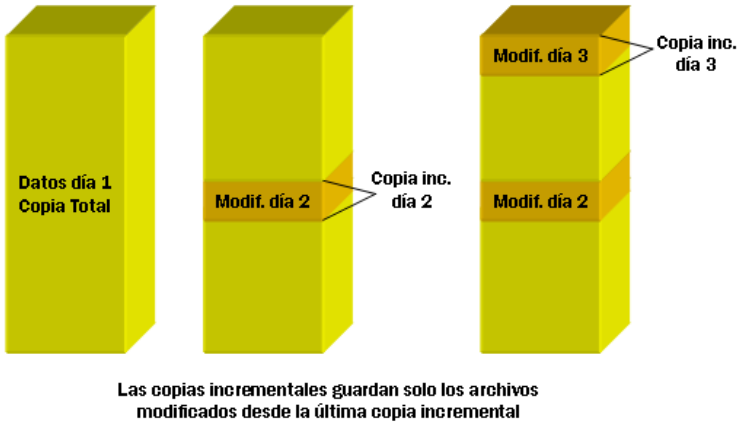
Existen varios tipos de copias de seguridad según los datos que respaldemos en ellas:

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.

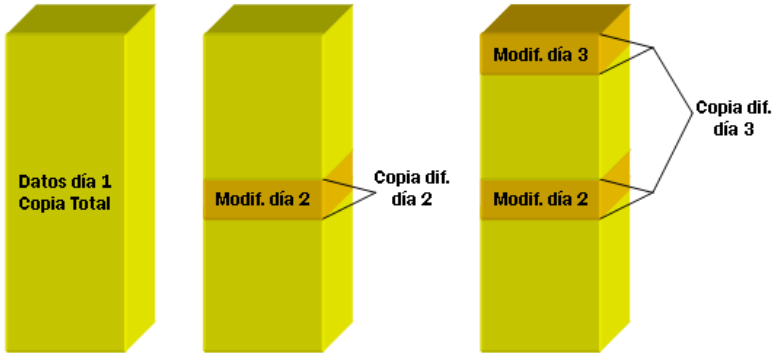
Ejemplo, si hacemos copia de seguridad total el día 1 de cada mes y copia de seguridad incremental el resto de los días, cada copia incremental solo guardará los archivos que se hayan modificado ese día. Si tenemos que realizar la restauración de archivos ante un desastre, debemos disponer de la copia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

7.2. Imágenes de respaldo.

Una **imagen de disco** es un archivo o un dispositivo que contiene la estructura y contenidos completos de un dispositivo o medio de almacenamiento de datos, como un disco duro, un disquete o un disco óptico (CD, DVD). Una imagen de disco usualmente se produce creando una copia completa, sector por sector, del medio de origen y por lo tanto *replicando perfectamente la estructura y contenidos de un dispositivo de almacenamiento.*

Algunas herramientas de creación de imágenes de disco omiten el espacio no utilizado del medio de origen, o comprimen el disco que representan para reducir los requisitos de almacenamiento, aunque estos se conocen comúnmente como archivos comprimidos, ya que no son literalmente imágenes de disco.

Debemos hacer una distinción entre imagen del sistema y copia de respaldo de datos. Por lo general, las copias de respaldo son hechas de forma continua o de manera muy regular, seleccionando los directorios a respaldar y casi siempre de forma incremental.

En cambio, el sistema cambia muy poco por lo que no hay necesidad de crear una imagen frecuentemente. Para crear una imagen, debemos elegir la partición y no los directorios. La copia de seguridad incremental consiste en hacer una copia de respaldo de todo lo que se especificó la primera vez, luego solamente de los archivos modificados posteriormente, guardando aparte una copia del archivo original. Por lo tanto, copia de respaldo e imagen del sistema son dos cosas muy distintas en cuanto a sus objetivos y métodos.

La creación de una imagen nos permite el ahorro de tiempo, por ejemplo tenemos un equipo con un sistema operativo instalado y varios aplicaciones que hemos tardado en configurar de media unas 3 horas, si creamos una imagen de esa configuración su restauración en otro equipo o partición no duraría más de 20 minutos.

PROCESO DE CREACIÓN.

El crear una imagen de disco se consigue con un programa adecuado. Distintos programas de creación de imágenes poseen capacidades diferentes, y pueden enfocarse en la creación de imágenes de discos duros (incluyendo la generación de copias de seguridad y restauración de discos duros), o de medios ópticos (imágenes de CD/DVD).

Creación de imágenes de discos duros

La creación de imágenes de discos duros es usada en varias áreas de aplicaciones mayores:

- **La *creación de imágenes forense*** es el proceso en el cual los contenidos enteros del disco duro son copiados a un archivo y los valores checksum son calculados para verificar la integridad del archivo de imagen. Las imágenes forenses son obtenidas mediante el uso de herramientas de software (algunas herramientas de clonación de hardware han añadido funcionalidades forenses).

- **La *clonación de discos duros***, es habitualmente usada para replicar los contenidos de un disco duro para usarlos en otro equipo. Esto puede ser hecho por programas de solo software ya que solo requiere la clonación de la estructura de archivos y los archivos mismos.

- **La *creación de imágenes para recuperación de datos*** (al igual que en la creación de imágenes forense) es el proceso de pasar a una imagen cada sector en el disco duro de origen a otro medio del cual los archivos necesarios puedan ser recuperados. En situaciones de recuperación de datos, uno no puede confiar en la integridad de la estructura de archivos y por lo tanto una copia de sector completa es obligatoria (también similar a la creación de imágenes forense).

7.3. Medios de almacenamiento.

Los materiales físicos en donde se almacenan los datos se conocen como **medios de almacenamiento** o **soportes de almacenamiento**. Ejemplos de estos medios son los discos magnéticos (disquetes, discos duros), los discos ópticos (CD, DVD), las cintas magnéticas, los discos magneto-ópticos (discos Zip, discos Jaz, uperDisk), las tarjetas de memoria, etc.

Los componentes de hardware que escriben o leen datos en los medios de almacenamiento se conocen como dispositivos o unidades de almacenamiento. Por ejemplo, una disquetera o una unidad de disco óptico, son dispositivos que realizan la lectura y/o escritura en disquetes y discos ópticos, respectivamente.

El propósito de los dispositivos de almacenamiento es almacenar y recuperar la información de forma automática y eficiente.

El almacenamiento se relaciona con dos procesos:

- Lectura de datos almacenados para luego transferirlos a la memoria de la computadora.
- Escritura o grabación de datos para que más tarde se puedan recuperar y utilizar.

Los medios de almacenamiento han evolucionado en forma notable desde las primeras computadoras. En la actualidad existe una gran variedad tecnologías y dispositivos nuevos, pero el disco rígido sigue siendo el "almacén" principal de la información en la computadora.

7.3.1. Soportes de almacenamiento.

Los soportes de almacenamiento, como nombre lo indica son implementos internos y externos de hardware de un ordenador, cuya función es la de almacenar datos, ya sean estos para ingresarlos o extraerlos de un PC.

Los soportes de almacenamiento se pueden clasificar de acuerdo al modo de acceso a los datos que contienen:

- ***Acceso secuencial:*** En el acceso secuencial, el elemento de lectura del dispositivo debe pasar por el espacio ocupado por la totalidad de los datos almacenados previamente al espacio ocupado físicamente por los datos almacenados que componen el conjunto de información a la que se desea acceder.

- ***Acceso aleatorio:*** En el modo de acceso aleatorio, el elemento de lectura accede directamente a la dirección donde se encuentra almacenada físicamente la información que se desea localizar sin tener que pasar previamente por la almacenada entre el principio de la superficie de grabación y el punto donde se almacena la información buscada.

  Podemos dividir los soportes en tres grupos:

  - Memorias
  - Soportes magnéticos.
  - Soportes ópticos.
  - Soportes extraíbles.

MEMORIAS.

Son dispositivos que retienen datos informáticos durante algún intervalo de tiempo. Las memorias de ordenadores proporcionan una de las principales funciones de la computación moderna, la retención o almacenamiento de información.

- ***Memoria ROM**:* Esta memoria es sólo de lectura, y sirve para almacenar el programa básico de iniciación, instalado desde fábrica. Este programa entra en función en cuanto se enciende el equipo y su primer función es la de reconocer los dispositivos del ordenador.

- ***Memoria RAM**:* Esta es la denominada memoria de acceso aleatorio, tiene la característica de ser volátil, esto es, que sólo opera mientras esté encendida la computadora. En ella son almacenadas tanto las instrucciones que necesita ejecutar el microprocesador como los datos que introducimos y deseamos procesar, así como los resultados obtenidos de esto. La RAM almacena todos los datos y programas que se están ejecutando en un momento dado. Esta memoria se puede leer y escribir en ella.

SOPORTES MAGNÉTICOS.

Las superficies de los disquetes, discos duros y cintas magnéticas están recubiertas con partículas de un material magnético sensible (por lo general óxido de hierro) que reacciona a un campo magnético.

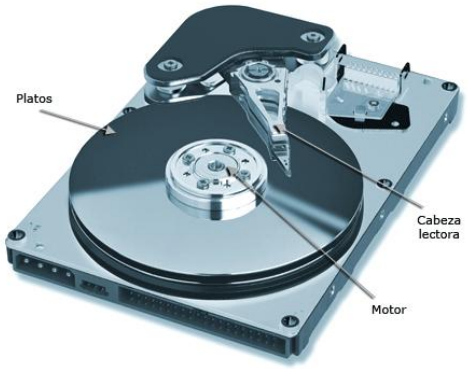
Cada partícula actúa como un imán, creando un campo magnético cuando se somete a un electroimán.

Las cabezas de lectura/escritura de la unidad, contienen electroimanes y graban cadenas de 1 y 0, alternando la dirección de la corriente en esos electroimanes.

- ***Cinta Magnética:*** Esta formada por una cinta de material plástico recubierta de material ferromagnético, sobre dicha cinta se registran los caracteres en formas de combinaciones de puntos, sobre pistas paralelas al eje longitudinal de la cinta. Estas cintas son soporte de tipo secuencial, esto supone un inconveniente puesto que para acceder a una información determinada se hace necesario leer todas las que le preceden, con la consiguiente pérdida de tiempo.

- ***Tambores Magnéticos:*** Están formados por cilindros con material magnético capaz de retener información, esta se graba y lee mediante un cabezal cuyo brazo se mueve en la dirección del eje de giro del tambor. El acceso a la información es directo y no secuencial.

- ***Disco Duro:*** Son en la actualidad el principal subsistema de almacenamiento de información en los sistemas informáticos. Es un dispositivo encargado de almacenar información de forma persistente en un ordenador, es considerado el sistema de almacenamiento más importante del ordenador y en él se guardan los archivos de los programas.



- ***Disquette o Disco flexible:*** Un disco flexible o también disquette (en inglés floppy disk), es un tipo de dispositivo de almacenamiento de datos formado por una pieza circular de un material magnético que permite la grabación y lectura de datos, fino y flexible (de ahí su denominación) encerrado en una carcasa fina cuadrada o rectangular de plástico. Los discos, usados usualmente son los de 3 ½ o 5 ¼ pulgadas, utilizados en ordenadores personales, aunque actualmente se encuentran en desuso.

SOPORTES ÓPTICOS.

Las técnicas de almacenamiento óptico usan la precisión exacta que sólo se obtiene con rayos láser.

La unidad enfoca un rayo láser sobre la superficie de un disco giratorio.

Algunos puntos del disco reflejan la luz en un sensor (plano = se interpreta como un 1) y otros dispersan la luz (orificio = se interpreta como un 0).

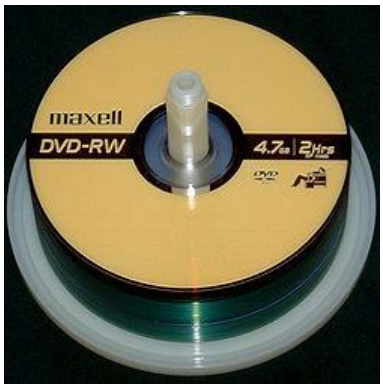
- ***El CD-R:*** es un disco compacto de 700 MB de capacidad que puede ser leído cuantas veces se desee, pero cuyo contenido no puede ser modificado una vez que ya ha sido grabado. Dado que no pueden ser borrados ni regrabados, son adecuados para almacenar archivos u otros conjuntos de información invariable.

- ***CD-RW:*** posee la capacidad del CD-R con la diferencia que estos discos son regrabables lo que les da una gran ventaja. Las unidades CD-RW pueden grabar información sobre discos CD-R y CD-RW y además pueden leer discos CD-ROM y CDS de audio. Este tipo de CD puede ser grabado múltiples veces, ya que permite que los datos almacenados sean borrados.

- ***DVD-R:*** es un disco óptico en el que se puede grabar o escribir datos con mucha mayor capacidad de almacenamiento que un CD-R, normalmente 4.7 GB (en lugar de los 700 MB de almacenamiento estándar de los CD). Es un disco que puede ser leído cuantas veces se desee, pero cuyo contenido no puede ser modificado una vez que ya ha sido grabado.

- **DVD-Rw:** es un DVD regrabable en el que se puede grabar y borrar la información varias veces. La capacidad estándar es de 4,7 GB, es el formato contrapuesto al DVD+RW. El DVD-RW es análogo al CD-RW, por lo que permite que su información sea grabada, borrada y regrabada varias veces,

esto es una ventaja respecto al DVD-R, ya que se puede utilizar como un diskette de 4,7 GB y también ahorra tener que adquirir más discos para almacenar nueva información pues se puede eliminar la antigua almacenada en el dvd.



- ***Pc - Cards:*** La norma de PCMCIA es la que define a las PC Cards. Las PC Cards pueden ser almacenamiento o tarjetas de I/O. Estas son compactas, muy fiable, y ligeras haciéndolos ideal para notebooks, palmtop, handheld y los PDAs. Debido a su pequeño tamaño, son usadas para el almacenamiento de datos, aplicaciones, tarjetas de memoria, cámaras electrónicas y teléfonos móviles.La norma de PCMCIA define tres PC Cards diferentes:
  - Tipo I 3.3 milímetros (mm) de espesor.
  - Tipo II son 5.0 mm espesor
  - Tipo III son 10.5 mm espesor.

- ***Flash Cards***: son tarjetas de memoria no volátil es decir conservan los datos aun cuando no estén alimentadas por una fuente eléctrica, y los datos pueden ser leídos, modificados o borrados. Con el rápido crecimiento de los dispositivos digitales como: asistentes personales digitales, cámaras digitales, teléfonos móviles y dispositivos digitales de música, las flash cards han sido

adoptadas como medio de almacenamiento de estos dispositivos haciendo que estas bajen su precio y aumenten su capacidad de almacenamiento muy rápidamente.

SOPORTES EXTRAÍBLES.

Son aquellos medios de almacenamiento diseñados para ser extraídos del ordenador sin tener que apagarla.

- ***Pen Drive o Memory Flash**:* Es un pequeño dispositivo de almacenamiento que utiliza la memoria flash para guardar la información sin necesidad de pilas. Los Pen Drive son resistentes a los rasguños y al polvo que han afectado a las formas previas de almacenamiento portable, como los CD y los disquetes.

- **Unidades de Zip**: La unidad Iomega ZIP es una unidad de disco extraíble. Está disponible en tres versiones principales, la hay con interfaz SCSI, IDE, y otra que se conecta a un puerto paralelo.

NUEVOS SOPORTES DE ALMACENAMIENTO.

- **Blue-Ray:** también conocido como Blu-ray o BD, es un formato de disco óptico de nueva generación de 12 cm de diámetro (igual que el CD y el DVD) para vídeo de gran definición y almacenamiento de datos de alta densidad. Su capacidad de almacenamiento llega a 25 GB por capa, aunque Sony y Panasonic han desarrollado un nuevo índice de evaluación (i-MLSE) que permite ampliar un 33% la cantidad de datos almacenados, desde 25 a 33,4 GB por capa.

- **Discos Rígidos externos:** es un disco duro que es fácilmente transportable de un lado a otro sin necesidad de consumir energía eléctrica o batería. Los discos USB microdrive y portátiles (2,5") se pueden alimentar de la conexión USB. Aunque algunas veces no es suficiente y requieren ser enchufados a dos USB a la vez. Las capacidades van desde el 2GB de los microdiscos a los cientos de Gb de los de 3,5".

7.3.2. Almacenamiento redundante y distribuido. RAID y centros de respaldo.

a) RAID.

En informática, el acrónimo RAID (del inglés Redundant Array of Independent Disks, conjunto redundante de discos independientes, hace referencia a un sistema de almacenamiento que usa múltiples discos duros o SSD entre los que distribuyen o replican los datos. Existen diferentes tipos de raid:

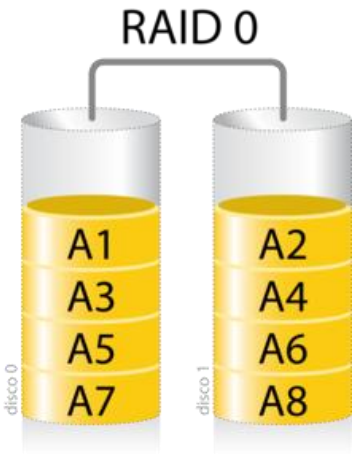
RAID 0

También llamado partición de los discos, los datos son distribuidos a través de discos paralelos. RAID 0 distribuye los datos rápidamente a los usuarios, pero no ofrece más protección a fallas de hardware que un simple disco.

El RAID 0 se usa normalmente para incrementar el rendimiento, aunque también puede utilizarse como forma de crear un pequeño número de grandes discos virtuales a partir de un gran número de pequeños discos físicos.

Una buena implementación de un RAID 0 dividirá las operaciones de lectura y escritura en bloques de igual tamaño, por lo que distribuirá la información equitativamente entre los dos discos.

Debido a su alta velocidad, pero hay que tener en cuenta de que si un disco rompe, se pierde absolutamente TODA la información de TODOS los discos.



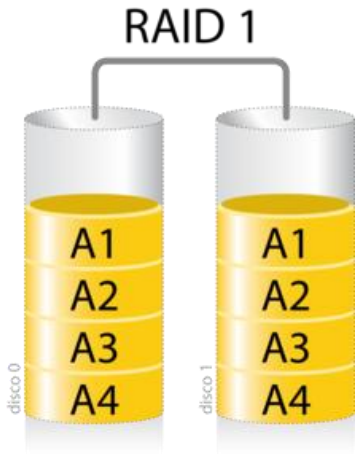
RAID 1

También llamado Disk espejo provee la más alta medida de protección de datos a través de una completa redundancia. Los datos son copiados a dos discos simultáneamente. La disponibilidad es alta pero el costo también dado que los usuarios deben comprar dos veces la capacidad de almacenamiento que requieren.

Esto resulta útil cuando el rendimiento en lectura es más importante que la capacidad.

Adicionalmente, dado que todos los datos están en dos o más discos, con hardware habitualmente independiente, el rendimiento de lectura se incrementa aproximadamente como múltiplo lineal del número del copias; es decir, un RAID 1 puede estar leyendo simultáneamente dos datos diferentes en dos discos diferentes, por lo que su rendimiento se duplica.

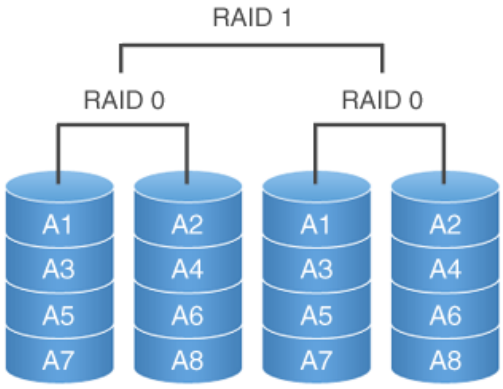
En caso de rotura de un disco, la información todavía está en el otro. Este el RAID que cualquier empresa por muy pequeña que sea debería de tener en su servidor de datos.



RAID 0+1

Combina Disk espejo y partición de datos. El resultado es gran disponibilidad al más alto desempeño de entrada y de salida para las aplicaciones de negocios más criticas. A este nivel como en el RAID 1 los discos son duplicados. Dado que son relativamente no costosos, RAID 0/1 es una alternativa para los negocios que necesitan solamente uno o dos discos para sus datos, sin embargo, el costo puede convertirse en un problema cuando se requieren más de dos discos.

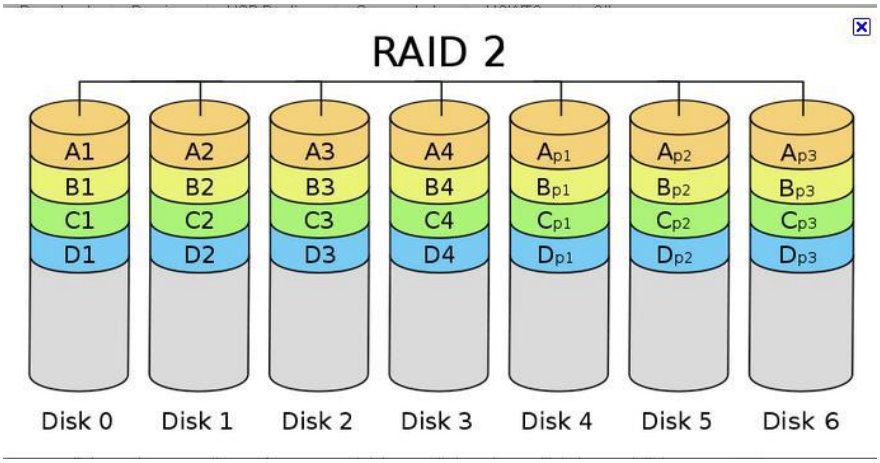
Combina el RAID 0 y el RAID 1. RAID (0+1) permite la perdida de múltiples discos debido a la redundancia de discos duros.



RAID 2

Un RAID 2 divide los datos a nivel de bits en lugar de a nivel de bloques y usa un código de Hamming para la corrección de errores. Los discos son sincronizados por la controladora para funcionar al unísono. Éste es el único nivel RAID original que actualmente no se usa. Permite tasas de trasferencias extremadamente altas.

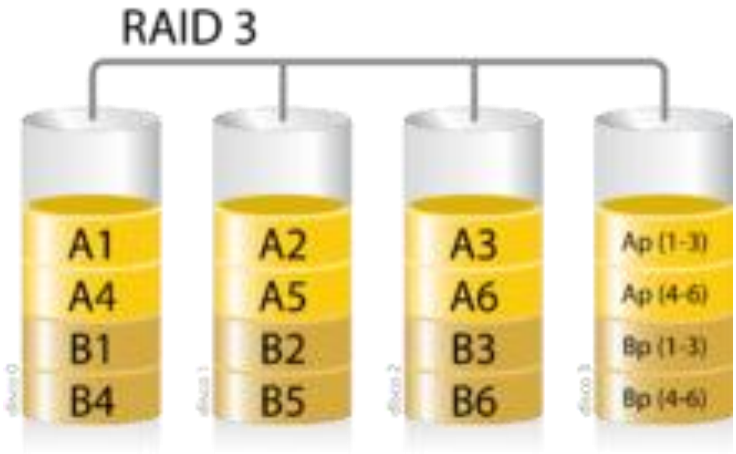
Teóricamente, un RAID 2 necesitaría 39 discos en un sistema informático moderno: 32 se usarían para almacenar los bits individuales que forman cada palabra y 7 se usarían para la corrección de errores.



RAID 3

Logra redundancia sin espejo completo. El flujo de los datos es particionado a través de todos los HD de datos en el arreglo. La información extra que provee la redundancia está escrita en un HD dedicado a la paridad. Si cualquier HD del arreglo falla, los datos perdidos pueden ser reconstruidos matemáticamente desde los miembros restantes del arreglo. RAID 3 es especialmente apropiado para procesamiento de imagen, colección de datos científicos, y otras aplicaciones en las cuales grandes bloques de datos guardados secuencialmente deben ser transferidos rápidamente.

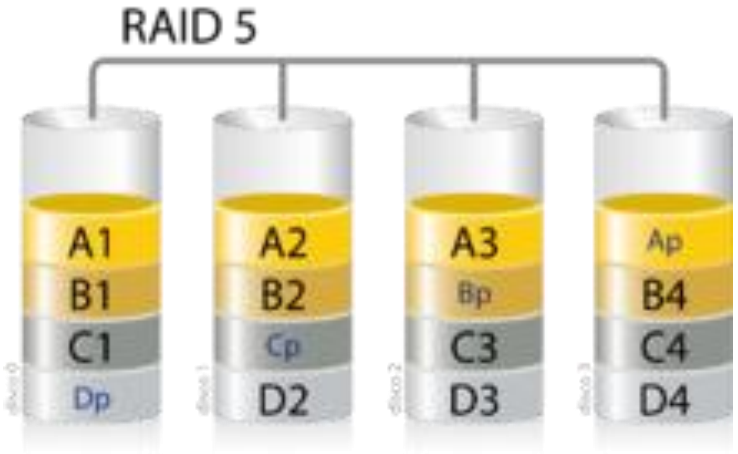
El RAID 3 se usa rara vez en la práctica. Uno de sus efectos secundarios es que normalmente no puede atender varias peticiones simultáneas, debido a que por definición cualquier simple bloque de datos se dividirá por todos los miembros del conjunto, residiendo la misma dirección dentro de cada uno de ellos.



RAID 5

Todos los HD en el arreglo operan independientemente. Un registro entero de datos es almacenado en un solo disco, permitiendo al arreglo satisfacer múltiples requerimientos de entrada y salida al mismo tiempo. La información de paridad está distribuida en todos los discos, aliviando el cuello de botella de acceder un solo disco de paridad durante operaciones de entrada y salida concurrentes. RAID 5 está bien recomendado para procesos de transacciones on-line, automatización de oficinas, y otras aplicaciones caracterizadas por gran numero de requerimientos concurrentes de lectura. RAID 5 provee accesos rápidos a los datos y una gran medida de protección por un costo más bajo que el Disk espejo.

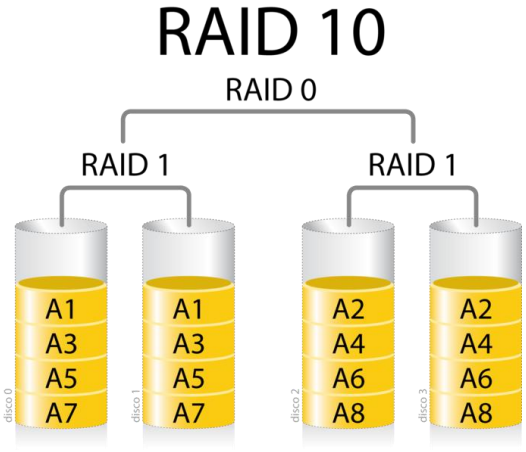
El RAID 5 ha logrado popularidad gracias a su bajo coste de redundancia. Generalmente, el RAID 5 se implementa con soporte hardware para el cálculo de la paridad. RAID 5 necesitará un mínimo de 3 discos para ser implementado.



RAID 10

La información se distribuye en bloques como en RAID-0 y adicionalmente, cada disco se duplica como RAID-1, creando un segundo nivel de arreglo. Se conoce como "striping de arreglos duplicados". Se requieren, dos canales, dos discos para cada canal y se utiliza el 50% de la capacidad para información de control. Este nivel ofrece un 100% de redundancia de la información y un soporte para grandes volúmenes de datos, donde el precio no es un factor importante. Ideal para sistemas de misión crítica donde se requiera mayor confiabilidad de la información, ya que pueden fallar dos discos inclusive (uno por cada canal) y los datos todavía se mantienen en línea. Es apropiado también en escrituras aleatorias pequeñas.

El RAID 10 es a menudo la mejor elección para bases de datos de altas prestaciones, debido a que la ausencia de cálculos de paridad proporciona mayor velocidad de escritura.



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.

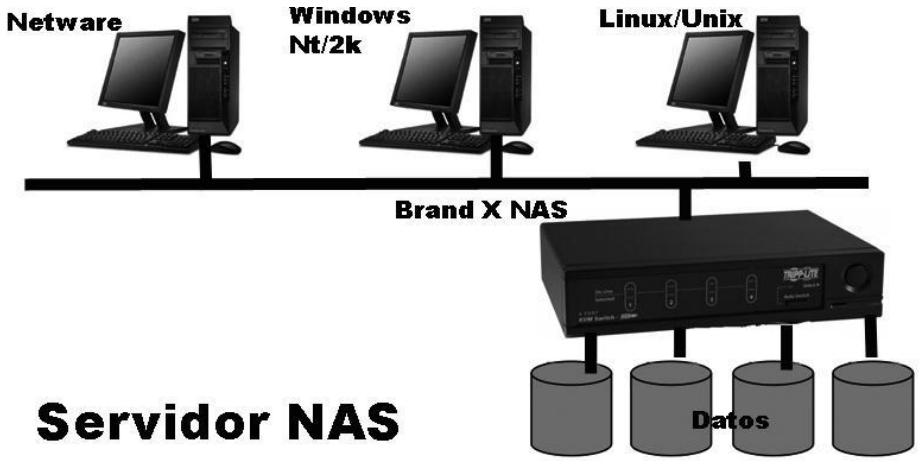
Generalmente, los sistemas NAS son dispositivos de almacenamiento específicos a los que se accede desde los equipos a través de protocolos de red (normalmente TCP/IP). También se podría considerar un sistema NAS a un servidor (Linux, Windows,...) que comparte sus unidades por red, pero la definición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



a) Almacenamiento Clouding.

El almacenamiento en la nube también es conocido como discos duros virtuales (no confundir con unidades virtuales). Un disco duro virtual es un espacio en un servidor que vamos a utilizar para guardar nuestros archivos. Es como si tuviéramos varios ordenadores conectados en red y en uno de ellos creamos una partición para guardar nuestros archivos. Esta información está accesible en un ordenador mediante internet.

En la red hay varias empresas que alquilan espacio en sus servidores, también hay páginas o empresas que ofrecen este servicio de forma gratuita, normalmente financiados mediante publicidad.

El acceso a estos discos se pude hacer de varias formas, siendo las principales mediante IP (trabajarían igual que una unidad más, y es lo que realmente sería un Cloud Storage), páginas web o FTP.

Almacenamiento en la nube es un modelo de red de almacenamiento en línea donde los datos se almacenan en las "piscinas" de almacenamiento virtualizado que en general son alojados por terceros. Empresas de hosting operan grandes centros de datos, y las personas que requieren que sus datos sean alojados alquilan capacidad de almacenamiento de los mismos y lo utilizan para sus necesidades de almacenamiento. El centro de datos de los operadores, se encarga de virtualizar los recursos de acuerdo a los requisitos del cliente y exponerlos como agrupaciones de almacenamiento, a los cuales los clientes pueden utilizar para almacenar archivos u objetos de datos. Físicamente, el recurso puede extenderse a lo largo de múltiples servidores.

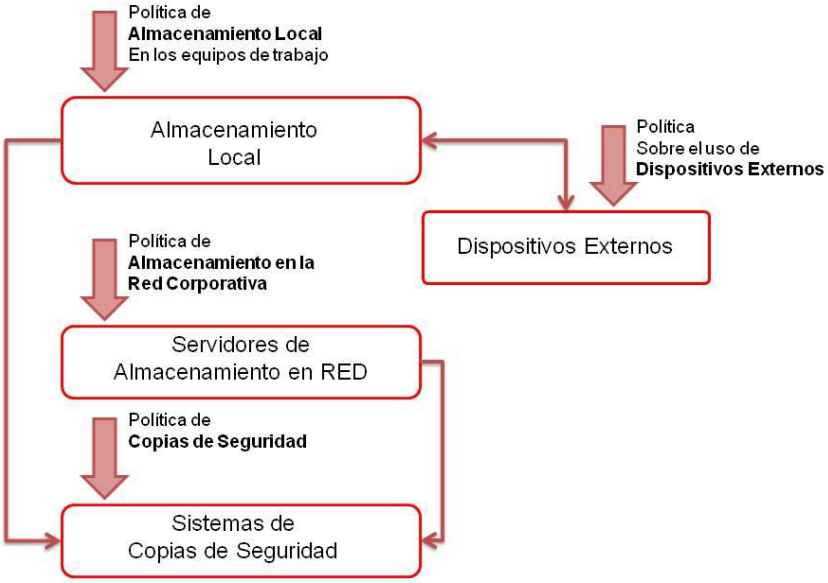
Las principales ventajas del almacenamiento en la nube son:

- Las empresas sólo tendrán que pagar por el almacenamiento que realmente utilizan.
- Nos es necesario instalar en las empresas dispositivos de almacenamiento físico en su propio centro de datos u oficinas, lo que reduce los costos de TI y hosting.
- Las tareas mantenimiento del almacenamiento, tales como copia de seguridad, replicación de datos, y la compra de dispositivos de almacenamiento adicionales quedan bajo la responsabilidad de un proveedor de servicios, permitiendo a las organizaciones centrarse en su negocio principal.

7.3.4. Políticas de almacenamiento.

Para poder mantener de un modo seguro y eficaz todos estos sistemas de almacenamiento es importante que la empresa especifique cuáles son las políticas que deben seguir todos los usuarios de los sistemas para evitar que aumente la capacidad de los mismos de modo desordenado y la consiguiente falta de control o pérdida de información. Así, se identifican cuatro políticas necesarias en la empresa, para que sean conocidas por los propios usuarios y controladas por los responsables:

- Política de almacenamiento local en los equipos de trabajo.
- Política de almacenamiento en la red corporativa.
- Política sobre el uso de dispositivos externos.
- Política de copias de seguridad.



➢ **Políticas de almacenamiento local en los equipos de trabajo**

En primer lugar, la empresa establece unas normas de almacenamiento para los equipos de trabajo de la empresa (equipos de sobremesa, equipos portátiles, teléfonos y otros dispositivos) que los usuarios deben cumplir. Esta política incluye al menos los siguientes aspectos:

- Qué tipo de información se puede almacenar en los equipos locales.
- Cuánto tiempo debe permanecer dicha información en los mismos.
- Permanencia de la información en la red local una vez transmitida a los servidores corporativos.
- Ubicación dentro del árbol de directorios del equipo.
- Utilización de sistemas de cifrado de información en los documentos empresariales.
- Normativa para los empleados relativa al almacenamiento de documentos personales, archivos de música, fotografías, etc, y en concreto relativa a archivos que estén bajo algún tipo de regulación en cuanto a derechos de autor (descargas desde los equipos de trabajo).

➢ Políticas de almacenamiento en la red corporativa

En la red corporativa es necesario distinguir entre información general de la empresa que deben utilizar todos los usuarios, e información de trabajo de los empleados almacenada en esta red corporativa:

1. Los servidores de almacenamiento disponibles en la red corporativa están configurados para poder almacenar y compartir aquella información de la empresa que deba ser utilizada por los empleados.
Los controles de acceso son definidos por la dirección y el responsable de sistemas, con el objetivo de definir quién puede acceder y a dónde, mientras que el contenido de la información almacenada se determina a través de una política de uso específica que debe cubrir al menos los siguientes aspectos:

• Tipo de información almacenada, momento de su almacenamiento y ubicación dentro de los directorios del sistema.
• Personas encargadas de la actualización de dicha información en caso de modificación.

2. Los empleados pueden disponer de buzones o carpetas personales dentro de la misma red corporativa. En estas carpetas se almacena información que, si bien tiene relación con su trabajo, no necesariamente es compartida por otros miembros del equipo. Para controlar dicha información, se deben especificar políticas que incluyan los mismos aspectos que los relacionados con el almacenamiento local.

Es importante concienciar al empleado que toda aquella información almacenada en estos buzones debe ser relevante para el trabajo. La información carente de valor se elimina una vez que se haya utilizado. Así se evita que la capacidad de almacenamiento se vea desbordada innecesariamente.

➢ Políticas sobre el uso de dispositivos externos conectados

Especialmente importante son las normas relativas al uso de equipos externos que, conectados directamente a los equipos de trabajo, permiten el almacenamiento extra de información con el objeto de trasportarla a otra ubicación o simplemente disponer de una copia de seguridad personal. Esta política incluye al menos los siguientes aspectos:

- Si está permitido o no el uso de estos dispositivos.
- En caso afirmativo, qué tipo de información en ningún caso está permitido almacenar, como aquella que contiene datos personales de clientes, etc.
- Qué medidas de borrado se han de utilizar cuando esta información deja de ser necesaria.

➢ Políticas de copias de seguridad

Una copia de seguridad, también conocida como backup, es un duplicado que se realiza sobre ficheros o aplicaciones contenidas en un ordenador con la finalidad de recuperar los datos en el caso de que el sistema de información sufra daños o pérdidas accidentales de los datos almacenados3 . Todo plan de contingencia de una empresa requiere contar con una planificación adecuada de las copias de seguridad que se realizan, ya que la pérdida de datos puede poner en peligro la continuidad del negocio.

Algunos de los requisitos que debe cumplir la planificación de copias de seguridad son:

- Identificar los datos que requieren ser preservados. Son aquellos cuya pérdida afectaría a la continuidad del negocio.

- Establecer la frecuencia con la que se van a realizar los procesos de copia. Esta frecuencia influye en la cantidad de información que se puede perder con respecto a la fuente original. Este parámetro es de suma importancia y requiere de un análisis exhaustivo.
  Por ejemplo, si se realiza una copia cada noche y el soporte se estropea a las 12h toda la información generada desde la noche anterior hasta las 12h no se encontrará en la copia de seguridad.

- Disponer el almacén físico para las copias. Este almacén se determina en función de la seguridad que requiere la información entre almacenes en el mismo edificio o remotos en edificios externos.
  Por ejemplo, si se produce un incendio en el edificio de la empresa, la información almacenada en un edificio externo sigue estando disponible.

- Buscar una probabilidad de error mínima, asegurándose que los datos son copiados íntegramente del original y en unos soportes fiables y en buen estado. No se deben utilizar soportes que estén cerca de cumplir su vida útil para evitar que fallen cuando vaya a recuperarse la información que contienen.

- Controlar los soportes que contienen las copias, guardándolos en un lugar seguro y restringiendo su acceso sólo a las personas autorizadas.

- Planificar la restauración de las copias: Formando a los técnicos encargados de realizarlas.
  Disponiendo de soportes para restaurar la copia, diferentes de los de producción.
  Estableciendo los medios para disponer de dicha copia en el menor tiempo posible.

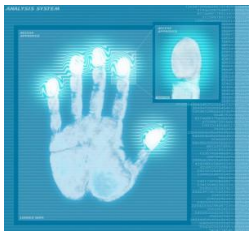
- Probar el sistema de forma exhaustiva para comprobar su correcta planificación y la eficacia de los medios dispuestos.

- Definir la vigencia de las copias, estableciendo un periodo en el que dicha copia deja de tener validez y puede sustituirse por una copia más actualizada de la información.

- Controlar la obsolescencia de los dispositivos de almacenamiento. Para el caso de aquellas copias que almacenan información histórica de la organización, por ejemplo proyectos ya cerrados, se debe tener en cuenta el tipo de dispositivo en el que se ha realizado la copia, para evitar que en el momento que se requiera la restauración de dicha información no existan ya lectores adecuados para dicho dispositivo.

Cuando se desechen los soportes de almacenamiento, porque hayan llegado al límite de vida útil fijado en la política de copias de seguridad, es importante realizar un proceso de borrado seguro o destrucción para asegurar que la información que contiene no podrá ser recuperada posteriormente.

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.

7.4.2. Política de contraseñas.

Para gestionar correctamente la seguridad de las contraseñas, se recomienda a los usuarios tener en cuenta las siguientes pautas para la creación y establecimiento de contraseñas seguras:

1) Se deben utilizar al menos 8 caracteres para crear la clave.
2) Se recomienda utilizar en una misma contraseña dígitos, letras y caracteres especiales.
3) Es recomendable que las letras alternen aleatoriamente mayúsculas y minúsculas. Hay que tener presente el recordar qué letras van en mayúscula y cuáles en minúscula.
4) Elegir una contraseña que pueda recordarse fácilmente y es deseable que pueda escribirse rápidamente, preferiblemente, sin que sea necesario mirar el teclado.
5) Las contraseñas hay que cambiarlas con una cierta regularidad. Y, a la vez, hay que procurar no generar reglas secuenciales de cambio. Por ejemplo, crear una nueva contraseña mediante un incremento secuencial del valor en relación a la última contraseña. P. ej.: pasar de “01Juitnx” a “02Juitnx”.
6) Utilizar signos de puntuación si el sistema lo permite. Dentro de ese consejo se incluiría utilizar símbolos como: ! " # $ % & ' ( ) * + , - . / : ; < = > ? @ [\ ] ^ _ ` { | } ~
7) Existen algunos trucos para plantear una contraseña que no sea débil y se pueda recordar más fácilmente. Por ejemplo se pueden elegir palabras sin sentido pero que sean pronunciables, etc. Nos podemos ayudar combinando esta selección con números o letras e introducir alguna letra mayúscula. Otro método sencillo de creación de contraseñas consiste en elegir la primera letra de cada una de las palabras que componen una frase conocida, de una canción, película, etc.

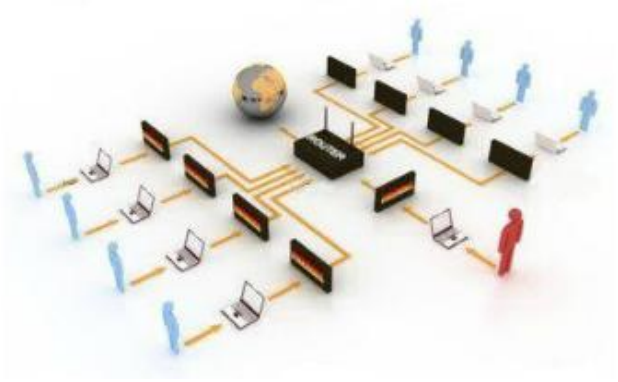
Del mismo modo para crear una contraseña segura debemos:

1) Se debe evitar utilizar la misma contraseña siempre en todos los sistemas o servicios.
2) No utilizar información personal en la contraseña.
3) Hay que evitar utilizar secuencias básicas de teclado (por ejemplo: ”qwerty”, “asdf” o las típicas en numeración: “1234” ó “98765”).
4) No repetir los mismos caracteres en la misma contraseña. (ej.: “111222”).
5) Hay que evitar también utilizar solamente números, letras mayúsculas o minúsculas en la contraseña.
6) No se debe utilizar como contraseña, ni contener, el nombre de usuario asociado a la contraseña.
7) No utilizar datos relacionados con el usuario que sean fácilmente deducibles (apodos, personaje favorito, etc).
8) No escribir ni reflejar la contraseña en un papel o documento donde quede constancia de la misma.
9) No se deben utilizar palabras que se contengan en diccionarios en ningún idioma. Hoy en día existen programas de ruptura de claves que basan su ataque en probar una a una las palabras que extraen
10) No enviar nunca la contraseña por correo electrónico o en un sms.
11) Si se trata de una contraseña para acceder a un sistema delicado hay que procurar limitar el número de intentos de acceso permitidos.

12) No utilizar en ningún caso contraseñas que se ofrezcan en los ejemplos explicativos de construcción de contraseñas robustas.
13) No escribir las contraseñas en ordenadores de los que se desconozca su nivel de seguridad y puedan estar monitorizados, o en ordenadores de uso público.
14) Cambiar las contraseñas por defecto proporcionadas por desarrolladores/fabricantes.

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

Realizar auditorías con cierta frecuencia asegura la integridad de los controles de seguridad aplicados a los sistemas de información. Acciones como el constante cambio en las configuraciones, la instalación de parches, actualización de los software y la adquisición de nuevo hardware hacen necesario que los sistemas estén continuamente verificados mediante auditoría.

7.5.2. Pruebas y herramientas de auditoría informática.

En la realización de una auditoría informática el auditor puede realizar las siguientes pruebas:

- **Pruebas clásicas:** Consiste en probar las aplicaciones / sistemas con datos de prueba, observando la entrada, la salida esperada, y la salida obtenida. Existen paquetes que permiten la realización de estas pruebas.
- **Pruebas sustantivas:** Aportan al auditor informático suficientes evidencias para que se pueda realizar un juicio imparcial. Se suelen obtener mediante observación, cálculos, muestreos, entrevistas, técnicas de examen analítico, revisiones y conciliaciones. Verifican asimismo la exactitud, integridad y validez de la información obtenida.
- **Pruebas de cumplimiento:** Determinan si un sistema de control interno funciona adecuadamente (según la documentación, según declaran los auditados y según las políticas y procedimientos de la organización).

Las principales herramientas de las que dispone un auditor informático son:

- Observación
- Realización de cuestionarios
- Entrevistas a auditados y no auditados
- Muestreo estadístico
- Flujogramas
- Listas de comprobación de realización de requisitos
- Mapas conceptuales

Algunas aplicaciones más conocidas que podemos utilizar para realizar las auditorías son:

Auditor de Seguridad Remoto. El cliente "The Nessus Security Scanner" es una herramienta de auditoría de seguridad. Hace posible evaluar módulos de seguridad intentando encontrar puntos vulnerables que deberían ser reparados. Está compuesto por dos partes: un servidor, y un cliente. El servidor/daemon, "nessusd" se encarga de los ataques, mientras que el cliente, "nessus", se ocupa del usuario por medio de una linda interfaz para X11/GTK+. Este paquete contiene el cliente para GTK+1.2, que además existe en otras formas y para otras platarformas.

SAINT (Security Administrator's Integrated Network Tool, es decir, Herramienta De Red Integrada Del Administrador de Seguridad) es una herramienta de evaluación de seguridad basada en SATAN. Incluye escaneos _a_través_ de un firewall, chequeos de seguridad actualizados de los boletines de CERT Y CIAC, 4 niveles de severidad (rojo, amarillo, marrón y verde) y una interfaz HTML rica en características.

Sniffit

Una herramienta de monitoreo y "packet sniffer" para paquetes de TCP/UDP/ICMP. sniffit es capaz de dar información técnica muy detallada acerca de estos paquetes (SEC, ACK, TTL, Window, ...) pero también los contenidos de los paquetes en diferentes formatos (hex o puro texto, etc.).

SATAN

Herramienta de Auditoría de Seguridad para Analizar Redes (Security Auditing Tool for Analysing Networks). Ésta es una poderosa herramienta para analizar redes en búsqueda de vulnerabilidades creada para administradores de sistema que no pueden estar constantemente chequeando bugtraq, rootshell y ese tipo de fuentes de info.

El Asistente de Investigación para el Auditor de Seguridad (Security Auditor's Research Assistant) es una herramienta de análisis de seguridad de tercera generación que está basada en el modelo de SATAN y distribuida bajo una licencia del estilo de la GNU GPL. Promueve un ambiente colaborativo y es actualizada periódicamente para tener en cuenta las últimas amenazas.

Es un programa de código abierto que sirve para efectuar rastreo de puertos escrito originalmente por Gordon Lyon. Se usa para evaluar la seguridad de sistemas informáticos, así como para descubrir servicios o servidores en una red informática.

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.

La historia de la criptografía es larga y abunda en anécdotas. Ya las primeras civilizaciones desarrollaron técnicas para enviar mensajes durante las campañas militares, de forma que si el mensajero era interceptado la información que portaba no corriera el peligro de caer en manos del enemigo. También los romanos utilizaron sistemas de sustitución, siendo el método actualmente conocido como César, porque supuestamente Julio César lo empleó en sus campañas, uno de los más conocidos en la literatura. Otro de los métodos criptográficos utilizados por los griegos fue la escítala espartana, un método de trasposición basado en un cilindro que servía como clave en el que se enrollaba el mensaje para poder cifrar y descifrar.

Durante la Primera Guerra Mundial, los Alemanes usaron el cifrado ADFGVX. Este método de cifrado es similar a la del tablero de ajedrez Polibio. Consistía en una matriz de 6 x 6 utilizado para sustituir cualquier letra del alfabeto y los números 0 a 9 con un par de letras que consiste de A, D, F, G, V, o X.

La máquina Enigma utilizada por los alemanes durante la II Guerra Mundial.

La más conocida de las máquinas de cifrado posiblemente sea la máquina alemana Enigma: una máquina de rotores que automatizaba considerablemente los cálculos que era necesario realizar para las operaciones de cifrado y descifrado de mensajes. Para vencer al ingenio alemán, fue necesario el concurso de los mejores matemáticos de la época y un gran esfuerzo computacional. No en vano, los mayores avances tanto en el campo de la criptografía como en el del criptoanálisis no empezaron hasta entonces.

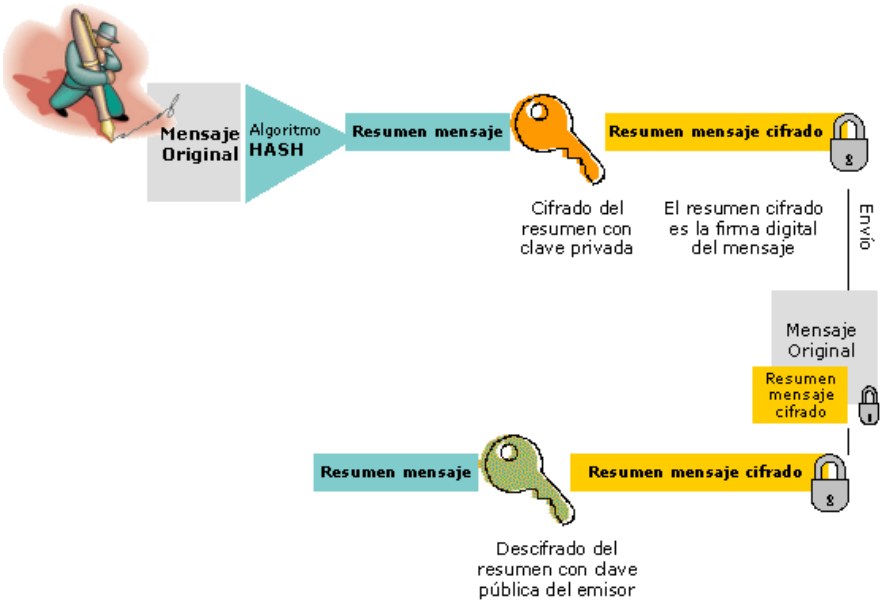
7.6.2. Cifrado y descifrado.

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. Medidas de Seguridad.

Todas las empresas, independientemente de su tamaño, organización y volumen de negocio, son conscientes de la importancia de tener implantadas una serie de políticas de Seguridad tendentes a garantizar la continuidad de su negocio en el caso de que se produzcan incidencias, fallos, actuaciones malintencionadas por parte de terceros, pérdidas accidentales o desastres que afecten a los datos e informaciones que son almacenados y tratados, ya sea a través de sistemas informáticos como en otro tipo de soportes, como el papel.

Los casos de incidentes informáticos que en el pasado causaron daños y perjuicios económicos importantes, han ido abriendo los ojos a muchas empresas a la necesidad de implantar mecanismos para proteger su información almacenada y tratada en los equipos informáticos de incidencias externas (intencionadas y/o accidentales); pero también, de la importancia de la protección de la información desde una órbita interna de la empresa: el acceso restringido a cierta documentación por determinados empleados, la firma de cláusulas de confidencialidad por parte del personal, el establecimiento de políticas y procedimientos de respaldo y recuperación de datos o el almacenamiento externo de información.

La seguridad informática de una organización debe garantizar:

- La **Disponibilidad** de los sistemas de información.
- La **Recuperación** rápida y completa de los sistemas de información.
- La **Integridad** de la información.
- La **Confidencialidad** de la información.

8.1. Política de Seguridad.

Una política de seguridad 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 requerirán.

El objetivo de la política de seguridad es establecer las pautas generales que permitan la gestión de la seguridad de la Información de manera integrada y coordinada con los requerimientos propios del negocio, las leyes que en su caso apliquen y la normativa interna de la empresa.

Dado que una lista de buenas intenciones no tiene valor por sí sola, se hace imprescindible distribuir y hacer llegar a todos y cada uno de los empleados que conforman nuestro negocio la Política de Seguridad de la Información.

La Política de Seguridad puede ser complementada con normativas específicas en aquellos aspectos del negocio en los que sea necesario establecer unas normas concretas de actuación.

Estas Políticas deben ser revisadas, y de ser necesario actualizadas, periódicamente.

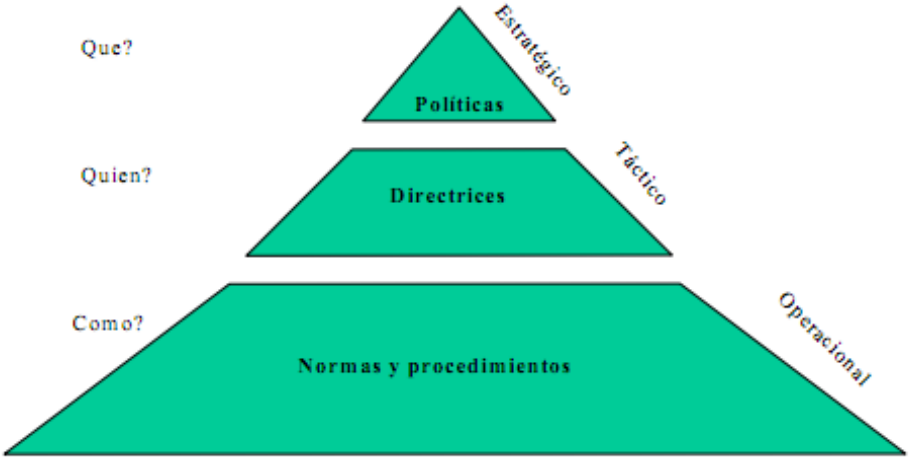
Lo más importante para que estas surtan efecto es lograr la concienciación, entendimiento y compromiso de todos los involucrados.

Una política de seguridad integral debe cumple las siguientes funciones esenciales:

- Protege a las personas y a la información
- Establece las normas de comportamiento esperado de los usuarios, de los administradores de sistemas, de la dirección y del personal de seguridad
- Autoriza al personal de seguridad a realizar controles, sondeos e investigaciones
- Define y autoriza las consecuencias de las violaciones

A partir de las Políticas podremos comenzar a desarrollar, primero las normas, y luego los procedimientos de seguridad que serán la guía para la realización de las actividades.

La siguiente figura muestra la estructura de una política de seguridad en la empresa.



Una política de seguridad debe:

- Ser holística (cubrir todos los aspectos relacionados con la misma). No tiene sentido proteger el acceso con una puerta blindada si a esta no se la ha cerrado con llave.
- Adecuarse a las necesidades y recursos. No tiene sentido adquirir una caja fuerte para proteger un lápiz.
- Ser atemporal. El tiempo en el que se aplica no debe influir en su eficacia y eficiencia.
- Definir estrategias y criterios generales a adoptar en distintas funciones y actividades, donde se conocen las alternativas ante circunstancias repetidas.

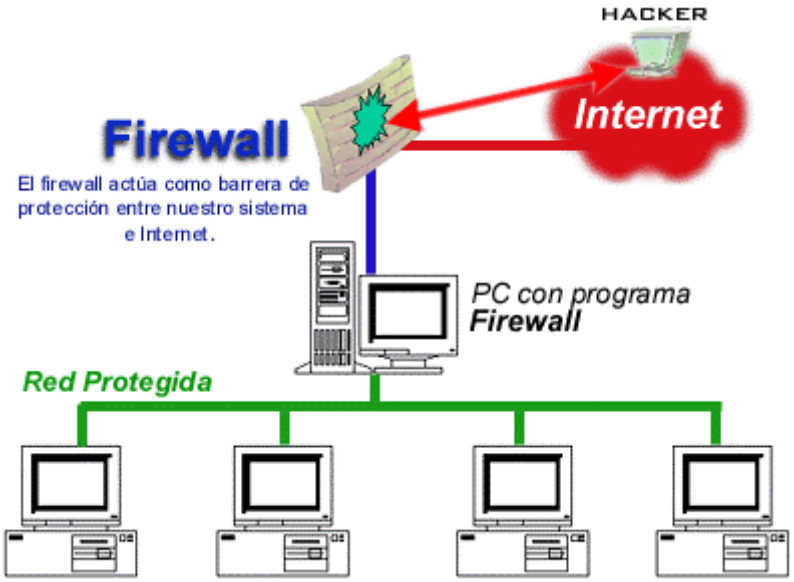
Cualquier política de seguridad ha de contemplar los elementos claves de seguridad ya mencionados: la Integridad, Disponibilidad, Privacidad y, adicionalmente, Control, Autenticidad y Utilidad.

En el siguiente enlace podemos ver un ejemplo de política de seguridad http://protegete.jccm.es/protegete/export/sites/default/Descargas/PYMES_-_Modelo_Polxtica_de_seguridad.pdf

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.

9. Análisis Forense en Sistemas Informáticos.

El análisis forense es la técnica de capturar, procesar e investigar información procedente de sistemas informáticos utilizando una metodología con el fin de que pueda ser utilizada en la justicia.

La Informática Forense se encarga de analizar sistemas informáticos en busca de evidencia que colabore a llevar adelante una causa judicial o una negociación extrajudicial.

8.3. Funcionalidad y Fases de un Análisis Forense.

1) Identificación del incidente: búsqueda y recopilación de evidencias.

Una de las primeras fases del análisis forense comprende el proceso de identificación del incidente, que lleva aparejado la búsqueda y recopilación de evidencias.

Antes de comenzar una búsqueda desesperada de señales del incidente que lo único que conlleve sea una eliminación de "huellas", actúe de forma metódica y profesional.

Asegúrese primero que no se trata de un problema de hardware o software de su red o servidor, no confunda un "apagón" en su router con un ataque DoS.

Deberá utilizar herramientas que no cambien los sellos de tiempo de acceso (timestamp), o provoquen modificaciones en los archivos, y por supuesto que no borren nada.

Recopilación de evidencias

Bien, ya está seguro de que sus sistemas informáticos han sido atacados. En este punto deberá decidir cuál es su prioridad:

A.- Tener nuevamente operativos sus sistemas rápidamente.

B.- Realizar una investigación forense detallada.

Piense que la primera reacción de la mayoría de los administradores será la de intentar devolver el sistema a su estado normal cuanto antes, pero esta actitud sólo hará que pierda casi todas las evidencias que los atacantes hayan podido dejar en "la escena del crimen", eliminando la posibilidad de realizar un análisis forense de lo sucedido que le permita contestar a las preguntas de ¿qué?, ¿cómo?, ¿quién?, ¿de dónde? y ¿cuándo? se comprometió el sistema, e impidiendo incluso llevar a cabo acciones legales posteriores si se diese el caso. Esto también puede que le lleve a volver a trabajar con un sistema vulnerable, exponiéndolo nuevamente a otro ataque.

Elegiremos el "Plan B", a partir de ahora seguiremos una serie de pasos encaminados a recopilar evidencias que le permitan determinar el método de entrada al sistema, la actividad de los intrusos,

su identidad y origen, duración del compromiso y todo ello extremando las precauciones para evitar alterar las evidencias durante el proceso de recolección.

Es aconsejable anotar datos como hora y fecha de inicio y fin de cada paso que se dé o el número de serie de los componentes de nuestro equipo. También sería aconsejable estar acompañado de algún testigo ó incluso un Notario.

Debemos decidir si comenzamos a tomar muestras sobre el sistema "vivo" o "muerto". Hay que tener en cuenta que si desactivamos el equipo, todas las "huellas" que se encuentren en la información volátil del mismo desaparecerán.

Si decidimos almacenar la información volátil es recomendable almacenarla en otro lugar distinto a nuestro equipo.

2) Preservación de la evidencia

Aunque el primer motivo que le habrá llevado a la recopilación de evidencias sobre el incidente sea la resolución del mismo, puede que las necesite posteriormente para iniciar un proceso judicial contra sus atacantes y en tal caso deberá documentar de forma clara cómo ha sido preservada la evidencia tras la recopilación.

Como primer paso deberá realizar dos copias de las evidencias obtenidas una de las copias será la "evidencia orignal", para un posible proceso jurídico, y la otra será la evidencia sobre la cual realizaremos el análisis.

Es aconsejable preparar un documento en el que se registren los datos personales de todos los implicados en el proceso de manipulación de las copias, desde que se tomaron hasta su almacenamiento.

Análisis de la evidencia

Una vez que disponemos de las evidencias digitales recopiladas y almacenadas de forma adecuada, pasemos a la fase quizás más laboriosa, el Análisis Forense propiamente dicho, cuyo objetivo es reconstruir con todos los datos disponibles la línea temporal del ataque o timeline, determinando la cadena de acontecimientos que tuvieron lugar desde el instante inmediatamente anterior al inicio del ataque, hasta el momento de su descubrimiento.

Este análisis se dará por concluido cuando conozcamos cómo se produjo el ataque, quién o quienes lo llevaron a cabo, bajo qué circunstancias se produjo, cuál era el objetivo del ataque, qué daños causaron, etc.

3) Preparación para el análisis: El entorno de trabajo

Antes de comenzar el análisis de las evidencias deberá acondicionar un entorno de trabajo adecuado al estudio que desee realizar.

Si dispone de recursos suficientes prepare dos estaciones de trabajo, en una de ellas, que contendrá al menos dos discos duros, instale un sistema operativo que actuará de anfitrión y que le servirá para realizar el estudio de las evidencias. En ese mismo ordenador y sobre un segundo disco duro, vuelque las imágenes manteniendo la estructura de particiones y del sistema de archivos tal y como estaban en el equipo atacado. En el otro equipo instale un sistema operativo configurado exactamente igual que el del equipo atacado, además mantenga nuevamente la misma estructura de particiones y ficheros en sus discos duros. La idea es utilizar este segundo ordenador como "conejillo

de Indias" y realizar sobre él pruebas y verificaciones conforme vayan surgiendo hipótesis sobre el ataque.

Reconstrucción de la secuencia temporal del ataque

Supongamos que ya tenemos montadas las imágenes del sistema comprometido en nuestra estación de trabajo independiente y con un sistema operativo anfitrión de confianza.

El primer paso que deberá dar es crear una línea temporal de sucesos o timeline, para ello recopile la siguiente información sobre los ficheros:

- Inodos asociados.
- Marcas de tiempo MACD (fecha y hora de modificación, acceso, creación y borrado).
- Ruta completa.
- Tamaño en bytes y tipo de fichero.
- Usuarios y grupos a quien pertenece.
- Permisos de acceso.
- Si fue borrado o no.

Determinación de cómo se realizó el ataque

Una vez que disponga de la cadena de acontecimientos que se han producido, deberá determinar cuál fue la vía de entrada a su sistema, averiguando qué vulnerabilidad o fallo de administración causó el agujero de seguridad y que herramientas utilizó el atacante para aprovecharse de tal brecha. Estos datos, al igual que en el caso anterior, deberá obtenerlos de forma metódica, empleando una combinación de consultas a archivos de logs, registro, claves, cuentas de usuarios, etc.

Si ya tiene claro cuál fue la vulnerabilidad que dejó su sistema "al desnudo", vaya un paso más allá y busque en Internet algún exploit anterior a la fecha del compromiso, que utilice esa vulnerabilidad.

Identificación del autor o autores del incidente

Si ya ha logrado averiguar cómo entraron en sus sistemas, ahora le toca saber quién o quiénes lo hicieron. Para este propósito le será de utilidad consultar nuevamente algunas evidencias volátiles que recopiló en las primeras fases, revise las conexiones que estaban abiertas, en qué puertos y qué direcciones IP las solicitaron, además busque entre las entradas a los logs de conexiones. También puede indagar entre los archivos borrados que recuperó por si el atacante eliminó alguna huella que quedaba en ellos.

Para identificar a su atacante tendrá que verificar y validar la dirección IP obtenida.

Otro aspecto que es interesante averiguar es el perfil de los atacantes, que podrá encontrarse entre los siguientes tipo:

- Hackers:
- SciptKiddies
- Profesionales:

Evaluación del impacto causado al sistema

Para poder evaluar el impacto causado al sistema, el análisis forense le ofrece laposibilidad de investigar qué es lo que han hecho los atacantes una vez que accedieron a sus sistemas. Esto le permitirá evaluar el compromiso de sus equipos y realizar una estimación del impacto causado. Generalmente se pueden dar dos tipos de ataques:

Ataques pasivos: en los que no se altera la información ni la operación normal de los sistemas, limitándose el atacante a fisgonear por ellos.

Ataques activos, en los que se altera, y en ocasiones seriamente, tanto la información como la capacidad de operación del sistema.

4) Documentación del incidente

Tan pronto como el incidente haya sido detectado, es muy importante comenzar a tomar notas sobre todas las actividades que se lleven a cabo. Cada paso dado debe ser documentado y fechado desde que se descubre el incidente hasta que finalice el proceso de análisis forense, esto le hará ser más eficiente y efectivo al tiempo que reducirá las posibilidades de error a la hora de gestionar el incidente.

Es recomendable además realizar los siguientes documentos.

- Utilización de formularios de registro del incidente.
- El Informe Técnico.
- El Informe Ejecutivo.

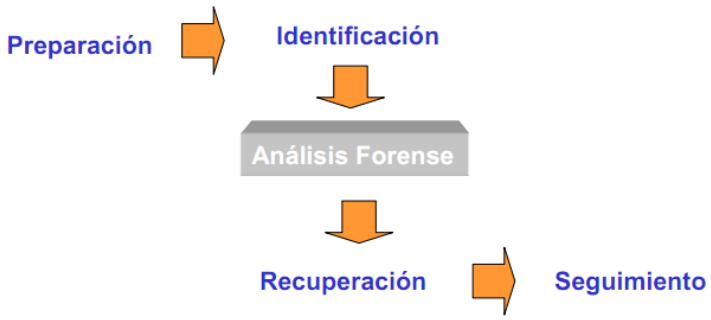
8.4. Respuesta a Incidentes.

Un incidente de Seguridad Informática está definido como un evento que atente contra la Confidencialidad, Integridad y Disponibilidad de la información.

Algunos tipos de incidentes son:

- Compromisos de integridad
- Uso no autorizado
- Denegación de servicio
- Daños
- Intrusiones

El proceso par una respuesta a un incidente es el siguiente:



La respuesta a incidentes persigue los siguientes objetivos:

- identificar, designar o custodiar evidencias.
- revisar cualquier diario existente de lo que ya se ha hecho en el sistema y/o como se detectó la intrusión
- empezar un nuevo diario o mantener el ya existente, instalar herramientas de monitorización (sniffers, detectores de puertos)
- sin re-arrancar el sistema o afectar los procesos en ejecución realizar una copia del disco físico
- capturar información de red
- capturar procesos y ficheros en uso (dll, exe, etc.)
- capturar información de configuración
- recoger y firmar datos

8.5. Análisis de Evidencias Digitales.

La "evidencia digital" es cualquier información obtenida a partir de un dispositivo electrónico o medio digital que sirve para adquirir convencimiento de la certeza de un hecho.

Tipos de evidencias:

- Testimonio humano.
- Evidencias físicas.
- Evidencias de red.
- Evidencias de host (memoria, conexiones de red, procesos, usuarios conectados, configuraciones de red, discos).

Consideraciones a tener en cuenta antes de realizar el análisis.

- NUNCA trabajar con datos ORIGINALES, evidencias, dispositivos, etc..
- Respetar la legislación y las políticas de la Organización
- Documentación
- Resultados Verificables y Reproducibles
- No existe un procedimiento estándar.

Preparación del entorno forense

- Laboratorio forense.
- El Sistema de análisis
- Entorno limpio
- Aislado de la red
- Herramientas limpias y esterilizadas
- Sistema de Simulación
- Sistema de Pruebas en caliente

Objetivo de Análisis: ¿Quién? ¿Cómo? ¿Con que? ¿Por qué? ¿Cuándo? Etc…

Reconstrucción temporal de los hechos: Timeline, Correlación de eventos. De donde ?

Análisis del sistema de ficheros

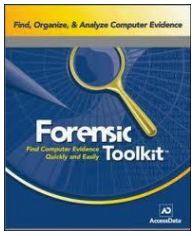
- Análisis de los ficheros corrientes del sistema: Comprobación de integridad de los binarios del sistema, ROOTKITS y Virus.
- Archivos temporales.
- Archivos o directorios "ocultos": Nombres camuflados
- Archivos borrados
- Slack space
- Partición swap
- Esteganografía, cifrado, etc…

8.6. Herramientas de Análisis Forense.

Las dificultades que se encuenstra el investigador a la hora de analizar determinadas evidencias digitales es que los atacantes emplean cada vez herramientas más sigilosas y perfeccionadas para realizar sus asaltos. Por lo tanto no estará de más disponer de un conjunto de herramientas específicas para el análisis de evidencias.

Dejando aparte el software comercial, en el que podrá encontrar herramientas específicas como EnCase de la empresa Guidance Software, considerado un estándar en el análisis forense de sistemas, nos centraremos en herramientas de código abierto (Open Source) que se pueden descargar libremente de las páginas de los autores.

The Forensic ToolKit



Se trata de una colección de herramientas forenses para plataforma Windows, creada por el equipo de Foundstone. Puede descargarse desde www.foundstone.com. Este ToolKit le permite recopilar información sobre el ataque, y se compone de una serie aplicaciones en línea de comandos que permiten generar diversos informes y estadísticas del sistema de archivos a estudiar. Para poder utilizarlos deberá disponer de un intérprete de comandos como cmd.exe.

Comando	Función
afind	Realiza búsqueda de archivos por su tiempo de acceso, sin modificar la información de acceso al mismo.
hfind	Busca archivos ocultos en el Sistema Operativo.
sfind	Busca flujos de datos ocultos en el disco duro, éstos son distintos de los archivos ocultos y no aparecerán con herramientas normales del sistema operativo. Su importancia radica en que pueden usarse para ocultar datos o software dañino.
filestat	Ofrece una lista completa de los atributos del archivo que se le pase como argumento (uno cada vez).
hunt	Permite obtener información sobre un sistema que utiliza las opciones de sesión NULL, tal como usuarios, recursos compartidos y servicios.

The Sleuth Kit y Autopsy

Consiste en una colección de herramientas forenses para entornos UNIX/Linux, que incluye algunas partes del conocido The Coroners ToolKit (TCT) de Dan Farmer. Puede analizar archivos de datos de evidencias generadas con utilidades de disco como por ejemplo dd. Pese a ser de libre distribución (puede descargarlo del sitio Web www.sleuthkit.org). Incluye funciones como registro de casos separados e investigaciones múltiples, acceso a estructuras de archivos y directorios de bajo nivel y eliminados, genera la línea temporal de actividad de los archivos (timestamp), permite buscar datos dentro de las imágenes por palabras clave, permite crear notas del investigador e incluso genera informes, etc.

Algunas de las funciones básicas con las que podrá contar son las siguientes opciones:

Opción	Descripción
Análisis de archivos	Muestra la imagen como archivos y directorios, permitiendo ver incluso aquellos que estarían ocultos por el sistema operativo.
Búsqueda por palabra clave	Permite buscar dentro de la imagen palabras clave, pueden ser archivos o cualquier otra referencia que se le pase como argumento.
Tipo de archivo	Permite tanto la búsqueda como la ordenación de archivos según su tipo.
Detalles de la imagen	Muestra en detalle la imagen a examinar, permitiendo saber dónde se encuentran físicamente los datos dentro de ella.
Matadatos	Permite ver elementos del sistema de archivos que no se muestran habitualmente, como las referencias a directorios o los archivos eliminados.
Unidad de datos	Ofrece la posibilidad de entrar en el máximo detalle de cualquier archivo, permitiendo examinar el contenido real del mismo, ya sea en ASCII o en hexadecimal.

Las herramientas expuestas anteriormente necesitan de la ejecución sobre un sistema operativo ya instalado. En ocasiones es de gran utilidad disponer de un entorno tipo *Live*, que nos permita realizar un examen forense de imágenes sin tener que dedicar un equipo específico para ello y sin necesidad cargar otro sistema operativo. Algunas de ellas son:

HELIX CD

Se trata de un Live CD de respuesta ante incidentes, basado en una distribución Linux denominada *Knoppix* (que a su vez está basada en Debian). Posee la mayoría de las herramientas necesarias para realizar un análisis forense tanto de equipos como de imágenes de discos. Se puede descargar gratuitamente de: http://www.e-fense.com/helix/.

F.I.R.E. Linux

Se trata de otro live CD que ofrece un entorno para respuestas a incidentes y análisis forense, compuesto por una distribución Linux a la que se le han añadido una serie de utilidades de seguridad, junto con un interfaz gráfico que hace realmente fácil su uso. Al igual que el kit anterior, por su forma de montar los discos no realiza ninguna modificación sobre los equipos en los que se ejecute, por lo que puede ser utilizado con seguridad. Este live CD está creado y mantenido por William Salusky y puede descargarse gratuitamente desde la dirección http://biatchux.dmzs.com.

BIBLIOGRAFÍA

- http://cert.inteco.es/Formacion/Conceptos_de_seguridad/
- http://es.wikipedia.org/wiki/Seguridad_de_la_informaci%C3%B3n
- http://es.wikipedia.org/wiki/Fiabilidad_de_sistemas
- http://www.alegsa.com.ar/Dic/vulnerabilidad.php
- http://redyseguridad.fi-p.unam.mx/proyectos/tsi/capi/Cap2.html (tutorial de seg.infor.)
- http://ldc.usb.ve/~poc/Seguridad-viejo/tcpip.pdf (vulnerabilidades)
- http://mmc.geofisica.unam.mx/LuCAS/Manuales-LuCAS/doc-unixsec/unixsec-html/node12.html
- http://www.arcert.gov.ar/politica/versionimpresa.htm
- http://www.segu-info.com.ar/fisica/seguridadfisica.htm
- http://www.internet-solutions.com.co/ser_fisica_logica.php
- ****http://www.ccee.edu.uy/ensenian/catcomp/material/Inform_%20II/SEGURIDAD2.pdf****
- http://www.segu-info.com.ar/fisica/seguridadfisica.htm
- http://rollanwar.blogspot.com/2010/07/ubicacion-y-proteccion-fisica-de-los.html
- http://es.tldp.org/Manuales-LuCAS/doc-como-seguridad-fisica/COMO-seguridad-fisica.html
- *****http://protegete.jccm.es/protegete/opencms/Pymes/Seguridad/SeguridadInformacion/proteccion.html
- http://cfievalladolid2.net/tecno/recursos/c_redes/archivos/Manual3.pdf
- http://www.uv.es/sto/cursos/icssu/html/ar01s04.html
- http://es.wikipedia.org/wiki/Sistema_de_alimentaci%C3%B3n_ininterrumpida
- http://www.cybernautas.es/seguridad_informatica/seguridad-fisica-informatica/
- http://es.wikipedia.org/wiki/Biometr%C3%ADa
- http://eju.tv/2009/04/que-son-los-sistemas-biometricos/
- http://es.wikipedia.org/wiki/Seguridad_l%C3%B3gica
- http://es.wikipedia.org/wiki/Copia_de_seguridad
- http://basicoyfacil.wordpress.com/2008/11/03/que-es-una-copia-de-seguridad/
- http://www.configurarequipos.com/doc44.html
- http://todosai.com/Tipos-de-SAI
- http://hobbies.fororama.com/t14-copias-de-seguridad-windows-sus-tipos
- http://es.kioskea.net/faq/180-crear-una-imagen-del-sistema-ghost
- http://www.slideshare.net/triplege/soportes-almacenamiento
- http://e-practica.blogspot.com/2009/09/soportes-y-formatos-view-more.html
- http://infomonica.galeon.com/enlaces1803415.html
- http://es.wikipedia.org/wiki/Blue-ray
- http://es.wikipedia.org/wiki/Centro_de_respaldo

- http://es.wikipedia.org/wiki/Red_de_%C3%A1rea_de_almacenamiento
- http://es.wikipedia.org/wiki/Network-attached_storage
- http://www.slideshare.net/MasterBase/cloud-computing-1282895
- http://www.abueloinformatico.es/vertutoriales.php?id=467&titulo=almacenamiento_en_la_nube_(cloud_storage)_o_discos_duros_virtuales&cat=Internet
- http://en.wikipedia.org/wiki/Cloud_storage
- http://www.nativeintelligence.com/SpanishDemo/spanish-demo-01.asp
- http://www.subinet.es/guias-y-tips/guias-tips-internet/%C2%BFque-es-el-control-de-acceso-en-sistemas-informaticos/
- http://www.unirioja.es/servicios/si/seguridad/difusion/politica_contrasenas.pdf
- http://es.wikipedia.org/wiki/Auditor%C3%ADa_de_seguridad_de_sistemas_de_informaci%C3%B3n
- http://e-archivo.uc3m.es/bitstream/10016/6136/1/PFC_German_Ramirez_Rodriguez.pdf
- http://www.zonagratuita.com/a-cursos/utilidades/50_herramientas_top.htm
- http://raulespinola.wordpress.com/2009/03/27/criptografia-y-la-informatica/
- http://es.wikipedia.org/wiki/Criptograf%C3%ADa
- http://www.microsoft.com/business/es-es/Content/Paginas/article.aspx?cbcid=323
- http://www.segu-info.com.ar/politicas/polseginf.htm
- http://david-jose.blogspot.com/2008/12/bitdefender-antivirus-2009-kaspersky.html
- http://www.netzweb.net/html/print/segurid/det_int.pdf
- http://mariia93.wikispaces.com/Seguridad+activa+y+pasiva
- http://www-2.dc.uba.ar/materias/crip/docs/ardita01.pdf
- http://www.oas.org/juridico/spanish/cyb_analisis_foren.pdf
- http://www.conectronica.com/Seguridad/Seguridad-forense-t%C3%A9cnicas-antiforenses-respuesta-a-incidentes-y-gesti%C3%B3n-de-evidencias-digitales.html
- http://www.kpmg.com/ES/es/QueHacemos/Advisory/PublishingImages/fasesEvidenciaDigital_gr.jpg