ISO 7498

Serie de mecanismos que minimizan la vulnerabilidad de bienes y recursos

TEMA 1

Criterios generales comúnmente aceptados sobre seguridad de los equipos informáticos

Apartados BOE

- Modelo de seguridad a la gestión del riesgo relacionado con el uso de los **sistemas de información**
- Relación de las **amenazas** más frecuentes, los **riesgos** que implican y las **salvaguardas** más frecuentes
- Salvaguardas y tecnologías de seguridad **más habituales**
- La **gestión de la seguridad informática** como complemento a salvaguardas y medidas tecnológicas

Conceptos generales

- Un **sistema de información** es un conjunto de elementos que interactúan entre sí con el fin de apoyar las **actividades de una empresa**, entre ellos s encuentran:
  - **Equipos informáticos**
  - **Personal** que interactúa con estos equipos

Las **actividades básicas** de un Sistema de información:

- Entrada
- Almacenamiento
- Procesamiento
- Salida de información

- **Amenaza** o Ataque a la seguridad
  - Cualquier acción que comprometa la seguridad de la información
- **Salvaguarda** o Mecanismo de seguridad
  - Un mecanismo diseñado para:
    - Detectar un ataque a la seguridad
    - Prevenirlo
    - Restablecerse de él
- **Servicio de Seguridad**
  - Servicio de procesamiento o de comunicación proporcionada por un sistema para dar un tipo **especial de protección a los recursos del sistema**
  - **Mejora la seguridad** de los sistemas de **procesamiento de datos** y la **transferencia** de datos
  - Los servicios de seguridad **implementan políticas de seguridad** y son **implementados**, a su vez, por **mecanismos de seguridad**

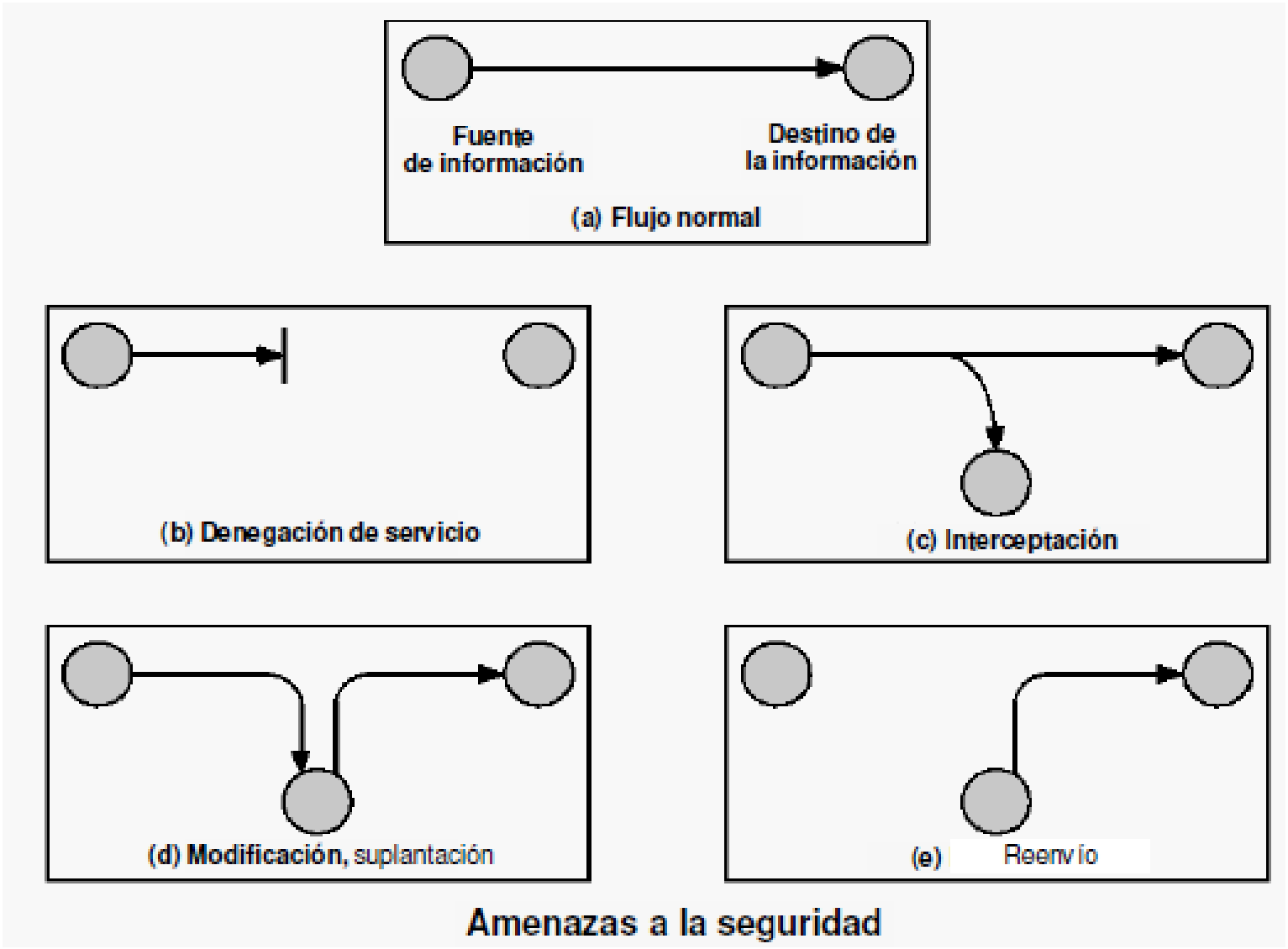
- **Objetivos de la seguridad** → Triada IAC (CIA)
- **Disponibilidad**, **confidencialidad** e **integridad**

Tipos de amenazas/ataques

- Hay **dos tipos de amenazas**
  - Amenaza **pasiva**
    - **Intenta conocer o hacer uso de información** del sistema pero **no afecta a los recursos del mismo**
    - **Difíciles de detectar** al no implicar alteración en los contenidos
    - (hay más **énfasis en la prevención** que en la detección)
  - Amenaza **activa**
    - Implican la **modificación del flujo de datos** o la **creación un flujo falso**

- Amenazas pasivas
  - **Obtención de contenidos de mensajes (<u>interceptación</u>)**
    - Ejp: mensajes de correo electrónico
    - Fichero con información confidencial
  - **Análisis de tráfico**
    - Patrón de mensajes:
      - Localización e identidad de los servidores que se comunican
      - Frecuencia y longitud de los mensajes

- Amenazas activas
  - **Modificación**
    - El oponente modifica el contenido de algún mensaje o texto
  - **Suplantación**
    - El oponente se hace pasar por otra persona
  - **Reenvío o repetición**
    - La entidad atacante obtiene un mensaje o texto en tránsito y más tarde lo reenvía para duplicar su efecto
  - **Denegación o interrupción de servicio**
    - La entidad atacante impide que un elemento cumpla su función



Amenazas a la seguridad

Servicios de seguridad

- **Autenticación**
  - ¿Es realmente quien dice ser?
- **Control de acceso**
  - ¿Tiene derechos a hacer lo que pide?
- **Confidencialidad** de los datos
  - ¿lo ha interceptado alguien?
- **Integridad** de los datos
  - ¿Puedo asegurar que este mensaje está intacto
- **No repudio**
  - ¿Ha enviado/recibido esto realmente la parte especificada?

Salvaguardas / Mecanismos de seguridad

- Mecanismos de seguridad **específicos**
  - Pueden ser **incorporados en la cada de protocolo adecuada** para proporcionar algunos de los servicios de seguridad
- Mecanismos de seguridad **generales**
  - No son específicos de ninguna capa de protocolo o sistema de seguridad OSI en particular

- Mecanismos de seguridad **específicos** (1/2)
  - **Cifrado**
    - Uso de **algoritmos matemáticos** para transformar datos de una forma inteligible
  - **Firma digital**
    - **Datos añadidos** a, o una **transformación criptográfica** de, una unidad de datos que permite al receptor verificar la fuente y la integridad de los datos y protegerla de falsificación
  - **Control de acceso**
    - Mecanismos que refuerzan los **derechos de acceso a los recursos**
  - **Integridad de los datos**
    - Mecanismos empleados para **verificar la integridad** de una unidad de datos o del flujo de las mismas
  - **Intercambio de autenticación**
    - Mecanismo diseñado para **verificar la identidad** de una entidad

- Mecanismos de seguridad **específicos** (2/2)
  - **Relleno de tráfico**
    - **Inserción de bits** de espacios de un flujo de datos con el objetivo de **frustrar los intentos de análisis de tráfico**
  - **Control de enrutamiento**
    - Permite la **selección de rutas físicamente seguras** para determinados datos y permite los cambios de enrutamiento, especialmente cuando se sospecha de una brecha de seguridad
  - **Notarización**
    - Uso de una **tercera parte confiable** para asegurar determinadas propiedades de un intercambio de datos

- Mecanismos de seguridad **generales**
  - **Funcionalidad fiable**
    - Lo que se considera fiable con respecto a algunos criterios
    - (según se haya definido en la política de seguridad)
  - **Etiquetas de seguridad**
    - La marca asociada a un recurso que designa los atributos de seguridad de dicho recurso
    - (dirección IP que puede utilizarse para permitir o no el acceso a una red)
  - **Informe para auditoría de seguridad**
    - Recopilación de datos para facilitar una auditoría de seguridad, que consiste en una revisión independiente de los informes y actividades del sistema
  - **Recuperación de la seguridad**
    - Lleva a cabo acciones de recuperación

Amenazas y sus salvaguardas más comunes

- **TOP 20** de las amenazas más comunes y la salvaguarda que ofrecen los proveedores:
  - IBM, McAffe, Symantec, Windows, etc

- Para la **Ciberdefensa**, estos controles no son críticos, hay otros que tienen más importancia.

Sistema de Gestión de Seguridad de la Información (SGSI)

- Para proteger la información de una manera coherente y eficiente, es necesario establecer un **Sistema de Gestión de Seguridad de la Información** (**SGSI**)
- La seguridad de la información se logra **implementando** un adecuado **conjunto de controles**

- Un **SGSI** es un sistema de gestión que comprende:
  - **Política**
  - **Estructura** organizativa
  - **Procedimientos**
  - **Procesos**
  - **Recursos** necesarios para implantar la gestión de la seguridad de la información
- Además debe cumplir con los siguientes **requisitos**
  - Cubre aspectos organizativos, lógicos, físicos, legales…
  - Independiente de la plataforma tecnológica y de mecanismos concretos
  - Fuerte contenido documental

- Los **objetivos** del SGSI
  - Definir, lograr, mantener y mejorar la seguridad de la información
  - Dirigir y dar soporte a la gestión de seguridad
  - Establecer el compromiso de la dirección y el enfoque de la organización para gestionar la seguridad de la información
- Un SGSI debe **basarse en un marco de seguridad** probado, evitando soluciones a medida:
  - **Norma ISO/IEC 27002**
    - **Code of practice for information security management**
    - Normas, criterios y recomendaciones básicas para establecer políticas de seguridad
  - **Norma ISO/IEC 27001**
    - **Information security management systems – Requerimients**
    - Especifica los requisitos necesarios para establecer, implantar, mantener un **SGSI → ES CERTIFICABLE**

- Se puede prever, que la certificación **ISO-27001**, será casi una **obligación de cualquier empresa** que desee competir en el mercado en el corto plazo, lo cual es lógico, pues si se desea interrelacionar
  - sistemas de clientes, control de stock, facturación, pedidos, productos, etc. entre diferentes organizaciones,
  - se deben exigir mutuamente niveles concretos y adecuados de seguridad informática, sino se abren brechas de seguridad entre sí . (**eslabón más débil**)