

# UD1. PRINCIPIOS DE SEGURIDAD Y ALTA DISPONIBILIDAD

Seguridad y Alta Disponibilidad

Raquel Esteve Sanjuan

# INTRODUCCIÓN

- DEFINICIÓN DE SEGURIDAD INFORMÁTICA

La *seguridad informática* consiste en asegurar que los recursos del sistema de información de una organización sean utilizados de la manera que se decidió y que el acceso a la información allí contenida, así como su modificación, solo sea posible a las personas que se encuentren acreditadas y dentro de los límites de su autorización.

- JUSTIFICACIÓN DE LA SEGURIDAD INFORMÁTICA

→ El espectacular auge de internet y de los servicios telemáticos ha hecho que los ordenadores y las redes se conviertan en un elemento cotidiano en nuestras casas y en un instrumento imprescindible en las tareas de las empresas.

→ Las empresas, sea cual sea su tamaño, disponen de equipos conectados a internet que les ayudan en sus procesos productivos. Cualquier fallo en los mismos puede suponer una gran perdida económica ocasionada por el parón producido, de modo que es muy importante asegurar un correcto funcionamiento de los sistemas y redes informáticas.

→ Con unas buenas políticas de seguridad, tanto físicas como lógicas, conseguiremos que nuestros sistemas sean menos vulnerables a las distintas amenazas.

→ Tenemos que intentar lograr un nivel de seguridad razonable y estar preparados para que, cuando se produzcan los ataques, los daños puedan ser evitados o en caso contrario haber sido lo suficientemente precavidos para realizar las copias de seguridad.

- OBJETIVOS PRINCIPALES DE LA SEGURIDAD INFOMÁTICA
  - Detectar los posibles problemas y amenazas
  - Garantizar la adecuada utilización de los recursos y de las aplicaciones de los sistemas.
  - Limitar las pérdidas y conseguir una adecuada recuperación en caso de un incidente
  - Cumplir con el marco legal y con los requisitos impuestos a nivel administrativo.

*“El único sistema que es totalmente seguro es aquel que se encuentra apagado y desconectado, guardado en una caja fuerte de titanio que está enterrada en cemento, rodeada de gas nervioso y de un grupo de guardias fuertemente armados. Aún así, no apostaría mi vida en ello”*

*Eugene H. Spafford*

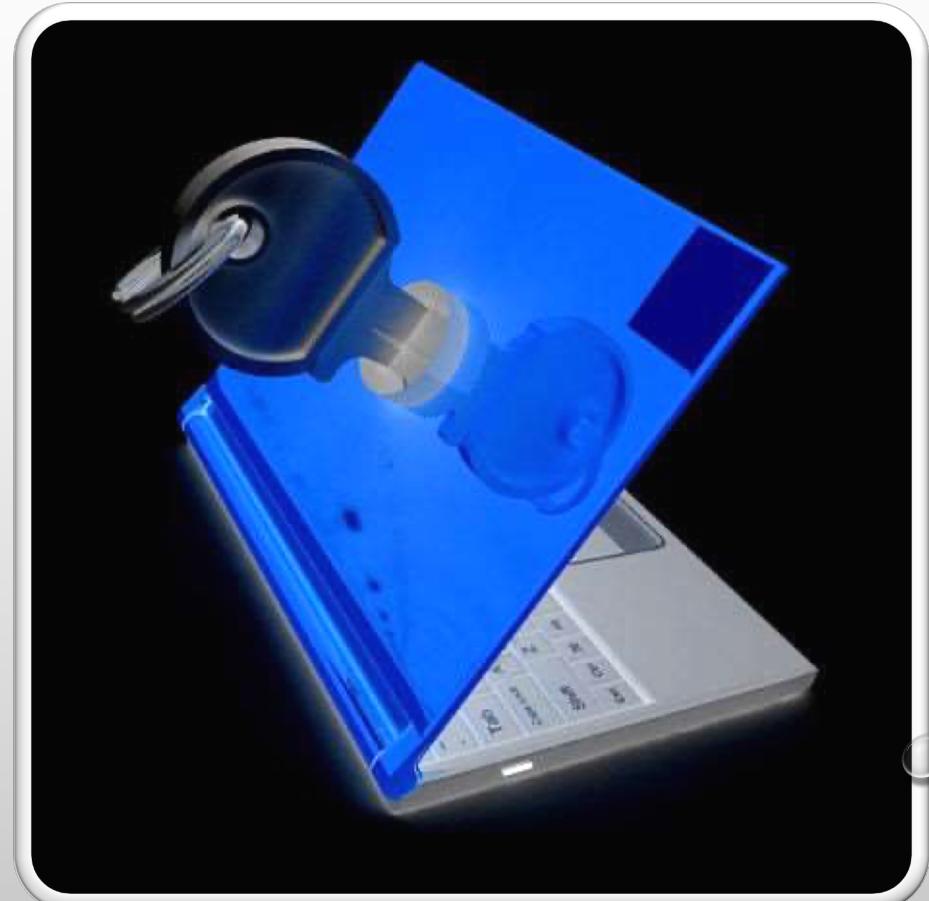
por lo que se deduce que...

→ La seguridad absoluta no existe

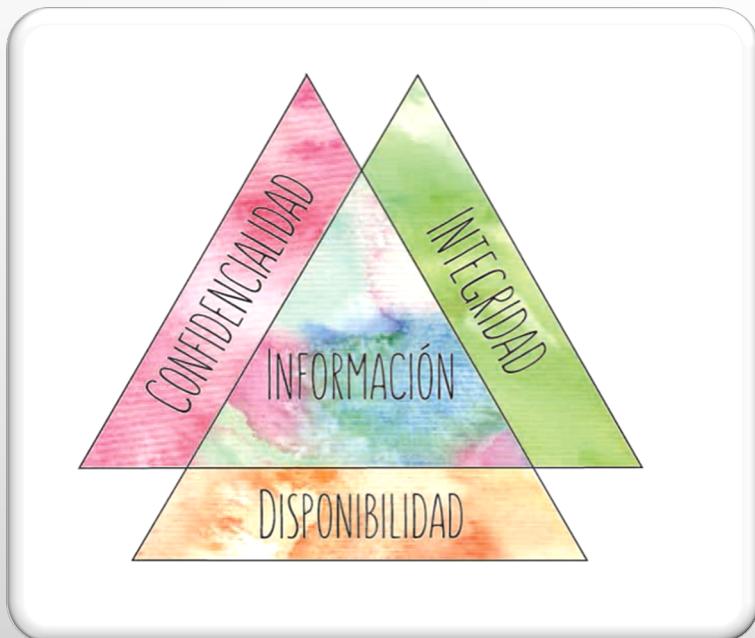
→ La seguridad informática son técnicas para obtener altos niveles de seguridad, por lo que realmente se pide **fiabilidad en el sistema**

→ Fiabilidad es la probabilidad de que un sistema se comporte tal y como se espera de él.

Pasamos a hablar de tener **sistemas fiables** en lugar de sistemas seguros.



# CONFIDENCIALIDAD, INTEGRIDAD Y DISPONIBILIDAD



- UN SISTEMA SEGURO (FIABLE) CONSISTE EN GARANTIZAR

CIDAN

CONFIDENCIALIDAD

INTEGRIDAD

DISPONIBILIDAD

+

AUTENTICACIÓN

NO REPUDIO

# CONFIDENCIALIDAD

- Propiedad de la información por la que se garantiza que está accesible únicamente a personal autorizado
- Para un usuario que no tiene permiso para acceder a la información, ésta debe ser ininteligible. sólo los individuos autorizados deben tener acceso a los recursos que se intercambian. (problema cuando se accede desde un live-usb)
- Ejemplos:
  - EFS (encrypted file system) cifrado de archivos a nivel de sistema
  - Bitlocker
  - cifrado simétrico/ asimétrico en comunicaciones



# CONFIDENCIALIDAD

## BITLOCKER

Bitlocker es una aplicación de cifrado que nos permite proteger nuestro disco duro de un posible robo de información. Encontramos esta herramienta disponible en Windows.



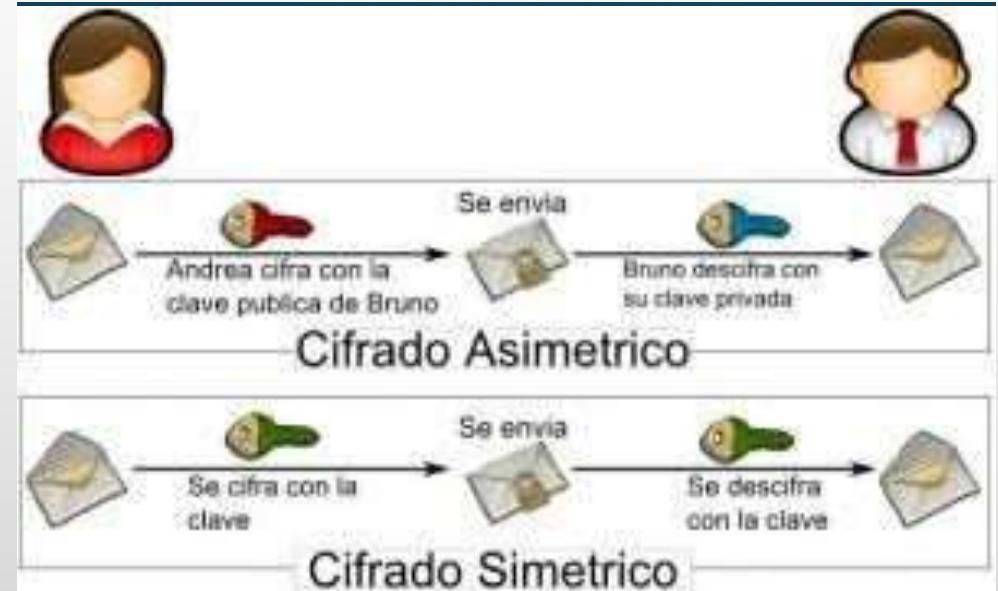
# CONFIDENCIALIDAD

## CIFRADO ASIMÉTRICO/SIMÉTRICO



→ **Cifrado simétrico**, también conocido como **cifrado de clave secreta**, usa una clave única para cifrar y descifrar datos. es necesario compartir esta clave con el destinatario.

→ **Cifrado asimétrico** requiere de dos claves para funcionar. en primer lugar, **una clave pública para poder cifrar los datos** y en segundo lugar, **una clave privada que se usa para descifrar los datos.**



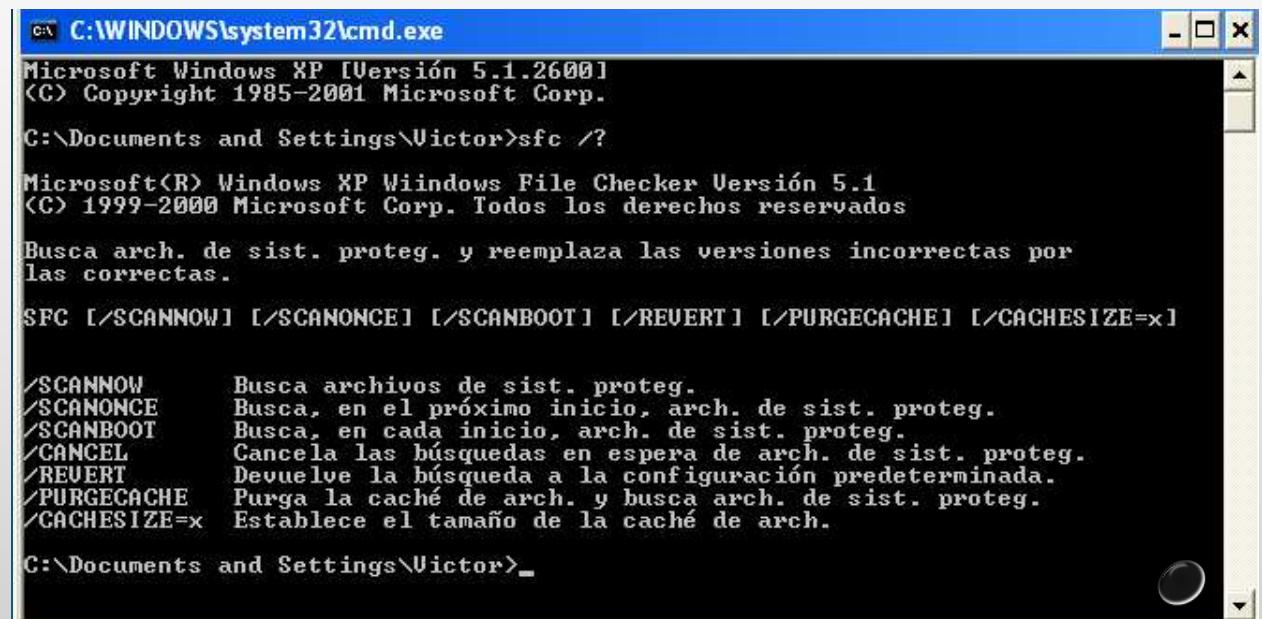
# INTEGRIDAD

- Propiedad que busca mantener los datos libres de modificaciones no autorizadas.
- Asegura que los datos del sistema no han sido alterados ni cancelados por personas o entidades no autorizadas y que el contenido de los mensajes recibidos es el correcto
- Diremos que es la capacidad de garantizar que los datos no han sido modificados desde su creación sin autorización.
- ejemplos:
  - SFC (windows)
  - Rootkit hunter
  - Firma digital y funciones resumen para comunicaciones

# INTEGRIDAD

- SFC (SYSTEM FILE CHECKER)

Utilidad de los sistemas Windows que comprueba la integridad de los archivos de sistema y reemplaza los que están corruptos o dañados por versiones correctas, si es posible.



```
C:\WINDOWS\system32\cmd.exe
Microsoft Windows XP [Versión 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

C:\Documents and Settings\Victor>sfc /?
Microsoft(R) Windows XP Windows File Checker Versión 5.1
(C) 1999-2000 Microsoft Corp. Todos los derechos reservados

Busca arch. de sist. proteg. y reemplaza las versiones incorrectas por
las correctas.

SFC [/SCANNOW] [/SCANONCE] [/SCANBOOT] [/REVERT] [/PURGECACHE] [/CACHESIZE=x]

/SCANNOW      Busca archivos de sist. proteg.
/SCANONCE     Busca, en el próximo inicio, arch. de sist. proteg.
/SCANBOOT     Busca, en cada inicio, arch. de sist. proteg.
/CANCEL       Cancela las búsquedas en espera de arch. de sist. proteg.
/REVERT       Devuelve la búsqueda a la configuración predeterminada.
/PURGECACHE   Purga la caché de arch. y busca arch. de sist. proteg.
/CACHESIZE=x  Establece el tamaño de la caché de arch.

C:\Documents and Settings\Victor>_
```

# INTEGRIDAD

- ROOTKIT HUNTER

Herramienta GNU/Linux que, además de realizar la comprobación de integridad de los archivos de sistema (es decir, verificar que no han sido modificados), examina los permisos de los ejecutables del sistema y busca rootkits conocidos rastreando ficheros ocultos.

Instalación: \$ sudo aptitude install rkhunter

Ejecución: \$ sudo rkhunter –checkall



# INTEGRIDAD

- Un ***Rootkit*** es un conjunto de software que permite un acceso de privilegio continuo a un ordenador pero que mantiene su presencia activamente oculta al control de los administradores al corromper el funcionamiento normal del sistema operativo o de otras aplicaciones.
- El término proviene de una concatenación de la palabra inglesa ***root***, que significa 'raíz' (nombre tradicional de la cuenta privilegiada en los sistemas operativos UNIX) y de la palabra inglesa ***kit***, que significa 'conjunto de herramientas' (en referencia a los componentes de software que implementan este programa). algunas versiones en español de programas informáticos, documentos de universidades y el propio ICANN lo han traducido como **encubridor**.

# INTEGRIDAD



- **FUNCIÓN RESUMEN**

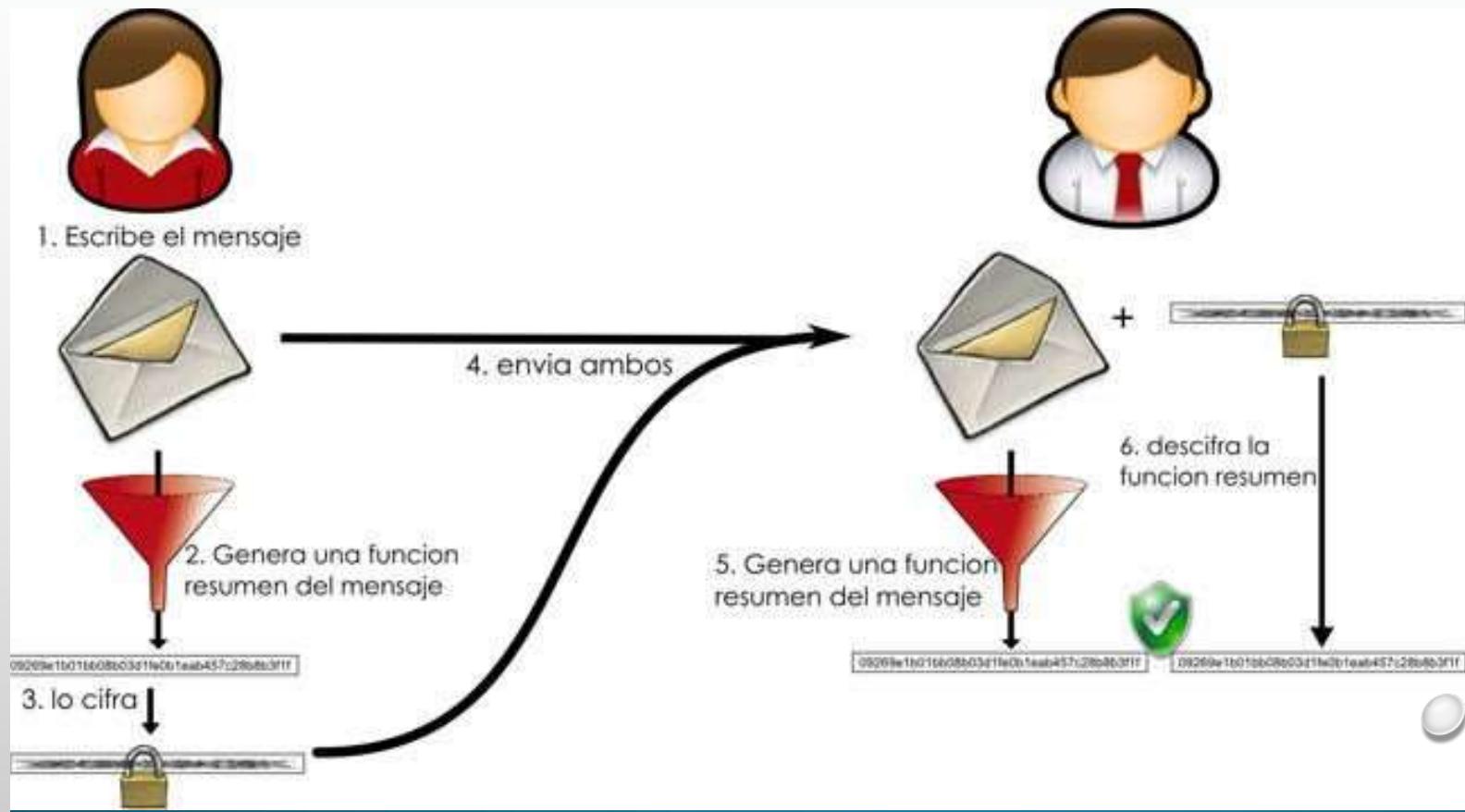
Un algoritmo que utiliza una *función resumen* o *una función hash* genera una cadena de longitud fija, llamada *resumen* o *fingerprint*, a partir de un mensaje de tamaño variable.

La función es de un solo sentido, imposible de invertir y realiza el resumen de forma que, mensajes casi idénticos producen resúmenes muy diferentes entre sí. Por esto es muy poco probable crear una entrada que produzca un resumen en particular.

De este modo, se obtiene una forma de control de integridad para detectar modificaciones al mensaje original que ha sido interceptado por algún tercero.

# INTEGRIDAD

- FUNCIÓN RESUMEN



# DISPONIBILIDAD

- Característica o condición de la información de encontrarse a disposición de quien debe acceder a ella
- Permitirá que la información esté disponible cuando lo requieran las personas o entidades autorizadas
- La definiremos como la capacidad de garantizar que tanto el sistema como los datos van a estar disponibles al usuario en todo momento.

# DISPONIBILIDAD

- EJEMPLOS
- [www.securityfocus.com](http://www.securityfocus.com) Informes sobre vulnerabilidades en aplicaciones y so.
- [www.nessus.org](http://www.nessus.org) Detecta vulnerabilidades tanto en windows como en gnu/Linux
- **MBSA** (Microsoft baseline security analyzer). Detecta los errores más comunes de configuración de seguridad y actualizaciones de seguridad que faltan para sistemas windows.
- **NMAP**. Escaneador de puertos. Herramienta de código abierto para efectuar rastreo de puertos. Se usa para evaluar la seguridad de sistemas informáticos y descubrir servicios o servidores en una red informática.  
[www.insecure.org/nmap](http://www.insecure.org/nmap)

# DISPONIBILIDAD

- Alta Disponibilidad (High Availability) es un protocolo de diseño del sistema y su implementación asociada que asegura un cierto grado absoluto de continuidad operacional durante un período de medición dado.
- *Disponibilidad* se refiere a la habilidad de la comunidad de usuarios para acceder al sistema, someter nuevos trabajos, actualizar o alterar trabajos existentes o recoger los resultados de trabajos previos. Si un usuario no puede acceder al sistema se dice que está no disponible.
- El término tiempo de inactividad (downtime) es usado para definir cuándo el sistema no está disponible.
- Ejemplo: CPD

## ALTA DISPONIBILIDAD



- Para medir la disponibilidad de un sistema, se utilizan dos métricas:

→MTTF (Mean Time To Failure):

tiempo medio entre fallos

→MTTR (Mean Time To Recover):

tiempo medio de recuperación tras  
un fallo

- Nuestro principal objetivo debe ser aumentar el MTTF y reducir el MTTR lo máximo posible



## ALTA DISPONIBILIDAD

- Existen diferentes niveles de disponibilidad en función del tiempo de inactividad al año, expresado en “número de nueves” (¿cuántos nueves?)
  - 99,9% = 43.8 minutos/mes u 8,76 horas/año ("tres nueves")
  - 99,99% = 4.38 minutos/mes o 52.6 minutos/año ("cuatro nueves")
  - 99,999% = 0.44 minutos/mes o 5.26 minutos/año ("cinco nueves")

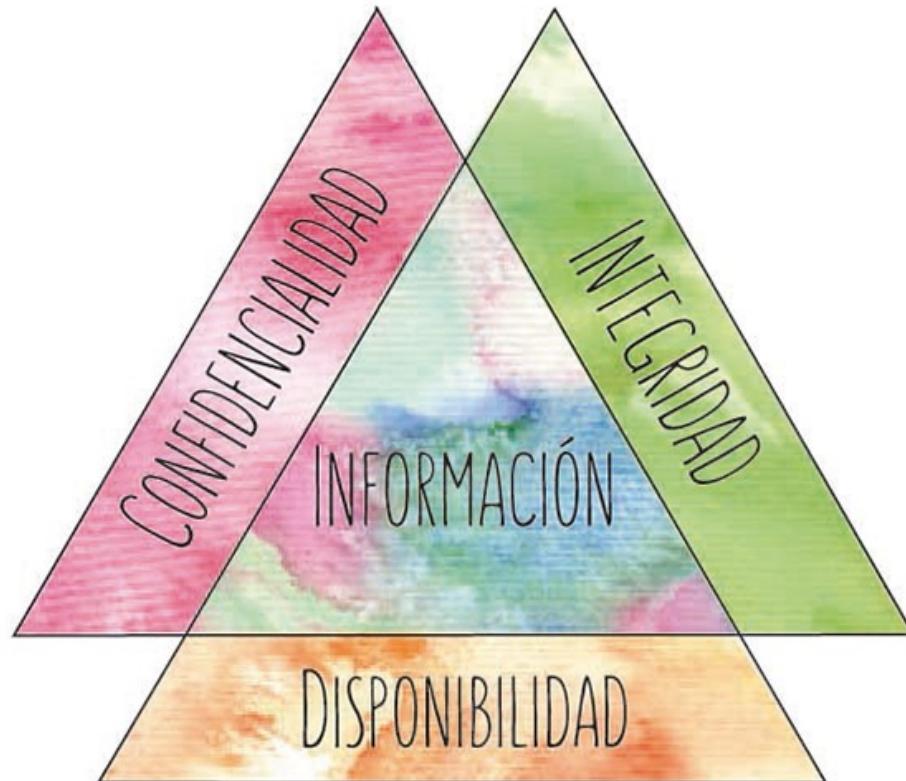
nota: 1 año = 525600 minutos

El mayor nivel acepta 5 minutos de inactividad al año → disponibilidad de 5 nueves: 99'999%



# CONFIABILIDAD, INTEGRIDAD Y DISPONIBILIDAD

- RECORDEMOS QUE..DEBEN EXISTIR LOS TRES ASPECTOS PARA QUE HAYA SEGURIDAD
- LA TRIADA DE LA SEGURIDAD



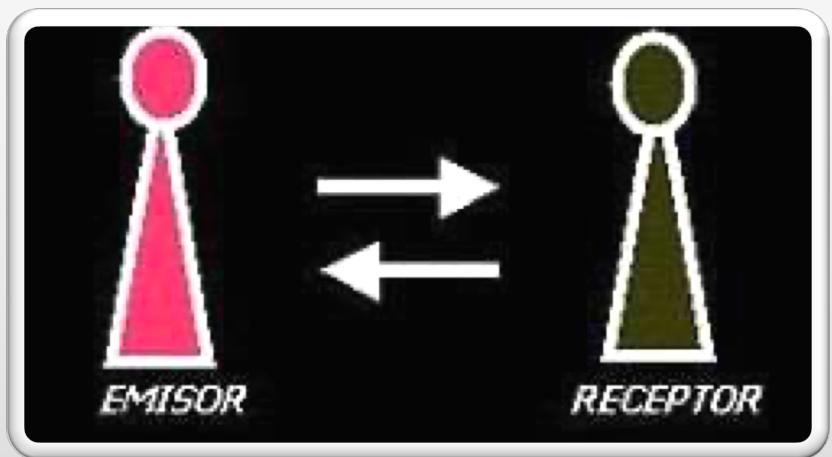
# AUTENTICACIÓN

- Confirmación de la identidad de un usuario, aportando algún modo que permita probar que es quien dice ser.
- El sistema debe ser capaz de verificar que un usuario identificado que accede a un sistema o que genera una determinada información, es quien dice ser.
- Solo cuando un usuario o entidad ha sido autenticado, podrá tener autorización de acceso.
- Se puede exigir autenticación en la entidad origen de la información, en la de destino o en ambas.
- Ejemplo: usuario o **login** + contraseña o **password**



# NO REPUDIO

- El no repudio en seguridad de la información es la **capacidad de demostrar o probar la participación de las partes** (origen y destino, emisor y receptor, remitente y destinatario), mediante su identificación, en una comunicación o en la realización de una determinada acción.
- Está estrechamente relacionado con la autenticación, permite probar la participación de las partes en una comunicación.
- Existen dos posibilidades:
  - NO REPUDIO EN EL ORIGEN: el emisor no puede negar el envío. La prueba la crea el propio emisor y la recibe el destinatario.
  - NO REPUDIO EN EL DESTINO: el receptor no puede negar que recibió el mensaje. La prueba la crea el receptor y la recibe el emisor



## RESUMIENDO...

- Los distintos servicios de seguridad dependen jerárquicamente unos de otros. Es imprescindible que exista el nivel inferior para se pueda aplicar el siguiente.



# ELEMENTO VULNERABLES EN EL SISTEMA INFORMÁTICO: HARDWARE, SOFTWARE Y DATOS

- ELEMENTOS VULNERABLES

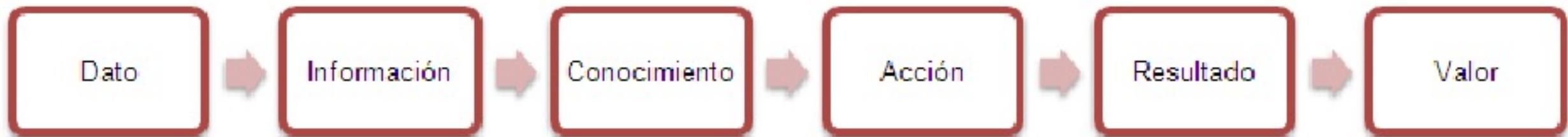
En un sistema informático lo que queremos proteger son sus activos, es decir, los recursos que forman parte del sistema y que podemos agrupar en:

- **hardware:** elementos físicos
- **software:** elementos lógicos
- **datos:** información manejada por el hardware y el software
- **otros:** fungibles, personas, infraestructuras,..

De ellos los más críticos son los datos, el hardware y el software. es decir, los datos que están almacenados en el hardware y que son procesados por las aplicaciones software.

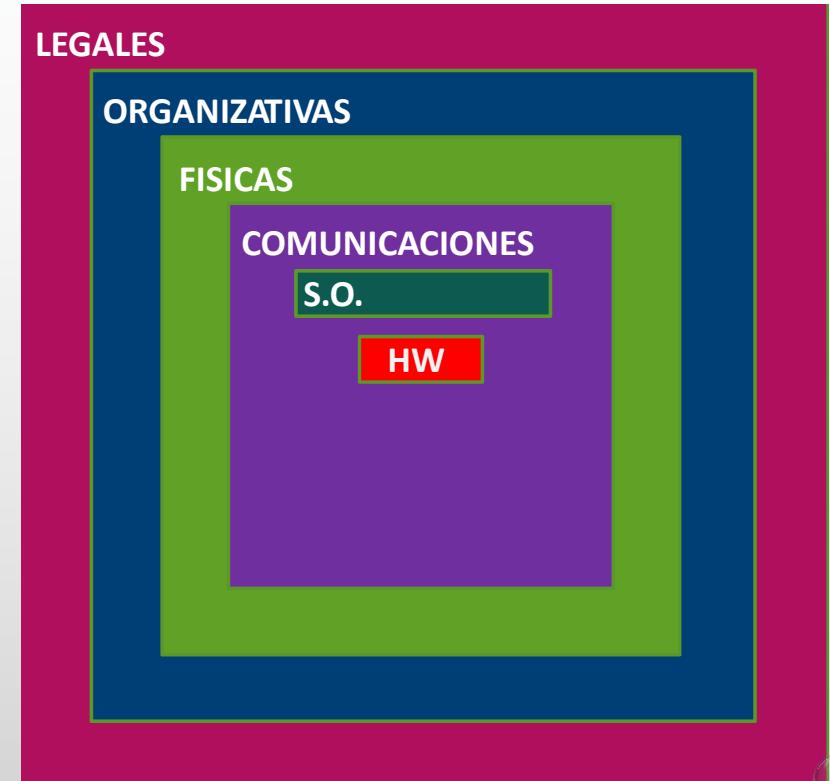
# ELEMENTO VULNERABLES EN EL SISTEMA INFORMÁTICO: HARDWARE, SOFTWARE Y DATOS

- Incluso de todos ellos, el activo más crítico son **los datos**. El resto se puede reponer con facilidad y los datos sabemos que dependen de que la empresa tenga una buena política de copias de seguridad y sea capaz de reponerlos en el estado más próximo al del momento en que se produjo la pérdida.
- Esto puede suponer para la empresa, por ejemplo, la dificultad o imposibilidad de reponer dichos datos con lo que conllevaría de pérdida de tiempo y dinero.



# ELEMENTOS VULNERABLES

- Tenemos pues distintos niveles de profundidad relativos a la seguridad informática
  - LEGALES: ley orgánica de protección de datos (LOPD)
  - ORGANIZATIVAS: políticas de seguridad de usuarios, niveles de acceso, contraseñas, normas, procedimientos...
  - FÍSICAS: ubicación de los equipos, suministro eléctrico, etc... 
  - COMUNICACIONES: protocolos y medios de transmisión seguros, etc...



# AMENAZAS

- Una amenaza se refiere a un incidente nuevo o recién descubierto que tiene el potencial de dañar un sistema o su empresa en general. Una amenaza es un evento hipotético en el que un atacante usa la vulnerabilidad.
- Las amenazas ciberneticas a veces se confunden incorrectamente con vulnerabilidades. Mirando la definición, la palabra clave es “potencial”. La amenaza no es un problema de seguridad que existe en una implementación u organización. En cambio, es algo que puede violar la seguridad. Esto se puede comparar con una vulnerabilidad que es una debilidad real que se puede explotar.
- La amenaza siempre existe, independientemente de cualquier contramedida.

# TIPOS DE AMENAZAS

- *Amenazas provocadas por personas:*

- PROPIO PERSONAL DE UNA ORGANIZACIÓN → POR DESCONOCIMIENTO O COMO VENGANZA...

<b>Hackers</b>	Expertos informáticos que vulneran sistemas por curiosidad, sin motivaciones económicas o dañinas.
<b>Crackers</b>	Hacker que quiere causar daño u obtener beneficio rompiendo la seguridad.
<b>Phreakers</b>	Crackers telefónicos. Sabotean redes telefónicas para conseguir llamadas gratuitas.
<b>Sniffers</b>	Analizan el tráfico de la red para obtener información de los paquetes transmitidos.
<b>Lammers</b>	Hacker de pose, que se define como tal pero cuyos conocimientos no están a la altura del título.
<b>Newbie</b>	Hacker novato.
<b>Ciberterrorista</b>	Terrorista que utiliza técnicas de vulneración de seguridad informática.
<b>Programadores de virus</b>	Crean programas dañinos para los sistemas o aplicaciones.
<b>Carders</b>	Atacan sistemas de tarjetas de crédito, como los cajeros automáticos.

# TIPOS DE AMENAZAS

- *Amenazas físicas y medioambientales*

Afectan a las instalaciones y/o el HW contenido en ellas. Suponen el primer nivel de seguridad a proteger para garantizar la disponibilidad de los sistemas.

Amenaza	Estrategia de defensa
<b>Incendio</b>	Mobiliario ignífugo Evitar el acercamiento del procesamiento de datos a sustancias inflamables o explosivas Implantación de sistemas anti-incendios (detectores de humo, extintores, etc.)
<b>Inundación</b>	Evitar la ubicación del procesamiento de datos en las plantas bajas. Realizar tareas que impermeabilicen las paredes y puertas
<b>Robos</b>	Proteger el centro de datos con cámaras de seguridad, vigilantes, etc.
<b>Señales electromagnéticas</b>	Evitar acerca del procesamiento de datos a radiación o utilizar cableado resistente a estas interferencias, como fibra óptica.
<b>Apagón</b>	Implantar Sistemas de Alimentación Ininterrumpida (SAI)
<b>Sobrecarga eléctrica</b>	Implantar SAI para evitar los picos de tensión eléctrica

# TIPOS DE AMENAZAS

- *Amenazas Lógicas:*

Software o código que de una forma u otra puede afectar o dañar a nuestros sistemas.

- Si son creados de manera intencionada → malware
- Si son creados por error--> bugs o agujeros

HERRAMIENTAS DE SEGURIDAD.

FALSOS PROGRAMAS DE SEGURIDAD (ROGUEWARE)

PUERTAS TRASERAS (BACKDOORS)

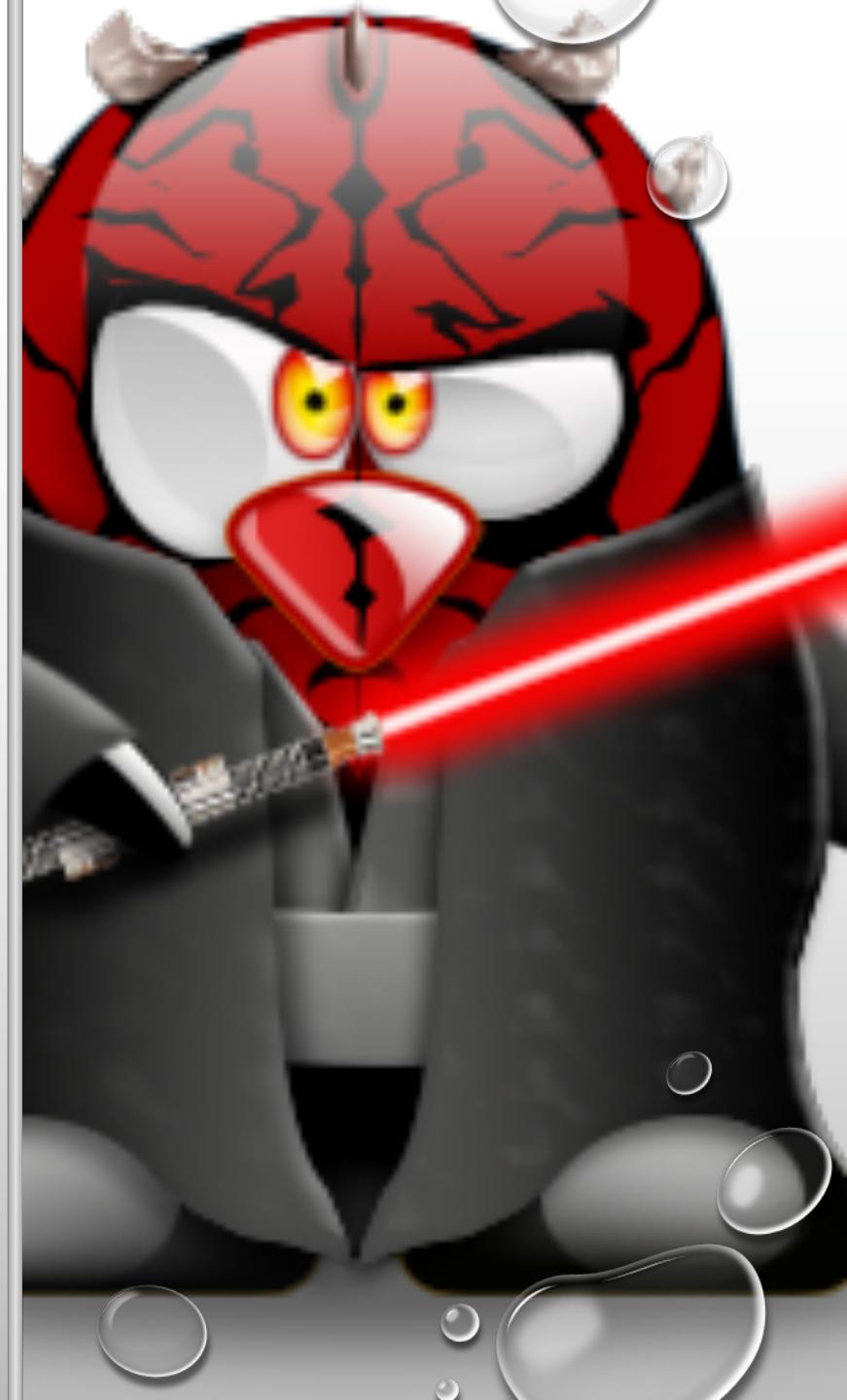
VIRUS

GUSANO (WORM)

TROYANOS

PROGRAMAS CONEJO O BACTERIAS. ([EJEMPLOS](#))

CANALES CUBIERTOS



# TIPOS DE ATAQUES

<b>Spoofing</b>	Suplanta la identidad de un PC.
<b>Sniffing</b>	Analiza el tráfico de red para hacerse con información.
<b>Conexión no autorizada</b>	Se busca un agujero de seguridad y se entra en el sistema.
<b>Malware</b>	Se introducen programas malintencionados en nuestro sistema.
<b>Keyloggers</b>	Almacenan lo que se teclea e incluso hacen capturas de pantalla para averiguar contraseñas.
<b>Denegación de servicio</b>	Interrumpe el servicio de servidores o redes. También se denomina DoS (denial of Service).
<b>Ingeniería social:</b>	Se obtiene información confidencial de una persona para utilizarla con fines maliciosos. Los ejemplos más llamativos son el phising y el spam.
<b>Phishing</b>	Se engaña al usuario para obtener su información confidencial suplantando la identidad de un organismo o página web.
<b>Spam</b>	Envío de correos electrónicos con diferentes fines (publicitarios, captura de datos) sin consentimiento previo del destinatario.

# PROTECCIÓN

- AUDITORÍA DE SEGURIDAD DE SISTEMA INFORMÁTICO

Consiste en el análisis de amenazas y riesgos potenciales para posteriormente adoptar medidas de seguridad.

Los objetivos de una auditoría de seguridad son:

- Revisar la seguridad en los entornos y sistemas
- Verificar el cumplimiento de la normativa y las legislaciones vigentes
- Elaborar un informe independiente

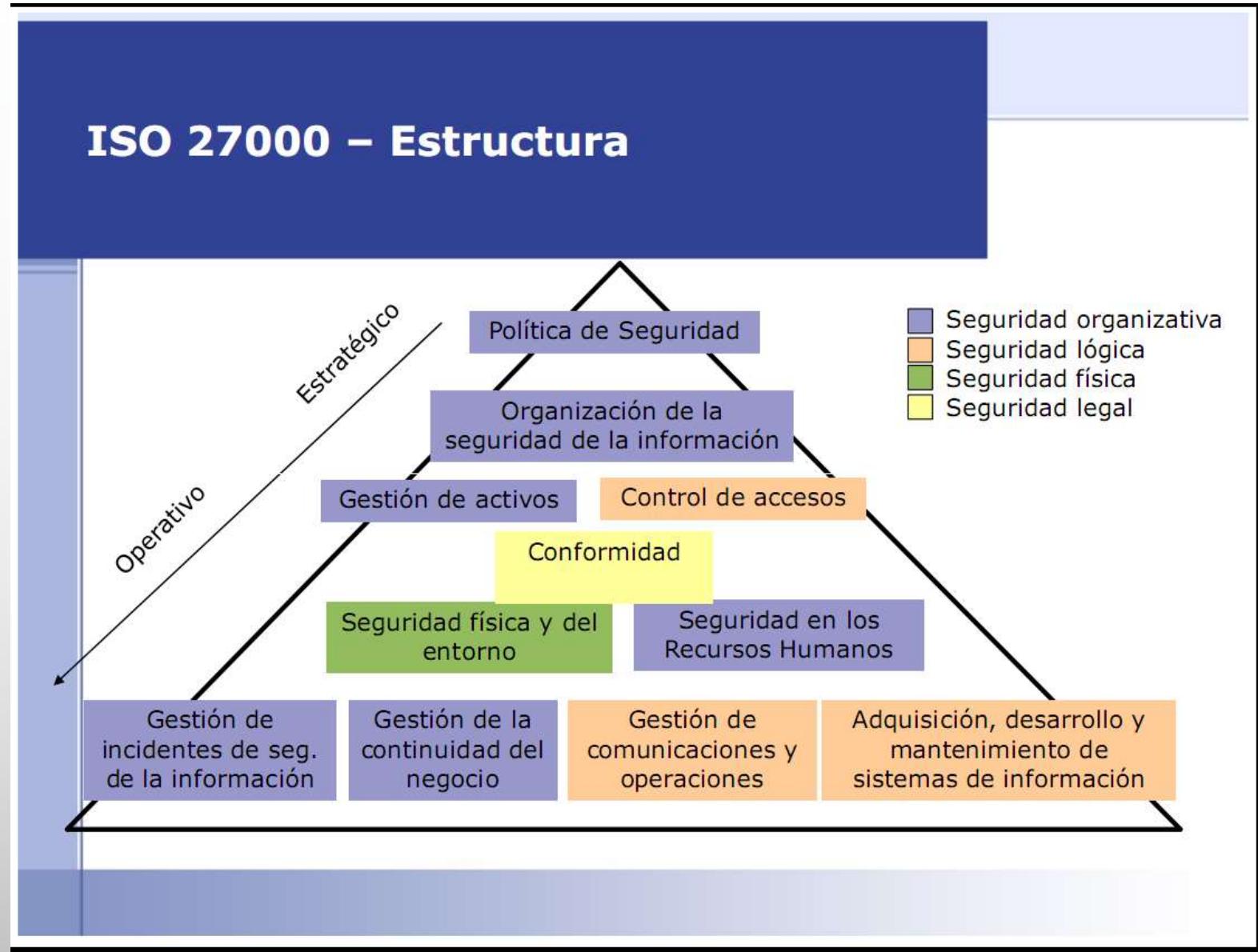


# PROTECCIÓN

- LA NORMATIVA VIGENTE ES LA SIGUIENTE
  - COBIT → Objetivos de Control de las Tecnologías de la Información.  
[\(más info\)](#)
  - ISO 27002 → Código internacional de las buenas prácticas de seguridad de la información [\(más info\)](#)
  - ISO 27001 → Sistemas de seguridad de gestión de la información. Requisitos. [\(más info\)](#)

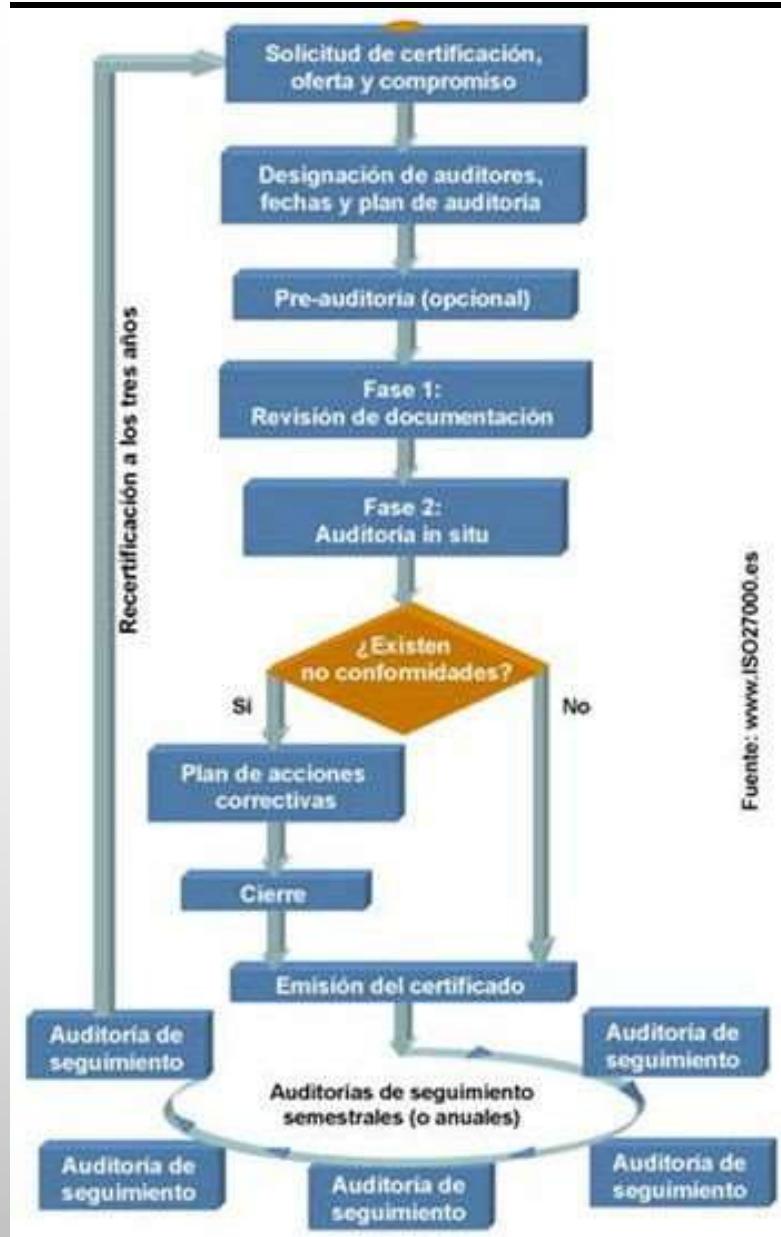


- AUDITORIA DE SEGUROIDAD DE S.I.



## • AUDITORÍA DE SEGURIDAD DE S.I.

Fases



*¿Por qué son necesarias las auditorías?*

Acciones como el constante cambio en las configuraciones, la instalación de parches, actualización del SW y la adquisición de nuevo HW hacen necesario que los sistemas estén continuamente verificados mediante auditoría.

Ejemplos prácticos:

- Auditoría Wireless.
- Auditoría de acceso a sistemas operativos.
- Auditoría de acceso a datos y aplicaciones seguras.
- Auditoría de versiones inseguras de aplicaciones y sistema operativo.

# MEDIDAS DE SEGURIDAD

- SEGÚN EL RECURSO A PROTEGER...

- **SEGURIDAD FÍSICA:**

- Trata de proteger el HW (robos, catástrofes naturales o artificiales...)
    - Medidas: ubicación correcta, medidas preventivas contra incendios o inundaciones, control de acceso físico.

- **SEGURIDAD LÓGICA:**

- Protege el SW (so + aplicaciones + información o datos del usuario)
    - Medidas: copias de seguridad, contraseñas, permisos de usuario, cifrado de datos y comunicaciones, SW antimalware, actualizaciones, filtrado de conexiones.

# MEDIDAS DE SEGURIDAD

- SEGÚN EL MOMENTO EN QUE SE PONEN EN MARCHA LAS MEDIDAS:
  - **SEGURIDAD ACTIVA:** Acciones previas a un ataque (medidas preventivas). Son todas las medidas de seguridad lógicas.
  - **SEGURIDAD PASIVA:** Acciones posteriores a un ataque o incidente (medidas correctivas). Son todas las medidas de seguridad física y las copias de seguridad que permiten minimizar el efecto de un incidente.

# SEGURIDAD FÍSICA

Amenaza	Defensa
Incendios	Mobiliario ignífugo. Evitar localización peligrosa Sistemas antiincendios, detectores de humo...
Inundaciones	Evitar plantas bajas. Impermeabilización de paredes, techos, sellado de puertas...
Robos	Puertas con medidas biométricas, cámaras, vigilantes...
Señales electromagnéticas	Evitar lugares con radiaciones electromagnéticas Filtros o cableado especial. La fibra óptica no es sensible a esto.
Apagones	SAI
Sobrecargas eléctricas	SAI. También estabilizan la señal eléctrica
Desastres naturales	Estar en contacto con los organismos que proporcionan información sobre terremotos o desastres meteorológicos.

# SEGURIDAD LÓGICA

Amenaza	Mecanismo de defensa
Robos	Cifrado. Contraseñas Sistemas biométricos
Pérdida de información	Copia de seguridad (distintas ubicaciones) Sistemas tolerantes a fallos Discos redundantes
Pérdida de integridad de la información	Programas de chequeo del equipo. Firma digital Comando sfc
Entrada de virus	Antivirus
Ataques desde la red	Firewall Programas de monitorización Proxys
Modificaciones no autorizadas	Contraseñas Listas de control de acceso Cifrar documentos

## SEGURIDAD ACTIVA

Técnicas	¿Qué previene?
Contraseñas	Previene el acceso a recursos a usuarios no autorizados
Listas de control de acceso	Previene acceso a ficheros a usuarios no autorizados
Encriptación	Evita a personas no autorizadas interpretar la información
Software de seguridad	Evita virus y accesos no deseados al sistema
Firmas y certificados digitales	Comprueba la procedencia, autenticidad e integridad de los mensajes
Sistemas de ficheros tolerantes a fallos	Previene fallos de integridad
Cuotas de disco	Previene el uso excesivo de disco por parte de algún usuario

## SEGURIDAD PASIVA

Técnicas	Resultado
Discos redundantes	Restaurar datos que han quedado inconsistentes
SAI	Proporcionan energía durante un periodo de tiempo.
Copias de seguridad	Podemos recuperar información en caso de pérdida de datos.

GRACIAS POR VUESTRA ATENCIÓN

