

# Tema 1. Conceptos básicos sobre seguridad informática

Conceptos y elementos

Seguridad en Sistemas Informáticos  
Curso 2022/23

Septiembre 2022

# Contenido

Conceptos básicos

Elementos

# Conceptos básicos I

(Basado en las definiciones de la familia de normas ISO 27000 y de la metodología Magerit)

## Definición (seguridad en sistemas de información)

*Protección de los activos de un sistema de información con la intención de garantizar unos niveles adecuados de confidencialidad, integridad y disponibilidad sobre los mismos*

## Principios básicos de la seguridad

**Confidencialidad** los activos sólo han de poder ser accedidos por los elementos autorizados a ello

→ los elementos autorizados no van a poder hacer disponibles dichos activos a terceros no autorizados

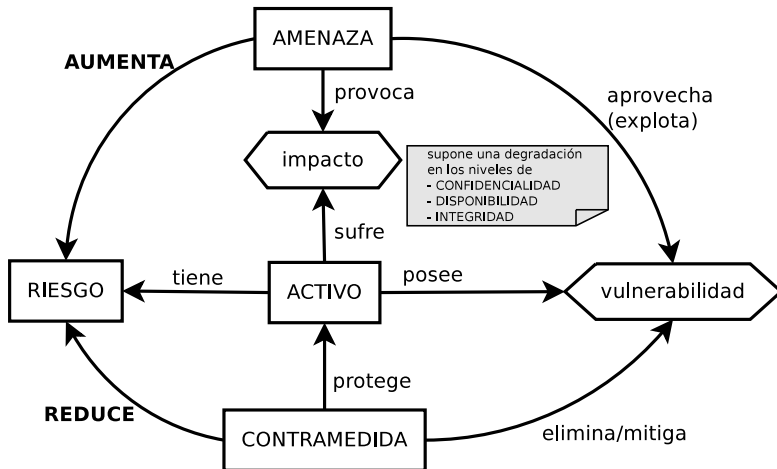
**Integridad** los activos sólo pueden ser modificados (creación, modificación, eliminación) por elementos autorizados de modo que se salvaguarde su exactitud y completitud

**Disponibilidad** los activos tienen que permanecer accesibles y utilizables por parte de los elementos autorizados cuando estos los requieran

# Conceptos básicos II

- ▶ Los mecanismos de seguridad se implementan para proteger uno o más de estos principios
- ▶ Riesgo, amenazas y vulnerabilidades se miden en función de su capacidad de comprometer alguno de estos principios
- ▶ Son principios **complementarios y contrapuestos**  $\Rightarrow$  deben balancearse

# Elementos I



# Elementos II

## Activos

Cualquier recurso (tangible o intangible) con valor para una organización

### Tipos de activos (según Libro II de la metodología MAGERIT ver. 3)

|                                 |                                                                                                                                                                                                                                       |
|---------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>activos esenciales</b>       | información (datos personales, datos clasificados, ...), servicios                                                                                                                                                                    |
| <b>arquitectura del sistema</b> | puntos de acceso al servicio, puntos de interconexión, ...                                                                                                                                                                            |
| <b>datos/información</b>        | ficheros, copias de seguridad, datos de configuración, credenciales, registros de control de acceso, registros de actividad, código fuente, ejecutables, datos de prueba, ...                                                         |
| <b>claves criptográficas</b>    | claves de cifrado, claves de firma, certificados, soportes físicos cifrados, ...                                                                                                                                                      |
| <b>servicios</b>                | internos, al público en general, a usuarios externos, web, correo electrónico, acceso remoto, directorio, transferencia de ficheros, almacenamiento, ...                                                                              |
| <b>software/aplicaciones</b>    | desarrollo propio, desarrollo a medida, software estándar (navegadores, servidor de aplicaciones, ofimática, sistema operativo, antivirus, sistema de backup, ...)                                                                    |
| <b>equipamiento informático</b> | grandes equipos, informática personal, informática móvil, equipo virtual, periféricos (impresoras, escaner, ...), dispositivos de red (modem, router, firewall, pasarela, punto de acceso inalámbrico...), centralita telefónica, ... |
| <b>redes de comunicaciones</b>  | red telefónica, enlace punto a punto, ADSL, red inalámbrica, red local, telefonía móvil, ...                                                                                                                                          |
| <b>soportes de información</b>  | electrónicos (discos, cintas, CD/DVD, almacenamiento en red, memorias USB, ...) y y no electrónicos (papel impreso, microfilm, ...)                                                                                                   |
| <b>equipamiento auxiliar</b>    | cableado, SAI, climatización, mobiliario, robots de cintas, generadores, ...                                                                                                                                                          |
| <b>instalaciones</b>            | recinto, edificio, sala, canalización, vehículo, instalaciones de respaldo, ...                                                                                                                                                       |
| <b>personal</b>                 | usuarios internos, usuarios externos, operadores, administradores (de red, de sistemas, de BD, de seguridad, ...), desarrolladores, proveedores, subcontratas, ...                                                                    |

También se consideran activos aspectos intangibles como "reputación", "confianza", "imagen de marca", etc

# Elementos III

## Amenazas (1)

Cualquier peligro potencial sobre un activo de la organización

- ▶ Algo o alguien que puede aprovechar una **vulnerabilidad** (explotarla) para causar un **impacto** sobre la confidencialidad, integridad o disponibilidad de un **activo**
- ▶ Pueden ser accidentales o intencionadas

### Tipos de amenazas (según Libro II de la metodología MAGERIT ver. 3)

|                                          |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
|------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>desastres naturales</b>               | fuego, daños por agua, terremotos, derrumbes, caídas, ...                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
| <b>de origen industrial</b>              | fuego, daños por agua, contaminación mecánica, contaminación electromagnética, avería física o lógica, corte de suministro eléctrico, temperatura/humedad inadecuada, fallo de comunicaciones, interrupción de servicios y suministros esenciales, degradación de soportes almacenamiento, ...                                                                                                                                                                                                                                           |
| <b>errores y fallos no intencionados</b> | errores de usuarios, errores de administrador, errores de monitorización, errores de configuración, deficiencias en la organización, difusión de software dañino, escapes de información, alteración accidental de la información, destrucción de la información, fugas de información, vulnerabilidades del software, errores de mantenimiento/actualización del software, errores de mantenimiento o actualización del hardware, caída del sistema por agotamiento de recursos, pérdida de equipos, indisponibilidad del personal, ... |
| <b>ataques intencionados</b>             | manipulación registros de actividad, manipulación de la configuración, suplantación de usuario, abuso de privilegios de acceso, uso no previsto, difusión de software dañino, repudio, acceso no autorizado, análisis de tráfico, interceptación/escucha de información, modificación o destrucción de información, divulgación de información, manipulación de programas, robo manipulación de equipos, denegación de servicio, ataque destructivo, ocupación enemiga, indisponibilidad del personal, extorsión, ingeniería social, ... |

# Elementos IV

## Amenazas (2)

### **Tipos genéricos de amenazas** (por su efecto sobre los activos)

**de interrupción** hacen que un activo del sistema se pierda o quede inutilizado

- ▶ atenta contra la disponibilidad

**de interceptación** un elemento no autorizado tiene acceso a un activo del sistema

- ▶ atenta contra la confidencialidad

**de modificación** además de acceder, el elemento no autorizado consigue modificar el activo

- ▶ atenta contra la integridad (y disponibilidad en caso de destrucción)

**de fabricación** un elemento no autorizado consigue "construir" una réplica de un activo legítimo

# Elementos V

## Vulnerabilidades

Debilidades que pueden proporcionar a una **amenaza** la posibilidad de comprometer y/o causar daño a un **activo**

- ▶ defectos de diseño o construcción
- ▶ deficiencias de configuración
- ▶ deficiencias en su instalación o uso, etc
- ▶ ausencia de **controles de seguridad**

## Riesgo

Cuantificación de la posibilidad de que una amenaza aproveche una vulnerabilidad causando un impacto en la confidencialidad, integridad o disponibilidad de un activo

- ▶ Suele tener asociada una valoración del coste que supone
- ▶ Cuantifica:  $\left\{ \begin{array}{l} \text{probabilidad de ocurrencia de la vulnerabilidad} \\ + \\ \text{coste del daño potencial sobre el activo} \end{array} \right.$

# Elementos VI

## Mecanismos/controles de seguridad (1)

Elementos físicos, técnicos o organizativos que permiten mitigar un riesgo potencial

- ▶ También: **contramedidas**, salvaguardas, ...
- ▶ **Reducen el riesgo** sobre uno o varios activos
  - ▶ **eliminando la vulnerabilidad** de lo causa
  - ▶ **reduciendo la posibilidad** de que la vulnerabilidad sea explotada

(también es posible **transferir** el riesgo a un tercero [contratando un seguro])

## Clasificación genérica

- ▶ controles **administrativos**: procedimientos, políticas, normas, etc
- ▶ controles **técnicos** (lógicos): cortafuegos, cifrado, antimalware, etc
- ▶ controles **físicos**: sistemas antiincendios, vigilancia, cerraduras, biometría, etc

# Elementos VII

## Mecanismos/controles de seguridad (2)

### Tipos de controles por su funcionalidad

- ▶ **preventivos:** pretenden **evitar** que un incidente de seguridad llegue a ocurrir
- ▶ **de detección:** permiten **identificar** las actividades propias de un incidente de seguridad que está siendo desencadenado por parte de un atacante/amenaza
- ▶ **de recuperación:** buscan **devolver el sistema** a un **estado** que permita su operación **normal**
- ▶ **correctivos:** **corrigen** los componentes, sistemas o controles que no han cumplido su labor (una vez que un incidente ya ha sucedido) para evitar futuros incidentes similares
- ▶ **disuasorios:** buscan **disuadir** a los posibles atacantes/amenazas

# Elementos VIII

## Ejemplos de tipos de controles

| <b>Seguridad física</b><br>(controles de seg. físicos)                                                                                                                                                                                                                                                                                                                                                                                                                       | <b>Seguridad lógica</b><br>(controles de seg. técnicos)                                                                                                                                                                                                                                                                                                                                                  | <b>Seguridad organizativa y legal</b><br>(controles organizativos y legales)                                                                                                                                                                                                                                                                     |
|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Preventivos</b><br>cerraduras<br>tarjetas de acceso<br>control biométrico<br>guardias de seguridad<br>bloqueo de ventanas<br>hacia el exterior<br>normativas de acceso<br>a activos físicos<br>formación de usuarios<br><b>De detección</b><br>detectores de movimiento<br>cámaras de circuito cerrado<br>detectores de humo<br><b>Disuasorios</b><br>vallas de seguridad<br><b>De recuperación</b><br>réplica de activos en<br>otra localización<br>extinción automática | <b>Preventivos</b><br>config. routers (reglas de filtrado)<br>firewalls<br>cifrado de la inform. en tránsito<br>cifrado de la inform. almacenada<br>software antivirus/antimalware<br><b>De detección</b><br>sistemas detección intrusiones<br>análisis de logs<br><b>De recuperación</b><br>sistemas y políticas de back-up<br><b>Correctivos</b><br>réplicas (imágenes) de<br>máquinas preconfiguradas | <b>Preventivos</b><br>políticas y procedimientos<br>procedimientos de<br>contratación de personal<br>clasificación y etiquetado<br>de recursos<br>cumplimiento de leyes/normas<br><b>De detección</b><br>rotación en puestos<br>investigación de actividades<br><b>Disuasorios</b><br>sanciones y penalizaciones<br>acuerdos de confidencialidad |

# Controles del Libro II de Magerit versión 3

|                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <p><b>Protecciones generales u horizontales</b></p> <p>Identificación y autenticación<br/>Control de acceso lógico<br/>Segregación de tareas<br/>Gestión de incidencias<br/>Herramientas de seguridad<br/>Herramienta contra código dañino<br/>IDS/IPS: Herramienta de detección y prevención de intrusión<br/>Herramienta de chequeo de configuración<br/>Herramienta de análisis de vulnerabilidades<br/>Herramienta de monitorización de tráfico<br/>Herramienta de monitorización de contenidos<br/>Herramienta para análisis de logs<br/>Honey net / honey pot<br/>Verificación de las funciones de seguridad<br/>Gestión de vulnerabilidades<br/>Registro y auditoría</p> <p><b>Protección de las aplicaciones (software)</b></p> <p>Copias de seguridad (backup)<br/>Puesta en producción<br/>Se aplican perfiles de seguridad<br/>Explotación / Producción<br/>Cambios (actualizaciones y mantenimiento)<br/>Terminación</p> <p><b>Protección de los equipos (hardware)</b></p> <p>Protección de los Equipos Informáticos<br/>Puesta en producción<br/>Se aplican perfiles de seguridad<br/>Aseguramiento de la disponibilidad<br/>Operación<br/>Cambios (actualizaciones y mantenimiento)<br/>Terminación<br/>Informática móvil<br/>Reproducción de documentos<br/>Protección de la centralita telefónica (PABX)</p> <p><b>Seguridad física - Protección de las instalaciones</b></p> <p>Protección de las Instalaciones<br/>Diseño<br/>Defensa en profundidad<br/>Control de los accesos físicos<br/>Aseguramiento de la disponibilidad<br/>Terminación</p> | <p><b>Protección de los datos / información</b></p> <p>Copias de seguridad de los datos (backup)<br/>Aseguramiento de la integridad<br/>Cifrado de la información<br/>Uso de firmas electrónicas<br/>Uso de servicios de fechado electrónico (time stamping)</p> <p><b>Protección de las claves criptográficas</b></p> <p>Gestión de claves criptográficas<br/>Gestión de claves de cifra de información<br/>Gestión de claves de firma de información<br/>Gestión de claves para contenedores criptográficos<br/>Gestión de claves de comunicaciones<br/>Gestión de certificados</p> <p><b>Protección de las comunicaciones</b></p> <p>Entrada en servicio<br/>Se aplican perfiles de seguridad<br/>Aseguramiento de la disponibilidad<br/>Autenticación del canal<br/>Protección de la integridad de los datos intercambiados<br/>Protección criptográfica de la confidencialidad de los datos intercambiados<br/>Operación<br/>Cambios (actualizaciones y mantenimiento)<br/>Terminación<br/>Seguridad Wireless (WiFi)<br/>Telefonía móvil<br/>Segregación de las redes en dominios</p> <p><b>Continuidad de operaciones</b></p> <p>Prevención y reacción frente a desastres.<br/>Continuidad del negocio<br/>Análisis de impacto (BIA)<br/>Recuperación de Desastres (DRP)</p> <p><b>Adquisición y desarrollo</b></p> <p>Adquisición / desarrollo<br/>Servicios: Adquisición o desarrollo<br/>Aplicaciones: Adquisición o desarrollo<br/>Equipos: Adquisición o desarrollo<br/>Comunicaciones: Adquisición o contratación<br/>Soportes de Información: Adquisición<br/>Productos certificados o acreditados</p> <p><b>Salvaguardas de tipo organizativo</b></p> <p>Organización<br/>Gestión de riesgos<br/>Planificación de la seguridad<br/>Inspecciones de seguridad</p> | <p><b>Protección de los servicios</b></p> <p>Aseguramiento de la disponibilidad<br/>Aceptación y puesta en operación<br/>Se aplican perfiles de seguridad<br/>Explotación<br/>Gestión de cambios (mejoras y sustituciones)<br/>Terminación<br/>Protección de servicios y aplicaciones web<br/>Protección del correo electrónico<br/>Protección del directorio<br/>Protección del servidor de nombres de dominio (DNS)<br/>Voz sobre IP</p> <p><b>Protección en los puntos de interconexión con otros sistemas</b></p> <p>Puntos de interconexión: conexiones entre zonas de confianza<br/>Sistema de protección perimetral<br/>Protección de los equipos de frontera</p> <p><b>Protección de los soportes de información</b></p> <p>Protección de los Soportes de Información<br/>Aseguramiento de la disponibilidad<br/>Protección criptográfica del contenido<br/>Limpieza de contenidos<br/>Destrucción de soportes</p> <p><b>Protección de los elementos auxiliares</b></p> <p>Aseguramiento de la disponibilidad<br/>Instalación<br/>Suministro eléctrico<br/>Climatización<br/>Protección del cableado</p> <p><b>Externalización</b></p> <p>SLA: nivel de servicio, si la disponibilidad es un valor<br/>NDA: compromiso de secreto, si la confidencialidad es un valor<br/>Identificación y calificación del personal encargado<br/>Procedimientos de escalado y resolución de incidencias<br/>Procedimiento de terminación (duración en el tiempo de las responsabilidades asumidas)<br/>Asunción de responsabilidades y penalizaciones por incumplimiento<br/>Acuerdos para intercambio de información y software<br/>Acceso externo<br/>Servicios proporcionados por otras organizaciones<br/>Personal subcontratado</p> <p><b>Salvaguardas relativas al personal</b></p> <p>Gestión del Personal<br/>Formación y concienciación<br/>Aseguramiento de la disponibilidad</p> |
|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

# Ejemplo

|                        |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
|------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Activo:</b>         | PCs de una organización                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
| <b>Amenaza:</b>        | Nuevo virus/malware (no reconocido por el software antivirus)                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
| <b>Vulnerabilidad:</b> | Firmas de virus no actualizadas en el antivirus corporativo                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
| <b>Riego:</b>          | <p>Posibilidad de que esos virus no reconocidos infecten los equipos y causen daños/pérdidas</p> <p>Supondrá cuantificar:</p> <ul style="list-style-type: none"><li>- <b>probabilidad</b> de que suceda la infección</li><li>- <b>coste</b> que supondría la infección, incluyendo<ul style="list-style-type: none"><li>* coste por posible pérdida/robo de datos</li><li>* coste de las molestias y pérdida de tiempo productivo de los usuarios</li><li>* coste de la eliminación del virus o la reinstalación de equipos</li><li>* otros costes</li></ul></li></ul> |
| <b>Contramedidas:</b>  | <p>técnicas:        - programar actualización del antivirus<br/>                              (adquiriéndolas si es preciso o cambiando de antivirus)</p> <p>organizativas:    - definir criterios para selección y compra de antivirus</p> <p>                              - definir procedimientos de instalación y<br/>                                          actualización de antivirus</p> <p>                              - establecer políticas de concienciación de usuarios</p>                                                                          |