Adopción de pautas de seguridad informática

Seguridad y Alta Disponibilidad

Autor: Miguel Ángel García Felipe

I.E.S GREGORIO PRIETO

UD 1: "Introducción a los servicios de red e Internet"

- **Introducción. Seguridad informática.**
- **Fiabilidad, confidencialidad, integridad y disponibilidad.**
- **Elementos vulnerables en el sistema informático: hardware, software y datos.**
- **Análisis de las principales vulnerabilidades de un sistema informático.**
- **Amenazas Físicas y Lógicas.**
- **Seguridad física y ambiental.**
- **Ubicación y protección física de los equipos y servidores.**
- **Sistemas de alimentación ininterrumpidas.**
- **Sistemas biométricos.**
- **Seguridad lógica: Copias de seguridad e imágenes de respaldo.**
- **Dispositivos de almacenamiento de datos.**
- **Almacenamiento redundante y distribuido: RAID y Centros de Respaldo.**
- **Centro de respaldo.**
- **Almacenamiento remoto: SAN, NAS y almacenamiento clouding.**
- **Políticas de almacenamiento.**
- **Identificación, autenticación y autorización.**
- **Política de contraseñas.**
- **Concepto. Tipos de auditorías.**
- **Pruebas y herramientas de auditoría informática.**
- **Criptografía. Objetivos. Conceptos. Historia.**
- **Políticas de Seguridad Informática.**
- **Seguridad Activa y Pasiva.**
- **Análisis Forense.**
- **Herramientas de análisis forense.**
- **Bibliografía.**

- **Introducción. Seguridad informática.**

Garantizar que los recursos informáticos de una compañía estén disponibles para cumplir sus propósitos, es decir, que no estén dañados o alterados por circunstancias o factores externos, es una definición útil para conocer lo que implica el concepto de seguridad informática.

En términos generales, la seguridad puede entenderse como aquellas reglas técnicas y/o actividades destinadas a prevenir, proteger y resguardar lo que es considerado como susceptible de robo, pérdida o daño, ya sea de manera personal, grupal o empresarial.

En este sentido, es la información el elemento principal a **proteger, resguardar y recuperar** dentro de las redes empresariales.

Existen dos tipos de seguridad con respecto a la naturaleza de la amenaza:

- **Seguridad lógica**: aplicaciones para seguridad, herramientas informáticas, etc.
- **Seguridad física:** mantenimiento eléctrico, anti-incendio, humedad, etc.

- **Fiabilidad, confidencialidad, integridad y disponibilidad.**

Fiabilidad

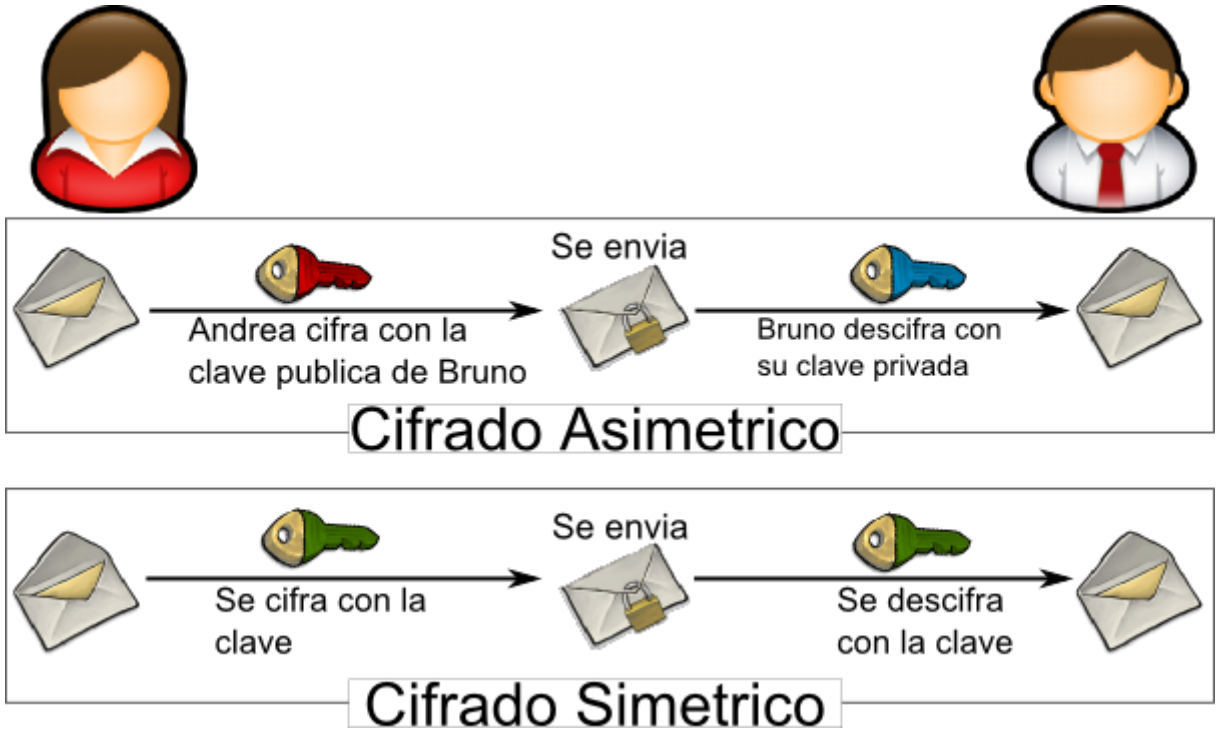
La fiabilidad de un sistema es la probabilidad de que ese sistema funcione o desarrolle una cierta función, bajo condiciones fijadas y durante un período determinado (por ejemplo, condiciones de presión, temperatura, velocidad, tensión o forma de una onda eléctrica, nivel de vibraciones, etc.).

Confidencialidad

Se trata de 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.

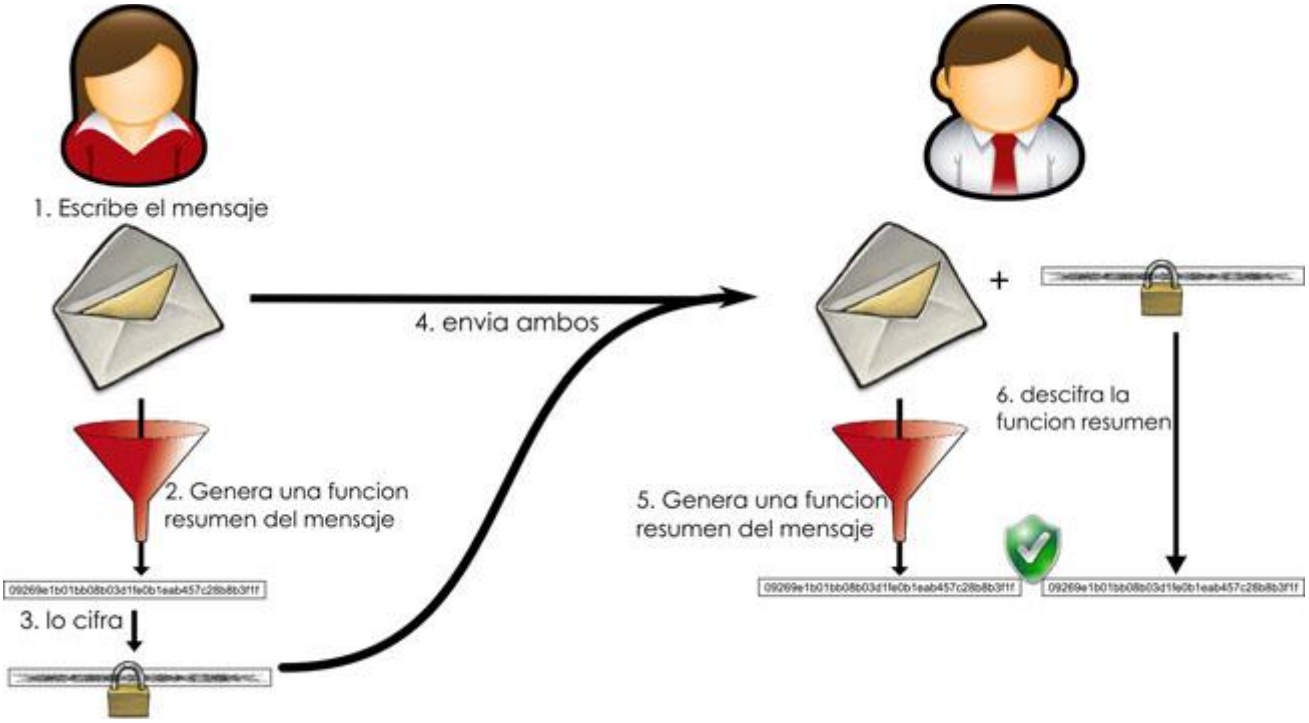
De esta manera se dice que un documento (o archivo o mensaje) es confidencial si y solo si puede ser comprendido por la persona o entidad a quien va dirigida o esté autorizada. En el caso de un mensaje esto evita que exista una intercepción de este y que pueda ser leído por una persona no autorizada.

Por ejemplo, si Andrea quiere enviar un mensaje a Bruno y que solo pueda leerlo Bruno, Andrea cifra el mensaje con una clave (simétrica o asimétrica), de tal modo que solo Bruno sepa la manera de descifrarlo, así ambos usuarios están seguros que solo ellos van a poder leer el mensaje.



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.



Teniendo como muestra el ejemplo anterior. Finalmente Bruno compara ambas funciones resumen, que se trata de una función que produce un valor alfanumérico que identifica cualquier cambio que se produzca en el mensaje, y si estas funciones son iguales, quiere decir que no ha existido manipulación del mensaje

Disponibilidad

Se trata de la capacidad de un servicio, de unos datos o de un sistema, a ser accesible y utilizable por los usuarios (o procesos) autorizados cuando estos lo requieran.

La disponibilidad además de ser importante en el proceso de seguridad de la información, es además variada en el sentido de que existen varios mecanismos para cumplir con los niveles de servicio que se requiera, tales mecanismos se implementan en infraestructura tecnológica, servidores de correo electrónico, de bases de datos, de web etc, mediante el uso de clusters o arreglos de discos, equipos en alta disponibilidad a nivel de red, servidores espejo, replicación de datos, redes de almacenamiento (SAN), enlaces redundantes, etc. La gama de posibilidades dependerá de lo que queremos proteger y el nivel de servicio que se quiera proporcionar.

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

Una **vulnerabilidad** o fallo de seguridad, es todo aquello que provoca que nuestros sistemas informáticos funcionen de manera diferente para lo que estaban pensados, **afectando a la seguridad** de los mismos, pudiendo llegar a provocar entre otras cosas la pérdida y robo de información sensible.

Algunas vulnerabilidades principales son:

-Físicas: están presentes en los ambientes en los cuales la información se está almacenando o manejando.

- Instalaciones inadecuadas.
- Ausencia de equipos de seguridad.
- Cableados desordenados y expuestos.
- Falta de identificación de personas, equipos y áreas.

-Naturales: Están relacionadas con las condiciones de la naturaleza.

- Humedad.
- Polvo.
- Temperaturas indebidas.
- Agentes contaminantes naturales.
- Desastres naturales.
- Seísmos.

-Hardware: Los defectos o fallas de fabricación o configuración de los equipos atacan y o alteran a los mismos.

- Ausencia de actualizaciones.
- Conservación inadecuada.

-Software: Permite la ocurrencia de accesos indebidos a los sistemas y por ende a la información.

- Configuración e instalación indebida de los programas.
- Sistemas operativos mal configurados y mal organizados.
- Correos maliciosos.
- Ejecución de macro virus.
- Navegadores de Internet.

-Medios de almacenaje: La utilización inadecuada de los medios de almacenaje afectan a la integridad, la confidencialidad y la disponibilidad de la información.

- Plazo de validez y de caducidad.
- Defectos de fabricación.
- Uso incorrecto.
- Mala calidad.
- Áreas o lugares de depósito inadecuados.

-Comunicación: Esto abarca todo el tránsito de la información, ya sea cableado, satelital, fibra óptica u ondas de radio inalámbricas.

- Fallo en cualquiera de estos medios.
- Defectos de fabricación.

- Mala calidad.

-Humanas: Son daños que las personas pueden causar a la información, a los equipos y a los ambientes tecnológicos. Los puntos débiles humanos pueden ser intencionados o no.

- La mayor tipo de vulnerabilidad es el desconocimiento de las medidas de seguridad adecuadas o simplemente el no acatarlas.

- **Análisis de las principales vulnerabilidades de un 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.

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 de Windows), para **ejecutar instrucciones que puedan comprometer la integridad del sistema**.

Secuencias de comandos en sitios cruzados (XSS)

Este tipo de vulnerabilidad abarca cualquier ataque que permita ejecutar código de "scripting", como VBScript 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 a XSS, o incluso el navegador en sí. El problema está 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 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. Un ejemplo es cuando un programa realiza una sentencia SQL sin querer con parámetros dados por el usuario para luego hacer una consulta de base de datos. En dichos parámetros que da el usuario estaría el código malicioso. Con estas inyecciones de código se pueden obtener múltiples resultados tales como datos escondidos, eliminar o sobrescribir datos en la base de datos y hasta lograr ejecutar comandos peligrosos en la máquina donde está 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. Se utilizan las funciones include, include_once, require, require_once las cuales son utilizadas para incluir en una página web otras páginas por tanto el atacante podrá obtener una Shell (es una interfaz con el sistema operativo, gracias a él podremos dar las órdenes y mandatos para que el sistema realice las tareas que necesitamos) en el servidor de la víctima y ejecutar un archivo. Para que se pueda ejecutar dicho archivo debe tener una extensión diferente a ".php" ya que con esta extensión el archivo se ejecutaría en el servidor del atacante y no en el de la víctima, así un archivo ".txt", ".gif"... serian algunos de los más adecuados.

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 (Buffer overflow u overrun): 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. Son defectos de programación y existen algunos lenguajes que impiden que los desbordamientos puedan ocurrir.

- El agotamiento del búfer (buffer underflow o underrun): 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. Esto requiere que la lectura del programa o del dispositivo del búfer detenga brevemente su proceso.

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.

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.

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 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.

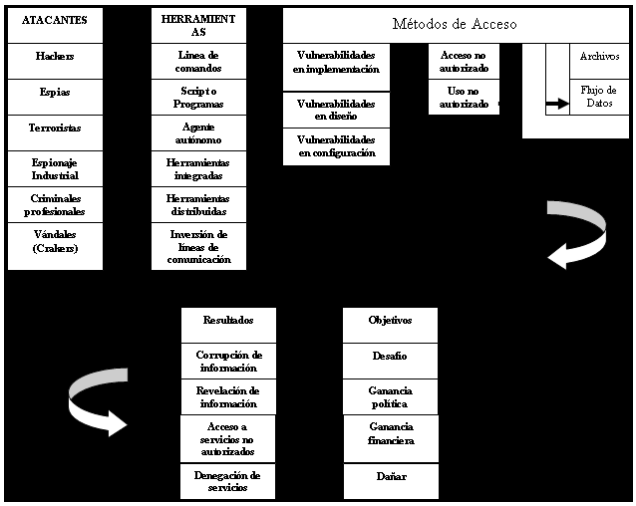
Error de diseño

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.


Vulnerabilidades por año
12000
10000
8000
6000
4000
2000
0
2001
2002
2003
2004
2005
2006
2007
2008
2009

- **Amenazas Físicas y Lógicas.**

- **Amenazas lógicas:**



- **Software incorrecto**

-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.

- **Herramientas de seguridad**

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.

- **Puertas traseras**

Lo peor que puede pasarle cuando está en el Messenger o en el ICQ no es que contraiga su PC un virus informático. Lo peor es que alguien instale un backdoor en su PC. Las puertas traseras son fáciles de entender. Como todo en Internet se basa en la arquitectura cliente / servidor, sólo se necesita instalar un programa servidor en una máquina para poder controlarla a distancia desde otro equipo, si se cuenta con el cliente adecuado, ésta puede bien ser la computadora de un usuario descuidado o poco informado.

- **Bombas lógicas**

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.

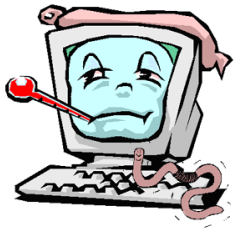
- **Canales cubiertos**

Ruido Como cualquier canal de comunicación, oculto o no, los canales cubiertos pueden ser ruidosos o inmunes al ruido; idealmente, un canal inmune al ruido es aquél en que la probabilidad de que el receptor escuche exactamente lo que el emisor ha transmitido es 1: sin importar factores externos, no hay interferencias en la transmisión. Evidentemente, en la práctica es muy difícil conseguir estos canales tan perfectos, por lo que es habitual aplicar códigos de corrección de errores aunque éstos reduzcan el ancho de banda del canal.

Flujos de información De la misma forma que en las líneas convencionales de transmisión de datos se aplican técnicas (multiplexación en el tiempo, multiplexación en frecuencia...) para maximizar el ancho de banda efectivo, en los canales cubiertos se puede hacer algo parecido. A los canales en los que se transmiten varios flujos de información entre emisor y receptor se les denomina agregados, y dependiendo de cómo se inicialicen, lean y reseteen las variables enviadas podemos hablar de agregación serie, paralela o híbrida; los canales con un único flujo de información se llaman no agregados.

- **Virus**

Amenazas:
-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...



- **Gusanos**

Los gusanos se basan en una red de computadoras para enviar copias de sí mismos a otros nodos (es decir, a otras terminales en la red) y son capaces de llevar esto a cabo sin intervención del usuario propagándose, utilizando Internet, basándose en diversos métodos, como SMTP, IRC, P2P entre otros.

- **Caballos de Troya**

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.

- **Programa conejo o bacteria**

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. Hemos de pensar hay ciertos programas que pueden actuar como conejos sin proponérselo; ejemplos típicos se suelen encontrar en los sistemas Unix destinados a prácticas en las que se enseña a programar al alumnado: es muy común que un bucle que por error se convierte en infinito contenga entre sus instrucciones algunas de reserva de memoria, lo que implica que si el sistema no presenta una correcta política de cuotas para procesos de usuario pueda venirse abajo o degradar enormemente sus prestaciones.

- **Técnicas salami**

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; si esto se automatiza para, por ejemplo, descontar una peseta de cada nómina pagada en la universidad o de cada beca concedida, tras un mes de actividad seguramente se habrá robado una enorme cantidad de dinero sin que nadie se haya percatado de este hecho, ya que de cada origen se ha tomado una cantidad ínfima.

- ## Amenazas físicas:

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:

- Disminuir siniestros.
- Trabajar mejor manteniendo la sensación de seguridad.
- Descartar falsas hipótesis si se produjeran incidentes.
- Tener los medios para luchar contra accidentes.

- **Seguridad física y ambiental.**

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, etc. (conceptos luego tratados); la seguridad de la misma será nula si no se ha previsto como combatir un incendio.

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 tratados a continuación se prevén, otros, como la detección de un atacante interno a la empresa que intenta a acceder físicamente a una sala de operaciones de la misma, no.

Esto puede derivar en que para un atacante sea más fácil lograr tomar y copiar una cinta de la sala, 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*"(1). 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.

Tipos de Desastres

No será la primera vez que se mencione en este trabajo, que cada sistema es único y por lo tanto la política de seguridad a implementar no será única. Este concepto vale, también, para el edificio en el que nos encontramos. Es por ello que siempre se recomendarán pautas de aplicación general y no procedimientos específicos. Para ejemplificar esto: valdrá de poco tener en cuenta aquí, en Entre Ríos, técnicas de seguridad ante terremotos; pero sí será de máxima utilidad en Los Angeles, EE.UU.

Este tipo de seguridad está enfocado a cubrir las amenazas ocasionadas tanto por el hombre como por la naturaleza del medio físico en que se encuentra ubicado el centro.

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.

No hace falta recurrir a películas de espionaje para sacar ideas de cómo obtener la máxima seguridad en un sistema informático, además de que la solución sería extremadamente cara.

A veces basta recurrir al sentido común para darse cuenta que cerrar una puerta con llave o cortar la electricidad en ciertas áreas siguen siendo técnicas válidas en cualquier entorno.

A continuación se analizan los peligros más importantes que se corren en un centro de procesamiento; con el objetivo de mantener una serie de acciones a seguir en forma eficaz y oportuna para la prevención, reducción, recuperación y corrección de los diferentes tipos de riesgos.

1. **Incendios**.
   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. Si hay sistemas de detección de fuego que activan el sistema de extinción, todo el personal de esa área debe estar entrenado para no interferir con este proceso automático.

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.

4. **Señales de Radar**

   La influencia de las señales o rayos de radar sobre el funcionamiento de una computadora 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.**
   En la medida que los sistemas se vuelven más complicados se hace más necesaria la presencia de un especialista para evaluar riesgos particulares y aplicar soluciones que estén de acuerdo con una norma de seguridad industrial.

6. **Ergometría.**
   La **Ergonomía** es una disciplina que se ocupa de estudiar la forma en que interactúa el cuerpo humano con los artefactos y elementos que lo rodean, buscando que esa interacción sea lo menos agresiva y traumática posible

Acciones Hostiles

1. **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.
   Es frecuente que los operadores utilicen la computadora de la empresa para realizar trabajos privados o para otras organizaciones y, de esta manera, robar tiempo de máquina. La información importante o confidencial puede ser fácilmente copiada.
2. **Fraude**
   Cada año, millones de dólares son sustraídos de empresas y, en muchas ocasiones, las computadoras han sido utilizadas como instrumento para dichos fines.
   Sin embargo, debido a que ninguna de las partes implicadas (compañía, empleados, fabricantes, auditores, etc.), tienen algo que ganar, sino que más bien pierden en imágen, no se da ninguna publicidad a este tipo de situaciones.

3. **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.

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.

- **Ubicación y protección física de los equipos y servidores.**

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.
Cuando hay que instalar un nuevo centro de cálculo es necesario fijarse en varios factores. En concreto, elegirá la ubicación en función de la disponibilidad física y la facilidad para modificar aquellos aspectos que vayan a hacer que la instalación sea más segura. Existen una serie de factores que dependen de las instalaciones propiamente dichas, como son:

- El edificio. Debemos evaluar aspecto como el espacio del que se dispone, cómo es el acceso de equipos y personal, y qué características tienen las instalaciones de suministro eléctrico, acondicionamiento térmico, etc.

- Tratamiento acústico. En general, se ha de tener en cuenta que habrá equipos, como los de aire acondicionado, necesarios para refrigerar los servidores, que son bastante ruidosos. Deben instalarse en entornos donde el ruido y la vibración estén amortiguados.

- Seguridad física del edificio. Se estudiará el sistema contra incendios, la protección contra inundaciones y otros peligros naturales que puedan afectar a la instalación.

- Suministro eléctrico propio del CPD. La alimentación de los equipos de un centro de procesamiento de datos tiene que tener unas condiciones especiales, ya que no puede estar sujeta a las fluctuaciones o picos de la red eléctrica que pueda sufrir el resto del edificio. No suele ser posible disponer de toda una red de suministro eléctrico propio, pero siempre es conveniente utilizar un sistema independiente del resto de la instalación y elementos de protección y seguridad específicos.

- Existen otra serie de factores inherentes a la localización, es decir, condiciones ambientales que rodean al local donde vayamos a instalar el CPD. Los principales son los factores naturales, los servicios disponibles, especialmente de energía eléctrica y comunicaciones, y otras instalaciones de la misma zona; y la seguridad del entorno, ya que la zona donde vaya situarse el CPD debe ser tranquila, pero no un sitio desolado.

Algunos tipos de protección física:

1. **Utilización de Guardias**.
2. **Utilización de Detectores de Metales.**
   El detector de metales es un elemento sumamente práctico para la revisión de personas, ofreciendo grandes ventajas sobre el sistema de palpación manual.
   La sensibilidad del detector es regulable, permitiendo de esta manera establecer un volumen metálico mínimo, a partir del cual se activará la alarma.

La utilización de este tipo de detectores debe hacerse conocer a todo el personal. De este modo, actuará como elemento disuasivo.

3. **Utilización de Sistemas Biométricos.**
   La biometría es el estudio de métodos automáticos para el reconocimiento único de humanos basados en uno o más rasgos conductuales o físicos intrínsecos. En las tecnologías de la información, la autentificación biométrica se refiere a las tecnologías para medir y analizar las características físicas y del comportamiento humanas con propósito de autentificación.

4. **Verificación Automática de Firmas (VAF)**
   En este caso lo que se considera es lo que el usuario es capaz de hacer, aunque también podría encuadrarse dentro de las verificaciones biométricas.
   Mientras es posible para un falsificador producir una buena copia visual o facsímil, es extremadamente difícil reproducir las dinámicas de una persona: por ejemplo la firma genuina con exactitud.
   La VAF, usando emisiones acústicas toma datos del proceso dinámico de firmar o de escribir. La secuencia sonora de emisión acústica generada por el proceso de escribir constituye un patrón que es único en cada individuo. El patrón contiene información extensa sobre la manera en que la escritura es ejecutada.
5. **Seguridad con Animales**
   Sirven para grandes extensiones de terreno, y además tienen órganos sensitivos mucho más sensibles que los de cualquier dispositivo y, generalmente, el costo de cuidado y mantenimiento se disminuye considerablemente utilizando este tipo de sistema.
   Así mismo, este sistema posee la desventaja de que los animales pueden ser engañados para lograr el acceso deseado.
6. **Protección Electrónica**.
   Se llama así a la detección de robo, intrusión, asalto e incendios mediante la utilización de sensores conectados a centrales de alarmas. Estas centrales tienen conectadas los elementos de señalización que son los encargados de hacerles saber al personal de una situación de emergencia. Cuando uno de los elementos sensores detectan una situación de riesgo, éstos transmiten inmediatamente el aviso a la central; ésta procesa la información recibida y ordena en respuesta la emisión de señales sonoras o luminosas alertando de la situación.

Conclusiones

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

Las distintas alternativas estudiadas son suficientes para conocer en todo momento el estado del medio en el que nos desempeñamos; y así tomar decisiones sobre la base de la información brindada por los medios de control adecuados.

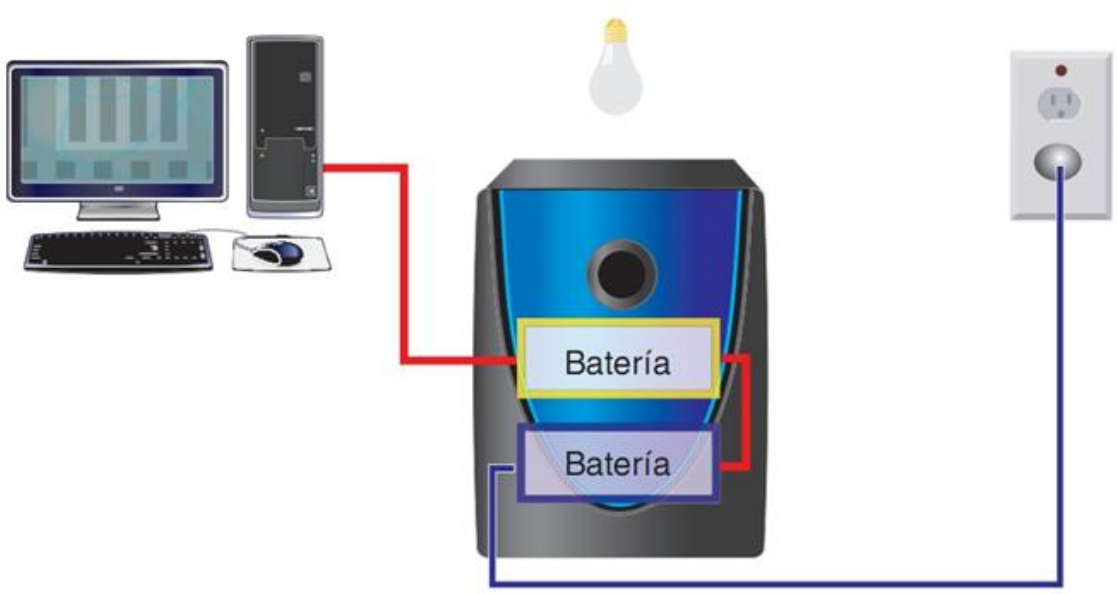
- **Sistemas de alimentación ininterrumpidas.**

Un **SAI** o sistema de alimentación ininterrumpida (en inglés Uninterruptible Power Supply, UPS), es un dispositivo electrónico que permite proteger a los equipos frente a los picos o caídas de tensión. De esta manera se dispone de una mayor estabilidad frente a los cambios del suministro eléctrico y de una fuente de alimentación auxiliar cuando se produce un corte de luz.
Este tipo de sistemas nacieron originalmente con el objetivo de proteger el trabajo que se estaba realizando en el momento en que se producía un apagón. Posteriormente se le ha agregado capacidad para poder continuar trabajando cierto tiempo, aunque no se disponga de suministro.

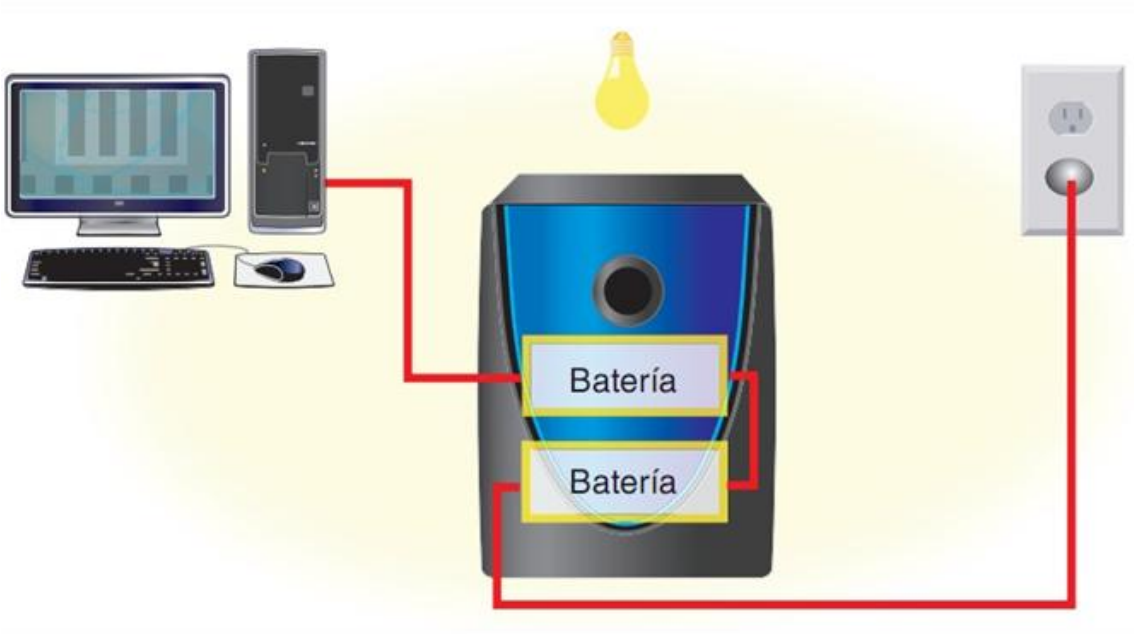
Tipos de SAI:

En general, podemos identificar dos tipos de SAI, en función de su forma de trabaja:

- Sistemas de alimentación en **estado de espera** o **Stand-by Power Systems (SPS)**. Este tipo de SAI activa la alimentación desde baterías automáticamente cuando detecta un fallo en el suministro eléctrico.



- **SAI en línea (on-line),** que alimenta el ordenador de modo continuo, aunque no exista un problema en el suministro eléctrico, y al mismo tiempo recarga su batería. Este dispositivo tiene la ventaja de que ofrece una tensión de alimentación constante.



- **Sistemas Biométricos.**

Entenderemos por *sistema biométrico* a un sistema automatizado que realiza labores de biometría. Es decir, un sistema que fundamenta sus decisiones de reconocimiento mediante una característica personal que puede ser reconocida o verificada de manera automatizada. En esta sección son descritas algunas de las características más importantes de estos sistemas.

Modelo del proceso de identificación personal

Cualquier proceso de identificación personal puede ser comprendido mediante un modelo simplificado. Este postula la existencia de tres indicadores de identidad que definen el proceso de identificación:

1. ***Conocimiento:*** **la persona tiene conocimiento (por ejemplo: un código).**
2. ***Posesión:*** **la persona posee un objeto (por ejemplo: una tarjeta).**
3. ***Característica:*** **la persona tiene una característica que puede ser verificada (por ejemplo: una de sus huellas dactilares).**

Cada uno de los indicadores anteriores genera una estrategia básica para el proceso de identificación personal. Además pueden ser combinados con el objeto de alcanzar grados de seguridad más elevados y brindar, de esta forma, diferentes niveles de protección. Distintas situaciones requerirán diferentes soluciones para la labor de identificación personal. Por ejemplo, con relación al *grado de seguridad*, se debe considerar el valor que está siendo protegido así como los diversos tipos de amenazas. También es importante considerar la reacción de los usuarios y el costo del proceso.

Características de un indicador biométrico

Un indicador biométrico es alguna característica con la cual se puede realizar biometría. Cualquiera sea el indicador, debe cumplir los siguientes requerimientos:

1-*Universalidad:* cualquier persona posee esa característica.

2-Unicidad: **la existencia de dos personas con una característica idéntica tiene una probabilidad muy pequeña.**
3-*Permanencia:* la característica no cambia en el tiempo.
4-***Cuantificación:*** **la característica puede ser medida en forma cuantitativa**.

Los requerimientos anteriores sirven como criterio para descartar o aprobar a alguna característica como *indicador biométrico*.

Características de un sistema biométrico para identificación personal

Las características básicas que un sistema biométrico para identificación personal debe cumplir pueden expresarse mediante las restricciones que deben ser satisfechas. Ellas apuntan, básicamente, a la obtención de un sistema biométrico con utilidad práctica. Las restricciones antes señaladas apuntan a que el sistema considere:

El desempeño, que se refiere a la exactitud, la rapidez y la robustez alcanzada en la identificación, además de los recursos invertidos y el efecto de factores ambientales y/u operacionales. El objetivo de esta restricción es comprobar si el sistema posee una exactitud y rapidez aceptable con un requerimiento de recursos razonable.

La aceptabilidad, que indica el grado en que la gente está dispuesta a aceptar un sistema biométrico en su vida diaria. Es claro que el sistema no debe representar peligro alguno para los usuarios y debe inspirar "confianza" a los mismos. Factores psicológicos pueden afectar esta última característica. Por ejemplo, el reconocimiento de una retina, que requiere un contacto cercano de la persona con el dispositivo de reconocimiento, puede desconcertar a ciertos individuos debido al hecho de tener su ojo sin protección frente a un "aparato". Sin embargo, las características anteriores están subordinadas a la aplicación específica. En efecto, para algunas aplicaciones el efecto psicológico de utilizar un sistema basado en el reconocimiento de características oculares será positivo, debido a que este método es eficaz implicando mayor seguridad.

La fiabilidad, que refleja cuán difícil es burlar al sistema. El sistema biométrico debe reconocer características de una persona viva, pues es posible crear dedos de látex, grabaciones digitales de voz prótesis de ojos, etc. Algunos sistemas incorporan métodos para determinar si la característica bajo estudio corresponde o no a la de una persona viva. Los métodos empleados son ingeniosos y usualmente más simples de lo que uno podría imaginar. Por ejemplo, un sistema basado en el reconocimiento del iris revisa patrones característicos en las manchas de éste, un sistema infrarrojo para chequear las venas de la mano detecta flujos de sangre caliente y lectores de ultrasonido para huellas dactilares revisan estructuras subcutáneas de los dedos.

Arquitectura de un sistema biométrico para identificación personal

Los dispositivos biométricos poseen tres componentes básicos. El primero se encarga de la adquisición análoga o digital de algún indicador biométrico de una persona, como por ejemplo, la adquisición de la imagen de una huella dactilar mediante un escáner. El segundo maneja la compresión, procesamiento, almacenamiento y comparación de los datos adquiridos (en el ejemplo una imagen) con los datos almacenados. El tercer componente establece una interfaz con aplicaciones ubicadas en el mismo u otro sistema. La arquitectura típica de un sistema

biométrico se presenta en la figura 1. Esta puede entenderse conceptualmente como dos módulos:

1. *Módulo de inscripción (enrollment module) y*
2. *Módulo de identificación (identification module).*

El módulo de inscripción se encarga de adquirir y almacenar la información proveniente del indicador biométrico con el objeto de poder contrastar a ésta con la proporcionada en ingresos posteriores al sistema. Las labores ejecutadas por el módulo de inscripción son posibles gracias a la acción del lector biométrico y del extractor de características.

El primero se encarga de adquirir datos relativos al indicador biométrico elegido y entregar una representación en formato digital de éste. El segundo extrae, a partir de la salida del lector, características representativas del indicador. El conjunto de características anterior, que será almacenado en una base de datos central u otro medio como una tarjeta magnética, recibirá el nombre de template. En otras palabras un template es la información representativa del indicador biométrico que se encuentra almacenada y que será utilizada en las labores de identificación al ser comparada con la información proveniente del indicador biométrico en el punto de acceso.

El módulo de identificación es el responsable del reconocimiento de individuos, por ejemplo en una aplicación de control de acceso. El proceso de identificación comienza cuando el lector biométrico captura la característica del individuo a ser identificado y la convierte a formato digital, para que a continuación el extractor de características produzca una representación compacta con el mismo formato de los *templates*. La representación resultante se denomina query y es enviada al comparador de *características* que confronta a éste con uno o varios *templates* para establecer la identidad.

Un sistema biométrico en su fase operacional puede operar en dos modos:

1. *Modo de verificación*
2. *Modo de identificación*

Un sistema biométrico operando en el modo de verificación comprueba la identidad de algún individuo comparando la característica sólo con los templates del individuo.

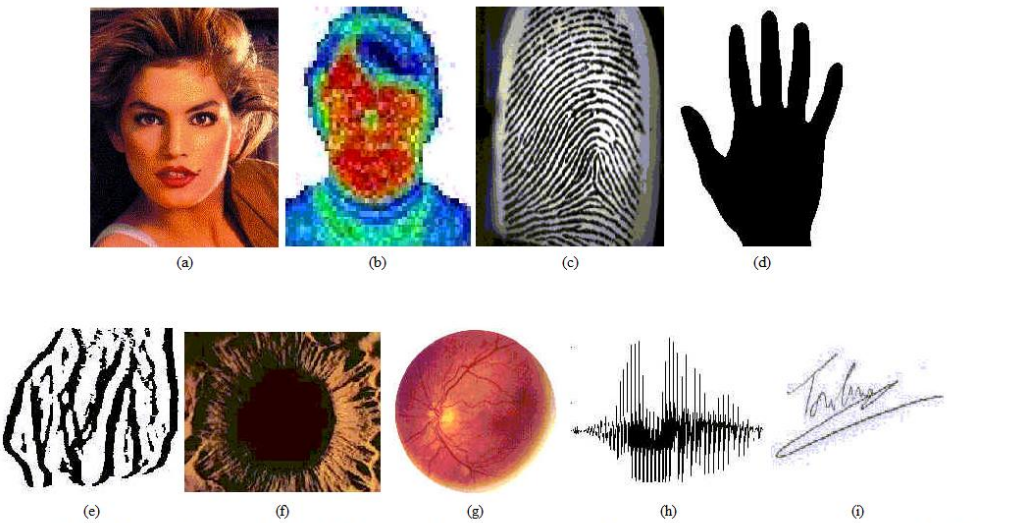
Un sistema biométrico operando en el modo de identificación descubre a un individuo mediante una búsqueda *exhaustiva* en la base de base de datos con los templates

Sistemas biométricos actuales.

En la actualidad existen sistemas biométricos que basan su acción en el reconocimiento de diversas características, como puede apreciarse en la figura 3. Las técnicas biométricas más conocidas son nueve y están basadas en los siguientes indicadores biométricos:

1. Rostro,
2. Termograma del rostro,
3. Huellas dactilares,
4. Geometría de la mano,
5. Venas de las manos,
6. Iris,
7. Patrones de la retina,
8. Voz,
9. Firma.

Cada una de las técnicas anteriores posee ventajas y desventajas comparativas, las cuales deben tenerse en consideración al momento de decidir que técnica utilizar para una aplicación específica. En particular deben considerarse las diferencias entre los métodos anatómicos y los de comportamiento. Una huella dactilar, salvo daño físico, es la misma día a día, a diferencia de una firma que puede ser influenciada tanto por factores controlables como por psicológicos no intencionales. También las máquinas que miden características físicas tienden a ser más grandes y costosas que las que detectan comportamientos.



Técnicas biométricas actuales: (a) Rostro, (b) Termograma Facial, (c) Huella dactilar, (d) Geometría de la mano, (e) Venas de la mano, (f) Iris, (g) Patrones de la retina, (h) Voz e (i) Firma.

Estándares Biométricos

BioAPI. El consorcio BioAPI nace en Abril de 1998 durante la conferencia CardTech/SecureTech con el apoyo de algunas de las compañías informáticas más importantes a nivel internacional como IBM y Hewlett-Packard. La primera especificación apareció en Septiembre de 2000 y la especificación final en Marzo de 2001.

Estándar BAPI. BAPI es un nuevo estándar biométrico desarrollado y planeado por un vendedor de soluciones biométricas llamado I/O Software en lugar de un consorcio de compañías e instituciones como fue el caso de BioAPI. En Mayo de 2000, Microsoft licenció BAPI, aunque había sido uno de los primeros en apostar por BioAPI, con la intención de incluirlo en las futuras versiones de sus sistemas operativos (Windows).

CBEFF (Common Biometric Exchange File Forma). Se ha desarrollado un estándar conocido como Formato de Ficheros Común para el Intercambio Biométrico (CBEFF), cuyo objetivo es definir los formatos de los patrones biométricos para facilitar el acceso y el intercambio de diferentes tipos de datos biométricos a los sistemas que integran esta tecnología o entre diferentes componentes de un mismo sistema.

Estándar ANSI X9.84. La industria de servicios financieros tiene necesidades particulares en cuanto a la integración de soluciones biométricas en sus propios procesos y sistemas. Estas necesidades especiales

influyen en la definición de los estándares biométricos recomendados por la industria financiera para la creación e integración de productos biométricos en sus plataformas y soluciones.

HA-API (Human Authentication Application Program Interface)El Consosrcio Biométrico americano (US Biometric Consortium) dirige, de forma coordinada con el gobierno americano, los esfuerzos en biometría que se llevan a cabo en Estados Unidos desde 1993.

NBCT (United States National Biometric Test Center) Este centro fue creado por el Consorcio Biométrico del Departamento de Defensa Americano a finales de 1997.

Seguridad Lógica

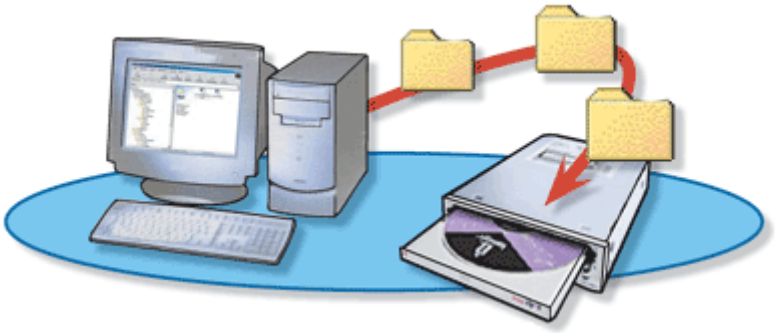
La **seguridad lógica** se refiere a la seguridad en el uso de software y los sistemas, la protección de los datos, procesos y programas, así como la del acceso ordenado y autorizado de los usuarios a la información. La "seguridad lógica" involucra todas aquellas medidas establecidas por la administración - 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.

- **Copias de seguridad e imágenes de respaldo.**

Una **copia de seguridad** o **backup** (su nombre en inglés) en tecnología de la 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. 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.



Tipos de copia de seguridad

La utilidad Copia de seguridad admite cinco métodos para hacer copia de seguridad de los datos del equipo o de la red.

-Copia de seguridad de copia

Copia todos los archivos seleccionados pero no los marca individualmente como copiados (es decir, no desactiva el atributo de modificado). Este método es útil cuando desea realizar copias de seguridad de archivos entre copias de seguridad normales e incrementales, ya que no afecta a estas otras operaciones.

-Copia de seguridad diaria

Copia todos los archivos seleccionados que se hayan modificado el día en que se realiza la copia diaria. Los archivos incluidos en la copia de seguridad no se marcan como copiados (es decir, no se desactiva el atributo de modificado).

-Copia de seguridad diferencial

Copia los archivos creados o modificados desde la última copia de seguridad normal o incremental. Los archivos no se marcan como copiados (es decir, no se desactiva el atributo de modificado). Si realiza una combinación de copias de seguridad normal y diferencial, para restaurar los archivos y las carpetas debe disponer de la última copia de seguridad normal y de la última copia de seguridad diferencial.

-Copia de seguridad incremental

Sólo copia los archivos creados o modificados desde la última copia de seguridad normal o incremental. Marca los archivos como copiados (es decir, se desactiva el atributo de modificado). Si usa una combinación de copias de seguridad normal e incremental, la restauración de los datos debe realizarse con el último conjunto copia de seguridad normal y todos los conjuntos de copia de seguridad incremental.

-Copia de seguridad normal

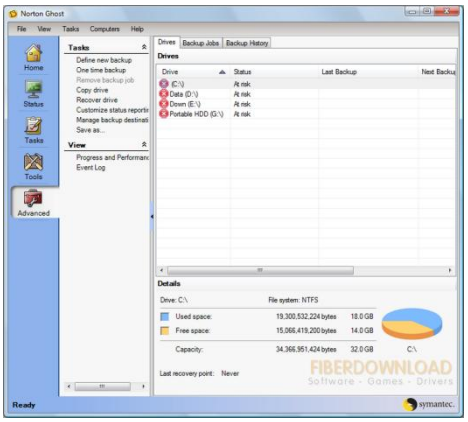
Copia todos los archivos seleccionados y los marca como copiados (es decir, se desactiva el atributo de modificado). En las copias de seguridad normales sólo necesita la copia más reciente del archivo o la cinta que contiene la copia de seguridad para restaurar todos los archivos. Las copias de seguridad normales se suelen realizar al crear por primera vez un conjunto de copia de seguridad.

La combinación de copias de seguridad normales e incrementales utiliza el mínimo espacio de almacenamiento posible y es el método de copia de seguridad más rápido. Sin embargo, la recuperación de archivos puede ser difícil y laboriosa ya que el conjunto de copia de seguridad puede estar repartido entre varios discos o cintas.

Si realiza una copia de seguridad de sus datos empleando una combinación de copias de seguridad normales y diferenciales consumirá más tiempo, especialmente si los datos sufren cambios frecuentes, aunque será más fácil restaurar los datos ya que el conjunto de copia de seguridad sólo estará repartido en unos pocos discos o cintas.

Imágenes de respaldo.

Una **imagen de respaldo** 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 respaldo usualmente se produce creando una copia, sector por sector, del medio de origen y por lo tanto replicando perfectamente la estructura y contenidos de un dispositivo de almacenamiento.



Copias de seguridad del sistema. Algunos programas de copias de seguridad solo copian los archivos de usuario; la información de arranque y los archivos bloqueados por el sistema operativo, como aquellos en uso al momento de la copia de seguridad, pueden no ser guardados en algunos sistemas operativos. Una imagen de disco contiene todos los archivos, replicando fielmente todos los datos. Por esta razón, también son usadas para hacer copias de seguridad de CD y de DVD.

Despliegue rápido de sistemas clones. Las empresas de tamaño considerable a menudo necesitan comprar o reemplazar computadoras nuevas en grandes números. Instalar el sistema operativo y los programas en cada una de ellas uno por uno exige mucho tiempo y esfuerzo y tiene una importante posibilidad de errores humanos. Por lo tanto, los administradores de sistema usan imágenes de disco para clonar rápidamente el entorno de software completamente preparado de un sistema que hace de referencia. Este método ahorra tiempo y esfuerzo y permite a los administradores enfocarse en las distinciones únicas que cada sistema deberá llevar.

Proceso de creación de una imagen

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*, como ya se ha mencionado, es habitualmente usada para replicar los contenidos de un disco duro para usarlos en otra computadora. 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). Pero las similitudes con la creación de imágenes forense terminan aquí. Las imágenes forenses se obtienen habitualmente usando herramientas de software como EnCase y FTK.

Formatos de archivo

En la mayoría de los casos, un formato de archivo está atado a un paquete de software particular. El software define y usa su propio, a menudo privativo, formato de imagen, aunque algunos formatos son ampliamente aceptados por productos competentes entre sí. Una excepción a los formatos de imagen privativos es la ***imagen ISO*** para discos ópticos, la cual incluye en conjunto los formatos ***ISO 9660*** **y UDF** *(Universal Disk Format, formato de disco universal),* ambos definidos por estándares abiertos. Estos formatos son soportados por casi todos los paquetes de software de discos ópticos.

- **Soportes de almacenamiento.**

Una parte fundamental para un sistema informático es su capacidad de leer y almacenar datos.

Algunos tipos o medios de almacenamiento son los siguientes:

DISQUETES

Es el primer sistema de almacenamiento extraíble que se instaló en un PC.

Los primeros disquetes salieron al mercado en 1.967 como dispositivos de solo lectura. Posteriormente, en el año 1.976, salieron al mercado los primeros disquetes aplicados a PC, de 5.25', que consistían en un estuche de cartón y en su interior un disco de plástico recubierto de material magnetizado, con una capacidad en los últimos modelos de 1.2 MB.

En el año 1.984 aparecen los primeros disquetes de 3.5”, con un estuche de plástico rígido y un disco de plástico de mayor densidad, lo que a pesar de la reducción de tamaño permitió incrementar la capacidad. Con una capacidad en principio de 360 Kb (una sola cara) pasó en 1.986 al formato DS o *Double Side* (2 caras x 360 Kb.) y posteriormente, en el año 1.987, a los disquetes de alta densidad (HD o *High Density*), de 1.44 Mb. (2 caras x 720 Kb.).

Estos son los mismos que utilizamos hoy en día, convirtiendo a las disqueteras de 3.5' en el elemento que menos ha evolucionado en la historia del PC, ya que no ha cambiado en nada en los últimos 20 años (de hecho, una disquetera de 1.987 es exactamente igual a una de 2.006 y funciona perfectamente en cualquier ordenador actual, por potente y avanzado que sea, al igual que el disquete correspondiente).

DISCOS DUROS

Es el medio de almacenamiento por excelencia. Desde que en 1.955 saliera el primer disco duro hasta nuestros días, el disco duro o HDD ha tenido un gran desarrollo.

El disco duro está compuesto básicamente de:

- Varios discos de metal magnetizado, que es donde se guardan los datos.
- Un motor que hace girar los discos.
- Un conjunto de cabezales, que son los que leen la información guardada en los discos.
- Un electroimán que mueve los cabezales.
- Un circuito electrónico de control, que incluye el interface con el ordenador y la memoria caché.
- Una caja hermética (aunque no al vacío), que protege el conjunto.

Si hablamos de disco duro podemos citar los distintos tipos de conexión que poseen los mismos con la placa base, es decir pueden ser **SATA, IDE, SCSI o SAS**:

- **IDE**: Integrated Device Electronics ("Dispositivo electrónico integrado") o ATA (Advanced Technology Attachment), controla los dispositivos de almacenamiento masivo de datos, como los discos duros y ATAPI (Advanced Technology Attachment Packet Interface) Hasta aproximadamente el 2004, el estándar principal por su versatilidad y asequibilidad. Son planos, anchos y alargados.
- **SCSI**: Son interfaces preparadas para discos duros de gran capacidad de almacenamiento y velocidad de rotación. Se presentan bajo tres especificaciones: SCSI Estándar (Standard SCSI), SCSI Rápido (Fast SCSI) y SCSI Ancho-Rápido (Fast-Wide SCSI). Su tiempo medio de acceso puede llegar a 7 milisegundos y su velocidad de transmisión secuencial de información puede alcanzar teóricamente los 5 Mbps en los discos SCSI Estándares, los 10 Mbps en los discos SCSI Rápidos y los 20 Mbps en los discos SCSI Anchos-Rápidos (SCSI-2). Un controlador SCSI puede manejar hasta 7 discos duros SCSI (o 7 periféricos SCSI) con conexión tipo margarita (daisy-chain). A diferencia de los discos IDE, pueden trabajar asincrónicamente con relación al microprocesador, lo que posibilita una mayor velocidad de transferencia.
- **SATA** (*Serial ATA*): El más novedoso de los estándares de conexión, utiliza un bus serie para la transmisión de datos. Notablemente más rápido y eficiente que IDE. Existen tres versiones, SATA 1 con velocidad de transferencia de hasta 150 MB/s *(hoy día descatalogado)*, SATA 2 de hasta 300 MB/s, el más extendido en la actualidad; y por último SATA 3 de hasta 600 MB/s el cual se está empezando a hacer hueco en el mercado. Físicamente es mucho más pequeño y cómodo que los IDE, además de permitir conexión en caliente.
- **SAS** (*Serial Attached SCSI*): Interfaz de transferencia de datos en serie, sucesor del SCSI paralelo, aunque sigue utilizando comandos SCSI para interaccionar con los dispositivos SAS. Aumenta la velocidad y permite la conexión y desconexión en caliente. Una de las principales características es que aumenta la velocidad de transferencia al aumentar el número de dispositivos conectados, es decir, puede gestionar una tasa de transferencia constante para cada dispositivo conectado, además de terminar con la limitación de 16 dispositivos existente en SCSI, es por ello que se vaticina que la tecnología SAS irá reemplazando a su predecesora SCSI. Además, el conector es el mismo que en la interfaz SATA y permite utilizar estos discos duros, para aplicaciones con menos necesidad de velocidad, ahorrando costes. Por lo tanto, las unidades SATA pueden ser utilizadas por controladoras SAS pero no a la inversa, una controladora SATA no reconoce discos SAS.

LAPICES DE MEMORIA

Creados por IBM en 1.998 para sustituir a los disquetes en las IBM Think Pad, los lápices de memoria (también llamados Memory Pen y Pendrive) funcionan bajo el Estándar **USB Mass Storage** (almacenamiento masivo USB).

Los actuales Pendrive usan el estándar USB 2.0, con una transferencia de hasta 480 Mbit/s, aunque en la práctica trabajan a 160 Mbit/s.

Están compuestos básicamente por:

- Un conector USB macho
- Un controlador USB, que incorpora un pequeño micro RISC y mini memorias RAM y ROM
- Uno o varios chips de memoria Flash NAND
- Un cristal oscilador a 12 Mh para el control de flujo de salida de datos

Dependiendo de su capacidad (pueden llegar hasta los 60 Gb), se puede trabajar con ellos como si de un disco duro se tratase, incluso (si la placa base del ordenador lo permite) arrancando desde ellos.
Tienen grandes ventajas sobre otros sistemas de almacenamiento, como su rapidez, resistencia al polvo, golpes, humedad, etc. (dependiendo de la carcasa que contenga el Pendrive) y estabilidad de los datos.

Su bajo coste actual los convierten en el 3er sistema de almacenaje más económico en relación capacidad/precio (por detrás de los discos duros y de los cd,s y dvd,s, aunque con grandísimas ventajas sobre estos últimos). Actualmente quizás sea la forma más cómoda y compatible de transportar datos.

Una variante de los lápices de memoria son los reproductores de MP3 y MP4. Estos no son más que lápices de memoria a los que se les ha incorporado una pila, una pantallita, una salida de audio y un chip programado para leer y reproducir ciertos archivos, de música en el caso de los MP3 y de música y video en los MP4, y controlar las demás funciones. Evidentemente, un MP3 también nos puede servir para transportar datos de un ordenador a otro, ya que, en la inmensa mayoría de los casos, los ordenadores lo reconocen como sistema de almacenamiento masivo.

TARJETAS DE MEMORIA

Basadas en memorias del tipo flash, pero, a diferencia de los lápices de memoria, sin controladores, por lo que necesitan de unidades lectoras para poder funcionar.

Los tipos más comunes son:

Secure Digital (SD)
Con una capacidad de hasta 4 Gb, son las más empleadas. Basadas en las MMC, algo anteriores en su creación, son físicamente del mismo tamaño, aunque algo más gruesas las SD. También son más rápidas que las MMC y tienen una pestaña anti sobre escritura en un lateral.

TransFlash o **Micro SD**
Usadas en telefonía Móvil. Con adaptador para lectores de tarjetas

Compact Flash (CF)
Con una capacidad de hasta 8 Gb.

Multimedia Card (MMC)
Con una capacidad de hasta 1 gb

Mini MMC
Usadas sobre todo en telefonía móvil. Con adaptador para lectores de tarjetas.

Smart Media (SM)
Con una capacidad de hasta 256 Mb.

XD
Tarjeta propietaria de Olympus y Fujitsu, con una capacidad de hasta 1 Gb.

Este medio está en plena evolución, por lo que las capacidades son solo orientativas. Entre ellas existen diferencias, tanto de velocidad de transmisión de datos (incluso entre tarjetas del mismo tipo) como, sobre todo, de forma y tamaño.
Es un medio práctico de transportar información debido a su tamaño y capacidad, pero tiene la desventaja sobles los lápices de memoria de que es necesario un adaptador para poder leerlas.

UNIDADES ZIP

En el año 1.994, la empresa Iomega saca al mercado un sistema de almacenamiento denominado ZIP, con un formato de 3 ½", pero bastante más gruesos (casi el doble) que un disquete. Con una capacidad en principio de 100 Mb y posteriormente de 250 Mb, pronto se convirtió en una excelente solución para el trasporte de archivos y copias de seguridad, al ser mucho más rápidos que los disquetes, más resistentes y mucho más estables en las grabaciones. En la actualidad, en su formato domestico, hay ZIP de hasta 1.44 Gb (750 Mb sin comprimir). La salida de los ZIP, en buena parte, impidió el desarrollo de los LS-120, ya que eran más económicos, mucho más rápidos y menos sensibles al medio que estos. El ZIP, al igual que el disquete, se puede usar como si fuero un disco más, pudiéndose ejecutar programas desde el (incluso SO, arrancando desde el ZIP), trabajar con los datos almacenados en él, etc.
Si bien para su uso profesional son sumamente interesantes, para el uso domestico nunca han tenido una gran difusión, debido a la aparición en el mercado de los cds grabables y, posteriormente, de los dvd´s.

CDs

Desde su aparición para uso en ordenadores en 1.985 han evolucionado bastante poco. Algo en capacidad (los más usados son los de 80 minutos / 700 Mb), aunque bastante en velocidad de grabación, desde las primeras grabadoras a 1x (150 Kb/s) hasta las grabadoras actuales, que graban a una velocidad de 52x (7.800 Kb/s). Los cds se han convertido en el medio estándar tanto para distribuir programas como para hacer copias de seguridad, grabaciones multimedia, etc., debido a su capacidad relativamente alta (hay cds de 800 mb y de 900 Mb) y, sobre todo, a su bajo coste.

DVDs

Por su mayor capacidad (de 4.5 Gb en los normales y de 8,5 Gb en los de doble capa) y mayor calidad en la grabación, es el medio ideal para multimedia de gran formato y copias de seguridad de gran capacidad. Existen dos tipos diferentes de e DVD: DVD –R y DVD +R. Ambos tipos son compatibles en un 90% de los lectores y su diferencia se debe más a temas de patentes que a temas técnicos (aunque existen algunas pequeñas diferencias). Al igual que ocurre con los cds, una vez cerrada su grabación, esta no se puede alterar, pero también existen DVDs regrabables, tanto **+R** como **–R**. Hay también DVD de 8 cm. que son usados por algunas videocámaras digitales en sustitución de la tradicional cinta de 8 mm.

Blu-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.

- **Almacenamiento redundante y distribuido: RAID y Centros de Respaldo**

¿Qué es 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. Dependiendo de su configuración (a la que suele llamarse «nivel»), los beneficios de un RAID respecto a un único disco son uno o varios de los siguientes: mayor integridad, mayor tolerancia a fallos, mayor rendimiento y mayor capacidad. En sus implementaciones originales, su ventaja clave era la habilidad de combinar varios dispositivos de bajo coste y tecnología más antigua en un conjunto que ofrecía mayor capacidad, fiabilidad, velocidad o una combinación de éstas que un solo dispositivo de última generación y coste más alto.
En el nivel más simple, un RAID combina varios discos duros en una sola unidad lógica. Así, en lugar de ver varios discos duros diferentes, el sistema operativo ve uno solo. Los RAID suelen usarse en servidores y normalmente (aunque no es necesario) se implementan con unidades de disco de la misma capacidad.

Diferentes tipos de RAID:

Raids Básicos:

RAID 0

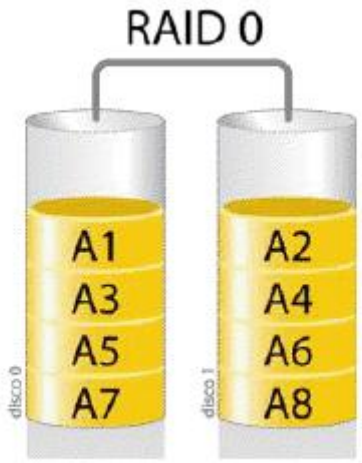


Diagrama de una configuración RAID 0.

Un **RAID 0** (también llamado **conjunto dividido** o **volumen dividido**) No tiene control de paridad ni es tolerante a fallos, lo que no lo hace utilizable como sistema de copia de seguridad. Este sistema multiplica la capacidad del menor de los discos por el número de discos instalados (aunque con algunas controladoras de gama alta se consigue que la capacidad total sea igual a la suma de la capacidad de los discos), creando una capacidad de almacenamiento equivalente al resultado de esta operación, utilizable como una sola unidad. A la hora de usar estos discos, divide los datos en bloques y escribe un

bloque en cada disco, lo que agiliza bastante el trabajo de escritura/lectura de los discos, dándose el mayor incremento de ganancia en velocidad cuando está instalado con varias controladoras RAID y un solo disco por controladora.

RAID 1

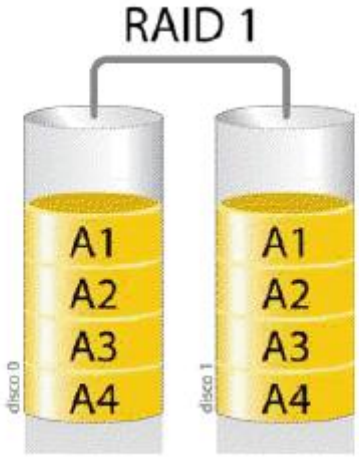


Diagrama de una configuración RAID 1.

El Raid 1 crea una copia exacta (espejo) de los datos en dos o más discos (array). Este sistema se suele utilizar cuando el rendimiento en la lectura resulta más importante que la capacidad de escritura. Si nos referimos a la seguridad, un Raid 0, como hemos comentado antes **no es tolerante al fallo de uno de sus discos**, sin embargo en un Raid 1 sí, ya que existe la misma información en cada uno de los discos.
Un Raid 1 clásico consiste en dos discos en espejo, lo que incrementa exponencialmente la fiabilidad respecto a un solo disco.
Al escribir, los datos deben de ser escritos en todos los discos del Raid 1, por lo que su rendimiento no mejora. El Raid 1 es un sistema muy utilizado cuando la disponibilidad es crítica 24 horas del día**.**

RAID 5

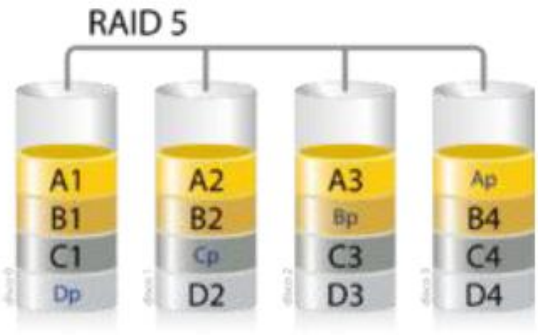


Diagrama de una configuración RAID 5.

Un **RAID 5** usa división de datos a nivel de bloques distribuyendo la información de paridad entre todos los discos miembros del conjunto. 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.

Cada vez que un bloque de datos se escribe en un RAID 5, se genera un bloque de paridad dentro de la misma división (stripe). Un bloque se compone a menudo de muchos sectores consecutivos de disco. Una serie de bloques (un bloque de cada uno de los discos del conjunto) recibe el nombre colectivo de división (stripe). Si otro bloque, o alguna porción de un bloque son escritos en esa misma división, el bloque de paridad (o una parte del mismo) es recalculada y vuelta a escribir. El disco utilizado por el bloque de paridad está escalonado de una división a la siguiente, de ahí el término «bloques de paridad distribuidos». Las escrituras en un RAID 5 son costosas en términos de operaciones de disco y tráfico entre los discos y la controladora.
El RAID 5 requiere al menos tres unidades de disco para ser implementado. El fallo de un segundo disco provoca la pérdida completa de los datos.El número máximo de discos en un grupo de redundancia RAID 5 es teóricamente ilimitado, pero en la práctica es común limitar el número de unidades. Los inconvenientes de usar grupos de redundancia mayores son una mayor probabilidad de fallo simultáneo de dos discos, un mayor tiempo de reconstrucción y una mayor probabilidad de hallar un sector irrecuperable durante una reconstrucción.

RAID 0+1

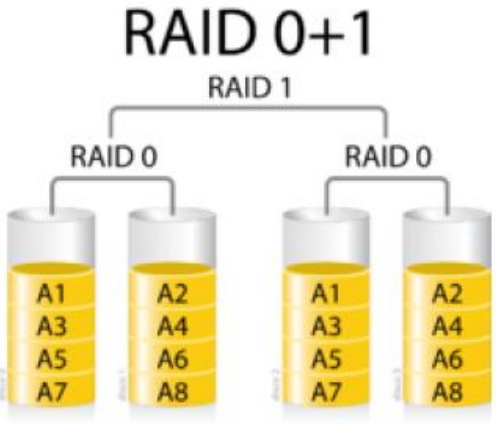


Diagrama de una configuración RAID 0+1.

Un **RAID 0+1** (también llamado **RAID 01**, que no debe confundirse con RAID 1) es un RAID usado para replicar y compartir datos entre varios discos. La diferencia entre un RAID 0+1 y un RAID 1+0 es la localización de cada nivel RAID dentro del conjunto final: un RAID 0+1 es un espejo de divisiones.
Como puede verse en el diagrama, primero se crean dos conjuntos RAID 0 (dividiendo los datos en discos) y luego, sobre los anteriores, se crea un conjunto RAID 1 (realizando un espejo de los anteriores). La ventaja de un RAID 0+1 es que cuando un disco duro falla, los datos perdidos pueden ser copiados del otro conjunto de nivel 0 para reconstruir el conjunto global. Sin embargo, añadir un disco duro adicional en una división, es obligatorio añadir otro al de la otra división para equilibrar el tamaño del conjunto.

RAID 1+0

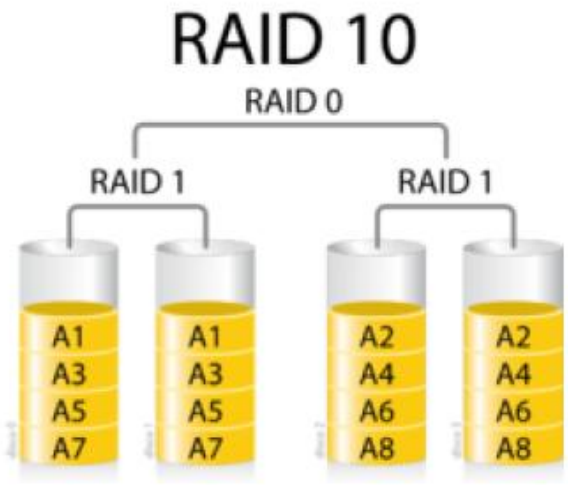


Diagrama de una configuración RAID 10.

Un **RAID 1+0**, a veces llamado **RAID 10**, es parecido a un RAID 0+1 con la excepción de que los niveles RAID que lo forman se invierte: el RAID 10 es una división de espejos.
En cada división RAID 1 pueden fallar todos los discos salvo uno sin que se pierdan datos. Sin embargo, si los discos que han fallado no se reemplazan, el restante pasa a ser un punto único de fallo para todo el conjunto. Si ese disco falla entonces, se perderán todos los datos del conjunto completo. Como en el caso del RAID 0+1, si un disco que ha fallado no se reemplaza, entonces un solo error de medio irrecuperable que ocurra en el disco espejado resultaría en pérdida de datos.
Debido a estos mayores riesgos del RAID 1+0, muchos entornos empresariales críticos están empezando a evaluar configuraciones RAID más tolerantes a fallos que añaden un mecanismo de paridad subyacente. Entre los más prometedores están los enfoques híbridos como el RAID 0+1+5 (espejo sobre paridad única) o RAID 0+1+6 (espejo sobre paridad dual).
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.

Centro de Respaldo

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.

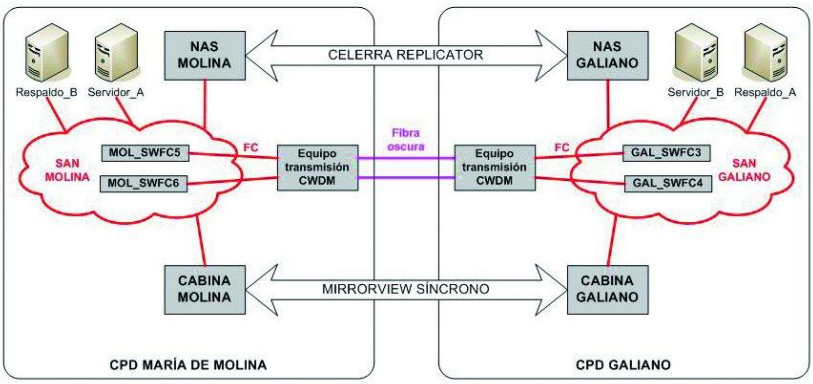
Existen dos políticas o aproximaciones a este problema:

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.

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.
- **Plan de emergencia**: Contempla las actuaciones necesarias durante un incidente.
- **Plan de recuperación:** Contempla las actuaciones necesarias después de un incidente.



- **Almacenamiento remoto: SAN, NAS y Clouding.**

El aumento del ancho de banda en las conexiones a internet y la mayor estabilidad de las mismas están favoreciendo la aparición de servicios de almacenamiento remoto que nos permiten subir nuestros ficheros y tenerlos tanto a nuestra disposición, como a la de nuestros clientes, compañeros o proveedores.

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.

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 computador (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 que un servidor Windows que comparte sus unidades por red es un sistema NAS, pero la definición suele aplicarse a sistemas específicos.

Los protocolos de comunicaciones NAS son 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.

COMPARATIVAS

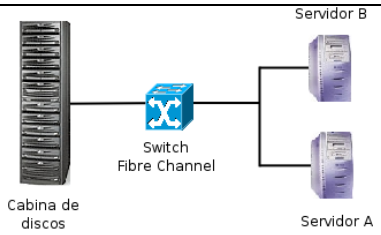
El opuesto a **NAS** es la conexión DAS (Direct Attached Storage) mediante conexiones SCSI o la conexión SAN (Storage Area Network) por fibra óptica, en ambos casos con tarjetas de conexión especificas de conexión al almacenamiento. Estas conexiones directas (DAS) son por lo habitual dedicadas.

En la tecnología NAS, las aplicaciones y programas de usuario hacen las peticiones de datos a los sistemas de ficheros de manera remota mediante protocolos CIFS y NFS, y el almacenamiento es local al sistema de ficheros. Sin embargo, DAS y SAN realizan las peticiones de datos directamente al sistema de ficheros.

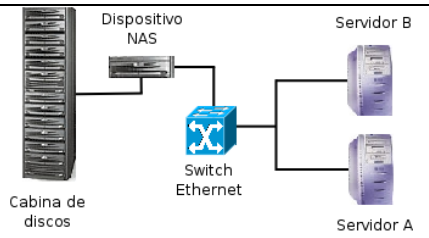
Las ventajas del NAS sobre la conexión directa (DAS) son la capacidad de compartir las unidades, un menor coste, la utilización de la misma infraestructura de red y una gestión más sencilla. Por el contrario, NAS tiene un menor rendimiento y fiabilidad por el uso compartido de las comunicaciones.

Una **SAN** se puede considerar una extensión de Direct Attached Storage (DAS). Donde en DAS hay un enlace punto a punto entre el servidor y su almacenamiento, una SAN permite a varios servidores

acceder a varios dispositivos de almacenamiento en una red compartida. Tanto en SAN como en DAS, las aplicaciones y programas de usuarios hacen sus peticiones de datos al sistema de ficheros directamente. La diferencia reside en la manera en la que dicho sistema de ficheros obtiene los datos requeridos del almacenamiento. En DAS, el almacenamiento es local al sistema de ficheros, mientras que en SAN, el almacenamiento es remoto. SAN utiliza diferentes protocolos de acceso como Fibre Channel y Gigabit Ethernet. En el lado opuesto se encuentra la tecnología Network-attached_storage (NAS), donde las aplicaciones hacen las peticiones de datos a los sistemas de ficheros de manera remota mediante protocolos CIFS y Network File System (NFS).



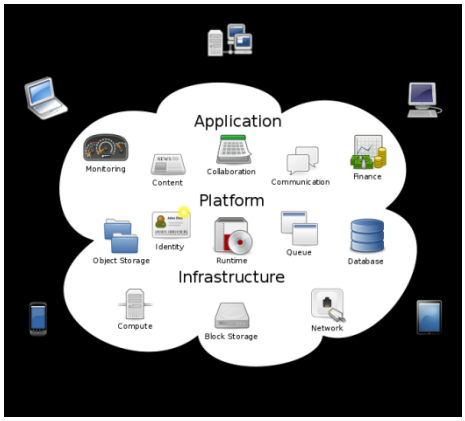
El **SAN** es un sistema de discos que se conecta a los servidores mediante redes de altísima velocidad (generalmente fibre channel). Se suele usar en servidores de BBDD donde los filesystems no se pueden montar por NFS o SAMBA y se necesita una comunicación rápida.



El **NAS** es un sistema de discos que se conecta a la red como cualquier otro dispositivo y se le asigna una dirección IP como un miembro más de la red. La comunicación puede darse por protocolos como SAMBA o NFS.

Cloud Computing

La **computación en la nube** concepto conocido también bajo los términos **informática en la nube**, **nube de cómputo** o **nube de conceptos**, del inglés *Cloud computing*, es un paradigma que permite ofrecer servicios de computación a través de Internet.



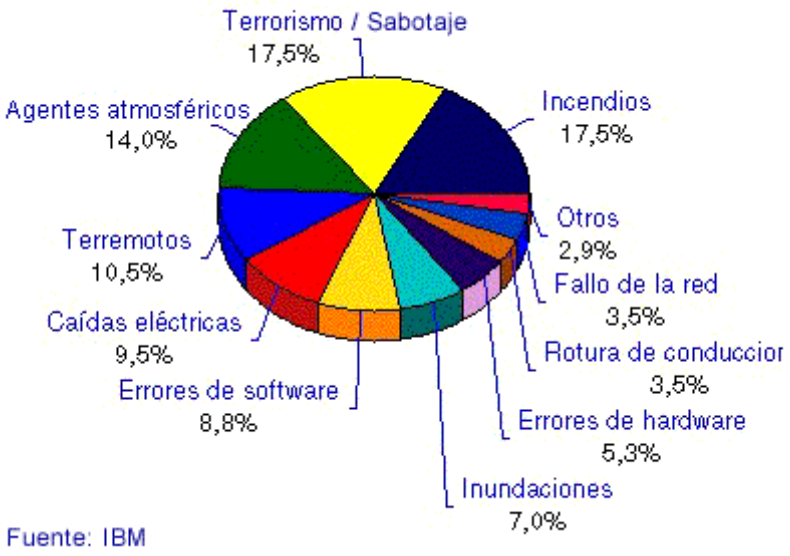
- **Políticas de almacenamiento.**

La tecnología no está exenta de fallas o errores, y los respaldos de información son utilizados como un plan de contingencia en caso de que una falla o error se presente.

Asimismo, hay empresas, que por la naturaleza del sector en el que operan (por ejemplo Banca) no pueden permitirse la más mínima interrupción informática.

Las interrupciones se presentan de formas muy variadas: virus informáticos, fallos de electricidad, errores de hardware y software, caídas de red, hackers, errores humanos, incendios, inundaciones, etc. Y aunque no se pueda prevenir cada una de estas interrupciones, la empresa sí puede prepararse para evitar las consecuencias que éstas puedan tener sobre su negocio. Del tiempo que tarde en reaccionar una empresa dependerá la gravedad de sus consecuencias.

Riesgo a los cuales se encuentran inmersos los Sistemas de Información



- Fuente: IBM

La única solución es tener copias de seguridad, actualizarlas con frecuencia y esperar que no deban usarse.

Respaldar la información significa copiar el contenido lógico de nuestro sistema informático a un medio que cumpla con una serie de exigencias:

- **1. Ser confiable:** Minimizar las probabilidades de error. Muchos medios magnéticos como las cintas de respaldo, los disquetes, o discos duros tienen probabilidades de error o son particularmente sensibles a campos magnéticos, elementos todos que atentan contra la información que hemos respaldado allí. Otras veces la falta de confiabilidad se genera al rehusar los medios magnéticos. Las cintas en particular tienen una vida útil concreta. Es común que se subestime este factor y se reutilicen más allá de su vida útil, con resultados nefastos, particularmente porque vamos a descubrir su falta de confiabilidad en el peor momento: cuando necesitamos RECUPERAR la información.

- **2. Estar fuera de línea, en un lugar seguro:** Tan pronto se realiza el respaldo de información, el soporte que almacena este respaldo debe ser desconectado de la computadora y almacenado en un lugar seguro tanto desde el punto de vista de sus requerimientos técnicos como

humedad, temperatura, campos magnéticos, como de su seguridad física y lógica. No es de gran utilidad respaldar la información y dejar el respaldo conectado a la computadora donde potencialmente puede haber un ataque de cualquier índole que lo afecte.

- **3. La forma de recuperación sea rápida y eficiente***:* Es necesario probar la confiabilidad del sistema de respaldo no sólo para respaldar sino que también para recuperar. Hay sistemas de respaldo que aparentemente no tienen ninguna falla al generar el respaldo de la información pero que fallan completamente al recuperar estos datos al sistema informático. Esto depende de la efectividad y calidad del sistema que realiza el respaldo y la recuperación.

Seguridad física y lógica:

Puede llegar a ser necesario eliminar los medios de entrada/salida innecesarios en algunos sistemas informáticos, tales como disqueteras y cdroms para evitar posible infecciones con virus traídos desde el exterior de la empresa por el personal, o la extracción de información de la empresa.

Las copias de seguridad son uno de los elementos más importantes y que requieren mayor atención a la hora de definir las medidas de seguridad del sistema de información, la misión de las mismas es la recuperación de los ficheros al estado inmediatamente anterior al momento de realización de la copia.

Control de acceso lógico

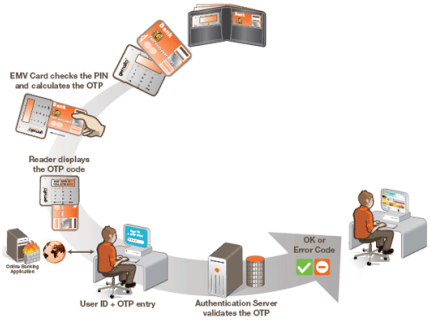
- **Identificación, autentificación y autorización.**

Identificación:

Es el proceso por el cual se comprueba que un usuario está autorizado a acceder a una serie de recursos. Este proceso de identificación se realiza normalmente mediante un nombre de usuario y contraseña; aunque actualmente también se utilizan los sistemas biométricos para realizar los procesos de identificación.

Autenticación:

Es la situación en la cual se puede verificar que un documento ha sido elaborado (o pertenece) a quien el documento dice. La autenticación se produce cuando el usuario puede aportar algún modo de que se pueda verificar que dicha persona es quien dice ser, a partir de ese momento se considera un usuario autorizado. Otra manera de definirlo seria, la capacidad de determinar si una determinada lista de personas ha establecido su reconocimiento sobre el contenido de un mensaje.



Autorización:

En ingeniería de seguridad y seguridad informática, la autorización es una parte del sistema operativo que protege los recursos del sistema permitiendo que sólo sean usados por aquellos consumidores a los que se les ha concedido autorización para ello. Los recursos incluyen archivos y otros objetos de dato, programas, dispositivos y funcionalidades provistas por aplicaciones. Ejemplos de consumidores son usuarios del sistema, programas y otros dispositivos.

- **Política de contraseñas**

Para gestionar correctamente la seguridad de las contraseñas, desde el Instituto Nacional de Tecnologías de la Comunicación (INTECO) se recomienda a los usuarios tener en cuenta las siguientes pautas para la creación y establecimiento de contraseñas seguras:

Política y acciones para construir contraseñas seguras:

1. Se deben utilizar al menos 8 caracteres para crear la clave. Según un estudio de la Universidad de Wichita, el número medio de caracteres por contraseña para usuarios entre 18 y 58 años habituales de Internet es de 7. Esto conlleva el peligro de que el tiempo para descubrir la clave se vea reducido a minutos o incluso segundos. Sólo un 36% de los encuestados indicaron que utilizaban un número de caracteres de 7 o superior.

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. Según el mismo estudio, el 86% de los usuarios utilizan sólo letras minúsculas, con el peligro de que la contraseña sea descubierta por un atacante casi instantáneamente.

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. Un 53% de los usuarios no cambian nunca la contraseña salvo que el sistema le obligue a ello cada cierto tiempo. 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. P. ej.: “Tr-.3Fre”. En este caso de incluir otros caracteres que no sean alfa-numéricos en la contraseña, hay que comprobar primero si el sistema permite dicha elección y cuáles son los permitidos. 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. Con ello, mediante esta sencilla mnemotecnia es más sencillo recordarla. Vg: de la frase “Comí mucho chocolate el domingo 3, por la tarde”, resultaría la contraseña: “cmCeD3-:xLt”. En ella, además, se ha introducido alguna mayúscula, se ha cambiado el “por” en una “x” y, si el sistema lo permite, se ha colocado algún signo de puntuación (-).

Acciones que deben evitarse en la gestión de contraseñas seguras:

1. Se debe evitar utilizar la misma contraseña siempre en todos los sistemas o servicios. Por ejemplo, si se utilizan varias cuentas de correo, se debe recurrir a contraseñas distintas para cada una de las cuentas. Un 55% de los usuarios indican que utilizan siempre o casi siempre la misma contraseña para múltiples sistemas, y un 33% utilizan una variación de la misma contraseña.

2. No utilizar información personal en la contraseña: nombre del usuario o de sus familiares, ni sus apellidos, ni su fecha de nacimiento. Y, por supuesto, en ninguna ocasión utilizar datos como el DNI o número de teléfono.

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, o derivados de estos. (ej.: no poner como contraseña apodos, el nombre del actor o de un personaje de ficción preferido, etc.).

8. No escribir ni reflejar la contraseña en un papel o documento donde quede constancia de la misma. Tampoco se deben guardar en documentos de texto dentro del propio ordenador o dispositivo (ej: no guardar las contraseñas de las tarjetas de débito/crédito en el móvil o las contraseñas de los correos en documentos de texto dentro del ordenador),

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 de diccionarios: Este método de ataque es conocido como *“ataque por diccionario”*.

10. No enviar nunca la contraseña por correo electrónico o en un sms. Tampoco se debe facilitar ni mencionar en una conversación o comunicación de cualquier tipo.

11. Si se trata de una contraseña para acceder a un sistema delicado hay que procurar limitar el número de intentos de acceso, como sucede en una tarjeta de crédito y cajeros, y que el sistema se bloquee si se excede el número de intentos fallidos permitidos. En este caso debe existir un sistema de recarga de la contraseña o “*vuelta atrás*”.

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 (bibliotecas, cibercafés, telecentros, etc.).

14. Cambiar las contraseñas por defecto proporcionadas por desarrolladores/fabricantes.

Auditorias de seguridad informática

• Concepto. Tipos de auditorías.

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.

Los servicios de auditoría constan de las siguientes fases:

- Enumeración de redes, topologías y protocolos
- Identificación de los sistemas operativos instalados
- Análisis de servicios y aplicaciones
- Detección, comprobación y evaluación de vulnerabilidades
- Medidas específicas de corrección
- Recomendaciones sobre implantación de medidas preventivas.

Tipos de auditoría

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 inoperatividad 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 softwares y la adquisición de nuevo hardware hacen necesario que los sistemas estén continuamente verificados mediante auditoría.

• 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:

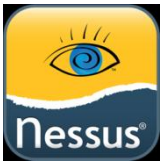
- Observación
- Realización de cuestionarios
- Entrevistas a auditados y no auditados
- Muestreo estadístico
- Flujogramas
- Listas de chequeo
- Mapas conceptuales

Algunas aplicaciones son:

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.

NMAP
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.

NESSUS
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.



AUTOAUDIT

Es una herramienta dirigida al departamento de auditoría, que permite realizar una planificación de Auditorías en función de Evaluación de Riesgos, siguiendo metodologías de evaluación vertical y/o por proceso. Soportando todo el proceso y flujo de trabajo, desde la fase de planificación, pasando por el trabajo de campo, hasta la preparación del informe final.

BACKTRACK

BackTrack es una distribución GNU/Linux en formato LiveCD pensada y diseñada para la auditoría de seguridad y relacionada con la seguridad informática en general.

Criptografía.

- **Objetivos. Concepto. Historia.**

La **criptografía** (del griego κρύπτω *krypto*, «oculto», y γράφως *graphos*, «escribir», literalmente «escritura oculta») es la técnica, bien sea aplicada al arte o la ciencia, que altera las representaciones lingüísticas de un mensaje.

Objetivo de la criptografia

En esencia la criptografía trata de enmascarar las representaciones caligráficas de una lengua, de forma discreta. Si bien, el área de estudio científico que se encarga de ello es la Criptología.

Para ello existen distintos métodos. Por ejemplo enmascarar las referencias originales de la lengua por un método de conversión gobernado por un algoritmo que permita el proceso inverso o descifrado de la información. El uso de esta u otras técnicas, permite un intercambio de mensajes que sólo puedan ser leídos por los destinatarios designados como 'coherentes'. Un destinatario coherente es la persona a la que el mensaje se le dirige con intención por parte del remitente. Así pues, el destinatario coherente conoce el discretismo usado para el enmascaramiento del mensaje. Por lo que, o bien posee los medios para someter el mensaje criptográfico al proceso inverso, o puede razonar e inferir el proceso que lo convierta en un mensaje de acceso público. En ambos casos, no necesita usar técnicas criptoanalíticas.

Un ejemplo cotidiano de criptografía es el que usamos cuando mandamos una carta. El mensaje origen queda enmascarado por una cubierta denominada sobre, la cual declara el destinatario coherente, que además conoce el proceso inverso para hacer público el mensaje contenido en el sobre.

Hay procesos más elaborados que, por decirlo de alguna manera, el mensaje origen trata de introducir cada letra usada en un 'sobre' distinto. Por ejemplo, la frase 'texto de prueba', pudiera estar representada por la siguiente notación cifrada: CF, F0, 114, 10E, 106, 72, F3, F6, 75, 10C, 111, 118, FB, F6, F5. El 'sobre' usado es de notación hexadecimal, si bien, el cálculo hexadecimal es de acceso público, no se puede decir que sea un mensaje discreto, ahora, si el resultado de la notación hexadecimal (como es el caso para el ejemplo) es consecuencia de la aplicación de un 'método' de cierre del 'sobre' (como lo es la cola de sellado, o el lacre en las tradicionales cartas), el destinatario debe de conocer la forma de abrirlo sin deteriorar el mensaje origen. En otras palabras, debe de conocer la contraseña. Para el ejemplo, la contraseña es '12345678'.

Conceptos

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. El verbo asociado es cifrar.

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:

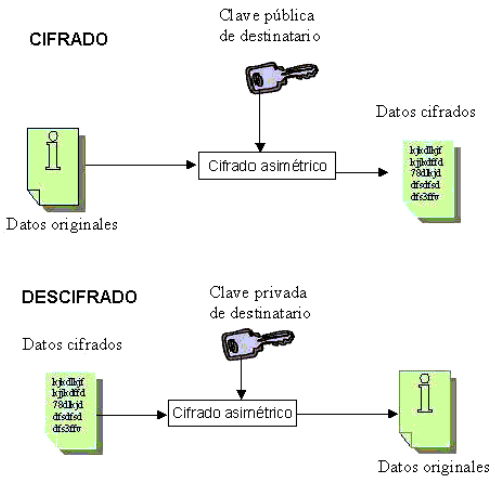
1.-Las claves simétricas: son las claves que se usan tanto para el cifrado como para el descifrado. En este caso hablamos de cifrado simétricos o cifrados con clave secreta.

2.-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. En inglés, el término decryption (descifrado) también se refiere al acto de intentar descifrar en forma ilegítima el mensaje (ya conozca o no el atacante la clave de descifrado). Cuando el atacante no conoce la clave de descifrado, hablamos de criptanálisis o criptoanálisis (también se usa el término decodificación).

La criptología es la ciencia que estudia los aspectos científicos de estas técnicas, es decir, combina la criptografía y el criptoanálisis.

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. Cifra es una antigua palabra arábiga para designar el número cero; en la Antigüedad, cuando Europa empezaba a cambiar del sistema de numeración romano al arábigo, se desconocía el cero, por lo que este resultaba misterioso, de ahí probablemente que cifrado signifique misterioso.

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.

En el lenguaje cotidiano, la palabra *código* se usa de forma indistinta con *cifra*. En la jerga de la criptografía, sin embargo, el término tiene un uso técnico especializado: los *códigos* son un método de criptografía clásica que consiste en sustituir unidades textuales más o menos largas o complejas, habitualmente palabras o frases, para ocultar el mensaje; por ejemplo, "cielo azul" podría significar «atacar al amanecer». Por el contrario, las *cifras* clásicas normalmente sustituyen o reordenan los elementos básicos del mensaje -letras, dígitos o símbolos-; en el ejemplo anterior, «rcnm arcteeaal aaa» sería un criptograma obtenido por *transposición*. Cuando se usa una técnica de códigos, la información secreta suele recopilarse en un *libro de códigos*.

Con frecuencia los procesos de cifrado y descifrado se encuentran en la literatura como *encriptado* y *desencriptado*, aunque ambos son neologismos erróneos —anglicismos de los términos ingleses *encrypt* y *decrypt*— todavía sin reconocimiento académico. Hay quien hace distinción entre *cifrado/descifrado* y *encriptado/desencriptado* según estén hablando de criptografía simétrica o asimétrica, pero la realidad es que la mayoría de los expertos hispanohablantes prefieren evitar ambos neologismos hasta el punto de que el uso de los mismos llega incluso a discernir a los aficionados y novatos en la materia de aquellos que han adquirido más experiencia y profundidad en la misma.

Las funciones de la criptografía

La criptografía se usa tradicionalmente para ocultar mensajes de ciertos usuarios. En la actualidad, esta función es incluso más útil ya que las comunicaciones de Internet circulan por infraestructuras cuya fiabilidad y confidencialidad no pueden garantizarse. La criptografía se usa no sólo para proteger la confidencialidad de los datos, sino también para garantizar su integridad y autenticidad.

Para qué sirve la criptografía

Los seres humanos siempre han sentido la necesidad de ocultar información, mucho antes de que existieran los primeros equipos informáticos y calculadoras.

Desde su creación, Internet ha evolucionado hasta convertirse en una herramienta esencial de la comunicación. Sin embargo, esta comunicación implica un número creciente de problemas estratégicos relacionados con las actividades de las empresas en la Web. Las transacciones que se realizan a través de la red pueden ser interceptadas y, sobretodo, porque actualmente resulta difícil establecer una legislación sobre Internet. La seguridad de esta información debe garantizarse: éste es el papel de la criptografía.

Historia de la criptografía

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. El primer método de criptografía fue en el siglo V a.C, era conocido como "Escítala". El segundo criptosistema que se conoce fue documentado por el historiador griego Polibio: un sistema de sustitución basado en la

posición de las letras en una tabla. 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 (según algunos autores, en realidad Julio César no usaba este sistema de sustitución, pero la atribución tiene tanto arraigo que el nombre de este método de sustitución ha quedado para los anales de la historia). 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.

En 1465 el italiano Leon Battista Alberti inventó un nuevo sistema de sustitución polialfabética que supuso un gran avance de la época. Otro de los criptógrafos más importantes del siglo XVI fue el francés Blaise de Vigenère que escribió un importante tratado sobre "la escritura secreta" y que diseñó una cifra que ha llegado a nuestros días asociada a su nombre. A Selenus se le debe la obra criptográfica "Cryptomenytices et Cryptographiae" (Luneburgo, 1624). Durante los siglos XVII, XVIII y XIX, el interés de los monarcas por la criptografía fue notable. Las tropas de Felipe II emplearon durante mucho tiempo una cifra con un alfabeto de más de 500 símbolos que los matemáticos del rey consideraban inexpugnable. Cuando el matemático francés François Viète consiguió criptoanalizar aquel sistema para el rey de Francia, a la sazón Enrique IV, el conocimiento mostrado por el rey francés impulsó una queja de la corte española ante del papa Pío V acusando a Enrique IV de utilizar magia negra para vencer a sus ejércitos. Por su parte, la reina María Estuardo, reina de Escocia, fue ejecutada por su prima Isabel I de Inglaterra al descubrirse un complot de aquella tras un criptoanálisis exitoso por parte de los matemáticos de Isabel.

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.

Desde el siglo XIX y hasta la Segunda Guerra Mundial, las figuras más importantes fueron la del holandés Auguste Kerckhoffs y la del prusiano Friedrich Kasiski. Pero es en el siglo XX cuando la historia de la criptografía vuelve a experimentar importantes avances. En especial durante las dos contiendas bélicas que marcaron al siglo: la Gran Guerra y la Segunda Guerra Mundial. A partir del siglo XX, la criptografía usa una nueva herramienta que permitirá conseguir mejores y más seguras cifras: las máquinas de cálculo. 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.

Tras la conclusión de la Segunda Guerra Mundial, la criptografía tiene un desarrollo teórico importante, siendo Claude Shannon y sus investigaciones sobre teoría de la información esenciales hitos en dicho desarrollo. Además, los avances en computación automática suponen tanto una amenaza para los sistemas existentes como una oportunidad para el desarrollo de nuevos sistemas. A mediados de los años 70, el Departamento de Normas y Estándares norteamericano publica el primer diseño lógico de un cifrador que estaría llamado a ser el principal sistema criptográfico de finales de siglo: el Estándar de Cifrado de Datos o DES. En esas mismas fechas ya se empezaba a gestar lo que sería la, hasta ahora, última revolución de la criptografía teórica y práctica: los sistemas asimétricos. Estos sistemas supusieron un salto cualitativo importante, ya que permitieron introducir la criptografía en otros campos que hoy día son esenciales, como el de la firma digital.

Medidas de seguridad

- **Política de seguridad.**

Una Política de Seguridad es un conjunto de requisitos definidos por los responsables de un sistema, que indica en términos generales que está y que no está permitido en el área de seguridad durante la operación general del sistema." **Política de Seguridad** se define como: "una declaración de intenciones de alto nivel que cubre la seguridad de los sistemas informáticos y que proporciona las bases para definir y delimitar responsabilidades para las diversas actuaciones técnicas y organizativas que se requerirán." La política se refleja en una serie de normas, reglamentos y protocolos a seguir, donde se definen las medidas a tomar para proteger la seguridad del sistema; pero... ante todo, "(...) una política de seguridad es una forma de comunicarse con los usuarios... Siempre hay que tener en cuenta que la seguridad comienza y termina con personas." y 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.
- Definición de violaciones y sanciones por no cumplir con las políticas.
- Responsabilidades de los usuarios con respecto a la información a la que tiene acceso.

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

- **Seguridad activa y 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.

Una práctica también para tener seguro nuestro ordenador es hacer particiones del disco duro, es decir dividirlo en distintas partes.

- **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.

Funcionalidades y fases de un análisis forense:

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.

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 original", 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.

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:

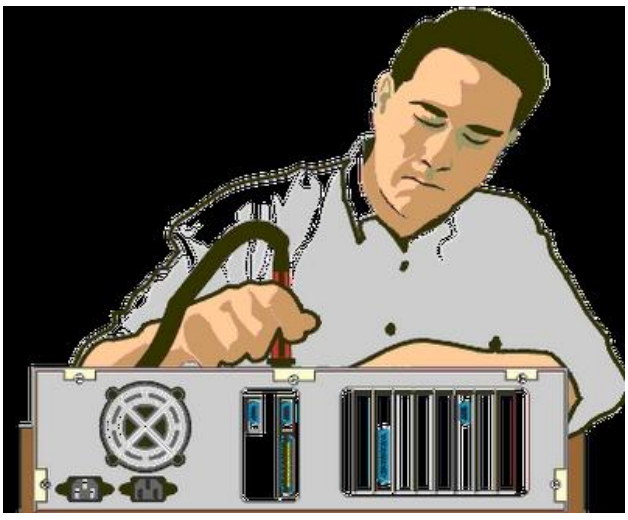
- Inodos asociados.
- Marcas de tiempo MACD (fecha y hora de modificación, acceso, creación y borrado).
- Ruta completa.
- Tamaño en bytes y tipo de fichero.
- Usuarios y grupos a quien pertenece.
- Permisos de acceso.
- Si fue borrado o no.

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 la posibilidad 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.

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.

- **Respuestas a incidentes**

(1) El proceso de identificar, preservar, analizar y presentar las evidencias digitales de una manera que sea aceptable legalmente en cualquier vista judicial o administrativa. Es decir recupera datos utilizando las reglas de evidencia.
(2) Implica obtener y analizar información digital para conseguir evidencias en casos administrativos, civiles o criminales.
(3) Implica examinar y analizar científicamente datos de medios de almacenamiento de computadores para que dichos datos puedan utilizarse como evidencias digitales en los juzgados.
(4) Aplicación de método científico para medios de almacenamiento digital para establecer información basada en los hechos para revisión judicial.
(5) Implica preservar, identificar, extraer, documentar e interpretar medios de almacenamiento de computador en busca de evidencias y/o análisis de la causa raíz. Se utilizan diversos métodos como:

(i) Descubrir datos en un sistema de computación.
(ii) Recuperar información de ficheros borrados, cifrados o dañados.
(iii) Monitorizar la actividad habida.
(iv) Detectar violaciones de la política corporativa. La información recogida permite el arresto, la persecución, el despido del empleado y la prevención de actividad ilegal futura. Una evidencia digital es cualquier información que puede estar o no sujeta a intervención humana que puede extraerse de un computador, debe estar en formato leíble por las personas y capaz de ser interpretado por una persona con experiencia en el tema.

- **Herramientas de análisis forenses**

HELIX CD
Este CD ofrece dos modos de funcionamiento, tras ejecutarlo nos permitirá elegir entre arrancar un entorno MS Windows o uno tipo Linux. En el primero de ellos disponemos de un entorno con un conjunto de herramientas, casi 90 Mb, que nos permitirá principalmente interactuar con sistemas "vivos", pudiendo recuperar la información volátil del sistema. En el arranque Linux, disponemos de un Sistema Operativo completo, con un núcleo modificado para conseguir una excelente detección de hardware, no realiza el montaje de particiones sswap, ni ninguna otra operación sobre el disco duro del equipo sobre el que se arranque. Es ideal para el análisis de equipos "muertos", sin que se modifiquen las evidencias pues montará los discos que encuentre en el sistema en modo sólo lectura. Además de los comandos de análisis propios de los entornos UNIX/Linux, se han incorporado una lista realmente interesante.

F.I.R.E. Linux
Se trata de otro CD de arranque 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. En esta interesantísima distribución podrá disponer de una serie de funcionalidades que le aportará muchas ventajas en su análisis, entre las que cabe

- ✓ Recolección de datos de un sistema informático comprometido y hacer un análisis forense.
- ✓ Chequear la existencia de virus o malware en general desde un entorno fiable.
- ✓ Posibilidad de realización de test de penetración y vulnerabilidad.
- ✓ Recuperación datos de particiones dañadas

- **Bibliografía.**

http://www.ciberhabitat.gob.mx/museo/cerquita/redes/seguridad/intro.htm
http://www.internet-solutions.com.co/ser_fisica_logica.php
http://cert.inteco.es/
http://www.segu-info.com.ar/fisica/seguridadfisica.htm
http://www.ecured.cu/index.php/Est%C3%A1ndar_biom%C3%A9trico
http://technet.microsoft.com/es-es/library/cc784306%28WS.10%29.aspx
http://www.monografias.com/trabajos14/respaldoinfo/respaldoinfo.shtml
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://es.wikipedia.org/wiki/Criptograf%C3%ADa
http://www.conectronica.com/Seguridad/Seguridad-forense-t%C3%A9cnicas-antiforenses-respuesta-a-incidentes-y-gesti%C3%B3n-de-evidencias-digitales.html