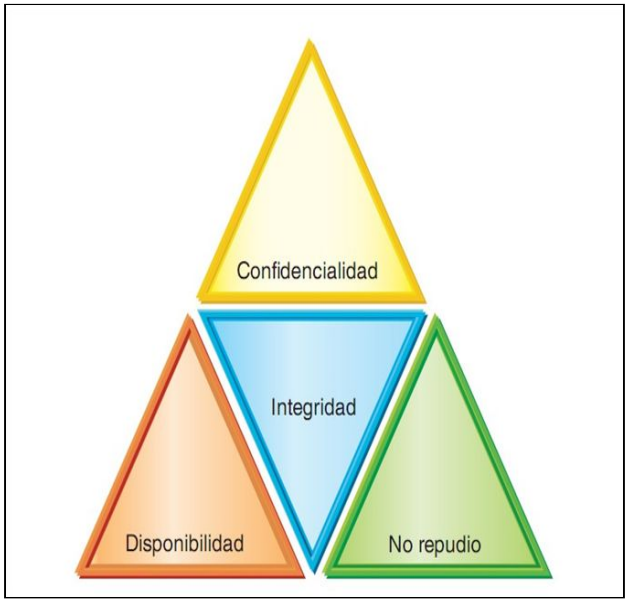
ACTIVIDAD 3: Buscar los mecanismos que existen a nuestra disposición para conseguir los objetivos que se indican en la tabla.

Generar un documento de trabajo completo, es decir textos explicativos e imágenes de esquemas complementarios que permitan comprender correctamente que se obtiene el objetivo deseado.

Número de páginas mínimo 15.



Mecanismos	Objetivos
Autenticación	No repudio
Autorización	Confidencialidad
Auditoría	Disponibilidad
Encriptación	Confidencialidad e integridad
Copias de seguridad	Disponibilidad
Imágenes de respaldo	Disponibilidad
Antivirus	Integridad y disponibilidad
Cortafuegos	Integridad
Servidores proxy	Integridad
Firma electrónica y certificados	No repudio y confidencialidad
LOPD	Confidencialidad

Tabla 1.1. *Relación de mecanismos y objetivos.*

1. INTRODUCCIÓN

Antes de empezar analizaremos la definición de **seguridad informática** según varias entidades:

- ISO/IEC 27002
- INFOSEC Glossary 2000:

1.1. ISO/IEC 27002

- Según la **ISO/IEC 27002** que es un estándar de seguridad para la seguridad de la información publicado por la Organización Internacional de Normalización y la Comisión Electrotécnica Internacional
  La versión más reciente de la norma **ISO 27002:2013.**

- Proporciona diferentes recomendaciones de las mejores prácticas en la gestión de la seguridad de la información a todos los interesados y responsables para iniciar, implementar o mantener sistemas de gestión de la seguridad de la información.
  La seguridad de la información se define en el estándar como la preservación de :

  1. **la confidencialidad**
  2. **la integridad**
  3. **la disponibilidad.**

- Se encuentra enfocada a todo tipo de empresas, independientemente del tamaño, tipo o naturaleza.

- Se encuentra organizado en base a los 14 dominios, 35 objetivos de control y 114 controles

- El contenido de las políticas se basa en el contexto en el que opera una empresa y suele ser considerado en su redacción todos los fines y objetivos de la empresa, las estrategias adoptadas para conseguir sus objetivos, la estructura y los procesos utilizados por la empresa..

- La estructura típica de los documentos de políticas puede ser:

  - Resumen: se establece una visión general de una extensión breve, uno o dos frases y que pueden aparecer fusionadas con la introducción.
  - Introducción: se establece una pequeña explicación del asunto principal de la política.
  - Ámbito de aplicación: es la descripción de los departamentos, áreas o actividades de una empresa a las que afecta la política. Cuando es relevante en este apartado se

mencionan otras políticas relevantes a las que se pretende ofrecer cobertura desde ésta.

- ➢ Objetivos: es la descripción de la intención de la política.
- ➢ Principios: se describen las reglas que conciernen a las acciones o decisiones para conseguir los objetivos
- ➢ Responsabilidades: descripción de quién es el responsable de qué acciones pueda cumplir con los requisitos de la política. En algunos casos, esto puede incluir una descripción de los mecanismos organizativos, además de las responsabilidades de las personas que tienen sus roles asignados.
- ➢ Resultados clave: describe todos los resultados relevantes para las actividades de la empresa que se obtienen cuando se cumplen los objetivos.
- ➢ Políticas relacionadas: se describen las políticas relevantes para cumplir con los objetivos, se indican detalles adicionales en relación con los temas específicos.
  - La política de alto nivel se encuentra relacionada con un *Sistema de Gestión de Seguridad de la Información*(SGSI) que suele estar apoyada por políticas de bajo nivel
  - por políticas de bajo nivel :específicas para aspectos concretos en temáticas como el control de accesos, la clasificación de la información, l,a seguridad física y ambiental, utilizar activos, dispositivos móviles y protección contra los malware.

- Si partimos del principio típico en seguridad “lo que no está permitido está prohibido” cada empresa debe detectar las necesidades de los usuarios y valorar los controles necesarios que fundamentan las políticas aplicables, que se aplican en una mejor estructura y relaciones entre ellas para su gestión.

- Directrices de la dirección en seguridad de la información
  - La gerencia debe establecer de forma clara las líneas de las políticas de actuación y manifiesta su apoyo y compromiso a la seguridad de la información, publicando y manteniendo políticas de seguridad en toda la empresa.

- Actividades de control del riesgo
  - La política para la seguridad de la información: se tiene que definir un conjunto de políticas para la seguridad de la información, esto se aprobó por la dirección de la organización, se publica y comunica a todos los empleados así como a todas las partes externas relevantes.

- Revisión de las políticas para la seguridad de la información: las políticas para la seguridad de la información se debe planificar y revisar con regularidad o si ocurren cambios significativos para garantizar su idoneidad, adecuación y efectividad.

- Métricas asociadas
  - Cobertura de la política, es decir, el porcentaje de secciones de la norma ISO 27002 para las cuales se han especificado, escrito, aprobado y publicado políticas y sus normas, procedimientos y directrices asociadas. El grado de despliegue y adoptar las políticas en las empresas

- Software ISO 27001
  - El **Software ISO 27001 para la Seguridad de la Información** se encuentra compuesta por diferentes aplicaciones que, al unirlas, trabajan para que la información que manejan las empresas no pierda ninguna de sus propiedades más importantes: disponibilidad, integridad y confidencialidad.

1.2. INFOSEC Glossary 2000

- Según **INFOSEC** (National Information Systems Security) Seguridad informática es:
  - *"Seguridad Informática son las medidas y controles que aseguran la confidencialidad, integridad y disponibilidad de los activos de los sistemas de información, incluyendo hardware, software, firmware y aquella información que procesan, almacenan y comunican"*.

- Principales objetivos de la seguridad informática

1) Confidencialidad : capacidad de garantizar que la información, almacenada en el sistema informático o transmitida por la red, solamente va a estar disponible para aquellas personas autorizadas a acceder a dicha información,
2) Disponibilidad : la capacidad de garantizar que tanto el sistema como los datos van a estar disponibles al usuario en todo momento.
3) Integridad : la capacidad de garantizar que los datos no han sido modificados desde su creación sin autorización.

4) No repudio : garantiza la participación de las partes en una comunicación.
   Existen 2 tipos de repudio:
   - No repudio de origen :garantiza que la persona que envía el mensaje no puede negar que es el emisor del mismo,
   - No repudio de destino :El receptor no puede negar que recibió el mensaje

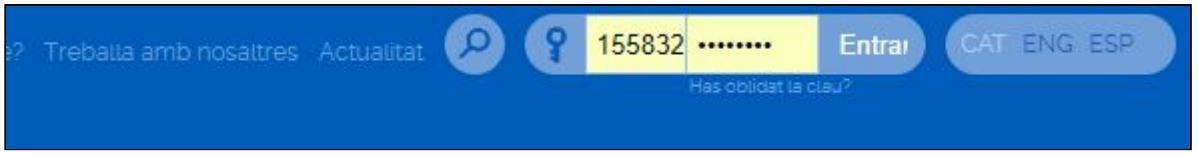
2. MECANISMOS DE SEGURIDAD

2.1. Autenticación :Permite identificar al emisor de un mensaje, al creador de un documento o al equipo que se conecta a una red o a un servicio.

2.1.1. Objetivo: No Repudio

Es posible identificarse de 3 formas :

- Por lo que uno sabe(contraseña)



- Por lo que uno tiene (tarjeta magnética)

- Por lo que uno es (huellas dactilares)


2.2. Autorización: Proceso por el cual se determina qué, cómo y cuándo, un usuario autenticado puede utilizar los recursos de la organización.

El mecanismo o el grado de autorización puede variar dependiendo de qué sea lo que se está protegiendo. No toda la información de la organización es igual de crítica. Los recursos en general y los datos en particular, se organizan en niveles y cada nivel debe tener una autorización.

2.2.1. Objetivo: Confidencialidad

2.3. Auditoría: Continua vigilancia de los servicios en producción y para ello se recaba información y se analiza. Este proceso permite a los administradores verificar que las técnicas de autenticación y autorización utilizadas se realizan según lo establecido y se cumplen los objetivos fijados por la organización. Pero auditar y registrar no tiene sentido si no van acompañados de un estudio posterior.

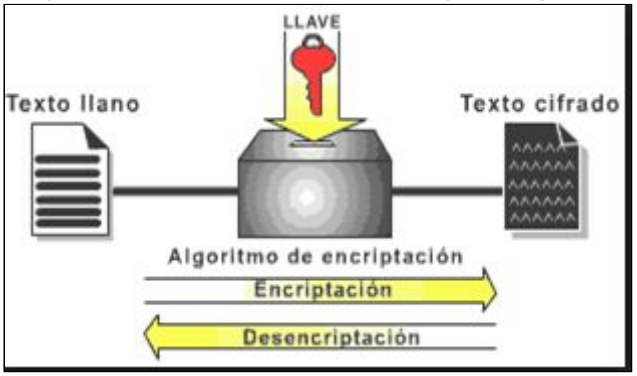
Monitorear la información registrada o auditar se puede realizar mediante medios manuales o automáticos, y con una periodicidad que dependerá de lo crítica que sea la información protegida y del nivel de riesgo

.

2.3.1. Objetivo: Disponibilidad

2.4. Encriptación: La encriptación es el proceso para volver ilegible cierta información considerada importante.La información una vez encriptada solo puede leerse aplicando una clave

2.4.1. Objetivo: Confidencialidad y integridad



2.4.2. **Metodos de Encriptación**:

2.4.2.1. Criptografia asimétrica(RSA): Este emplea claves para el envió del mensaje, estas pertenecen a la persona a la que se le envía el mensaje una clave es pública y otra es privada.

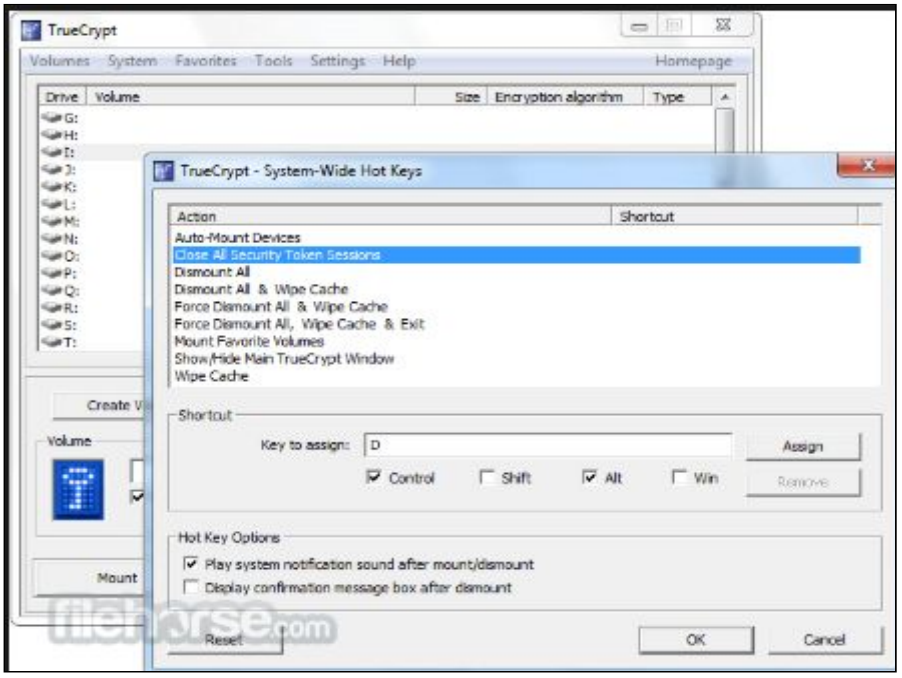
2.4.2.2. Criptografia simétrica: En este se emplea la una clave para la transformación del mensaje y/o información encriptada, esta tiene un problema el cual recide en que tanto el emisor como el receptor conozca la clave.

2.4.2.3. Algoritmo HASH:Este algoritmo efectúa un cálculo matemático sobre los datos que constituyen el documento y da como resultado un número único llamado MAC. Un mismo documento dará siempre un mismo MA

2.4.3. Herramientas para desencriptar

2.4.3.1. Criptoanálisis: Es el método para desencriptar sin conocer las llaves , no se conoce nada acerca del contenido del mensaje.

2.4.3.2. Truecrypt: El programa puede encriptar un texto, un archivo, una partición o un disco de almacenamiento como usb o disco duro.



2.4.3.3. Winrar: Desarrollado por RARLAB nos permite comprimir o encriptar cualquier tipo de archivo, en la encriptación se le puede añadir alguna clave sin esta no se podrá descomprimir o desencriptar el archivo

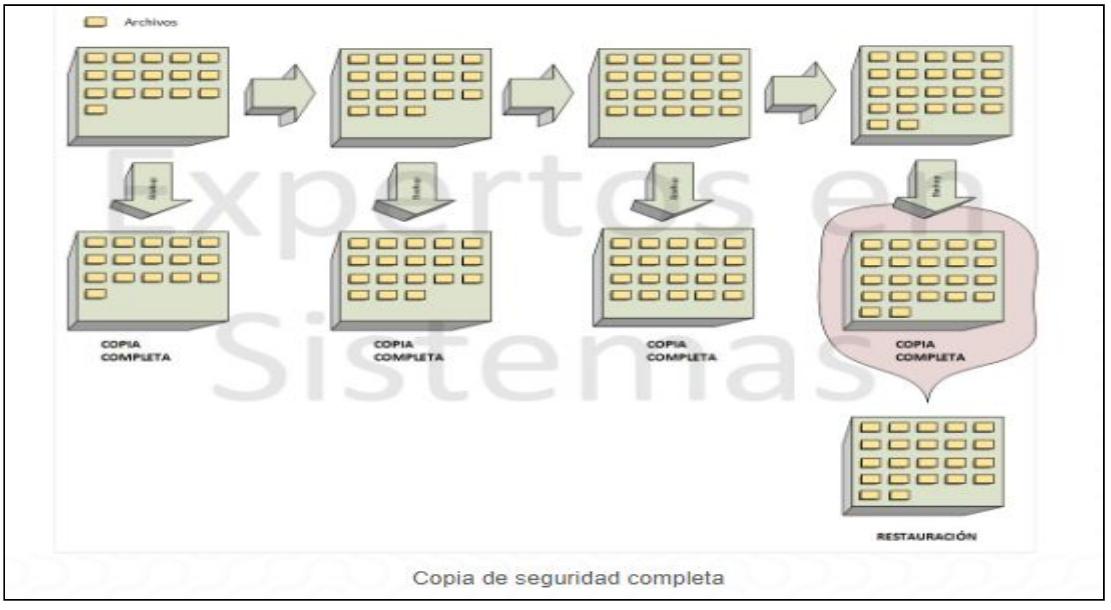
:

2.5. Copias de Seguridad: Una Copia de Seguridad, es un duplicado de nuestra información más importante, que realizamos para salvaguardar los documentos, archivos, fotos, etc., de nuestro ordenador, por si acaso ocurriese algún problema que nos impidiese acceder a los originales que tenemos en él.

2.5.1. Objetivo: Disponibilidad

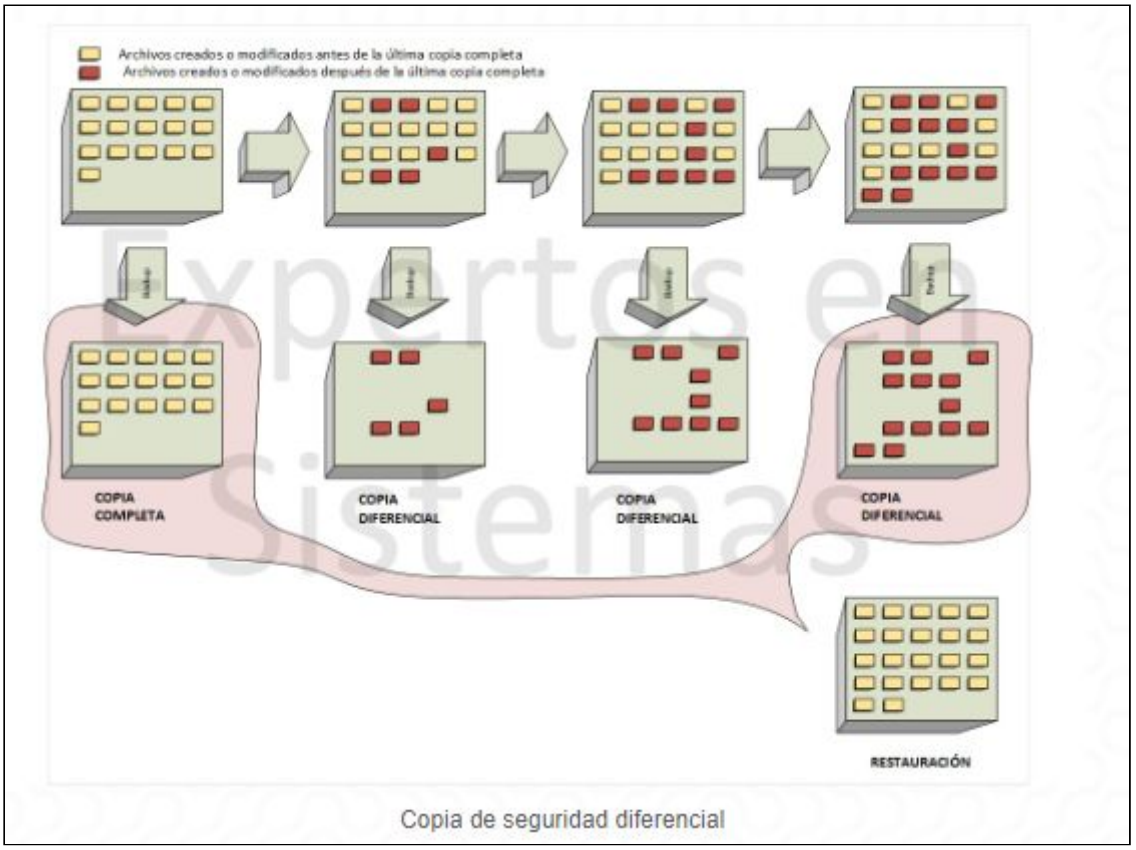
2.5.2. Clases de Copias de Seguridad

2.5.2.1. Completa: realiza una copia de todos los archivos y directorios seleccionados. Es la copia que debemos hacer cuando creamos la primera copia de seguridad.



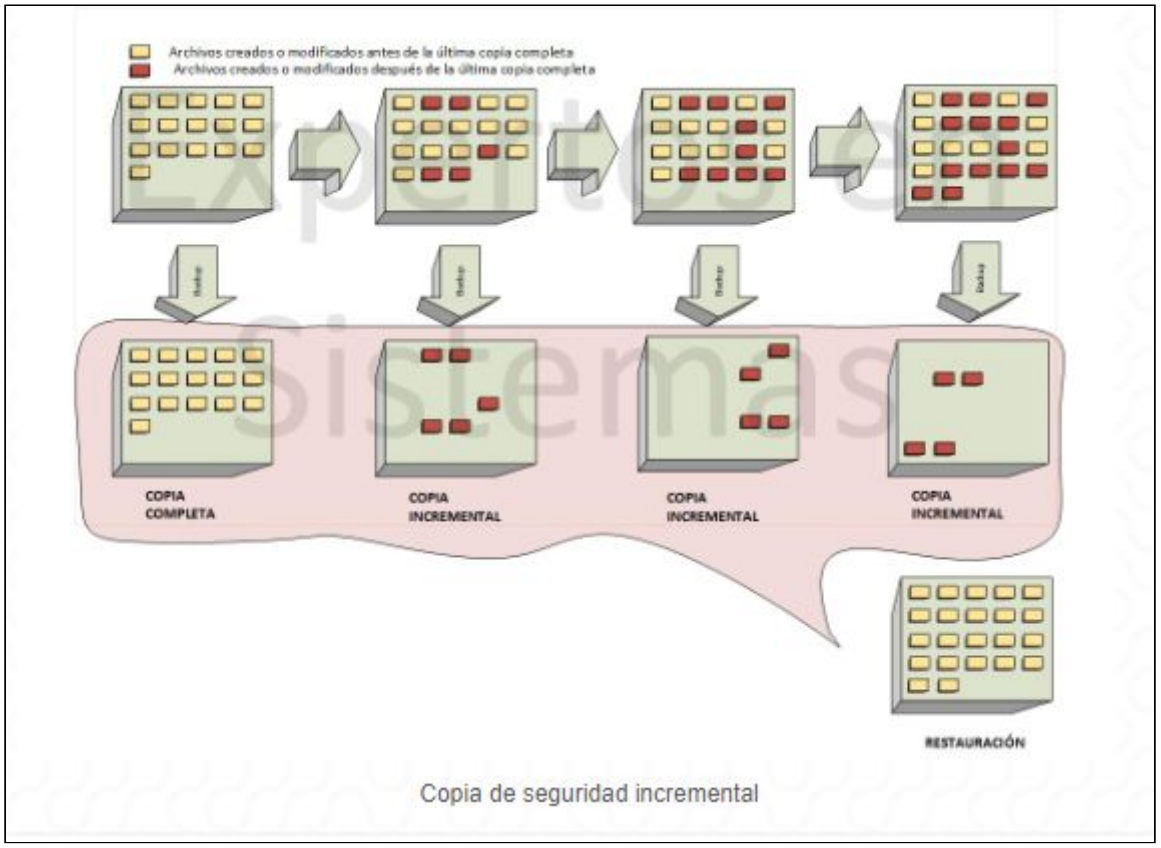
2.5.2.2. Diferencial: se copian todos los archivos que se han creado o actualizado desde la última copia completa que se ha hecho.

2.5.2.3.



Copia de seguridad diferencial

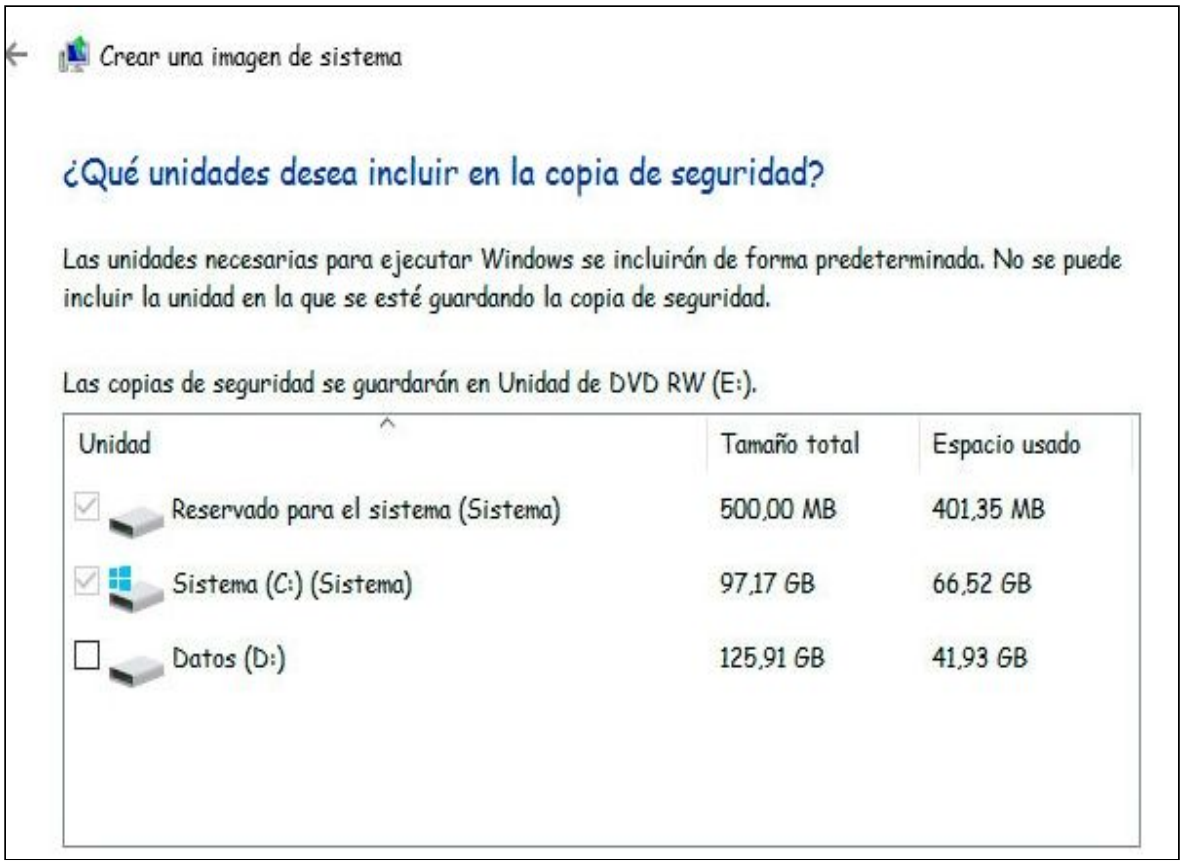
2.5.2.4. Incremental: se copian los archivos que se han modificada desde la última copia de seguridad completa o diferencial realizada.



Copia de seguridad incremental

2.6. Imagenes de respaldo : Estas copias de seguridad de imagen del sistema son como una fotografía de nuestro equipo en ese momento que puede ser utilizada en el caso de que falle el disco o el sistema y poder restaurar el equipo tal y como lo teníamos en el momento de su creación sin necesidad de tener que reinstalar todo de nuevo. Es decir, no tendremos que volver a instalar ni el propio sistema operativo ni nuestras aplicaciones.

2.6.1. Objetivo: Disponibilidad



2.7. Antivirus : Un antivirus es una gran base de datos con la huella digital de todos los virus conocidos para identificarlos y también con las pautas que más contienen los virus. Los fabricantes de antivirus avanzan tecnológicamente casi en la misma medida que lo hacen los creadores de virus. Esto sirve para combatirlos, aunque no para prevenir la creación e infección de otros nuevos.

2.7.1. Objetivo: Integridad y Disponibilidad

2.7.2. Funciones de un Antivirus :

2.7.2.1. Detección del virus

2.7.2.2. Identificación de un virus - Hay varias técnicas:

- Scannig
- Heurísitca : búsqueda de acciones potencialmente dañinas perteneciente a un virus informático

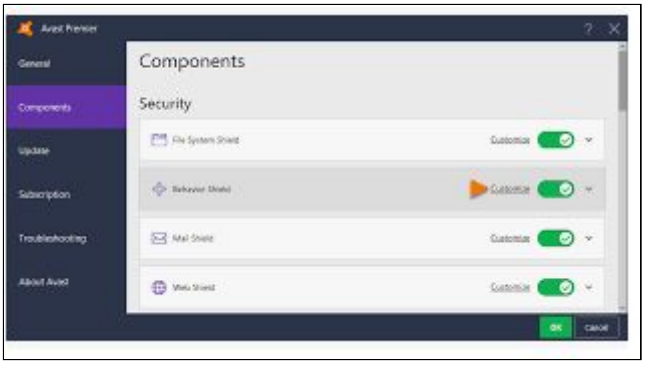
2.7.2.3. Chequeo de Integridad

2.7.3. ¿De qué me tiene que proteger?- Si lo utilizamos para uso doméstico, las versiones gratuitas de Antivirus como Avast, AVG para la protección de nuestro ordenador , nos proporcionan protección suficiente. pero la cosa cambia en el ámbito comercial

2.7.3.1. Otras funciones para ámbito comercial :

- Protección de identidad
- Protección de los datos personales
- Protección de la dirección IP (bloqueando los cookies)
- Compras en líneas seguras
- Impedir ataques de hackers

AVAST(versión gratuita) ejemplo de Antivirus para uso doméstico.



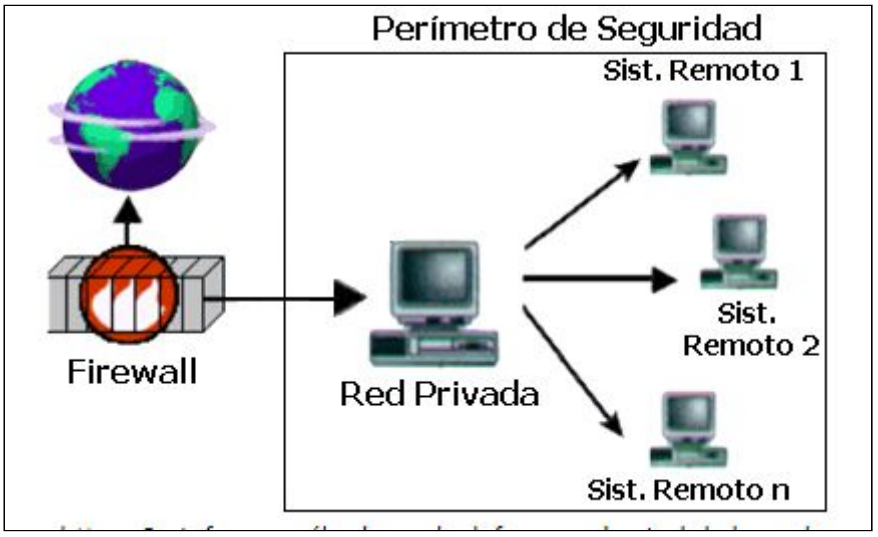
ESET MULTI DEVICE SECURITY (recomendable para uso comercial). Si supongamos que queramos proteger una pequeña empresa con 15 ordenadores , valdría 297,66€.

2.8. Cortafuegos(o Firewall) : es un sistema (o conjunto de ellos) ubicado entre dos redes y que ejerce la una política de seguridad establecida. Es el mecanismo encargado de proteger una red confiable de una que no lo es (por ejemplo Internet).

2.8.1. Objetivo: Integridad

2.8.2. Funciones del Firewall:

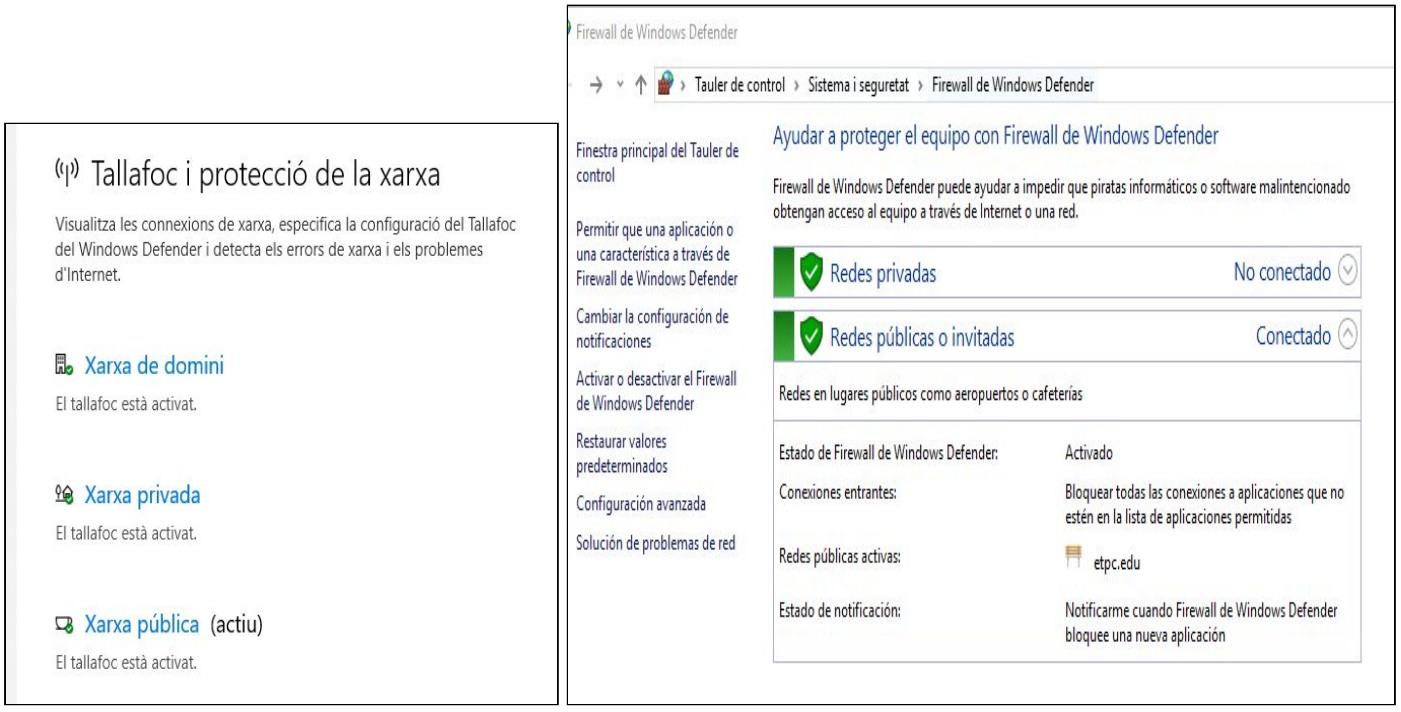
- Todo el tráfico desde dentro hacia fuera, y viceversa, debe pasar a través de él.
- Sólo el tráfico autorizado, definido por la política local de seguridad, es permitido

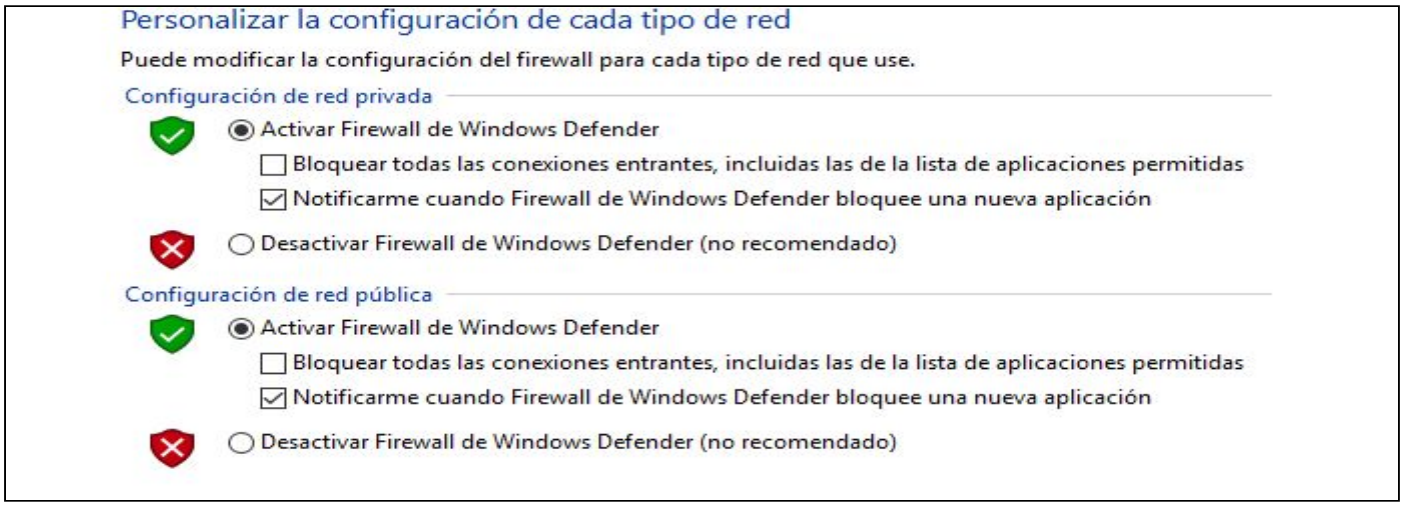


2.8.3. Tipos de Firewall:

- Firewall de hardware. Este cortafuegos, normalmente, se halla instalado en el router que empleamos para acceder a Internet y, por tanto, sirve para proteger a todos los ordenadores de una red que hagan uso del mismo.
  - **Ejemplo** : ZyXEL ZyWall 110 1000Mbit/s ZYWALL110-EU0101F a 552,62€

- **Firewall de software**. Se trata del firewall que viene con el sistema operativo del ordenador y, por tanto, en este caso, tan sólo protege un equipo –y no todos los que integran una red–. Se ocupa de rastrear el tráfico para bloquear aquél que no está autorizado. Un cortafuegos como éste es, por ejemplo, el que se puede instalar desde Windows.
    - **Ejemplo** : En Windows 10 viene incorporado el Windows Defender

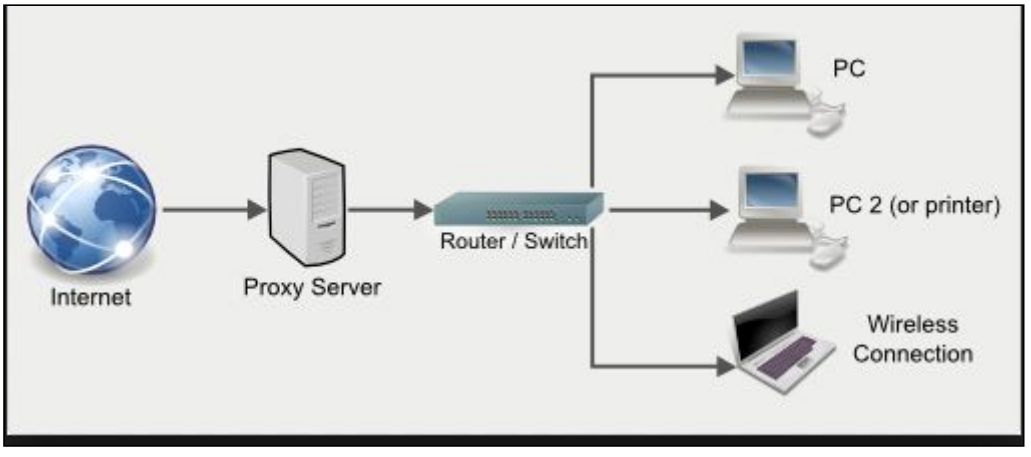




- Firewall de software comercial. Es el que está integrado en las suites de antivirus. Funciona de la misma manera que los anteriores, aunque ofrece mejores niveles de protección y mayores posibilidades de control y configuración.

    - **Ejemplo** : Ashampoo Firewall (Gratuito)

- Servidores Proxy : Un servidor proxy es un equipo informático que media entre las conexiones que se realizan habitualmente al navegar en páginas web. Es el encargado de recibir las peticiones de acceso de un usuario y de transmitirlas al servidor web. Es quien notifica que tú y tus datos de IP quieren acceder a una página web en concreto.



2.8.4. Objetivo: Integridad

2.8.5. Funciones de los Servidores Proxy

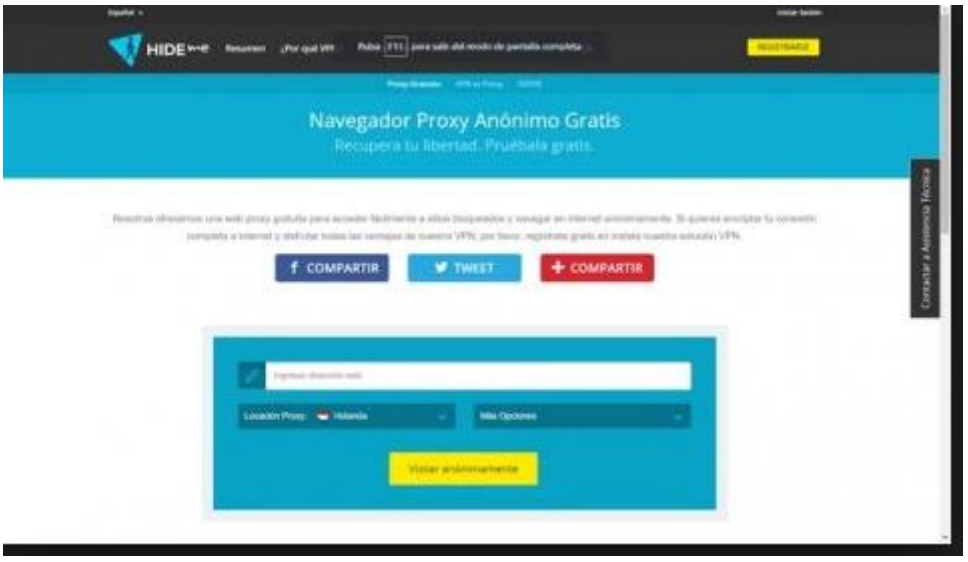
- Te permite acceder a contenidos que están bloqueados a determinadas IP ya que está camuflada y puedes pasar por un usuario de Internet de otro país.
- Bloquea cookies, scripts y otros objetos que utilizan los sitios web para conocer nuestro comportamiento por la web.
- Para navegar por Internet de una forma más privada y anónima.

2.8.6. ¿Cómo funcionan Servidores Proxy?

Hay que ir con cuidado antes de usar uno de estos recursos web:

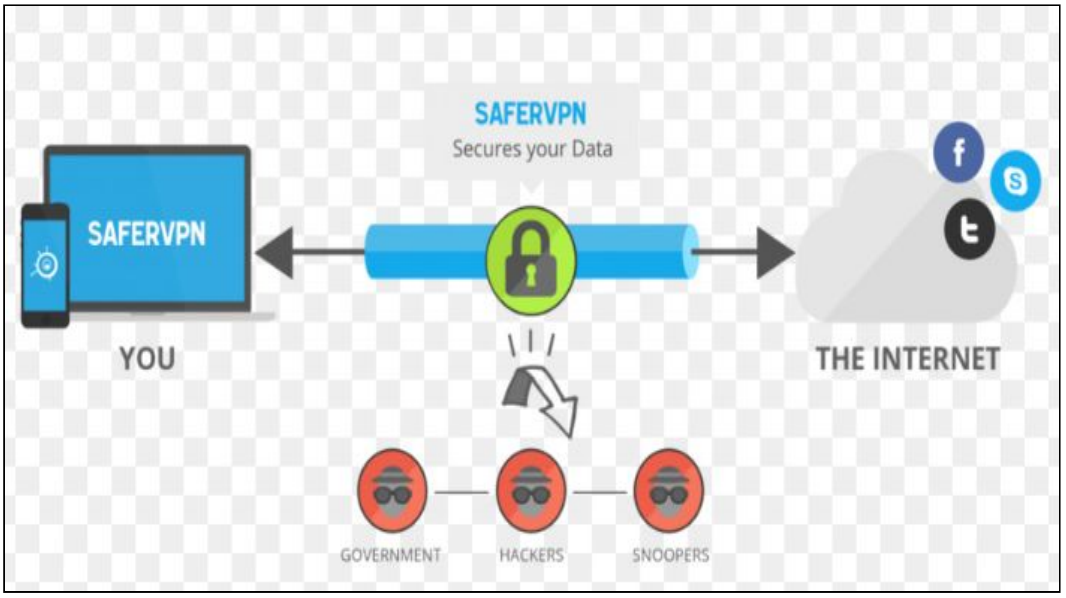
- Hay muchos servidores proxy en Internet pero no todos son de confianza.
- *El Servidor Proxy oculta nuestra IP pero no hace lo mismo con los datos que transmites al navegar*, con lo que alguien podría espiar tu tráfico.
- Se aconseja usar Servidores Proxys seguros como : Hide.me o VPNBook

Servidor Proxy Hide.me



2.8.7. Alternativas más seguras y fiables

2.8.7.1. VPN o red privada virtual ya que cifran todo el tráfico que pasa a través .



2.9. Firma electrónica y certificados digital :

2.9.1. El certificado digital tiene como función principal autenticar al poseedor pero puede servir también para cifrar las comunicaciones y firmar digitalmente. En algunas administraciones públicas y empresas privadas es requerido para poder realizar ciertos trámites que involucren intercambio de información delicada entre las partes.

2.9.2. La firma electrónica es el conjuntos de datos asociados a un documento electrónico que nos permite hacer las siguientes acciones:

- Identificar al firmante de forma inequívoca. Para ello se necesita una clave privada que únicamente conozca el firmante.
- Asegurar la integridad del documento firmado. Sirve para saber si el documento firmado es igual al original y que no ha sufrido ningún tipo de manipulación ni alteración.
- No repudio. Asegura que los datos que el firmante ha utilizado para realizar la firma son únicos y exclusivos.

2.9.3. Objetivo: No Repudio y Confidencialidad.

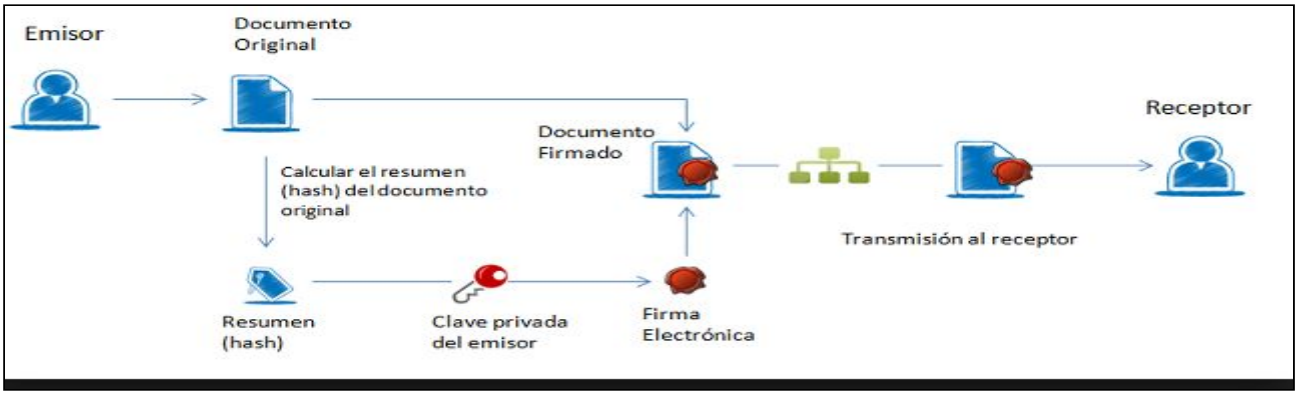
2.9.4. ¿Cómo funciona la firma electrónica?

2.9.5. ¿Que nos permite hacer con la firma electrónica?

- El firmante crea un resumen mediante una ***función hash*** que se utiliza como **huella digita**l del mensaje. El resultado que se obtiene del resumen se llama "**firma digital**", y se enviará adjunta al mensaje original.

2.9.6. ¿Cómo se firma un documento?

- Se utiliza una aplicación en el dispositivo. Existen aplicaciones que se pueden descargar en el equipo, como, por ejemplo, Microsoft Office Word (donde puedes firmar documentos).
- Firmar directamente en Internet. Se utiliza este método al firmar formularios o solicitudes.



Firma electrónical

Certificado digital

2.10. LOPD : **Ley Orgánica 15/1999 de Protección de Datos de carácter personal** :

es una ley orgánica que tiene el objeto de proteger la intimidad y la privacidad personal y familiar. Fue aprobada a las Cortes españolas el 13 de diciembre del 1999.

- Su objetivo principal es regular el tratamiento de los datos y ficheros, de carácter personal, independientemente del apoyo en el cual sean tratados, los derechos de los ciudadanos sobre ellos y las obligaciones de aquellos que los crean o tratan.
- Esta ley afecta a todos los datos que hacen referencia a personas físicas registradas sobre cualquier apoyo, informático o no. Quedan excluidas de esta normativa aquellos datos recogidos para uso doméstico, las materias clasificadas del estado y aquellos ficheros que recogen datos sobre Terrorismo y otras formas de delincuencia organizada (no simple delincuencia).

2.10.1. Objetivo: Confidencialidad

2.10.2. Órgano de control: El órgano de control del cumplimiento de la normativa de protección de datos dentro del territorio español, a todos los efectos es la **Agencia Española de Protección de Datos (AEPD)**

2.10.3. Otras Agencias de PRotección de Datos (ámbito autonómico)

2.10.3.1. Órgano de control:

- **A.C.P.D.** : Agencia Catalana de Protección de Datos (Catalunya)
- **A.V.P.D.** : “Agencia Vasca de Protección de Datos”(Euskadi)

2.10.4. Niveles de Seguridad según LOPD

2.10.4.1. Nivel Básico de seguridad de los ficheros :El nivel básico de seguridad, se aplicará entre otros, a los ficheros que solamente contengan datos identificativos y a todos los niveles mediano y alto de seguridad. Procedimiento de notificación y gestión de incidencias
Ejemplos: Nombre, domicilio, teléfono, DNI, número de afiliación a la seguridad social, fotografía, firmas, correos electrónicos, datos bancarios, edad, fecha de nacimiento, sexo, nacionalidad, etc

2.10.4.2. Nivel Mediano de seguridad :En el nivel mediano de seguridad, se aplicará esta protección, entre otros, a los ficheros que contengan datos relativos a solvencia patrimonial, operaciones financieras y de crédito. Procedimiento de notificación y gestión de incidencias. Límite de intentos reiterados de acceso no autoriza
Ejemplos: Datos de personalidad, hábitos de consumo, hábitos de carácter, datos de seguridad social, solvencia patrimonial y crédito, antecedentes penales, sanciones administrativas, pruebas psicotécnicas, currículums, etc.

2.10.4.3. Nivel Alto de seguridad :En el nivel alto de seguridad, se aplicará a los ficheros que contienen datos especialmente protegidos como los relativos a ideología, afiliación sindical y política, religión y creencias, origen racial, salud, alimentación, bajas laborales, vida y práctica sexual, etc. cifrado de datos en la distribución de apoyos..