Seguridad y Alta Disponibilidad

UNIDAD 1.
PRINCIPIOS DE SEGURIDAD Y ALTA DISPONIBILIDAD

Objetivos

- Analizar la problemática general de la seguridad informática.
- Conocer los principios sobre los que se sustenta.
- Conocer el significado de alta disponibilidad.
- Identificar las principales vulnerabilidades, ataques y medidas de seguridad a adoptar sobre los sistemas.
- Diferenciar la seguridad física y lógica, y la pasiva de la activa

Contenidos

1. Introducción a la Seguridad Informática
2. Fiabilidad, Confidencialidad, Integridad y Disponibilidad
3. Elementos vulnerables en el sistema informático: Hardware, Software y Datos.
4. Amenazas
   - 4.1. Amenazas provocadas por las personas
   - 4.2. Amenazas físicas y lógicas
   - 4.3. Técnicas de ataque
5. Protección
   - 5.1. Auditoría de seguridad de sistemas de información
   - 5.2. Medidas de seguridad

1

INTRODUCCIÓN A LA SEGURIDAD INFORMÁTICA

Introducción a la Seguridad Informática (1)

- Hoy en día, un sistema informático totalmente seguro es imposible. La conectividad global extiende el campo de posibles amenazas.

- Seguridad informática:

  Asegurar que los recursos del sistema de información sean utilizados de la manera que se decidió y que el acceso y modificación a la información sólo sea posible a las personas que se encuentren acreditadas y dentro de los límites de su autorización.

Introducción a la Seguridad Informática (2)

- Principales objetivos de la seguridad informática:
  - ✓ 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 organizativo.

2

FIABILIDAD, CONFIDENCIALIDAD, INTEGRIDAD Y DISPONIBILIDAD

Fiabilidad

- La **seguridad absoluta** no es posible.
- **Seguridad informática**: técnicas para obtener altos niveles de seguridad → **FIABILIDAD**
- **Fiabilidad**: 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

Fiabilidad

" 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

Confidencialidad, Integridad y Disponibilidad

- Un sistema seguro (o 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.

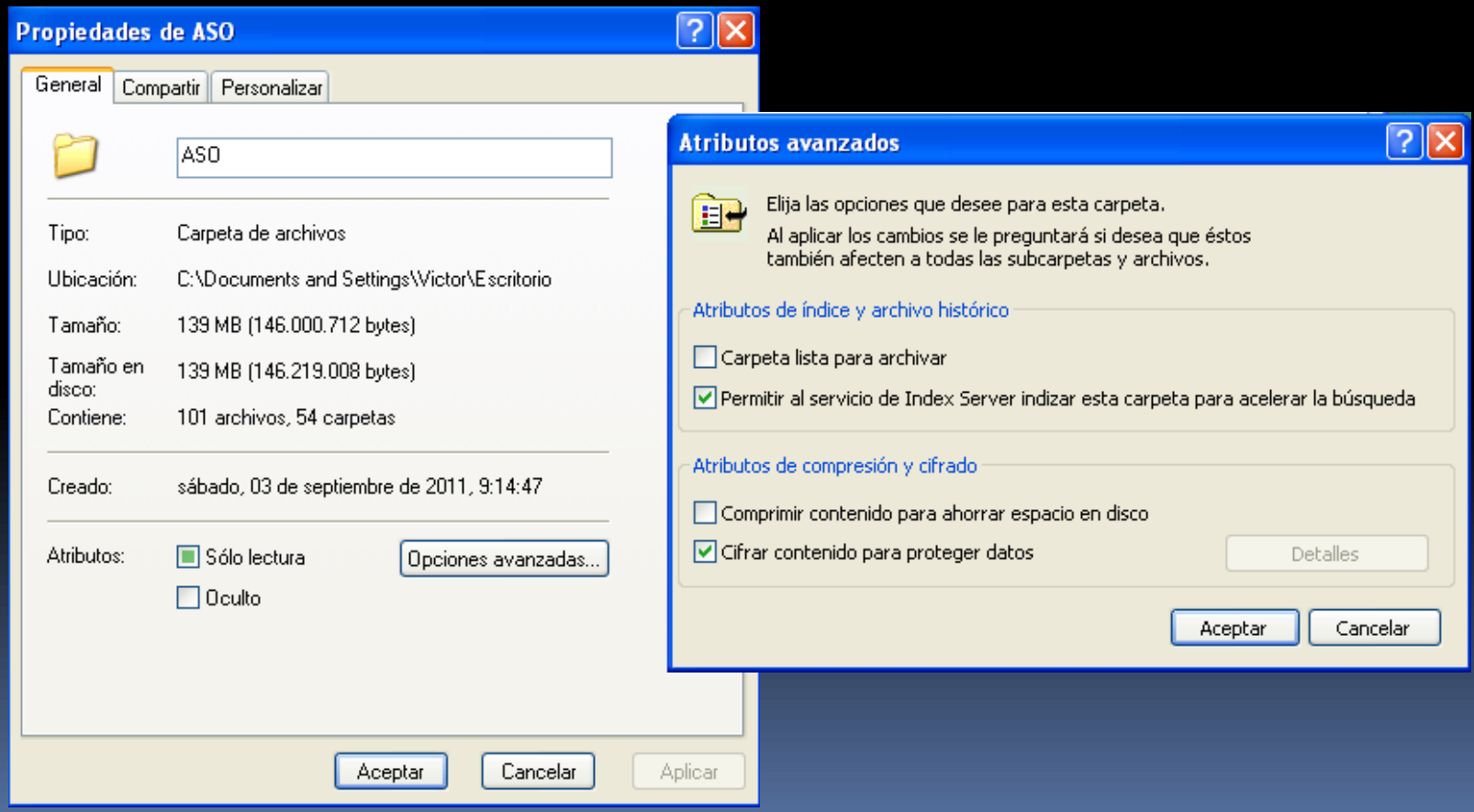
- Para un usuario que no tiene permiso para acceder a la información, ésta debe ser ininteligible. Sólo los individuos autorizados deben tener acceso a los recursos que se intercambian.

- Ejemplos:
  - **EFS** *(Encrypted File System)*.
  - Cifrado asimétrico/simétrico en comunicaciones.

Confidencialidad

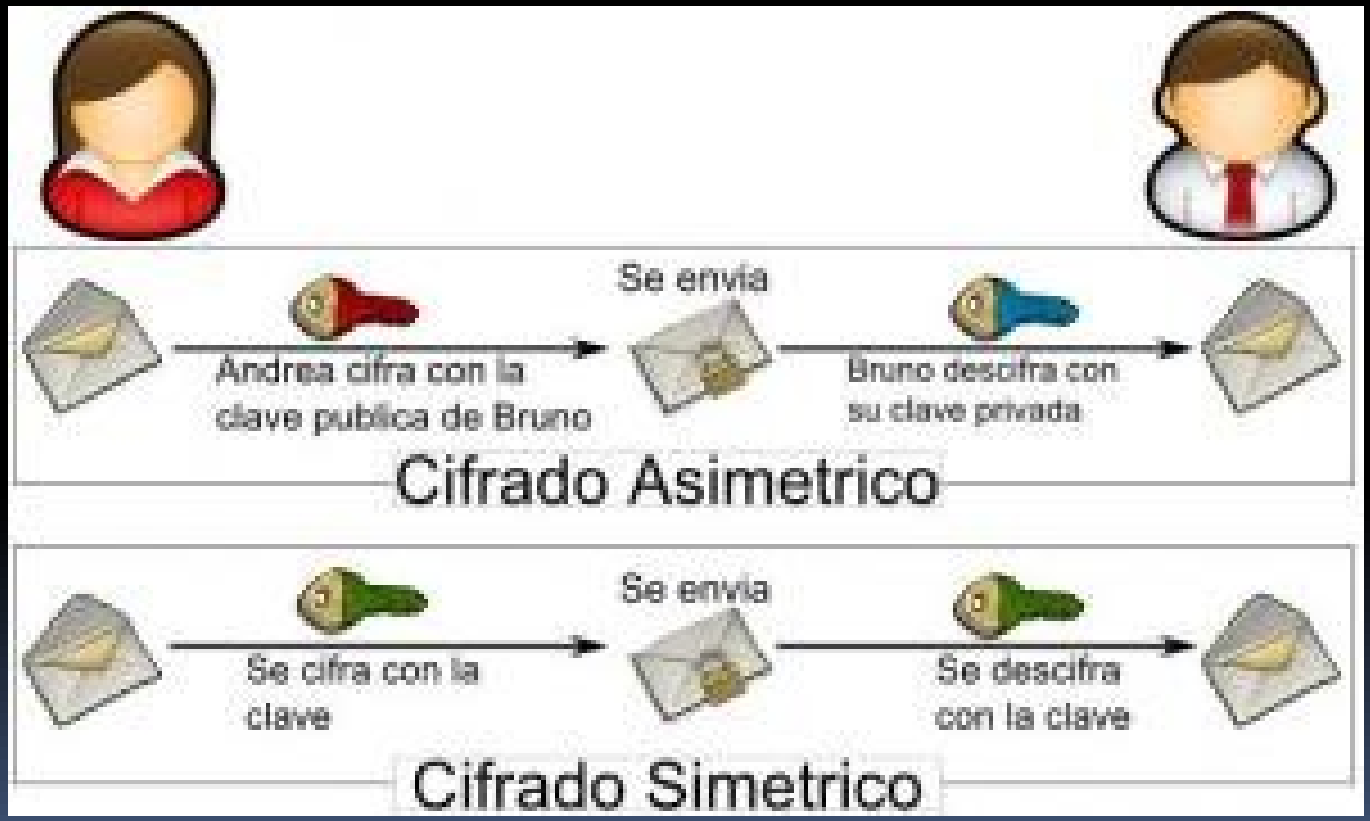
- **EFS** *(Encrypted File System)*.

  Cifrado de archivos en *Windows* para particiones *NTFS*.



Confidencialidad

- Cifrado asimétrico/simétrico en comunicaciones



Integridad

- Propiedad que busca mantener los datos libres de modificaciones no autorizadas.

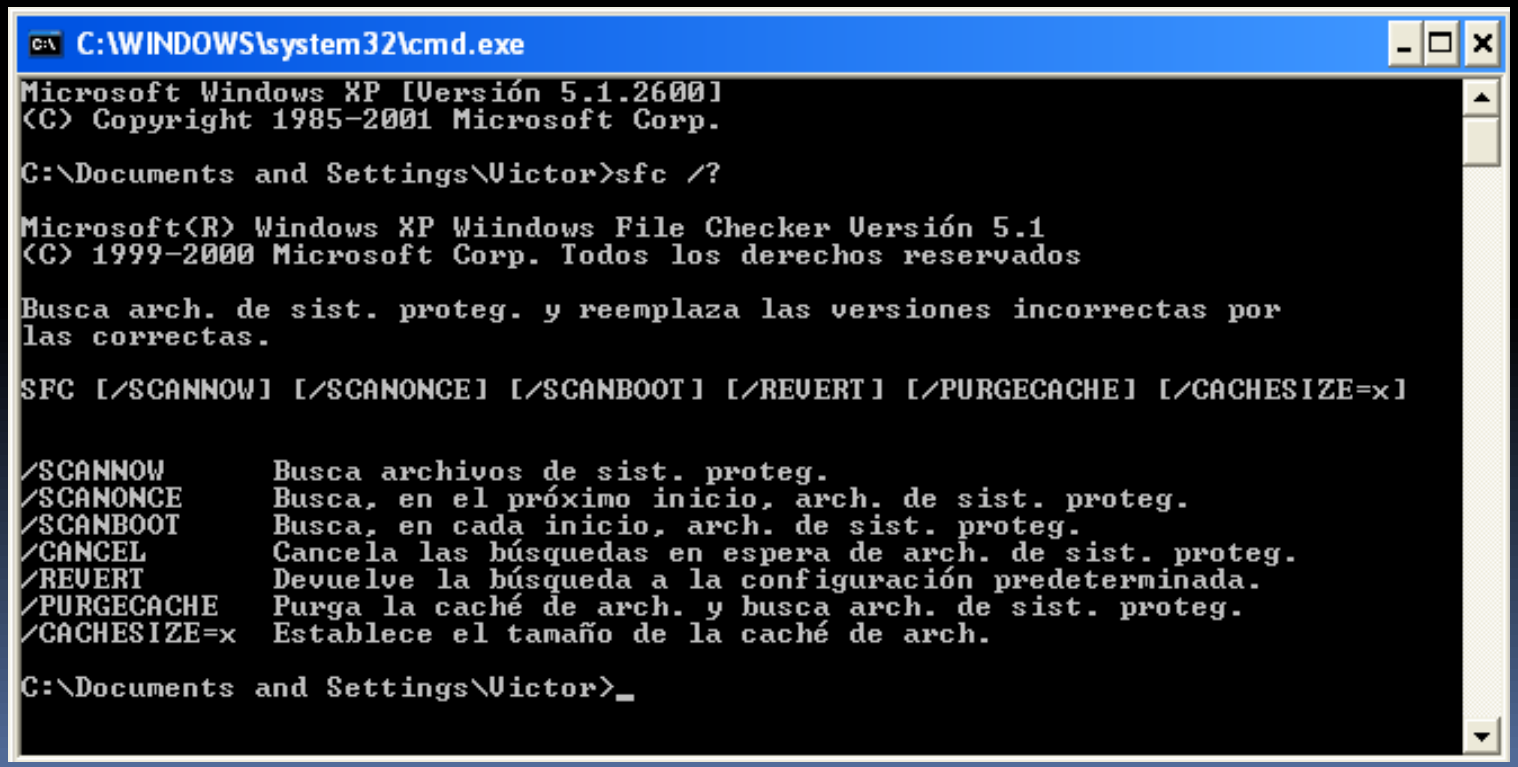
- Asegura que los datos del sistema no han sido alterados ni cancelados por personas o entidades no autorizadas y que el contenido de los mensajes recibidos es el correcto.

- Ejemplos:
  - **SFC** (*Windows*)
  - **Rootkit hunter** (*Linux*)
  - 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.



Integridad

- **Rootkit Hunter**

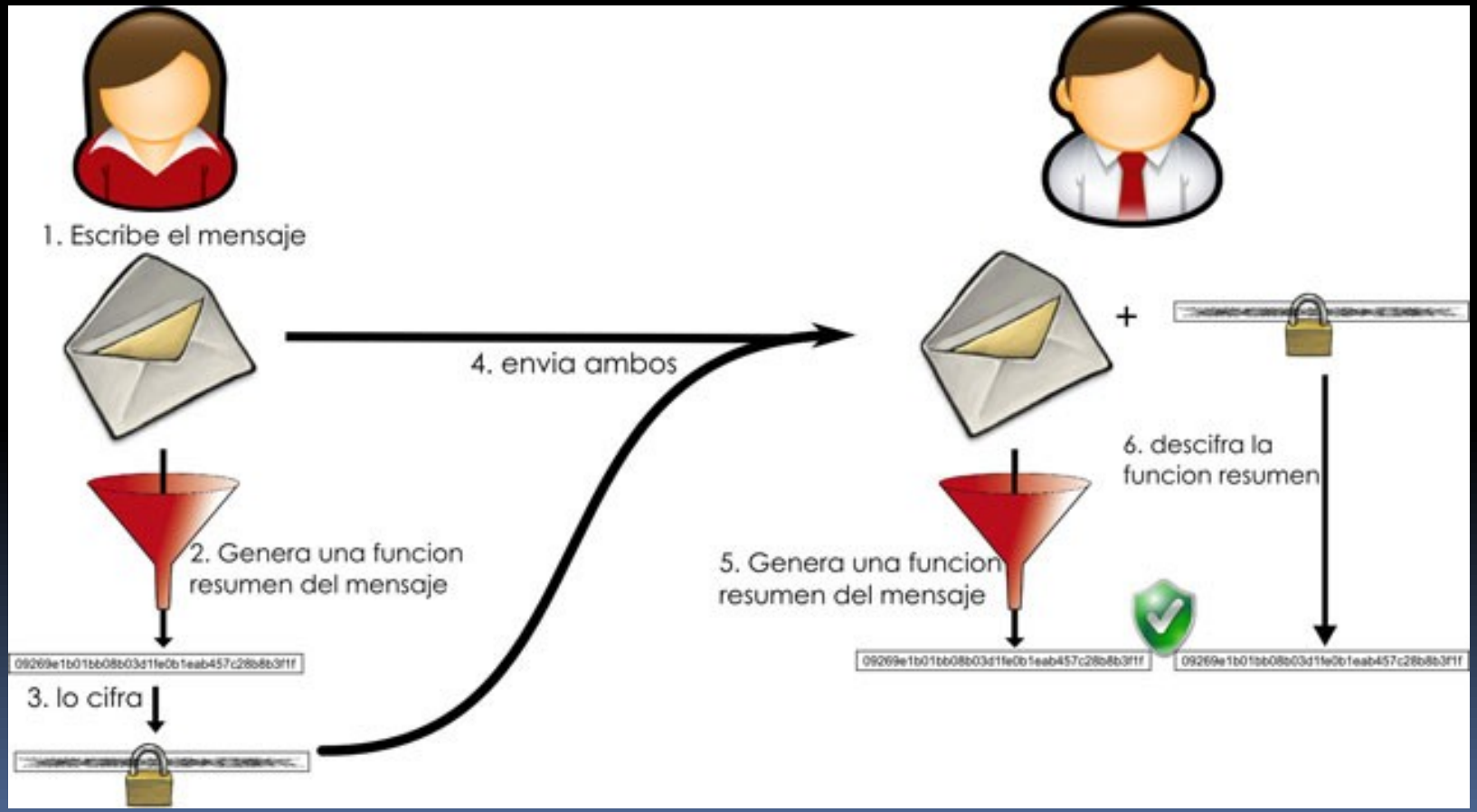
  Herramienta GNU/Linux que, además de realizar la comprobación de integridad de los archivos de sistema (es decir, verificar que no han sido modificados), examina los permisos de los ejecutables del sistema y busca *rootkits* conocidos rastreando ficheros ocultos.

Instalación: `$ sudo aptitude install rkhunter`

Ejecución: `$ sudo rkhunter –checkall`

Integridad

- 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

- Ejemplos:
  - www.securityfocus.com. Informes sobre vulnerabilidades en aplicaciones y SO.
  - www.nessus.org. Detecta vulnerabilidades tanto para Windows como GNU/Linux.
  - **MBSA** *(Microsoft Baseline Security Analyzer).* Detecta los errores más comunes de configuración de seguridad y actualizaciones de seguridad que falten para sistemas Windows.
  - **NMAP** *("Mapeador de redes").* 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.

Disponibilidad

- **Alta Disponibilidad** *(High Availability)*

  Capacidad de que aplicaciones y datos se encuentren operativos para los usuarios autorizados en todo momento y sin interrupciones.

  Sistemas "24x7x365"

  Mantener los sistemas funcionando 24 horas al día, 7 días a la semana y 365 días al año a salvo de interrupciones (previstas o imprevistas)

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

Ejemplo de Alta Disponibilidad: ***CPD***

Confidencialidad, Integridad y Disponibilidad

Tienen que existir los tres aspectos para que haya 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.

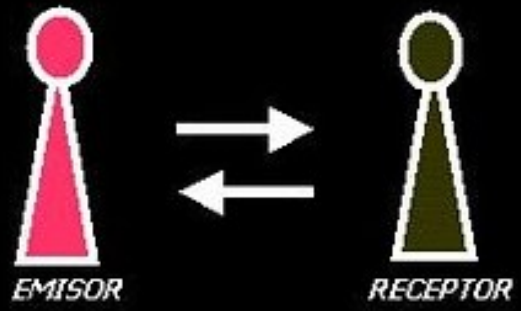
  Se puede exigir autenticación en la entidad origen de la información, en la de destino o en ambas.

- Ejemplo: Usuario o ***login*** + contraseña o ***password***

No Repudio

- 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.

CIDAN

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

3

ELEMENTOS VULNERABLES EN EL SISTEMA INFORMÁTICO: HARDWARE, SOFTWARE Y DATOS

Elementos vulnerables

- Seguridad = problema integral

  Los problemas de seguridad no pueden tratarse aisladamente.

Seguridad de todo el sistema = seguridad de su punto más débil.

- Elementos a proteger:
  - Software
  - Hardware
  - Datos ← Principal: es el más amenazado y el más difícil de recuperar

Elementos vulnerables

- 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…

4

AMENAZAS

Amenazas provocadas por personas

- Propio personal de una organización
- **Hackers**
  - White|Grey| Black Hat
  - Cracker
  - Newbie
  - Wannaber
  - Phreaker
  - Script kiddie o Lammer
  - Luser *(looser + user)*

- Pirata informático, ciberdelincuente o delincuente informático.

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.

  - ✓ Robos, sabotajes, destrucción de sistemas.
  - ✓ Cortes, subidas y bajadas bruscas de suministros eléctricos
  - ✓ Condiciones atmosféricas adversas. Humedad relativa excesiva o temperaturas extremas.
  - ✓ Catástrofes (naturales o artificiales): terremotos, inundaciones, incendios, humo o atentados de baja magnitud, etc.
  - ✓ Interferencias electromagnéticas que afecten al normal comportamiento de circuitos y comunicaciones.

Amenazas lógicas

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

  Creados de forma intencionada (malware) o por error (bugs o agujeros).

  - Herramientas de seguridad.
  - Falsos programas de seguridad (*rogueware*)
  - Puertas traseras (*backdoors*)
  - Virus
  - Gusano (*worm*)
  - Troyanos
  - Programas conejo o bacterias
  - Canales cubiertos

Técnicas de ataque

- Los tipos de amenazas pueden clasificarse en función de la **técnica que empleen para realizar el ataque**:
  - Malware
  - Ingeniería social
  - Scam
  - Spam
  - Sniffing
  - Spoofing
  - Pharming
  - Phishing
  - Password cracking
  - Botnet
  - Denegación de servicio o *Denial of Service* (DoS)

5
PROTECCIÓN

Auditoría de seguridad de S.I.

- Análisis de amenazas y riesgos potenciales para posteriormente adoptar medidas de seguridad.

- Los objetivos de una auditoría de seguridad en los S.I. son:
  - ✓ Revisar la seguridad de los entornos y sistemas.
  - ✓ Verificar el cumplimiento de la normativa y legislación vigentes.
  - ✓ Elaborar un informe independiente

Auditoría de seguridad de S.I.

- Normativa:
  - **COBIT**

    Objetivos de Control de las Tecnologías de la Información y relacionadas.

  - **ISO 27002**

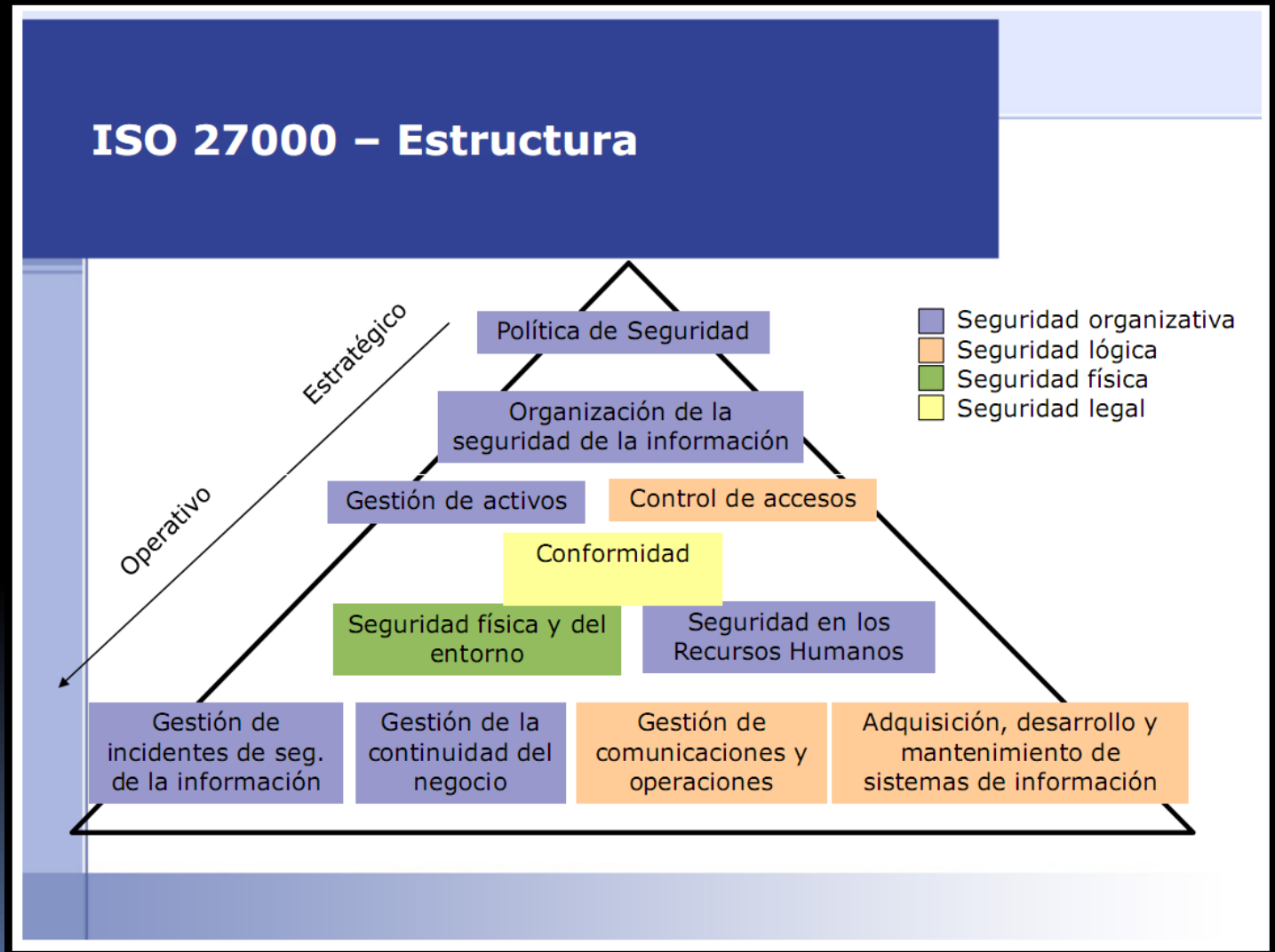
    Código Internacional de buenas prácticas de seguridad de la información.

  - **ISO 27001**

    Sistemas de Gestión de Seguridad de la Información (***SGSI***). Requisitos.

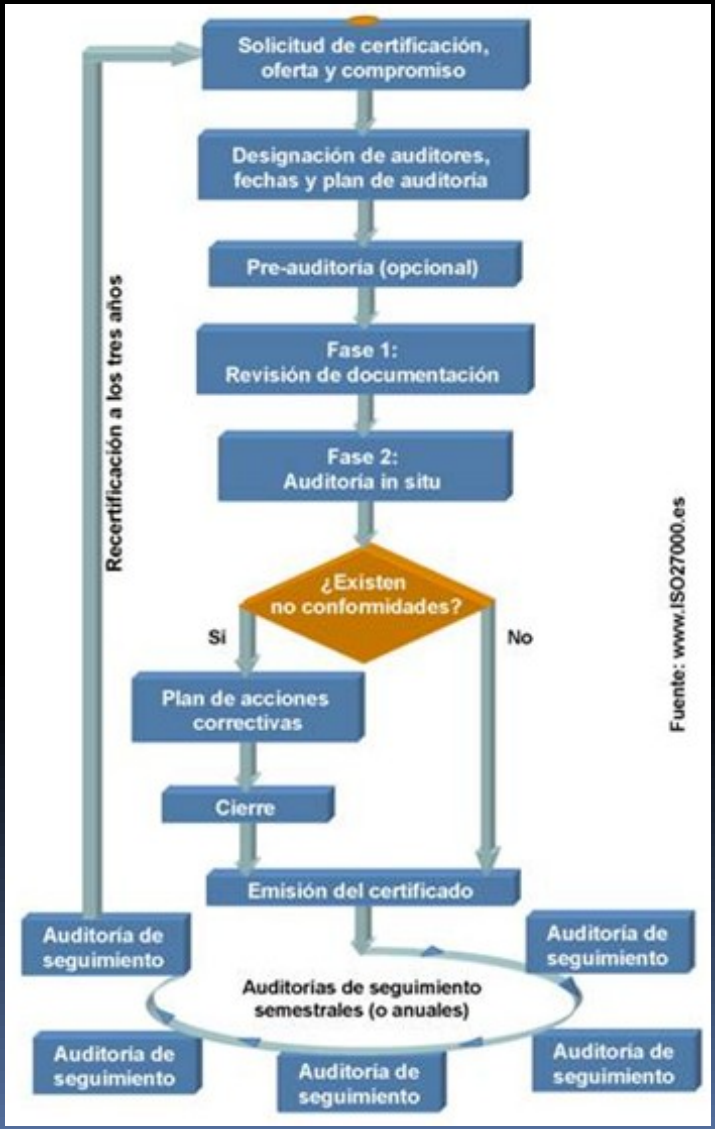
Portal de **ISO 27001** en español: www.iso27000.es

Auditoría de seguridad 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.
- 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.

Mantenerse siempre informado y al día es la primera y mejor recomendación en materia de seguridad informática