TEMA 1

ADOPCIÓN DE PAUTAS DE SEGURIDAD INFORMÁTICA

1. *Seguridad informática.*

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

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

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

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

2. Fiabilidad, confidencialidad, integridad y disponibilidad.

2.1. Fiabilidad.

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

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

2.2. Confidencialidad.

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

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

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

2.3. Integridad.

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

2.4. Disponibilidad.

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

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

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

Errores numéricos

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

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

Error en la gestión de recursos

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

Error de diseño

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

5. Amenazas. Tipos: físicas y lógicas.

5.1. Amenazas Lógicas

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

a) *Software incorrecto.*

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

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

b) *Herramientas de seguridad*

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

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

c) *Puertas traseras.*

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

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

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

d) Bombas lógicas

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

Ejemplos de acciones que puede realizar una bomba lógica:

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

e) Canales cubiertos

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

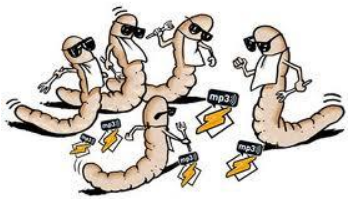
f) Virus

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

Algunas acciones que puede realizar un virus son:

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

g) gusanos



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

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

h) Caballos de Troya

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

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

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

i) Programa conejo o bacteria

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

j) Técnicas salami

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

5.2. Amenazas Físicas.

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

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

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

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

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

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

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

6. Seguridad física y ambiental.

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

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

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

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

1) Incendios.

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

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

2) Inundaciones

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

3) Condiciones Climatológicas

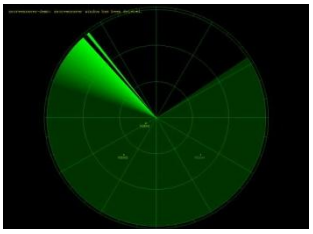
Normalmente se reciben por anticipado los avisos de tormentas, tempestades, tifones y catástrofes sísmicas similares. Las condiciones atmosféricas severas se asocian a ciertas partes del mundo y la probabilidad de que ocurran está documentada.

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

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

4) Señales de Radar

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



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

5) Instalaciones Eléctricas

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

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

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

6) Ergonometría

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

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

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

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

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

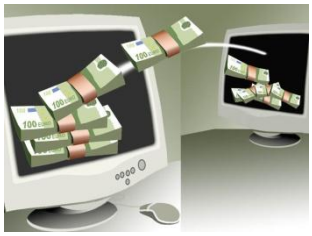
7) Acciones Hostiles

a) **Robo**

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

b) **Fraude**

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



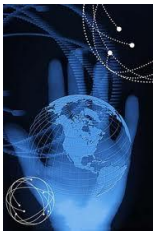
c) **Sabotaje**

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

8) Control de Accesos

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

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



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

Tener controlado el ambiente y acceso físico permite:

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

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

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

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

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

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

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

Sistemas contra incendios:

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

Sistemas de control de acceso:

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

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

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

➢ Protección del hardware

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

Problemas a los que nos enfrentamos:

- **Acceso físico**

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

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

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

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

- **Desastres naturales**

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

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

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

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

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

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

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

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

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

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

RS-232

USB

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

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

Algunos de los estándares más importantes son:

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

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

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

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

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

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

7. Seguridad Lógica.

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

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

7.1. Copias de seguridad.

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

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

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

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

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

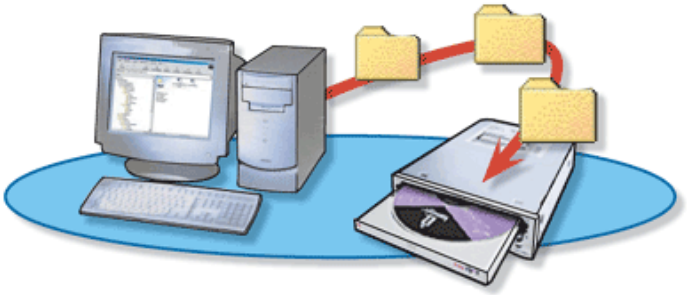
La periodicidad para realizar las copias de seguridad de nuestros datos, dependerá del mayor o menor movimiento de información que realicemos en nuestro equipo.

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

7.1.1. Tipos de copias de seguridad.

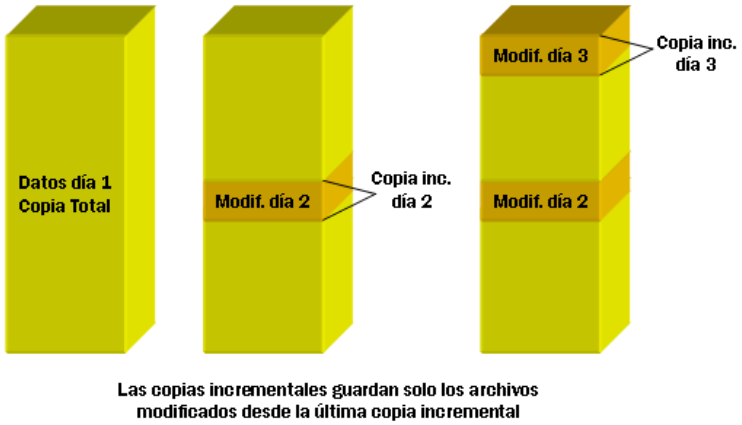
Existen varios tipos de copias de seguridad según los datos que respaldemos en ellas:

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



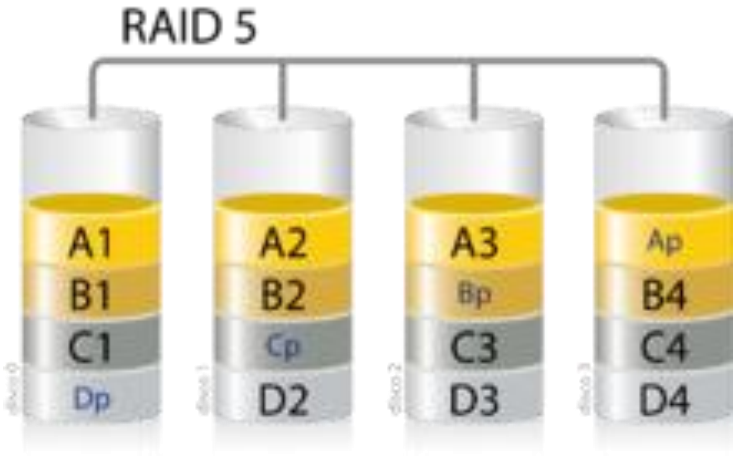
INCREMENTAL: En un proceso de copia de seguridad incremental, el programa examina el bit de modificado y hace una copia de seguridad sólo de los archivos que han cambiado desde la última copia de seguridad incremental o normal. Al igual que en la copia de seguridad normal, esta tarea borra el bit de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

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



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

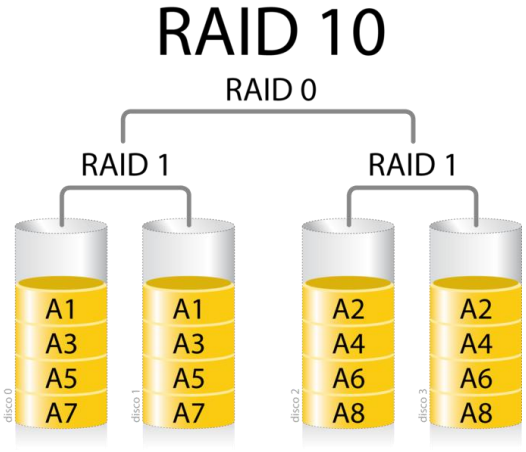
El RAID 5 ha logrado popularidad gracias a su bajo coste de redundancia. Generalmente, el RAID 5 se implementa con soporte hardware para el cálculo de la paridad. RAID 5 necesitará un mínimo de 3 discos para ser implementado.



RAID 10

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

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



b) Centros de Respaldo.

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

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

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

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

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

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

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

Existen dos políticas o aproximaciones a este problema:

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

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

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

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

- iSCSI.
- Fibre Channel.

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

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

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

a) SAN.

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

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

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

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

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

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

Las SAN se componen de tres capas:

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

La red de almacenamiento puede ser de dos tipos:

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Sniffit

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

SATAN

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

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

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

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

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

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

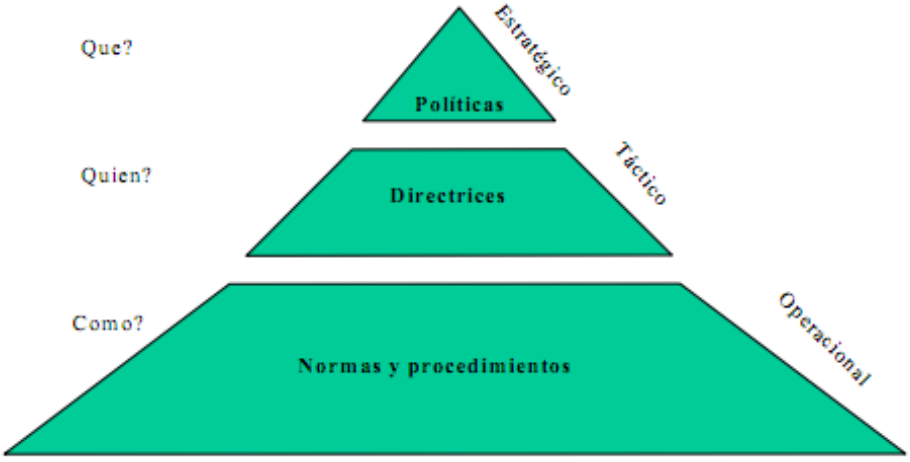
La más conocida de las máquinas de cifrado posiblemente sea la máquina alemana Enigma: una máquina de rotores que automatizaba considerablemente los cálculos que era necesario realizar para las operaciones de cifrado y descifrado de mensajes. Para vencer al ingenio alemán, fue necesario el concurso de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

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

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

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

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



Una política de seguridad debe:

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

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

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