SEGURIDAD INFORMÁTICA

JOSÉ PABLO HERNÁNDEZ

SEGURIDAD INFORMÁTICA

1.3.1. Capítulo 3
Parte 2 de 2
Gestión de riesgos

JOSÉ PABLO HERNÁNDEZ

3. METODOLOGÍAS ANÁLISIS DE RIESGOS

Lo que no se puede medir no se puede gestionar.

Buscar activos que resulten vulnerables a unas amenazas.

Metodología Magerit.

3.1. MAGERIT

Consejo Superior de Administración Electrónica dependiente del Ministerio de Administraciones Públicas publica una Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información (MAGERIT):

1997 Primera versión, 2006 segunda versión y 2012 tercera versión.

Se organiza en tres volúmenes:

MAGERIT v3, I – Método

MAGERIT v3, II – Catálogo de Elementos

MAGERIT v3, III – Guía de Técnicas

https://administracionelectronica.gob.es/pae_Home/pae_Documentacion/pae_Metodolog/pae_Magerit.html

3.1. MAGERIT

Exhaustivo pero:

- **Si el sistema es simple o reducido, o solo se requiere una primera aproximación, puede bastar un planteamiento informal.**
- **Que solo se requiera el estudio de los ficheros afectados por la legislación LOPD.**
- **Que solo se requiera el estudio de las garantías de confidencialidad.**
- **Que solo se requiera el estudio de la disponibilidad de los servicios, por ejemplo, para desarrollar un plan de contingencia.**

3.1. MAGERIT

FASE 1. Análisis de riesgos

Se trata de ejecutar 5 pasos sencillos, para obtener una lista de los riesgos que soporta el sistema de información:

Paso 1: determinar los activos y su valoración de C, I y A

Paso 2: determinar las amenazas, cuánto degradan la C, I y A de un activo, y con qué frecuencia o probabilidad aparecen.

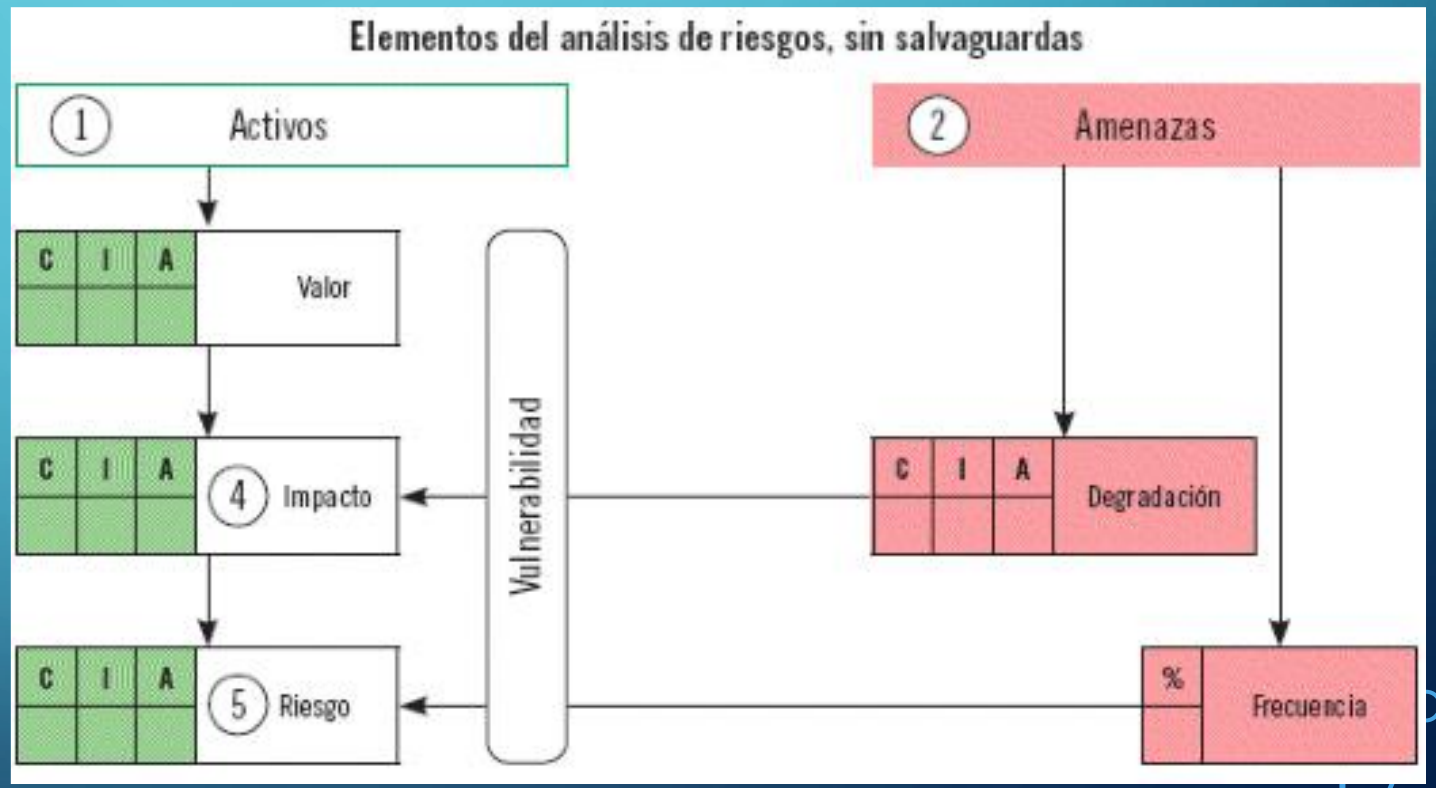
Paso 3: determinar las salvaguardas existentes y su eficacia (cuánto evitan la degradación C, I, y A de un activo, y cuánto reducen la frecuencia de la amenaza).

Paso 4: determinar el impacto, o medida del daño posible al activo por la materialización de una amenaza.

Paso 5: determinar el riesgo, o medida del daño probable al activo (impacto ponderado por la tasa de ocurrencia de la amenaza).

Actividades

REPRESENTAR EN UN DIAGRAMA LOS PASOS A REALIZAR EN LA FASE 1 DE APLICACIÓN DE LA METODOLOGÍA MAGERIT. SEÑALAR QUÉ INFORMACIÓN SE OBTIENE COMO RESULTADO DE CADA FASE.



3.1. MAGERIT. FASE 1. PASO 1: ACTIVOS

Para MAGERIT, por definición, los activos son los recursos del sistema de información o relacionados con este, necesarios para que la organización funcione correctamente, y alcance los objetivos propuestos por su Dirección.

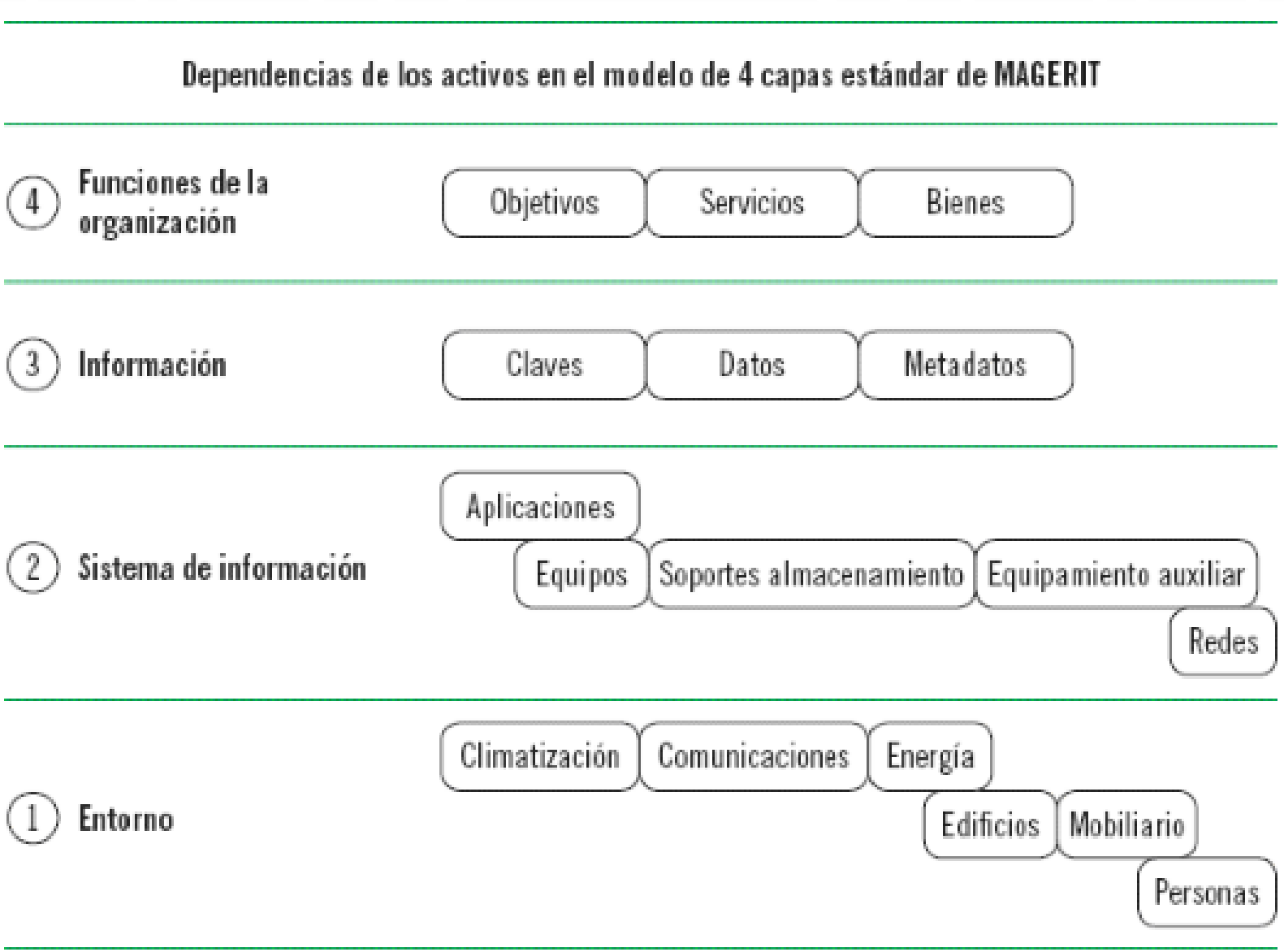
3.1. MAGERIT. FASE 1. PASO 1: ACTIVOS

El activo esencial es **la información, o datos (D),** y alrededor se encuentran:

- **Los servicios (S),** que se prestan gracias a los datos, y que se necesitan para los mismos.
- **Las aplicaciones (SW),** que manejan dichos datos.
- **Los equipos informáticos (HW),** que ejecutan las aplicaciones, y entregan los servicios y los datos.
- **Los soportes de almacenamiento (SI),** que almacenan los datos.
- **El equipamiento auxiliar (AUX),** que complementa a los equipos.
- **Las redes de comunicaciones (COM),** que intercambian los datos.
- **Las instalaciones (L),** donde residen los equipos y las redes.
- **Las personas (P),** que explotan u operan los elementos anteriores.

Para cada activo, se tendrán unas amenazas y unas salvaguardas.

3.1. MAGERIT. FASE 1. PASO 1: ACTIVOS

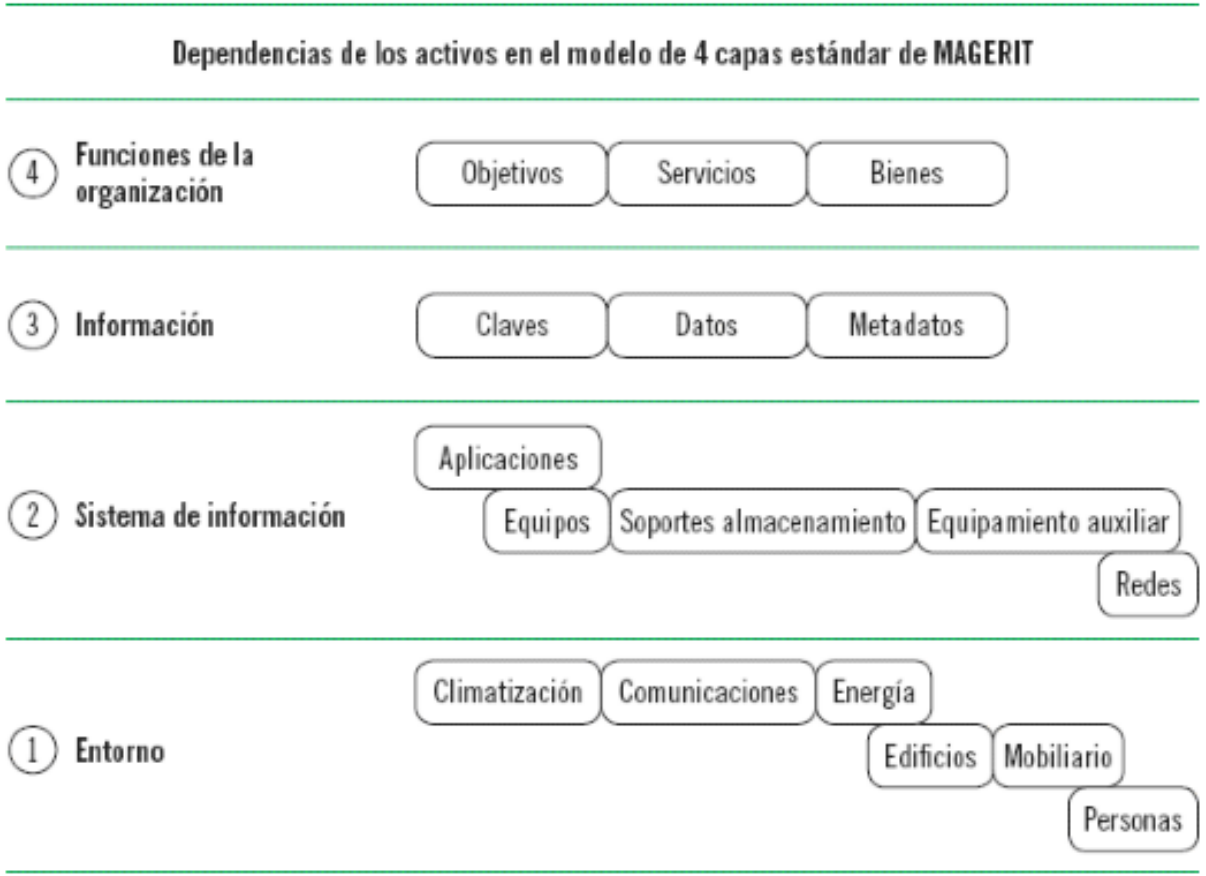


3.1. MAGERIT. FASE 1. PASO 1: ACTIVOS

Para la seguridad de la información, la valoración de los activos no se corresponde a lo que cuesta.

El valor de un activo puede ser propio o acumulado.

El valor acumulado es el que van heredando los activos inferiores de los superiores.



3.1. MAGERIT. FASE 1. PASO 1: ACTIVOS

Dimensiones MAGERIT de valoración de activos (pueden usarse todas o sólo algunas):

- **Confidencialidad.**
- **Integridad.**
- **Disponibilidad.**

- **La autenticidad**, midiendo el perjuicio que causaría no saber exactamente quién ha hecho cada cosa, es decir, ¿quién hace qué?, distinguiendo:
  - **En el uso de un servicio**, o autenticidad del usuario.
  - **En el acceso a los datos**, o autenticidad de quién accede para consultar los datos o para modificarlos.

- **La trazabilidad**, es decir, ¿quién hace qué, y cuándo? en dos aspectos:
  - **En el uso de un servicio**, midiendo el perjuicio que causaría no saber exactamente quién ha usado un servicio.
  - **En el acceso a datos**, midiendo el perjuicio que causaría no saber exactamente quién ha accedido a unos datos, y qué ha hecho con ellos.

3.1. MAGERIT. FASE 1. PASO 1: ACTIVOS

En MAGERIT, se propone determinar el **valor de un activo** como el coste que supondría salir de una incidencia que destrozara el activo. Por ejemplo:

- Coste de reposición (adquisición e instalación).
- Coste de mano de obra invertida en recuperar el activo.
- Lucro cesante o pérdida de ingresos.
- Capacidad de operar (confianza usuarios y proveedores).
- Sanciones por incumplimiento de ley u obligaciones contractuales.
- Daño a otros activos propios o ajenos.
- Daño a personas.
- Daños medioambientales.

3.1. MAGERIT. FASE 1. PASO 1: ACTIVOS

Descripción homogénea de los criterios de valoración de los diferentes activos.

Técnicas a emplear similares a las BIA:

- Formularios.
- Entrevistas.
- Reuniones.

3.1. MAGERIT. FASE 1. PASO 2: AMENAZAS

Consiste en reflexionar sobre qué cosas pueden ocurrirle al activo que puedan causarle daño.

Existen catálogos de amenazas publicadas:

- El método MAGERIT incluye un catálogo de amenazas.
- La norma ISO 13335-4: 2000 incluye un catálogo de amenazas y de salvaguardas para ellas.
- El ISF (Information Security Forum), en su publicación anual “The 2013 Standard of Good Practice for Information Security”, también incluye una amplia lista de amenazas.
- La “Federal Office for Information Security (BSI)” alemana, entrega un catálogo de amenazas elementales, para aplicar su metodología IT-Grundschutz, (BSI-Standard 100-2)”.

3.1. MAGERIT. FASE 1. PASO 2: AMENAZAS

De las amenazas, se deberá calcular:

- La **degradación** que producen.
- La **frecuencia** con que aparecen.

Estos datos son imposibles de calcular, o hacerlo con precisión supondría un esfuerzo desproporcionado a la finalidad del AGR.

La solución es emplear aproximaciones proporcionales al objetivo del análisis de riesgos, que, normalmente, se concretan en usar valoraciones cualitativas.

3.1. MAGERIT. FASE 1. PASO 2: AMENAZAS

Degradación.

Mide el daño causado por un incidente si ocurriera.

- Para cada activo.
- Para cada dimensión.

3.1. MAGERIT. FASE 1. PASO 2: AMENAZAS

Degradación. Ejemplos.

Para un activo como un ordenador, y una amenaza de incendio, la degradación en la confidencialidad e integridad será nula, pero máxima en la disponibilidad.

Para un activo como una aplicación, y una amenaza de un programa malintencionado, la degradación en confidencialidad e integridad puede ser mediana o baja, y puede ser alta en la disponibilidad.

Para un activo como una base de datos, y una amenaza de error de usuario, la degradación en confidencialidad puede ser nula, alta en integridad, y mediana en disponibilidad.

3.1. MAGERIT. FASE 1. PASO 2: AMENAZAS

Degradación.

Simplificación de la valoración.

Notas:

- Las amenazas intencionadas producirán normalmente una degradación muy alta, porque están dirigidas, y hay una intención concreta de causar ese daño.
- Cuando no son intencionales, por ejemplo, en errores y fallos humanos, la degradación no tiene por qué ser total.
- En general, los desastres, naturales o industriales, producirán una degradación total.

Valoración cualitativa *"la dimensión se ve..."*	**Degradación**	**Dato para MAGERIT**
Totalmente degradada	Completa	100 %
Algo afectada	Parcial	10 %
Prácticamente nada afectada	Inexistente	1 %

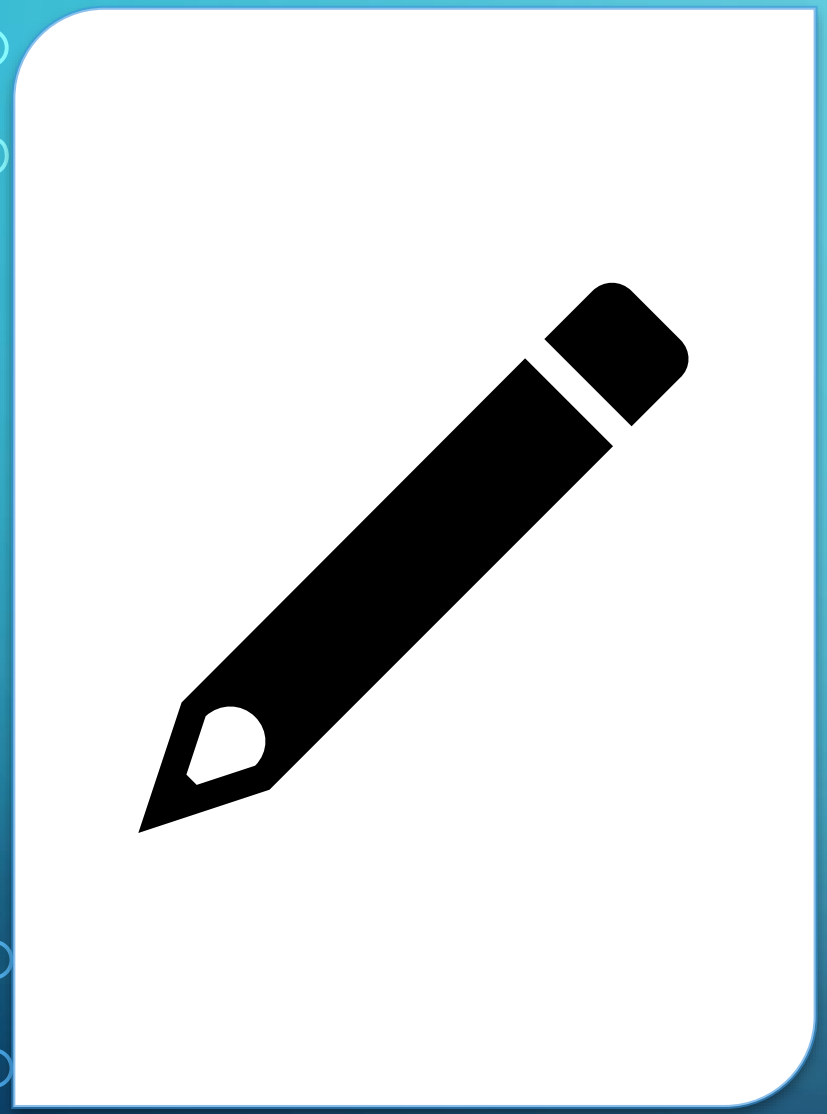
3.1. MAGERIT. FASE 1. PASO 2: AMENAZAS

Degradación. Ejemplos.

Para un activo como un ordenador, y una amenaza de incendio, la degradación en la confidencialidad e integridad será nula, pero máxima en la disponibilidad.

Para un activo como una aplicación, y una amenaza de un programa malintencionado, la degradación en confidencialidad e integridad puede ser mediana o baja, y puede ser alta en la disponibilidad.

Para un activo como una base de datos, y una amenaza de error de usuario, la degradación en confidencialidad puede ser nula, alta en integridad, y mediana en disponibilidad.



Actividades

SELECCIONE UNA AMENAZA DE CADA CATEGORÍA (DESASTRE NATURAL, DESASTRE INDUSTRIAL, ERRORES NO INTENCIONADOS, Y ATAQUES INTENCIONADOS). PARA CADA AMENAZA, IMAGINE TRES INCIDENTES CON DEGRADACIONES COMPLETAS, PARCIALES, O INEXISTENTES.

3.1. MAGERIT. FASE 1. PASO 2: AMENAZAS

Frecuencia de la amenaza.

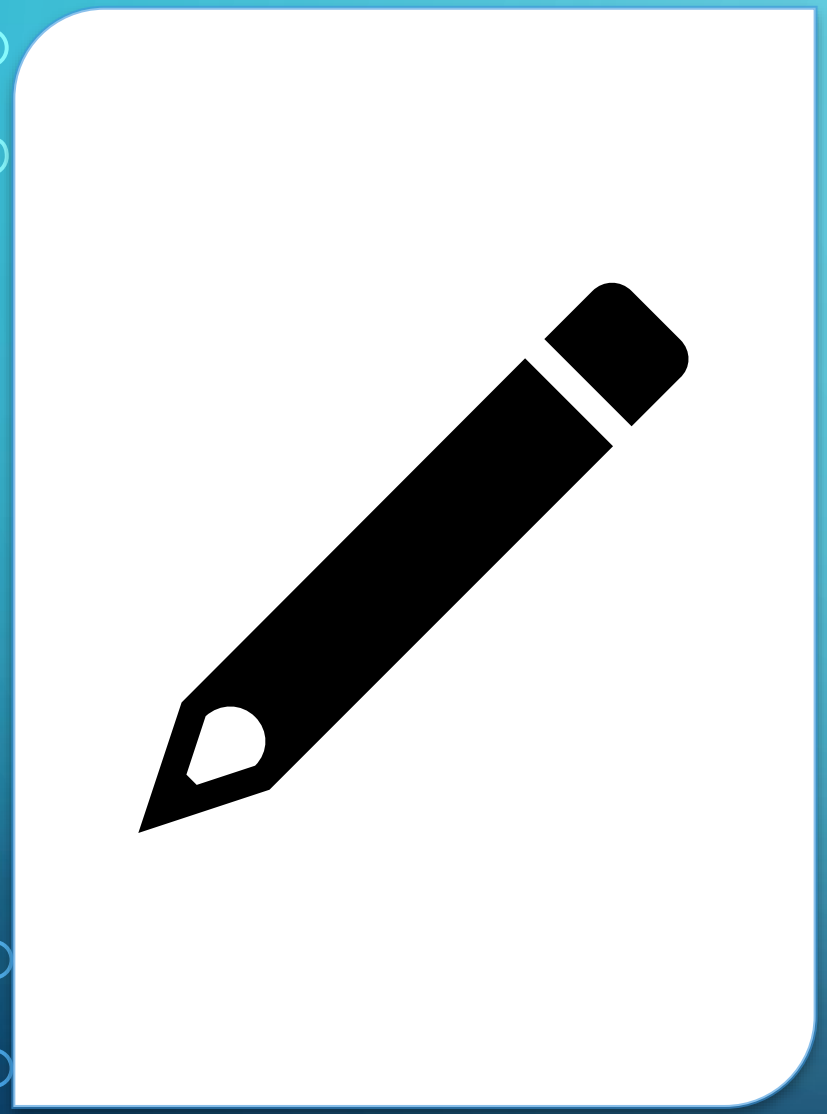
Carácter temporal o la posibilidad de ocurrencia de una amenaza.

Un incendio puede acarrear una degradación completa del valor del activo, pero ser de muy improbable materialización.

Un error de usuario puede producir una degradación menor, pero mucho más frecuente.

3.1. MAGERIT. FASE 1. PASO 2: AMENAZAS

Valoración cualitativa *"la amenaza sucede..."*	**Frecuencia**	**Dato para MAGERIT**
A diario	Muy frecuente (MF)	100
Mensualmente	Frecuente (F)	10
Una vez al año	Normal (N)	1
Cada varios años	Poco frecuente (PF)	1/10



Actividades

SELECCIONE UNA AMENAZA DE CADA CATEGORÍA (DESASTRE NATURAL, DESASTRE INDUSTRIAL, ERRORES NO INTENCIONADOS, Y ATAQUES INTENCIONADOS). PARA CADA AMENAZA, IMAGINE TRES INCIDENTES CON FRECUENCIAS MUY FRECUENTES O FRECUENTES, NORMALES, Y POCO FRECUENTES.

3.1. MAGERIT. FASE 1. PASO 4: IMPACTO

Impacto

Medida del daño sobre el activo por la materialización de la amenaza.

Se calcula para cada activo, para cada amenaza, y para cada dimensión.

Impacto = Valor x Degradación

3.1. MAGERIT. FASE 1. PASO 4: IMPACTO

Impacto. Ejemplo.

Un activo tiene un valor CIA = (5, 8, 6),

se conoce una amenaza con una degradación CIA = (100 %, 0 %, 50 %),

el **impacto de la amenaza en el activo será (5, 0, 3)**, que es el daño que causa en el valor.

No se debe confundir el impacto, que es daño o valor perdido, con el valor que tendría el activo tras la amenaza:

VALOR FINAL = VALOR INICIAL - IMPACTO

En el ejemplo anterior, tras la materialización de la amenaza, el valor del activo sería:

(5, 8, 6) – (5, 0, 3) = (0, 8, 3).

3.1. MAGERIT. FASE 1. PASO 5: RIESGO

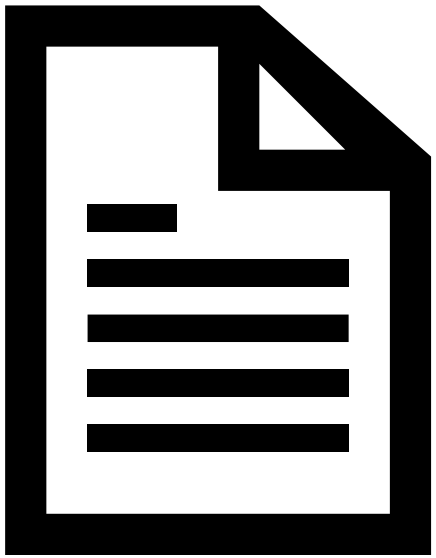
Riesgo

El riesgo crece con la frecuencia y con el impacto.

Se calcula para cada activo, para cada amenaza, y en cada dimensión.

RIESGO = IMPACTO x FRECUENCIA

Ejemplo



1.3.2.MF0486_3-CAPITULO3_EJEMPLO.DOCX

3.2. OTRAS METODOLOGÍAS

ISO 27005

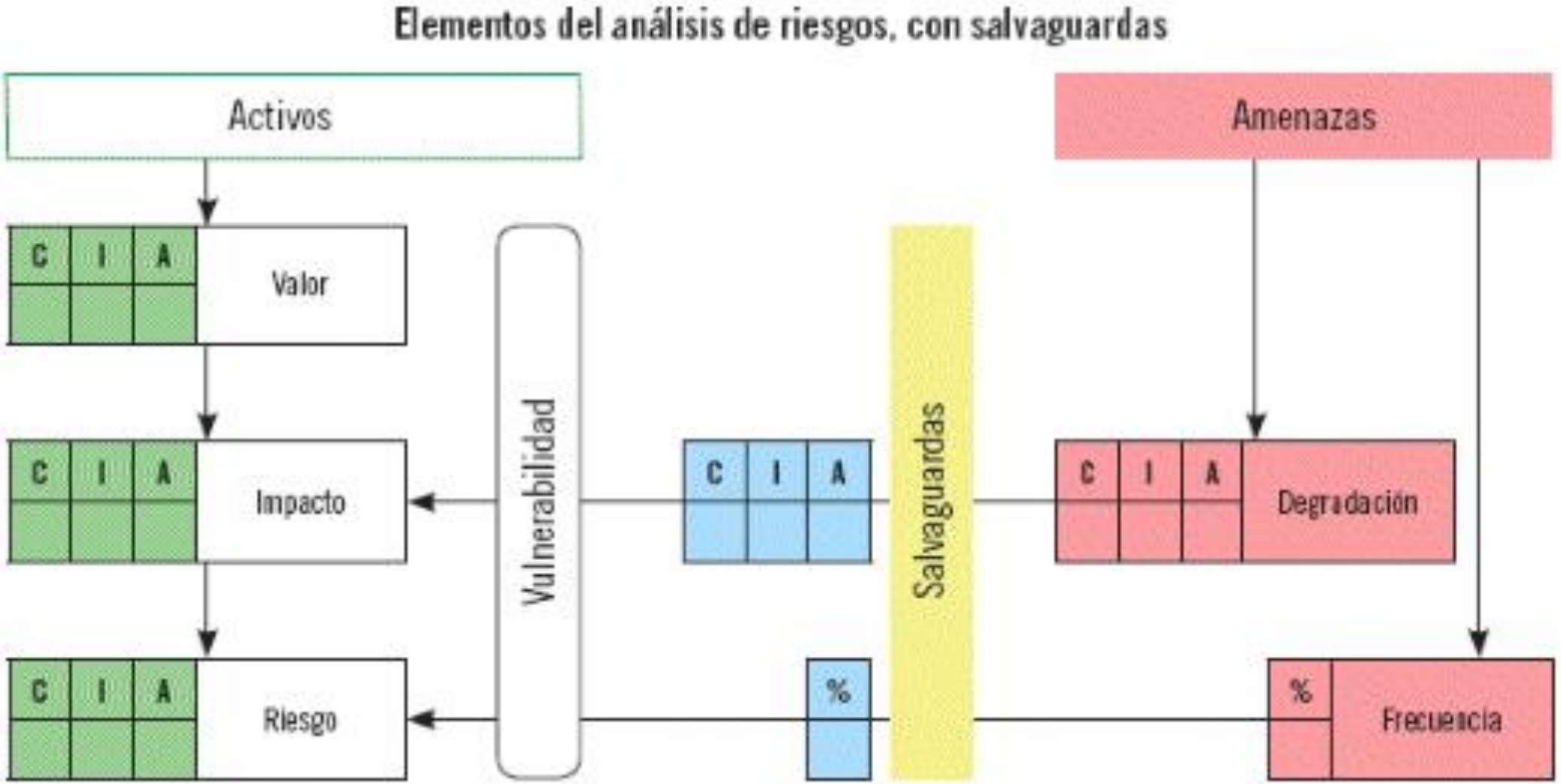
Octave

CRAMM

UNE 71504

FAIR

4. MEDIDAS DE SALVAGUARDA



4.1. RIESGO TRAS LA INTRODUCCIÓN DE SALVAGUARDAS

La aplicación de controles reduce el riesgo, y esto debe poder evaluarse.

4.1. RIESGO TRAS LA INTRODUCCIÓN DE SALVAGUARDAS

FASE 1. Paso 3: salvaguardas o contramedidas

Son los procedimientos o mecanismos tecnológicos que reducen el riesgo.

Al igual que las amenazas, no existe una lista completa de contramedidas.

El profesional de Sistema de Información deberá seleccionarlas en cada caso de AGR y empresa concreta.

Las salvaguardas intervienen reduciendo el riesgo de dos maneras:

- **Limitando el daño causado.**
- **Reduciendo la frecuencia de las amenazas.**

Ampliación

EXISTEN METODOLOGÍAS Y DOCUMENTACIÓN QUE RECOGEN MILES DE CONTROLES O SALVAGUARDAS, COMO POR EJEMPLO:

- EL MÉTODO CRAMM, INTRODUCIDO EN EL EPÍGRAFE ANTERIOR.

- LA ASOCIACIÓN SIN ÁNIMO DE LUCRO ISF (INFORMATION SECURITY FORUM) PUBLICA ANUALMENTE UN DOCUMENTO, THE STANDARD OF GOOD PRACTICE FOR INFORMATION SECURITY (SOGP ISF), QUE RECOGE MÁS DE 3.000 SALVAGUARDAS, O CONTROLES PARA REDUCIR

- LAS AMENAZAS. LA NORMA IT-GRUNDSCHUTZ, CATÁLOGO EXHAUSTIVO DE SALVAGUARDAS Y CONTROLES, Y ES UN MATERIAL QUE CONSTITUYE UNA VERDADERA ENCICLOPEDIA DE SEGURIDAD.

- ISO 27002, INTRODUCE 133 CONTROLES O CONTRAMEDIDAS, AGRUPADAS EN DIFERENTES CATEGORÍAS

4.1. RIESGO TRAS LA INTRODUCCIÓN DE SALVAGUARDAS

FASE 1. Paso 3: salvaguardas o contramedidas

Limitando el daño causado.

Se aplican cuando la amenaza se materializa, limitando sus consecuencias.

Por ejemplo, pueden reducir la degradación, o pueden ayudar a detectar la materialización de la amenaza, para frenar el avance de la degradación. Incluso pueden consistir en facilitar la pronta recuperación del sistema, una vez que la amenaza ha destruido el activo.

4.1. RIESGO TRAS LA INTRODUCCIÓN DE SALVAGUARDAS

FASE 1. Paso 3: salvaguardas o contramedidas. Limitando el daño causado.

Indicadores para medir la eficacia de una contramedida, se pueden valorar cada uno de los siguientes aspectos, que solo cumpliría una contramedida con eficacia del 100 %:

- **Es teóricamente idónea.**
- **Está perfectamente desplegada, configurada, y mantenida.**
- **Se emplea siempre.**
- **Existen procedimientos claros de uso en caso de incidencias.**
- **Los usuarios están formados y concienciados.**
- **Existen controles que avisan de posibles fallos.**

En el extremo opuesto, con una eficacia del 0 %, estarían las que pueden eliminarse o apagarse sin repercusión alguna en el sistema.

4.1. RIESGO TRAS LA INTRODUCCIÓN DE SALVAGUARDAS

FASE 1. Paso 3: salvaguardas o contramedidas. Reduciendo la frecuencia de las amenazas.

Son las medidas preventivas.

Idealmente, llegan a impedir completamente que la amenaza se materialice.

Por ejemplo, si la contramedida reduce la frecuencia de "diario" a "anual", la frecuencia ha pasado de ser 100 a ser 1.

4.1. RIESGO TRAS LA INTRODUCCIÓN DE SALVAGUARDAS

FASE 1. Paso 3: salvaguardas o contramedidas. Reduciendo la frecuencia de las amenazas.

Impacto residual.

Analizadas las salvaguardas, resulta muy rápido estimar el nuevo riesgo del sistema, a partir de la nueva degradación mejorada (nuevo impacto residual), y de la frecuencia mejorada (nuevo riesgo residual).

4.1. RIESGO TRAS LA INTRODUCCIÓN DE SALVAGUARDAS

FASE 1. Paso 3: salvaguardas o contramedidas. Reduciendo la frecuencia de las amenazas.

Impacto residual.

Si las salvaguardas son 100 % eficaces, eliminan completamente la degradación que producirían las amenazas, y el impacto residual sería despreciable.

En la realidad, existirán normas imprecisas, procedimientos incompletos, salvaguardas inadecuadas, y otros factores, que hacen que el sistema de información permanezca sometido a un impacto residual.

El cálculo es sencillo, ya que lo único que varía es la degradación de la amenaza que se ve mejorada por la eficacia de la contramedida:

4.1. RIESGO TRAS LA INTRODUCCIÓN DE SALVAGUARDAS

FASE 1. Paso 3: salvaguardas o contramedidas. Reduciendo la frecuencia de las amenazas.

Impacto residual.

El cálculo es sencillo, ya que lo único que varía es la degradación de la amenaza que se ve mejorada por la eficacia de la contramedida:

DEGRADACIÓN MEJORADA = DEGRADACIÓN x (100 – EFICACIA CONTRAMEDIDA)

IMPACTO RESIDUAL = VALOR x DEGRADACIÓN MEJORADA

IMPACTO RESIDUAL = IMPACTO x (100 – EFICACIA CONTRAMEDIDA)

4.1. RIESGO TRAS LA INTRODUCCIÓN DE SALVAGUARDAS

FASE 1. Paso 3: salvaguardas o contramedidas. Reduciendo la frecuencia de las amenazas.

Riesgo residual.

Si las salvaguardas son 100 % eficaces, eliminan completamente la frecuencia de las amenazas, y el riesgo residual sería despreciable.

En la realidad, el sistema de información permanece sometido a un riesgo residual.

RIESGO RESIDUAL = IMPACTO RESIDUAL x FRECUENCIA MEJORADA

4.2. GESTIÓN DEL RIESGO RESIDUAL

Si el riesgo residual es despreciable, o admisible para las normas de aceptación de la empresa, se ha terminado.

En caso contrario, es preciso reducirlo aún más.

Un riesgo residual no despreciable precisa ser interpretado.

Por ejemplo, si el valor es similar al riesgo potencial (sin considerar ninguna salvaguarda), se puede concluir que las salvaguardas aplicadas no sirven; no significa que no se haya hecho nada, sino que hay cosas fundamentales sin hacer.

4.2. GESTIÓN DEL RIESGO RESIDUAL

Selección de medidas a aplicar

- Las medidas deseables son **preventivas**, pero no siempre será posible o su coste asumible.
- Inmediatamente después, conviene disponer de contramedidas de **detección**, ya que en ningún caso debe permitirse que un ataque pase inadvertido.
- Posteriormente, conviene aplicar las medidas **reactivas de emergencia**, que paren y limiten el incidente.
- Por último, las medidas **reactivas de recuperación**, para regresar a donde se debe estar, con un plan de continuidad adecuado.

4.2. GESTIÓN DEL RIESGO RESIDUAL

Selección de medidas a aplicar por su naturaleza:

- De tipo **técnico** (aplicaciones, equipos, y comunicaciones),
- **Físicas** (aplicadas para proteger el entorno y los equipos),
- **Organizativas** (de prevención y gestión de incidencias) y
- **Política de personal** (contratación, formación, organización, plan de reacción y por último, medidas disciplinarias).

4.2. GESTIÓN DEL RIESGO RESIDUAL

Selección de medidas a aplicar de tipo económico:

- Para la selección se debe considerar también un criterio económico, porque no resulta proporcionado aplicar contramedidas cuyo coste supere al del activo a proteger.

La Dirección debe determinar el nivel de impacto y riesgo que está dispuesta a asumir.

4.2. GESTIÓN DEL RIESGO RESIDUAL

Revisión del riesgo introducido por las salvaguardas

Es frecuente olvidar que las salvaguardas, sobre todo las técnicas, introducen indirectamente en los sistemas de información nuevos riesgos, porque los activos a los que protegen pasan a depender de ellas, y porque las propias salvaguardas están sujetas a amenazas.

Ejercicios

1.3.100.1.EJERCICIOSCAPITULO_3.DOCX