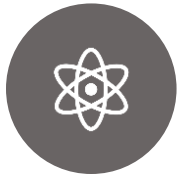
UT1. LA SEGURIDAD INFORMÁTICA

Módulo: Seguridad y Alta Disponibilidad

Curso 2023/2024. 2º ASIR

CONTENIDOS

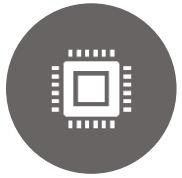
Visión global de la seguridad informática



Seguridad física y lógica

Copias de seguridad

Seguridad física eléctrica: el SAI



Seguridad en los medios de almacenamiento online DAS, NAS, SAN

Criptografía

VISIÓN GLOBAL

“El único sistema verdaderamente seguro es aquel que se encuentra apagado, encerrado en una caja fuerte de titanio, enterrado en un bloque de hormigón, rodeado de gas nervioso y vigilado por guardias armados y muy bien pagados. Incluso entonces, yo no apostaría mi vida por ello.”

Gene Spafford,

Experto en seguridad informática.

- La Seguridad es un concepto confuso porque se compone de muchos elementos interrelacionados entre sí

- A lo largo del módulo se irán exponiendo muchos conceptos…
  - MAPAS MENTALES

1ER PRINCIPIO DE LA SEGURIDAD INFORMÁTICA

PREGUNTA

¿CUÁLES SON LOS PUNTOS DÉBILES DE UN SISTEMA INFORMÁTICO?

1ER PRINCIPIO DE LA SEGURIDAD INFORMÁTICA

PREGUNTA

¿CUÁLES SON LOS PUNTOS DÉBILES DE UN SISTEMA INFORMÁTICO?

- **El intruso utilizará cualquier artilugio que haga más fácil su acceso al sistema y posterior ataque**

- Existirá una diversidad de frentes desde los que pueden producirse **ataques**. Esto dificulta el **análisis de riesgos**

2º PRINCIPIO DE LA SEGURIDAD INFORMÁTICA

PREGUNTA

¿CUÁNTO TIEMPO DEBERÁ PROTEGERSE EL DATO?

2º PRINCIPIO DE LA SEGURIDAD INFORMÁTICA

PREGUNTA

¿CUÁNTO TIEMPO DEBERÁ PROTEGERSE EL DATO?

- **Los datos confidenciales deben protegerse sólo hasta que esa información pierda su valor**

- Por tanto, se habla de la caducidad del sistema de protección: tiempo en que debe mantenerse la **confidencialidad** o secreto del dato

3º PRINCIPIO DE LA SEGURIDAD INFORMÁTICA

- Las **medidas de control** se implementan para ser utilizadas de forma efectiva. Deben ser eficientes, fáciles de usar y apropiadas al medio. Deben:
  - Funcionar en el momento oportuno
  - Y optimizando los recursos del sistema
  - Ser desapercibidas al usuario

3º PRINCIPIO DE LA SEGURIDAD INFORMÁTICA

- Las **medidas de control** se implementan para ser utilizadas de forma efectiva. Deben ser eficientes, fáciles de usar y apropiadas al medio. Deben:
  - Funcionar en el momento oportuno
  - Y optimizando los recursos del sistema
  - Ser desapercibidas al usuario

¡¡Ningún sistema de control resulta efectivo hasta que es utilizado!!

SEGURIDAD INFORMÁTICA ¿POR QUÉ?

La **seguridad informática** es la disciplina que se ocupa de diseñar las normas, procedimientos, métodos y técnicas destinados a conseguir un sistema de información seguro y confiable.

"todo lo que no está permitido debe estar prohibido *"*

La **seguridad informática** consiste en asegurar que los recursos de un 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, sólo sea posible a las personas que se encuentren acreditadas y dentro de los límites de su autorización.

SEGURIDAD INFORMÁTICA

- La **seguridad informática** es el área de la informática que se enfoca en la protección de la infraestructura computacional y todo lo relacionado con esta (incluyendo la información contenida).
- Para ello existen una serie de **estándares, protocolos, métodos, reglas, herramientas y leyes** concebidas para minimizar los posibles riesgos a la infraestructura o a la información.
- La seguridad informática comprende software, bases de datos, metadatos, archivos y todo lo que la organización valore (activo) y signifique un riesgo si ésta llega a manos de otras personas.
- Este tipo de información se conoce como información privilegiada o confidencial.

Seguridad

según la RAE

Dicho de un mecanismo: Que asegura algún buen funcionamiento, precaviendo que este falle, se frustre o se violente.

Asegurar

según la RAE

1. Preservar o resguardar de daño a alguien o algo; defenderlo e impedir que pase a poder de otra persona
2. Poner a cubierto una cosa de la pérdida que por naufragio, incendio o cualquier otro accidente o motivo pueda tener en ella su dueño, obligándose a indemnizar a este del importe total o parcial de dicha pérdida, con sujeción a las condiciones pactadas.

SEGURIDAD INFORMÁTICA: OBJETIVOS

Detectar los posibles problemas y amenazas a la seguridad, minimizando y gestionando los riesgos.

Cumplir con el marco legal y con los requisitos impuestos a nivel organizativo.

Garantizar la adecuada utilización de los recursos y de las aplicaciones de los sistemas.

Limitar las perdidas y conseguir la adecuada recuperación del sistema en caso de un incidente de seguridad.

SEGURIDAD INFORMÁTICA: OBJETIVOS CID

¿Qué debemos asegurar?

Los **DATOS**
Información dispuesta de manera adecuada para su tratamiento por un ordenador.

¿De qué debemos preocuparnos?

Confidencialidad
No todo el mundo debe acceder a los datos, sólo los autorizados.

Integridad
Los datos no han sido modificados sin autorización

Disponibilidad
Siempre deben ser accesibles y estar disponibles.

SEGURIDAD INFORMÁTICA: OBJETIVOS SECUNDARIOS

AUTENTICIDAD Y CONTROL DE ACCESO

NO REPUDIO O IRRENUNCIABILIDAD

FIABILIDAD

AUDITABILIDAD

SEGURIDAD INFORMÁTICA: OBJETIVOS SECUNDARIOS

AUTENTICIDAD Y CONTROL DE ACCESO

Comprueba la identidad del agente que accede a un recurso y le facilita o deniega el acceso en función de esta identidad

NO REPUDIO O IRRENUNCIABILIDAD

Garantiza la autoría de una información o un proceso

FIABILIDAD

Mantiene la consistencia entre el comportamiento del sistema y los resultados obtenidos del mismo. Es decir, evalúa si el sistema se comporta como se espera de él

AUDITABILIDAD

Registra el comportamiento del sistema para su evaluación posterior

Confidencialidad, Disponibilidad e Integridad

- **Confidencialidad**: la 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. Es decir, que si los contenidos cayesen en manos ajenas, estas no podrían acceder a la información o a su interpretación.

  Este es uno de los principales problemas a los que se enfrentan muchas empresas. En los últimos años se ha incrementado el robo de los portátiles y móviles, con la consecuente pérdida de información confidencial, de clientes, líneas de negocio…

  En relación a este objetivo, más adelante se analizará la Ley de Protección de Datos de Carácter Personal (**LOPD**).

Confidencialidad, Disponibilidad e Integridad

- **Disponibilidad**: la capacidad de garantizar que tanto el sistema como los datos van a estar disponibles al usuario en todo momento.

  Pensemos, por ejemplo, en la importancia que tiene este objetivo para una empresa encargada de impartir ciclos formativos a distancia. Constantemente está recibiendo consultas, descargas a su sitio Web, etc., por lo que siempre deberá estar disponible para los usuarios.

Confidencialidad, Disponibilidad e Integridad

- **Integridad**: la capacidad de garantizar que los datos no han sido modificados desde su creación sin autorización. La información que disponemos es válida y consistente.

  Este objetivo es muy importante cuando estamos realizando trámites bancarios por Internet. Se deberá garantizar que ningún intruso pueda capturar y modificar los datos en tránsito.

AUTENTIFICACIÓN Y NO REPUDIO

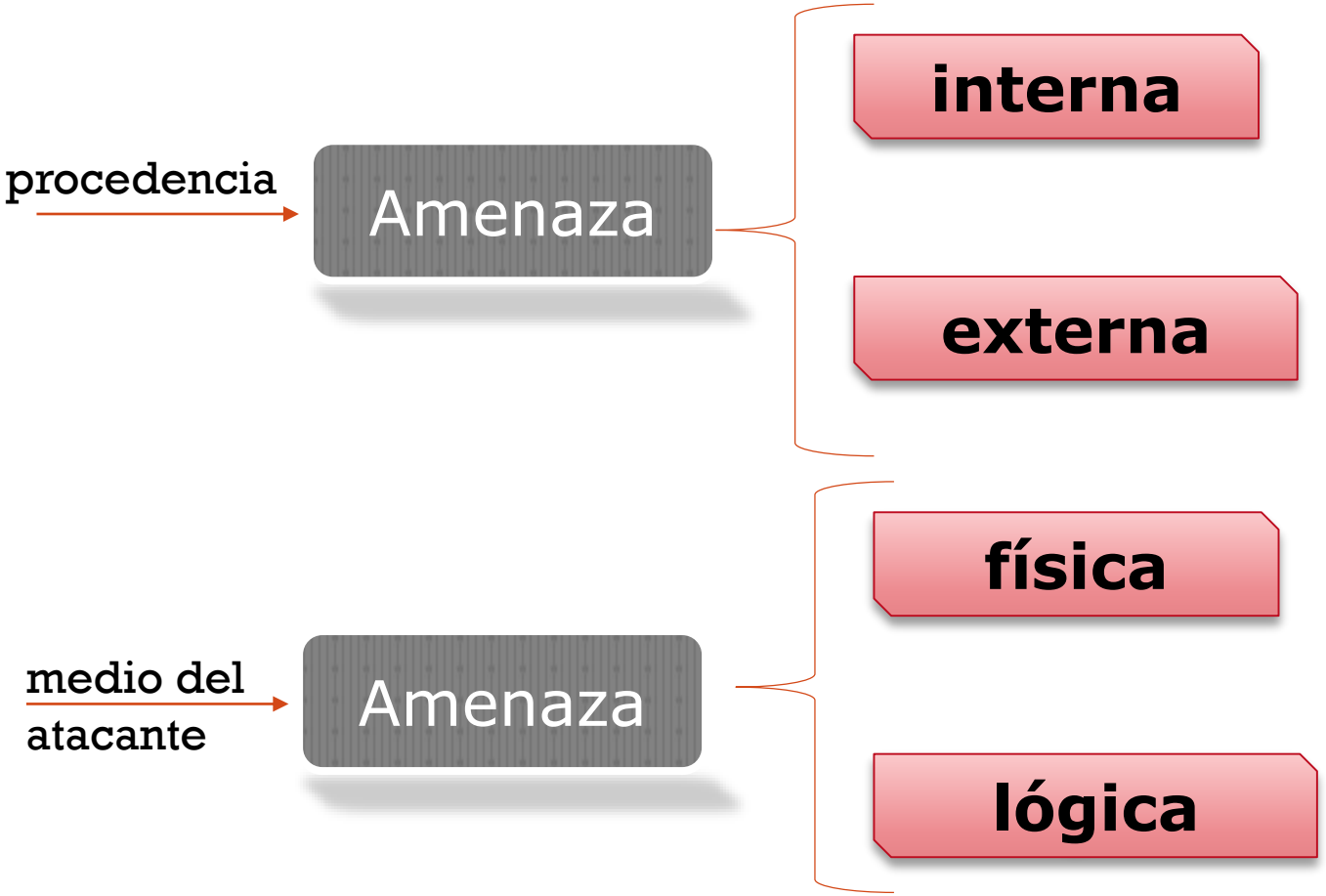
- **Autenticación:** Permite identificar al emisor de un mensaje, al creador de un documento o al equipo que se conecta a una red o a un servicio.
- **No repudio**: garantiza la participación de las partes en una comunicación. En toda comunicación, existe un emisor y un receptor, por lo que podemos distinguir dos tipos de no repudio:
  - **No repudio en origen**: garantiza que la persona o equipo que envía el mensaje no puede negar que es el emisor del mismo, ya que el receptor tendrá pruebas del envío.
  - **No repudio en destino**: el receptor no puede negar que recibió el mensaje, porque el emisor tiene pruebas de la recepción del mismo.

AMENAZAS, RIESGOS Y ATAQUES

Conviene precisar el significado de algunos conceptos relacionados con las AMENAZAS propios de la jerga profesional que se utilizarán frecuentemente

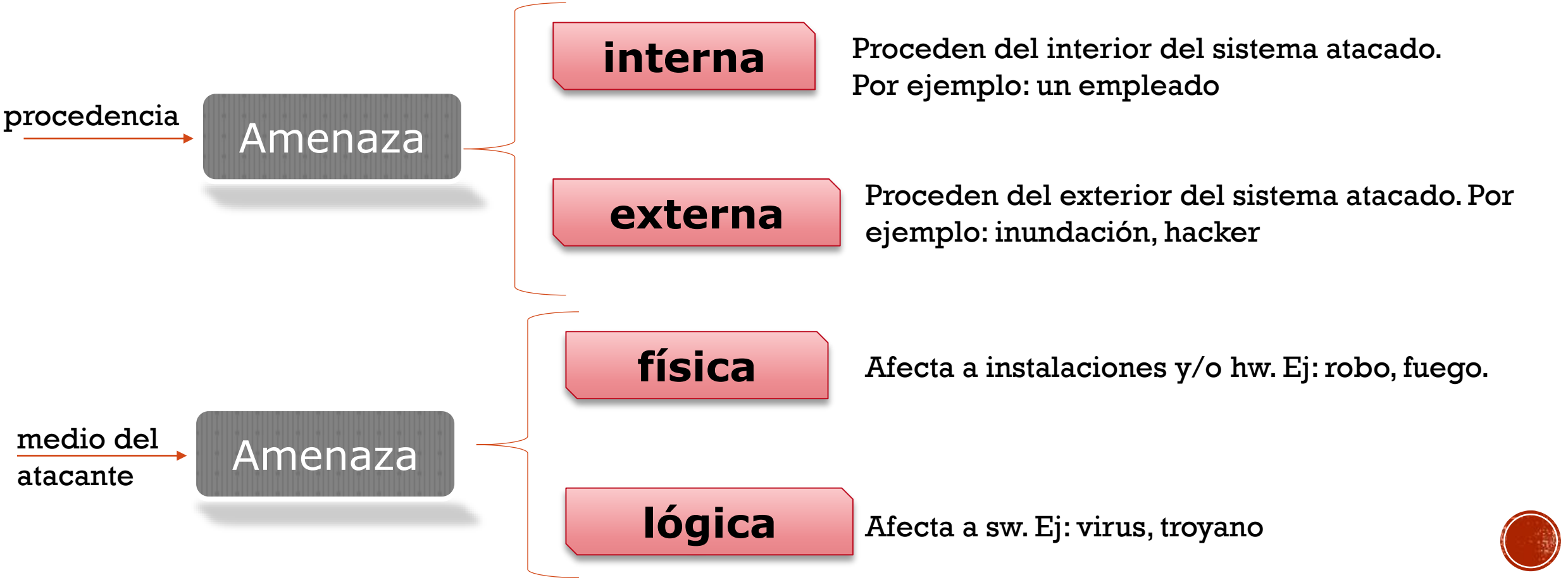
TIPOS DE AMENAZAS

- Conocer las amenazas es de vital importancia para poder combatirlas.
- Hay muchos tipos pero se pueden clasificar



TIPOS DE AMENAZAS

- Conocer las amenazas es de vital importancia para poder combatirlas.
- Hay muchos tipos pero se pueden clasificar



SEGURIDAD INFORMÁTICA: AMENAZAS

- **Activo:** todo aquello que es propiedad de la empresa: datos, software, hardware, redes, soportes, instalaciones, personal, servicios a clientes y usuarios.
- **Amenaza:** presencia de uno o más factores de diversa índole que, de tener la oportunidad, atacarían al sistema produciendo daños, aprovechando alguna vulnerabilidad.
- **Vulnerabilidad:** probabilidad existente de que una amenaza se materialice. Grado de exposición del sistema amenazado a las amenazas del atacante.
- **Contramedida:** es la acción que pretende la prevención de una amenaza que actúa aprovechándose de una vulnerabilidad. Por ejemplo, el administrador del sistema puede definir una política de actualización diaria del antivirus

SEGURIDAD INFORMÁTICA: AMENAZAS

- **Atacante:** es el agente activo que perpetra la amenaza que subyace a una vulnerabilidad.

- **Impacto (daño):** consecuencia de la materialización de una o más amenazas sobre uno o varios activos.

- **Riesgo:** Posibilidad de que se materialice o no una amenaza aprovechando una vulnerabilidad. Una amenaza no es riesgo cuando no hay vulnerabilidad, ni lo es una vulnerabilidad cuando no hay amenaza.

$$\text{Riesgo} = \frac{\text{Amenazas} * \text{Vulnerabilidades}}{\text{Contramedidas}}$$

GESTIÓN DEL RIESGO

Una vez evaluado el riesgo por conocimiento de las amenazas, vulnerabilidades y contramedidas…

¿Cómo podemos gestionar el riesgo?

GESTIÓN DEL RIESGO

Ante cualquier riesgo tenemos cuatro posibilidades:

- **Evitar el riesgo**: Es riesgo se evita cuando la organización rechaza aceptarlo. Es decir, no se acepta ningún tipo de exposición, lo que exige el compromiso de no realizar nunca la acción que origina el riesgo.
- **Reducir el riesgo**: Cuando el riesgo no puede evitarse, se puede reducir hasta que llegue a unos mínimos asumibles.
- **Retener, asumir o aceptar el riesgo**: Se acepta el riesgo y se asumen sus consecuencias en caso de que ocurra.
- **Transferir o compartir el riesgo**: Buscar un respaldo y compartir el riesgo con otros controles o entidades.

VULNERABILIDADES DEL SISTEMA

- Seguridad = Tecnología + organización

VULNERABILIDADES DEL SISTEMA

- Seguridad = Tecnología + organización

ELEMENTOS

- Routers
- Switch
- Fáx
- Cámaras
- Impresoras
- Etc

- S.O
- Servidores
- BBDD
- Aplicaciones
- Etc.

- Comunicación: transporte de datos
- Documentos

EJ

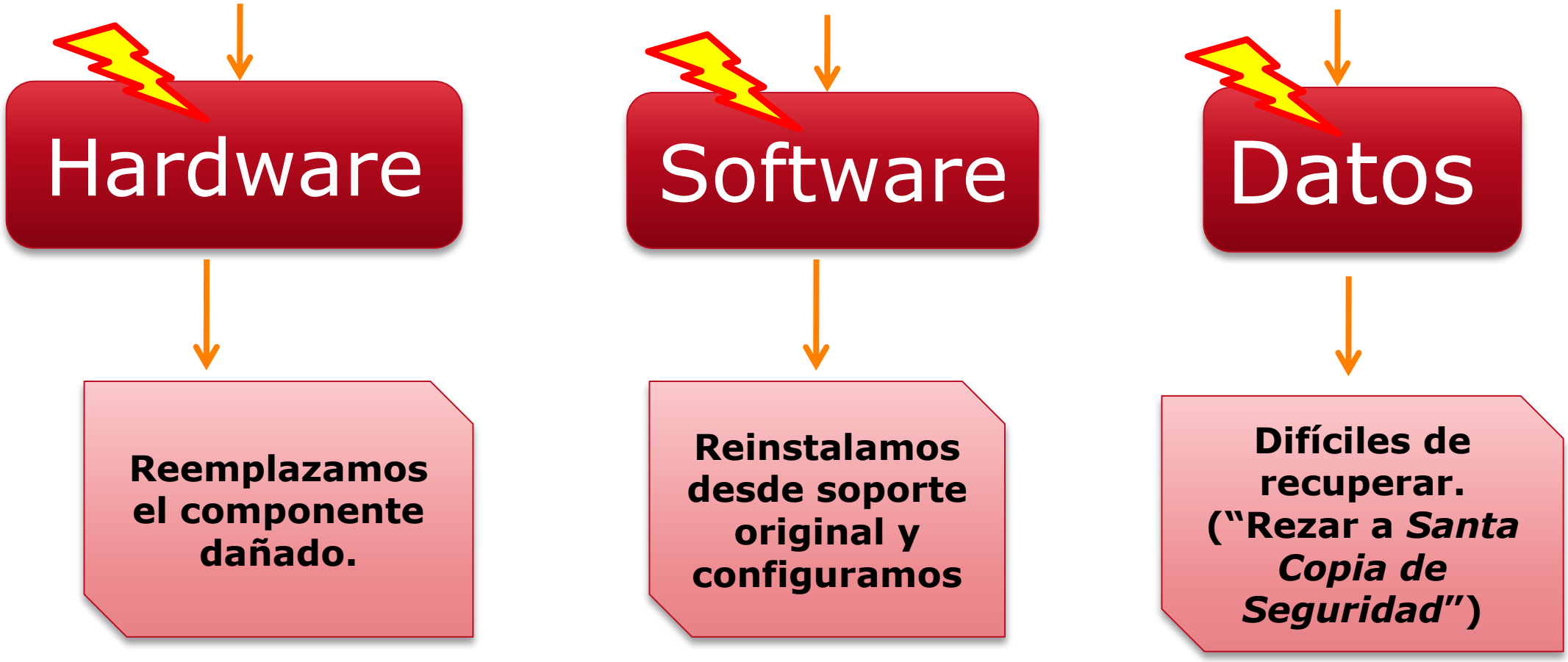
- Persona desconecte la alimentación del servidor

- Virus dañe el sector de arranque del disco de SO

- Persona escuche una conversación

VULNERABILIDADES DEL SISTEMA

- Seguridad = Tecnología + organización



AMENAZAS

- Las amenazas afectan principalmente al HW, SW y DATOS

Según el tipo de ataque:

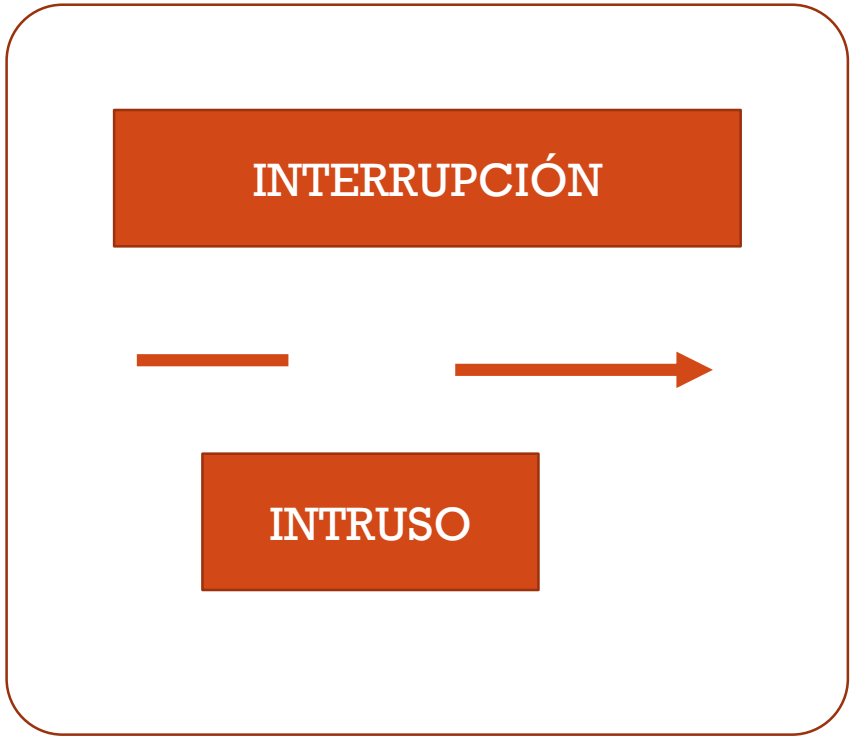
- Interrupción
- Modificación
- Intercepción
- Fabricación o Generación

Según la actuación del ataque

- Spoofing
- Sniffing
- Conexión no autorizada
- Malware
- Password cracking
- Denegación de servicio
- Ingeniería social (phishing)
- Scam
- Spam
- Pharming
- Botnet

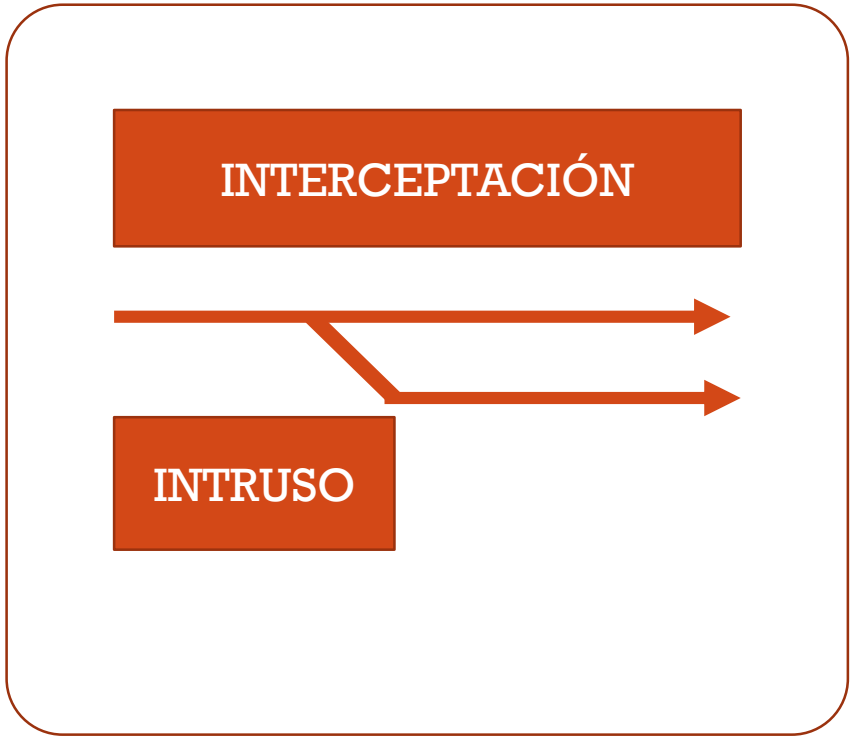
AMENAZAS DE INTERRUPCIÓN

- Se daña, pierde o deja de funcionar un punto del sistema
- Su detección es inmediata
- Ejemplos:
  - Destrucción del hw
  - Borrado de datos
  - Fallo en SO



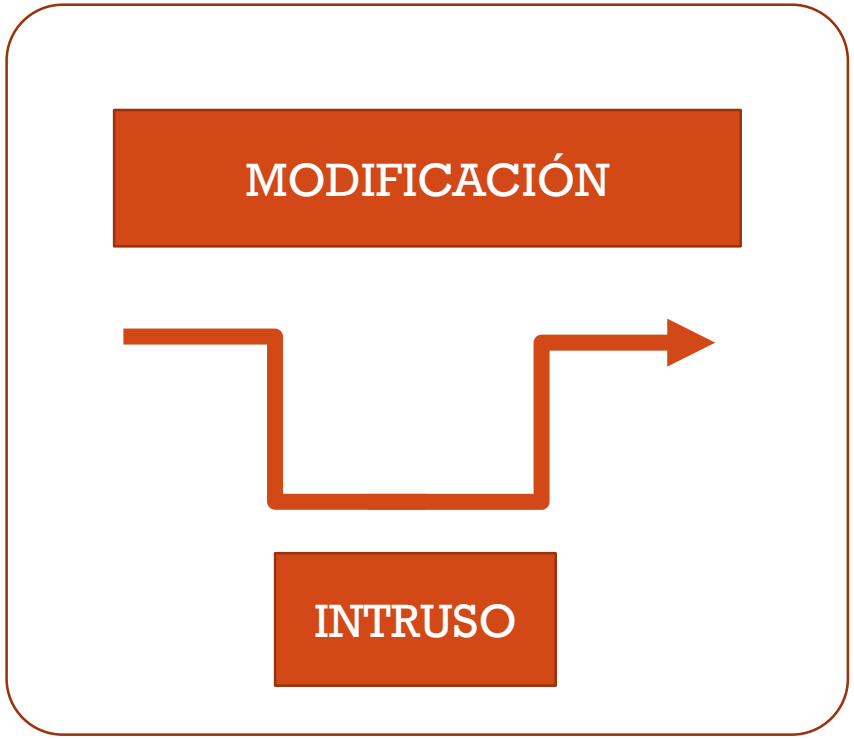
AMENAZAS DE INTERCEPTACIÓN

- Acceso a la información por personas no autorizadas,
- Uso de privilegios no adquiridos
- Detección difícil, a veces no deja huellas.
- Ejemplos:
  - Copias ilícitas de programas
  - Escucha en línea de datos



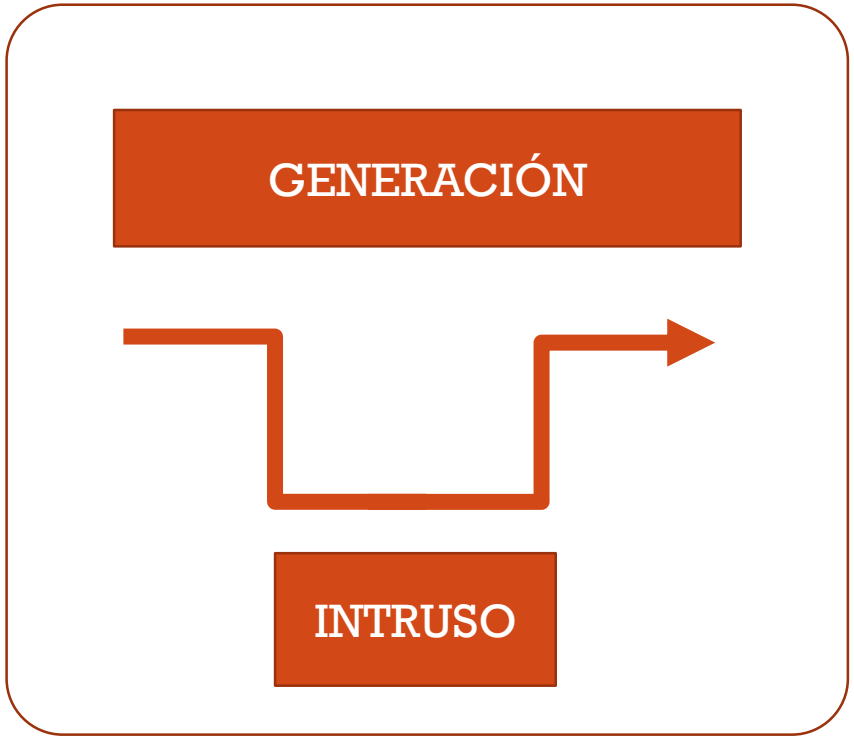
AMENAZAS DE MODIFICACIÓN

- Acceso no autorizado que cambia el entorno para su beneficio
- Detección difícil
- Ejemplos:
  - Modificación de B.D



AMENAZAS DE GENERACIÓN

- Creación de nuevos objetos dentro del sistema
- Detección difícil: delitos de falsificación
- Ejemplos:
  - Añadir transacciones en red
  - Añadir registros a una base de datos



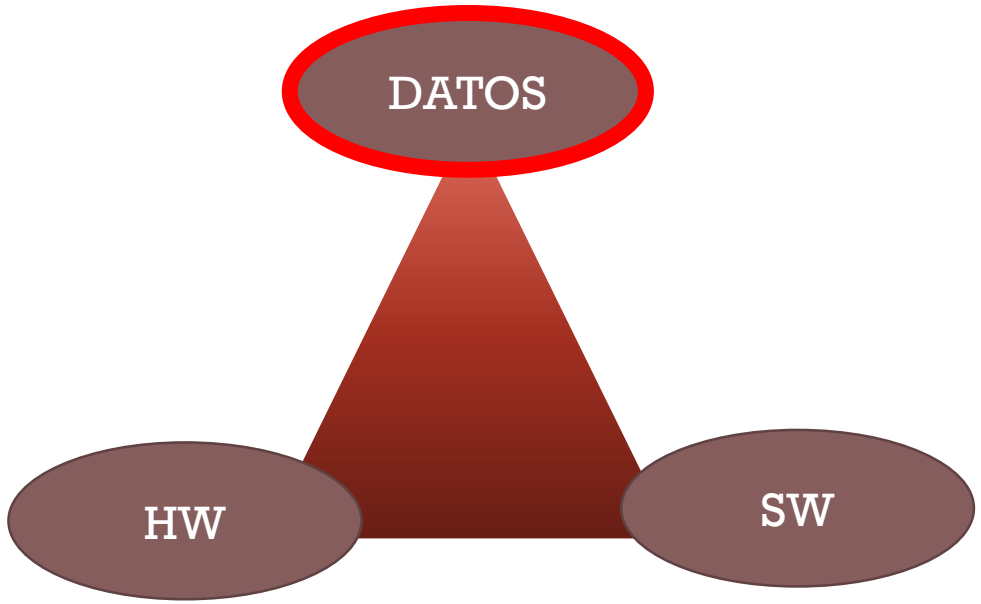
EL TRIÁNGULO DE LAS DEBILIDADES

Interrupción (pérdida)

Interceptación (acceso)

Modificación (cambio)

Generación (alteración)



Interrupción (denegar servicio)
Interceptación (robo)

Modificación (falsificación)
Interrupción (borrado)
Interceptación (copia)

PLANES DE SEGURIDAD

La mejor solución contra un ataque es **organizar una buena defensa**, sobre todo a través de la PREVENCIÓN

PLANES DE SEGURIDAD

- Mantener un sistema seguro pasa por cumplir unos requisitos que básicamente se agrupan entorno a las siguientes políticas recomendadas

1. Tener un **PLAN DE SEGURIDAD** de los sistemas de información, que debe haber sido probado antes de que se produzca un posible ataque
2. **RESPETAR** los **CÓDIGOS ÉTICOS** de comportamiento personal y profesional
3. Proveer **PLANES DE CONTINGENCIA** específicos para cada activo informático, validados mediante pruebas
4. Disponer de un sistema eficaz de **EVALUACIÓN** de la seguridad informática

PLANES DE SEGURIDAD

- Toda información de seguridad, las acciones preventivas y las reactivas después de sufrir un ataque se formulan en un plan de seguridad, también llamado a veces plan de contingencia o plan de respuesta a incidentes.

- Básicamente el plan de respuesta a incidentes (reactivo que no preventivo) tiene cuatro fases:
  1. Acción inmediata para detener o minimizar el incidente de seguridad
  2. Investigación del incidente
  3. Restauración de los recursos afectados, dañados o comprometidos debido al incidente
  4. Reporte del incidente y de los daños a los responsables de nivel superior

- Para poder desarrollar estas fases, el departamento de seguridad debe disponer de profesionales necesarios suficientemente formados, además debe seguir una estrategia legal revisada y aprobada.
  - Caso pymes externalizan a otra empresa o se encarga el administrador de sistemas

PLANES DE SEGURIDAD

Objetivos

- Identificar los activos (lo que se quiere proteger. Auditoría de seguridad: COBIT, ISO27001, ISO27002).
- Formar a los trabajadores en materia de seguridad.
- Concienciar de la importancia de la seguridad informática a los trabajadores
- Evaluar los riesgos: valorar el impacto sobre los daños producidos.
- Diseño del Plan de actuación:
  - Prevenir los daños minimizando la existencia de vulnerabilidades.
  - Minimizar el impacto de los daños ya producidos.
- Revisar periódicamente las medidas de seguridad adoptadas.

TECNOLOGÍAS DE SEGURIDAD DE SISTEMAS

- El material técnico con el que cuenta el administrador de la seguridad es muy variado y está en constante evolución puesto que a cada nueva vulnerabilidad se abre una línea de investigación para tratar de atajarla

- A continuación, se enumeran estas tecnologías:
  - Cortafuegos
  - Administración de las cuentas de los usuarios y servicios
  - Detección y prevención de intrusos
  - Antivirus y antimalware
  - Infraestructura de clave pública, técnicas de cifrado y firma digital
  - Técnicas de seguridad de comercio electrónico
  - Capa de socket segura (SSL)
  - IPSec
  - Single Sign On (SSO) o técnicas de conexión única
  - Biometría
  - Control de accesos remotos
  - Redes privadas virtuales
  - Informática forense
  - Recuperación de datos
  - Monitorización y auditoría del sistema

ESTÁNDARES

- Un estándar es un conjunto de reglas que deben cumplir todos los fabricantes y pueden ser creadas por hecho (se aceptan en el mercado por el uso generalizado) o por derecho (creados por una organización de estandarización)

- Las organizaciones de estándares pueden ser empresas privadas, departamentos de gobierno, grupos de investigación, etc.

ESTÁNDARES RELACIONADOS CON LA SEGURIDAD

- El estándar de seguridad de sistemas por antonomasia se recoge en la familia de normas ISO/IEC 27000
- Esta norma contiene las mejores prácticas recomendadas sobre la seguridad de la información para desarrollar, implementar y mantener especificaciones para los Sistemas de Gestión de la Seguridad de la Información (SGSI)

SGSI son las siglas utilizadas para referirse a un Sistema de Gestión de la Seguridad de la Información, una herramienta de gran utilidad y ayuda para la gestión de las organizaciones informáticas sobre el que se construye la nora ISO/IEC 27001 que es un elemento integrante de la familia ISO/IEC 27000

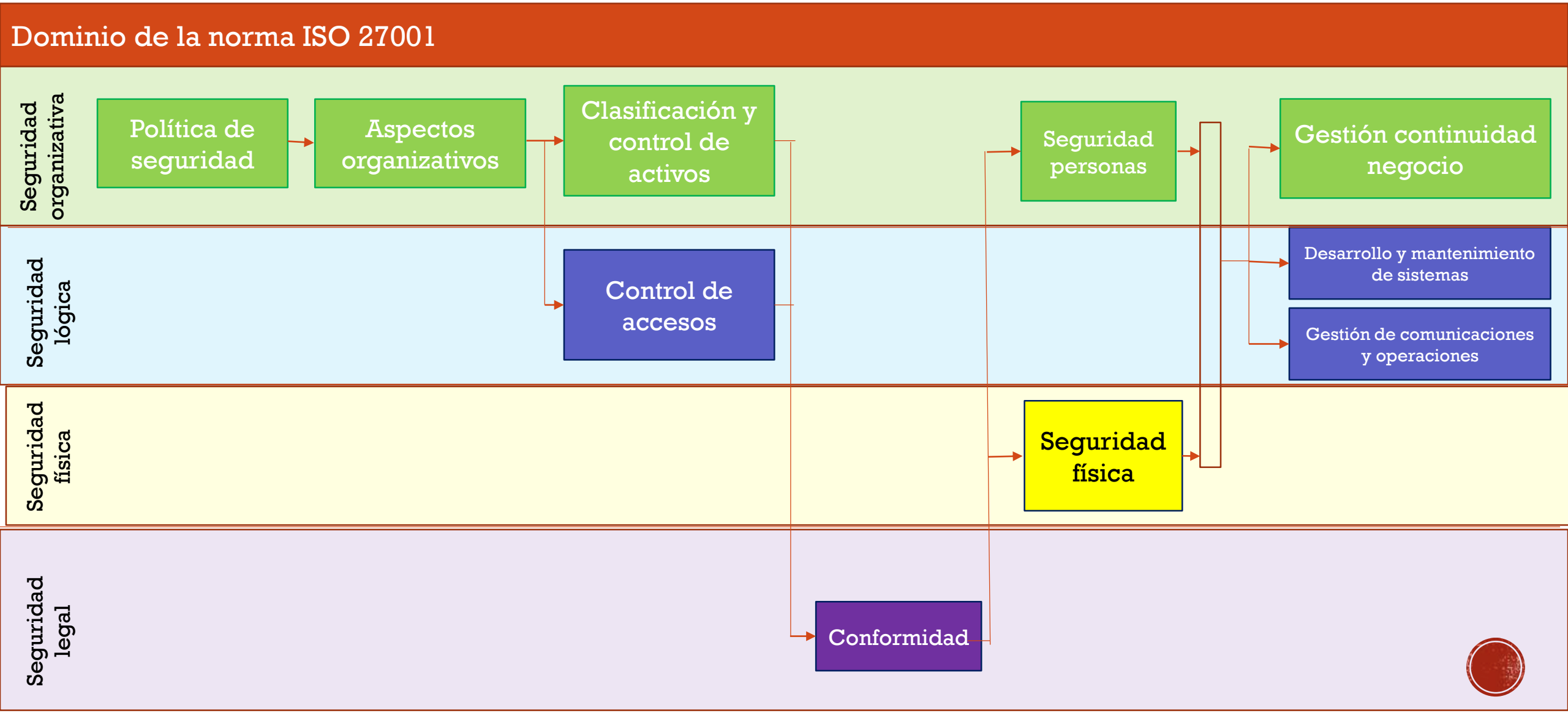
CONTENIDO NORMA ISO/IEC 27000

Norma ISO/IEC	Título
27000	Gestión de la Seguridad de la Información: fundamentos y vocabulario
27001	Especificaciones para un SGSI
27002	Código de buenas prácticas
27003	Guía de implantación de un SGSI
27004	Sistema de métricas e indicadores
27005	Guía de análisis y gestión de riesgos
27006	Especificaciones para organismos certificadores de SGSI
27007	Guía para auditar un SGSI
2701X	Guías sectoriales

EJEMPLO ESPECIFICACIÓN ISO/IEC 27001

- Contiene elementos de tipo estratégico, táctico y operacional para distintas áreas de seguridad:
  - Física
  - Lógica
  - Operacional
- Además añade que se ha de respetar la legalidad: fugas de información sensible, confidencialidad de datos, etc.

EJEMPLO DOMINIOS ISO/IEC 27001



EJEMPLO ESPECIFICACIÓN ISO/IEC 27002

- Se gestiona como un sistema de documentación jerárquico
- En vértice superior se establecen las **POLÍTICAS** que sientan las bases de la seguridad y en las que se redactan los objetivos generales sin un gran detalle técnico
  - Estas políticas deben ser conocidas por todo el personal de la organización
  - No se requieren de conocimientos técnicos
- Por debajo, se establecen los **PROCEDIMIENTOS** que desarrollan los detalles técnicos marcados por los objetivos contenidos en las políticas.
  - No es necesario que todas las personas conozcan los procedimientos, solo los que los tienen que desarrollar en su puesto
- A continuación, las **INSTRUCCIONES** que desarrollan cada uno de los procedimientos.
  - Órdenes o comandos necesarios para la ejecución de cada procedimientos
- En base se sitúan los **REGISTROS** que evidencian la efectiva implantación del SGSI
  - Evalúan un conjunto de indicadores o métricas de seguridad que activan alarmas frente a incidentes de seguridad

Jerarquía de documentación ISO 27002

EJEMPLO DOMINIOS ISO/IEC 27002

0-Introducción

5-Políticas de seguridad

4-Análisis y gestión de riesgos

6-Estructura organizativa

7-Control de activos

8-Seguridad personal

9-Seguridad física y del entorno

10-Seguridad lógica

12-Desarrollo y mantenimiento de sistemas

11-Control de accesos

13-Gestión de incidencias

14-Gestión de la continuidad del negocio

15-Cumplimiento

https://www.iso27000.es/assets/files/ControlesISO27002-2013.pdf

AUDITORÍA DE SEGURIDAD

- Es el estudio que comprende el análisis y gestión de sistemas para identificar y posteriormente corregir las diversas vulnerabilidades que pudieran presentarse en una revisión exhaustiva de las estaciones de trabajo, redes de comunicaciones o servidores.

- Los resultados se detallan, archivan y reportan a los responsables que deberán establecer medidas preventivas de refuerzo.

OBJETIVOS DE LA AUDITORÍA DE SEGURIDAD

- Revisar la seguridad de los entornos y sistemas.
- Verificar el cumplimiento de la normativa y la legislación vigente
- Elaborar un informe independiente.

TIPOS DE AUDITORÍA DE SEGURIDAD

- **Seguridad interna:** Redes locales y corporativas internas.
- **Seguridad perimetral**. Perímetro de la red local conectado a redes públicas.
- **Test de intrusión**: Intenta acceder a los sistemas para comprobar el nivel de resistencia a intrusos.
- **Análisis forense**: Posterior al incidente, intentando reconstruir como se ha penetrado en el sistema y valorar los daños ocasionados.
- **Código de aplicaciones:** Independiente del lenguaje empleado, en análisis de sitios web para detectar la inyección de código SQL.

SEGURIDAD INFORMÁTICA "A REMOLQUE"

El conjunto de amenazas, vulnerabilidades, ataques y medidas de seguridad aumentan y cambian con el tiempo a una velocidad vertiginosa.

Hay que estar al día

FUENTES

- Abad Domingo, Alfredo, “Seguridad y Alta Disponibilidad”, Ed. Garceta
- Aguilera, Purificación, “Seguridad Informática”, Ed. Editex.
- Costas Santos, Jesús, “Seguridad y Alta Disponibilidad”; Ed. Ra-ma
- Ramió Aguirre, Jorge, “Curso de Seguridad Informática y Criptografía”