Gestión de Proyectos Software

Tema 5. Riesgos

Riesgos de Seguridad - MAGERIT

Carlos Blanco
Universidad de Cantabria

Objetivos

- Profundizar en la Gestión de Riesgos que afectan a la dimensión de Seguridad de los sistemas software.

- Conocer MAGERIT, la Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información, elaborada por el MAP-España.

Contenido

- 1. Introducción a los Riesgos de Seguridad.
  - Modelo de Madurez para Seguridad en SI.
- 2. MAGERIT.
  - 2.1 Introducción y Componentes.
  - 2.2 Análisis de Riesgos.
    - Activos, amenazas, impactos, riesgos, salvaguardas, equilibrios.
  - 2.3 Método.
    - Proceso P1 – Planificación.
    - Proceso P2 – Análisis.
    - Proceso P2 – Gestión.
  - 2.4 Técnicas
    - Específicas
      - Tablas de Análisis, Algoritmos de Análisis, Árboles de Ataque
    - Generales

Bibliografía

- MAGERIT – versión 3. Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información.
  - Ministerio de de Hacienda y Administraciones Públicas.
  - Portal de Administración Electrónica
    - http://administracionelectronica.gob.es

GENERACIONES RESPECTO A LA SEGURIDAD

Marcelo (2003)

70: 1ª generación de métodos de riesgos basados en listas de chequeo

80: 2ª generación de métodos más formalizados: CRAMM

90: 3ª generación más avanzada para nuevos problemas de seguridad: MAGERIT

2000: 4ª generación preocupada por un nivel de seguridad certificable de los componentes que asegure una confianza en el compuesto.

MODELO DE MADUREZ

Marcelo (2003)

Escalón 0: el “sentido común”

Escalón 1: cumplimiento de la legislación obligatoria

Escalón 2: evaluación del proceso de gestión de seguridad

Escalón 3: análisis de riesgos y gestión de su resolución

Escalón 4: adquisición de productos certificados para integrarlos en sistemas

Escalón 5: integración de componentes certificados en sistemas compuestos

MODELO DE MADUREZ

Escalón 0: el "sentido común"

- Principio de simplicidad
- Principio de la cadena
- Principio de adecuación
- Principio de economía
- Principio de redundancia y de no-reincidencia
- Principio del equilibrio
- Principio de comodidad
- Principio de finalidad

MODELO DE MADUREZ

Escalón 1: cumplimiento de la legislación obligatoria

- Intimidad: LOPD, RD 994/1999
- Validez de documentos y aplicaciones de las administraciones públicas:
  - Administración General del Estado (RD 263/1996)
  - Administración Autonómica

MODELO DE MADUREZ

Escalón 2: Evaluación del proceso de gestión de seguridad

- Utilización del Código de Práctica de la Gestión de Seguridad de la Información (ISO/IEC 17799)
- La organización debe establecer y mantener un SGSI bien documentado, que identifique de manera precisa los activos a proteger, el enfoque de la gestión del riesgo, los objetivos y medidas a tomar, así como al grado requerido de aseguramiento

MODELO DE MADUREZ

Escalón 3: Gestión global de la seguridad

- Análisis y gestión de riesgos
- Determinación de objetivos, estrategia y política
- Establecimiento de la planificación de la seguridad
- Determinación de la organización de la seguridad
- Implantación de salvaguardas
- Aprendizaje
- Reacción a eventos, manejo y registro de incidencias, y recuperación de estados de seguridad
- Monitorización y gestión de configuración y cambios

MODELO DE MADUREZ

Escalones 4 y 5: aplicación de los criterios de evaluación

- Computing Trusted Security Evaluation Criteria (CTSEC), años 80, DoD de EEUU
- Information Technologies Security Evaluation Criteria (ITSEC), años 90 en Europa
- Criterios Comunes, año 2000, ISO/IEC 15408

Nivel 4: producto como caja negra

Nivel 5: producto como caja transparente

MAGERIT

Objetivos:

Directos:

1. concienciar a los responsables de los SI de la existencia de riesgos y de la necesidad de atajarlos a tiempo
2. ofrecer un método sistemático para analizar tales riesgos
3. ayudar a descubrir y planificar las medidas oportunas para mantener los riesgos bajo control

Indirectos:

1. preparar a la Organización para procesos de evaluación, auditoría, certificación o acreditación, según corresponda en cada caso

Riesgo:
estimación del grado de exposición a que una amenaza se materialice sobre uno o más activos causando daños o perjuicios a la Organización.

Análisis de riesgos:
proceso sistemático para estimar la magnitud de los riesgos a que está expuesta una Organización.

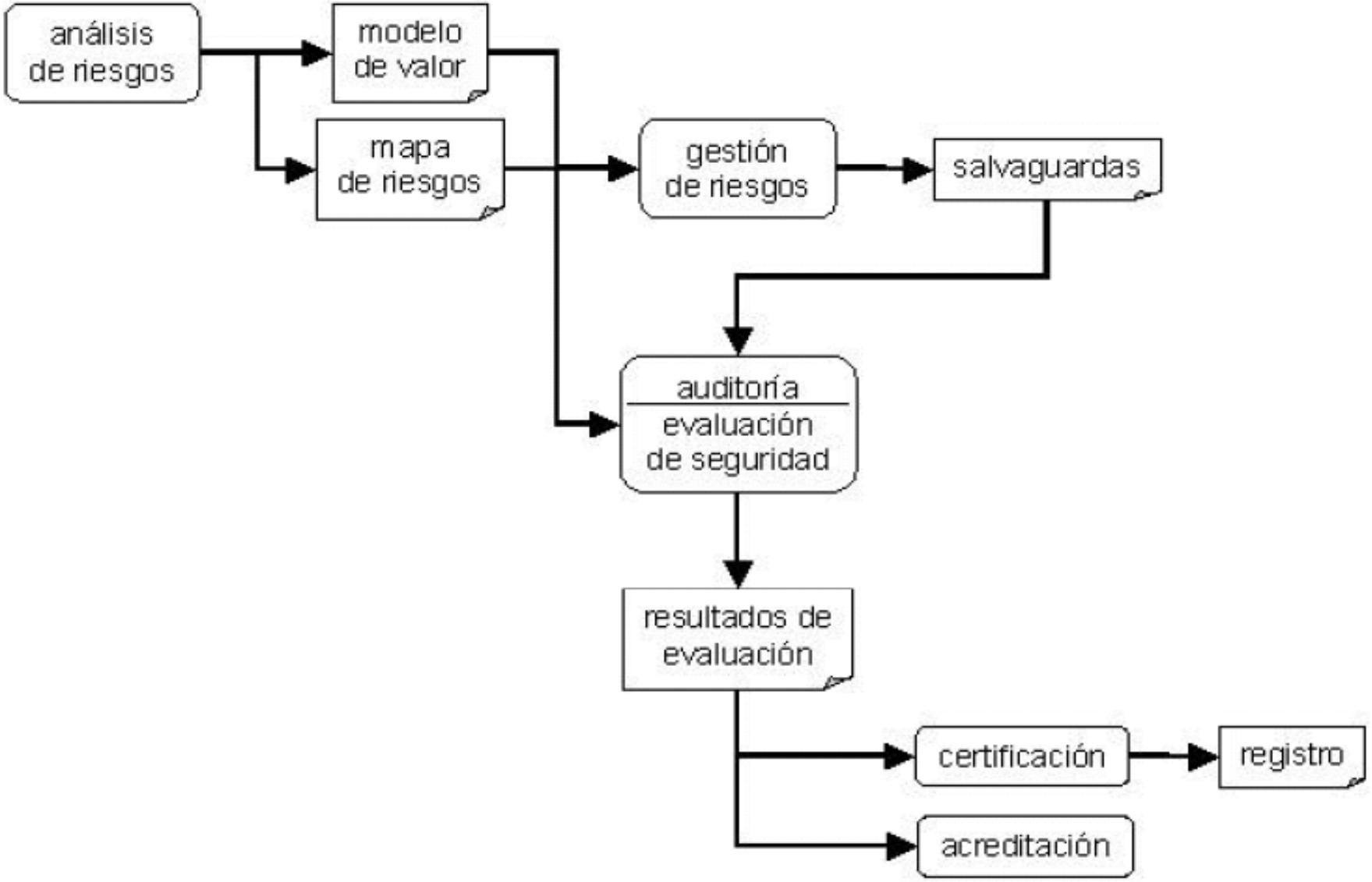
Gestión de riesgos:
selección e implantación de salvaguardas para conocer, prevenir, impedir, reducir o controlar los riesgos identificados.

MAGERIT

Libro I: Método

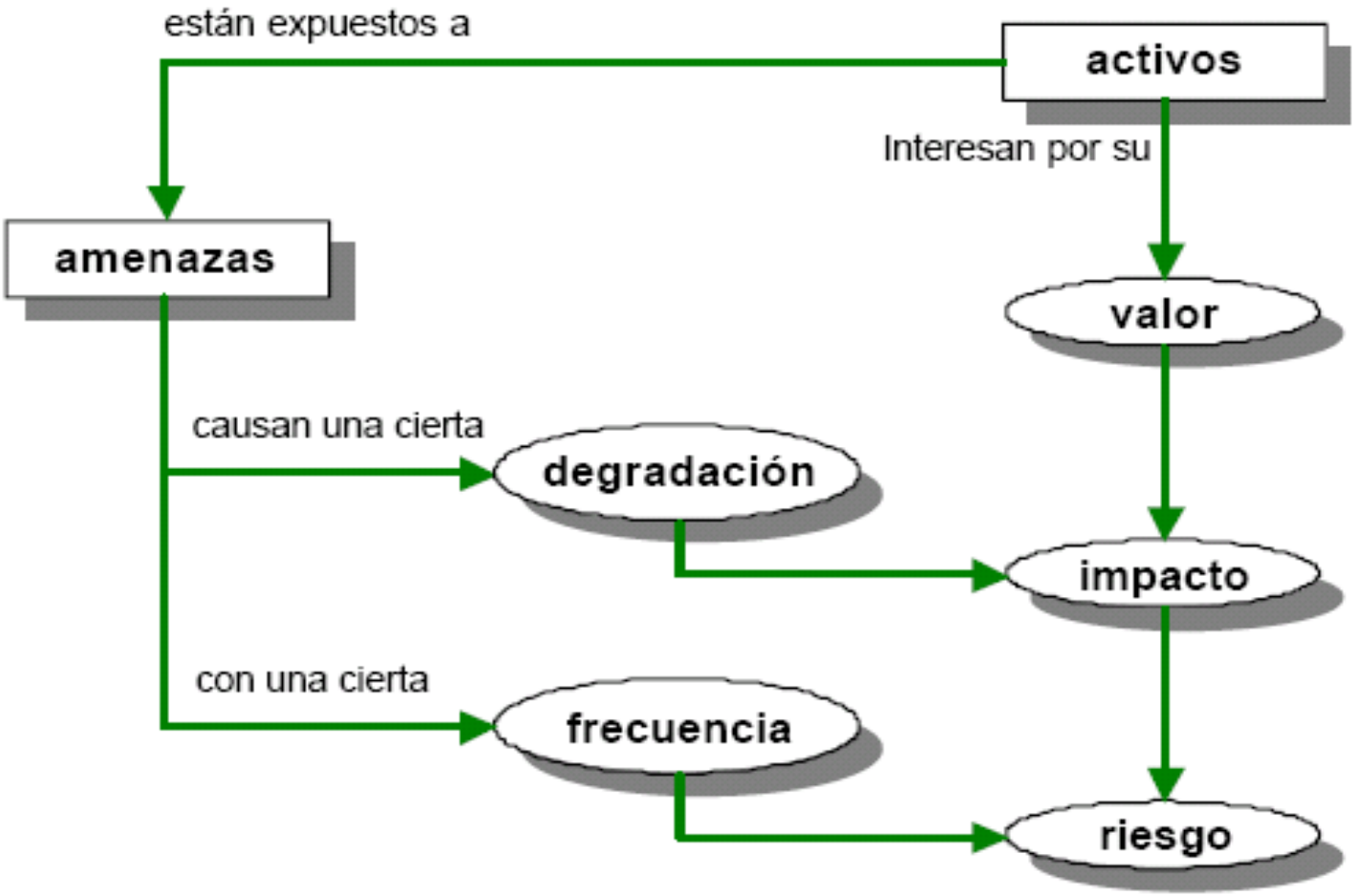
Libro II: Catálogo de Elementos

Libro III: Guía de técnicas


análisis de riesgos
modelo de valor
mapa de riesgos
gestión de riesgos
salvaguardas
auditoría
evaluación de seguridad
resultados de evaluación
certificación
registro
acreditación

Análisis de Riesgos

1. determinar los activos relevantes para la Organización, su interrelación y su valor, en el sentido de qué perjuicio (coste) supondría su degradación
2. determinar a qué amenazas están expuestos aquellos activos
3. determinar qué salvaguardas hay dispuestas y cuán eficaces son frente al riesgo
4. estimar el impacto, definido como el daño sobre el activo derivado de la materialización de la amenaza
5. estimar el riesgo, definido como el impacto ponderado con la tasa de ocurrencia (o expectación de materialización) de la amenaza


están expuestos a
activos
Interesan por su
amenazas
valor
causan una cierta
degradación
impacto
con una cierta
frecuencia
riesgo

PASO 1: ACTIVOS

El activo esencial: **información (datos)**

- **Los servicios**
- **Las aplicaciones informáticas** *(software)*
- **Los equipos informáticos** *(hardware)*
- **Los soportes de información**
- **El equipamiento auxiliar**
- **Las redes de comunicaciones**
- **Las instalaciones**
- **Las personas**

- capa 1: **el entorno**: activos que se precisan para garantizar las siguientes capas
  - equipamiento y suministros: energía, climatización, comunicaciones
  - personal: de dirección, de operación, de desarrollo, etc.
  - otros: edificios, mobiliario, etc.

- capa 2: **el sistema de información** propiamente dicho
  - equipos informáticos *(hardware)*
  - aplicaciones *(software)*
  - comunicaciones
  - soportes de información: discos, cintas, etc.

- capa 3: **la información**
  - datos
  - meta-datos: estructuras, índices, claves de cifrado, etc.

- capa 4: **las funciones de la Organización**, que justifican la existencia del sistema de información y le dan finalidad
  - objetivos y misión
  - bienes y servicios producidos

- capa 5: **otros** activos
  - credibilidad o buena imagen
  - conocimiento acumulado
  - independencia de criterio o actuación
  - intimidad de las personas
  - integridad física de las personas

Dimensiones

- su **autenticidad:** ¿qué perjuicio causaría no saber exactamente quien hace o ha hecho cada cosa?
- su **confidencialidad**: ¿qué daño causaría que lo conociera quien no debe?
- su **integridad**: ¿qué perjuicio causaría que estuviera dañado o corrupto?
- su **disponibilidad**: ¿qué perjuicio causaría no tenerlo o no poder utilizarlo?
- la **trazabilidad** del uso del servicio: ¿qué daño causaría no saber a quién se le presta tal servicio?
- la **trazabilidad** del acceso a los datos: ¿qué daño causaría no saber quién accede a qué datos y qué hace con ellos?

valoración

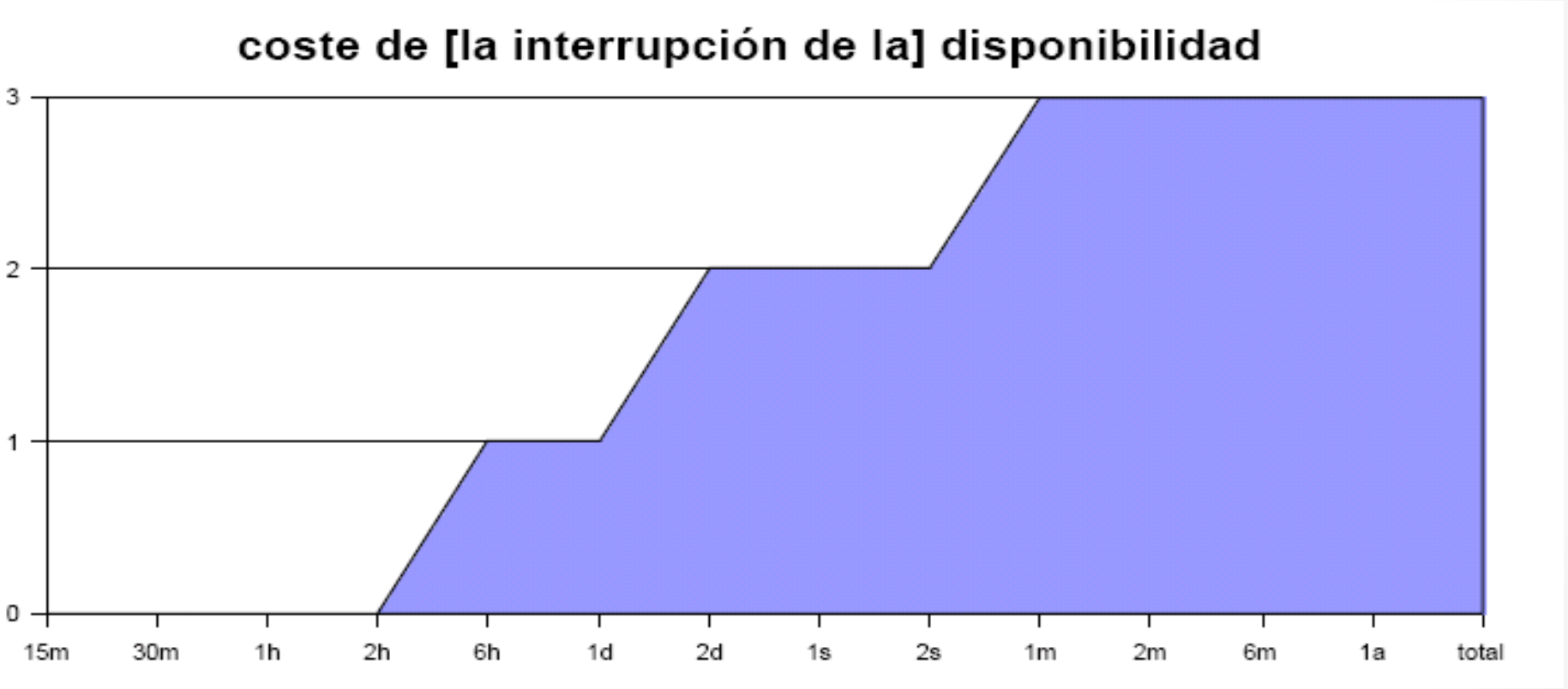
factores

- coste de reposición: adquisición e instalación
- coste de mano de obra (especializada) invertida en recuperar (el valor) del activo
- lucro cesante: pérdida de ingresos
- capacidad de operar: confianza de los usuarios y proveedores que se traduce en una pérdida de actividad o en peores condiciones económicas
- sanciones por incumplimiento de la ley u obligaciones contractuales
- daño a otros activos, propios o ajenos
- daño a personas
- daños medioambientales

VALORACIÓN

- cuantitativa (con una cantidad numérica)
- cualitativa (en alguna escala de niveles)

- criterios :
  - la **homogeneidad**
  - la **relatividad**


coste de [la interrupción de la] disponibilidad
3
2
1
0
15m
30m
1h
2h
6h
1d
2d
1s
2s
1m
2m
6m
1a
total

PASO 2: AMENAZAS

Valoración

- **degradación:** cuán perjudicado resultaría el activo
- **frecuencia:** cada cuánto se materializa la amenaza

100	muy frecuente	a diario
10	frecuente	mensualmente
1	normal	una vez al año
1/10	poco frecuente	cada varios años

PASO 4: DETERMINACIÓN DEL IMPACTO

Impacto acumulado

Es el calculado sobre un activo teniendo en cuenta

- su valor acumulado (el propio mas el acumulado de los activos que dependen de él)
- las amenazas a que está expuesto

Impacto repercutido

Es el calculado sobre un activo teniendo en cuenta

- su valor propio
- las amenazas a que están expuestos los activos de los que depende

Agregación de valores de impacto

- puede agregarse el impacto repercutido sobre diferentes activos,

- puede agregarse el impacto acumulado sobre activos que no sean dependientes entre sí, ni dependan de ningún activo superior común,

- no debe agregarse el impacto acumulado sobre activos que no sean independientes,

- puede agregarse el impacto de diferentes amenazas sobre un mismo activo,

- puede agregarse el impacto de una amenaza en diferentes dimensiones.

PASO 5: DETERMINACIÓN DEL RIESGO

Riesgo acumulado

Es el calculado sobre un activo teniendo en cuenta

· el impacto acumulado sobre un activo debido a una amenaza y

· la frecuencia de la amenaza

Riesgo repercutido

Es el calculado sobre un activo teniendo en cuenta

· el impacto repercutido sobre un activo debido a una amenaza y

· la frecuencia de la amenaza

Agregación de riesgos

· puede agregarse el riesgo repercutido sobre diferentes activos,

· puede agregarse el riesgo acumulado sobre activos que no sean dependientes entre sí, ni dependan de ningún activo superior común,

· no debe agregarse el riesgo acumulado sobre activos que no sean independientes,

· puede agregarse el riesgo de diferentes amenazas sobre un mismo activo,

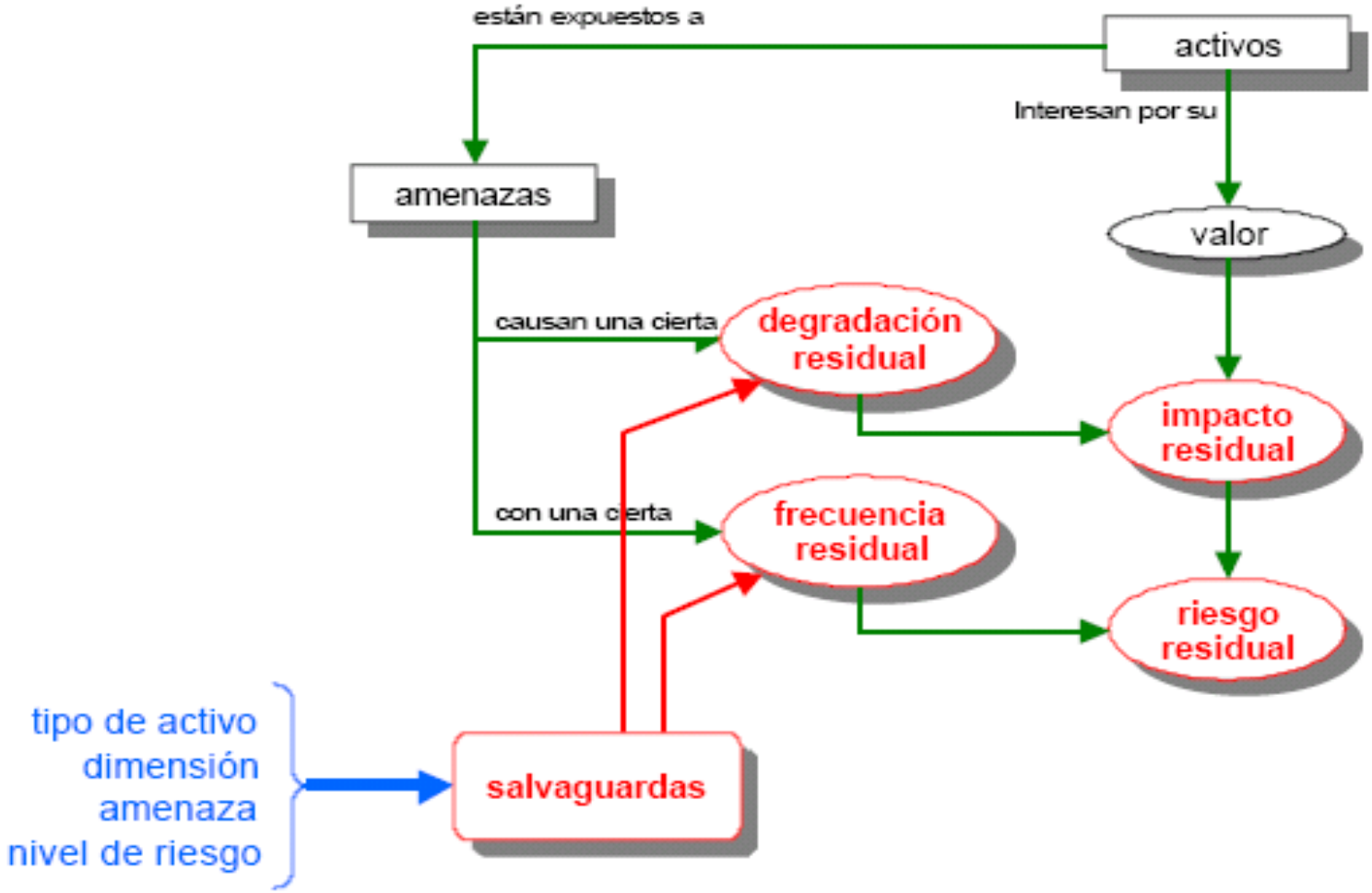
· puede agregarse el riesgo de una amenaza en diferentes dimensiones.

PASO 3: SALVAGUARDAS

Entran en el cálculo del riesgo de dos formas:

- **Reduciendo la frecuencia de las amenazas.**
Se llaman salvaguardas preventivas. Las ideales llegan a impedir completamente que la amenaza se materialice.

- **Limitando el daño causado.**
Hay salvaguardas que directamente limitan la posible degradación, mientras que otras permiten detectar inmediatamente el ataque para frenar que la degradación avance. Incluso algunas salvaguardas se limitan a permitir la pronta recuperación del sistema cuando la amenaza lo destruye.


están expuestos a
activos
Interesan por su
amenazas
valor
causan una cierta
degradación residual
impacto residual
con una cierta
frecuencia residual
riesgo residual
tipo de activo
dimensión
amenaza
nivel de riesgo
salvaguardas

La salvaguarda ideal es 100% eficaz, lo que implica que:

- es teóricamente idónea
- está perfectamente desplegada, configurada y mantenida
- se emplea siempre
- existen procedimientos claros de uso normal y en caso de incidencias
- los usuarios están formados y concienciados
- existen controles que avisan de posibles fallos

Entre una eficacia del 0% para aquellas que están de adorno y el 100% para aquellas que son perfectas, se estimará un grado de eficacia real en cada caso concreto.

Gestión de Riesgos
Interpretación de los valores de impacto y riesgo residuales

Si el valor residual es igual al valor potencial, las salvaguardas existentes no valen para nada, típicamente
no porque no haya nada hecho, sino porque hay elementos fundamentales sin hacer.

Si el valor residual es despreciable, ya está. Esto no quiere decir descuidar la guardia; pero si afrontar el día con cierta confianza. Mientras el valor residual sea más que despreciable, hay una cierta exposición.

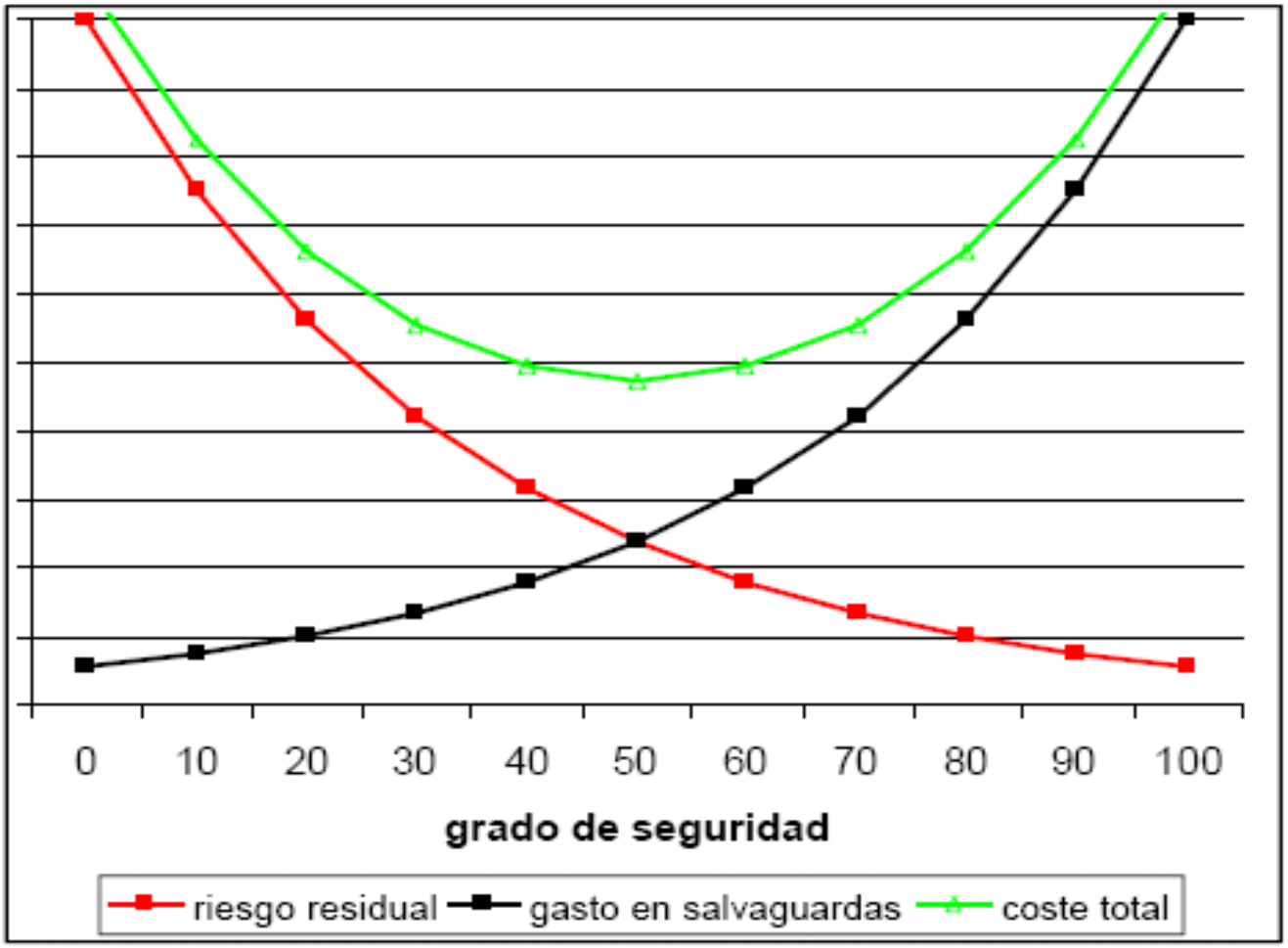
Informe de Insuficiencias.

Selección de salvaguardas

1. establecer una política de la Organización al respecto: directrices generales de quién es responsable de cada cosa
2. establecer una norma: objetivos a satisfacer para poder decir con propiedad que la amenaza ha sido conjurada
3. establecer unos procedimientos: instrucciones paso a paso de qué hay que hacer
4. desplegar salvaguardas técnicas que efectivamente se enfrenten a las amenazas con capacidad para conjurarlas
5. desplegar controles que permitan saber que todo lo anterior está funcionando según lo previsto

Equilibrio entre

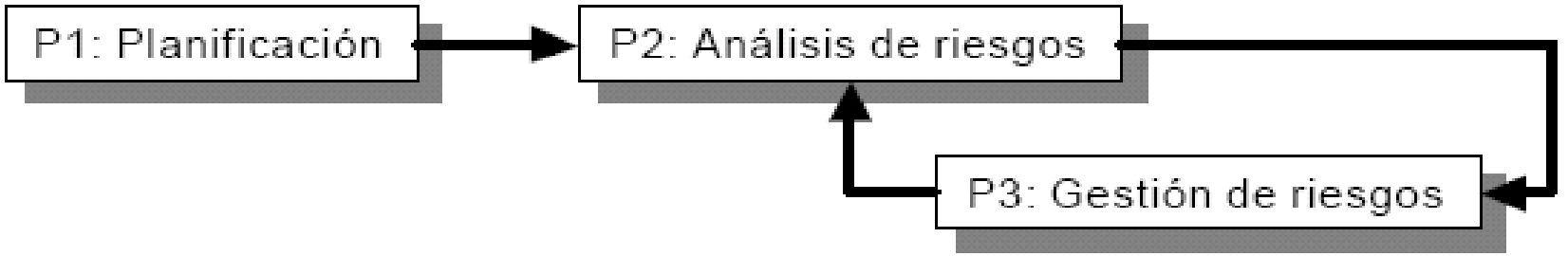
- **salvaguardas técnicas:** en aplicaciones, equipos y comunicaciones
- **salvaguardas físicas:** protegiendo el entorno de trabajo de las personas y los equipos
- **medidas de organización:** de prevención y gestión de las incidencias
- **política de personal:** que, a fin de cuentas, es el eslabón imprescindible y más delicado: política de contratación, formación permanente, Organización de reporte de incidencias, plan de reacción y medidas disciplinarias.


0
10
20
30
40
50
60
70
80
90
100
grado de seguridad
riesgo residual
gasto en salvaguardas
coste total

Estructuración del proyecto

-Proyecto de análisis y gestión de riesgos (AGR)

-Los pasos se organizan en tres grandes procesos:



Proceso P1: Planificación

- Se establecen las consideraciones necesarias para arrancar el proyecto AGR.
- Se investiga la oportunidad de realizarlo.
- Se definen los objetivos que ha de cumplir y el dominio (ámbito) que abarcará.
- Se planifican los medios materiales y humanos para su realización.
- Se procede al lanzamiento del proyecto.

Proceso P2: Análisis de riesgos

- Se identifican los activos a tratar, las relaciones entre ellos y la valoración que merecen.
- Se identifican las amenazas significativas sobre aquellos activos y se valoran en términos de frecuencia de ocurrencia y degradación que causan sobre el valor del activo afectado.
- Se identifican las salvaguardas existentes y se valora la eficacia de su implantación.
- Se estima el impacto y el riesgo al que están expuestos los activos del sistema.
- Se interpreta el significado del impacto y el riesgo.

Proceso P3: Gestión de riesgos

- Se elige una estrategia para mitigar impacto y riesgo.
- Se determinan las salvaguardas oportunas para el objetivo anterior.
- Se determina la calidad necesaria para dichas salvaguardas.
- Se diseña un plan de seguridad (plan de acción o plan director) para llevar el impacto y el riesgo a niveles aceptables.
- Se lleva a cabo el plan de seguridad.

DOCUMENTOS

P1: Planificación

- Tipología de activos
- Dimensiones de seguridad relevantes
- Criterios de evaluación

P2: Análisis de riesgos

- Modelo de valor
- Mapa de riesgos
- Evaluación de salvaguardas
- Estado de riesgo
- Informe de insuficiencias

P3: Gestión de riesgos

- Plan de seguridad

Proceso P1: Planificación

Actividad A1.1: Estudio de oportunidad

- Tarea T1.1.1: Determinar la oportunidad

Actividad A1.2: Determinación del alcance del proyecto

- Tarea T1.2.1: Objetivos y restricciones generales
- Tarea T1.2.2: Determinación del dominio y límites
- Tarea T1.2.3: Identificación del entorno
- Tarea T1.2.4: Estimación de dimensiones y coste

Actividad A1.3: Planificación del proyecto

- Tarea T1.3.1: Evaluar cargas y planificar entrevistas
- Tarea T1.3.2: Organizar a los participantes
- Tarea T1.3.3: Planificar el trabajo

Actividad A1.4: Lanzamiento del proyecto

- Tarea T1.4.1: Adaptar los cuestionarios
- Tarea T1.4.2: Criterios de evaluación
- Tarea T1.4.3: Recursos necesarios
- Tarea T1.4.4: Sensibilización

Resultados

Documentación intermedia

· Resultados de las entrevistas.

· Documentación de otras fuentes: estadísticas, observaciones de expertos y observaciones de los analistas.

· Documentación auxiliar: planos, organigramas, requisitos, especificaciones, análisis funcionales, cuadernos de carga, manuales de usuario, manuales de explotación, diagramas de flujo de información y de procesos, modelos de datos, etc.

· Análisis de los resultados, con la detección de las áreas críticas claves.

· Información existente utilizable por el proyecto (p.ej. inventario de activos)

· Resultados de posibles aplicaciones de métodos de análisis y gestión de riesgos realizadas anteriormente (p.ej. catalogación, agrupación y valoración de activos, amenazas, vulnerabilidades, impactos, riesgo, mecanismos de salvaguarda, etc.).

Resultados

Documentación final

- Tipología de activos
- Dimensiones de seguridad relevantes
- Criterios de evaluación
- Informe de "Planificación del Proyecto de Análisis y Gestión de riesgos" que contendrá una síntesis de los productos obtenidos en las actividades realizadas en proceso

Proceso P2: Análisis de riesgos

- Actividad A2.1: Caracterización de los activos
  - Tarea T2.1.1: Identificación de los activos
  - Tarea T2.1.2: Dependencias entre activos
  - Tarea T2.1.3: Valoración de los activos
- Actividad A2.2: Caracterización de las amenazas
  - Tarea T2.2.1: Identificación de las amenazas
  - Tarea T2.2.2: Valoración de las amenazas
- Actividad A2.3: Caracterización de las salvaguardas
  - Tarea T2.3.1: Identificación de las salvaguardas existentes
  - Tarea T2.3.2: Valoración de las salvaguardas existentes
- Actividad A2.4: Estimación del estado de riesgo
  - Tarea T2.4.1: Estimación del impacto
  - Tarea T2.4.2: Estimación del riesgo
  - Tarea T2.4.3: Interpretación de los resultados

Documentación intermedia

- Resultados de las entrevistas.
- Documentación de otras fuentes: estadísticas, observaciones de expertos y observaciones de los analistas.
- Información existente utilizable por el proyecto (por ejemplo inventario de activos)
- Documentación auxiliar: planos, organigramas, requisitos, especificaciones, análisis funcionales, cuadernos de carga, manuales de usuario, manuales de explotación, diagramas de flujo de información y de procesos, modelos de datos, etc.

Documentación final

- **Modelo de valor**

Informe que detalla los activos, sus dependencias, las dimensiones en las que son valiosos y la estimación de su valor en cada dimensión.

- **Mapa de riesgos**:

Informe que detalla las amenazas significativas sobre cada activo, caracterizándolas por su frecuencia de ocurrencia y por la degradación que causaría su materialización sobre el activo.

- **Evaluación de salvaguardas:**

Informe que detalla las salvaguardas existentes calificándolas en su eficacia para reducir el riesgo que afrontan.

- **Estado de riesgo:**

Informe que detalla para cada activo el impacto y el riesgo residuales frente a cada amenaza.

- **Informe de insuficiencias:**

Informe que detalla las salvaguardas necesarias pero ausentes o insuficientemente eficaces.

Proceso P3: Gestión de riesgos

Actividad A3.1: Toma de decisiones
- Tarea A3.1.1: Calificación de los riesgos

Actividad A3.2: Plan de seguridad
- Tarea T3.2.1: Programas de seguridad
- Tarea T3.2.2: Plan de ejecución

Actividad A3.3: Ejecución del plan
- Tarea T3.3: Ejecución de cada programa de seguridad

Documentación intermedia

· Decisiones de calificación de los escenarios de impacto y riesgo

Documentación final

· Plan de Seguridad

Técnicas específicas

1. Análisis mediante tablas

Estimación del impacto

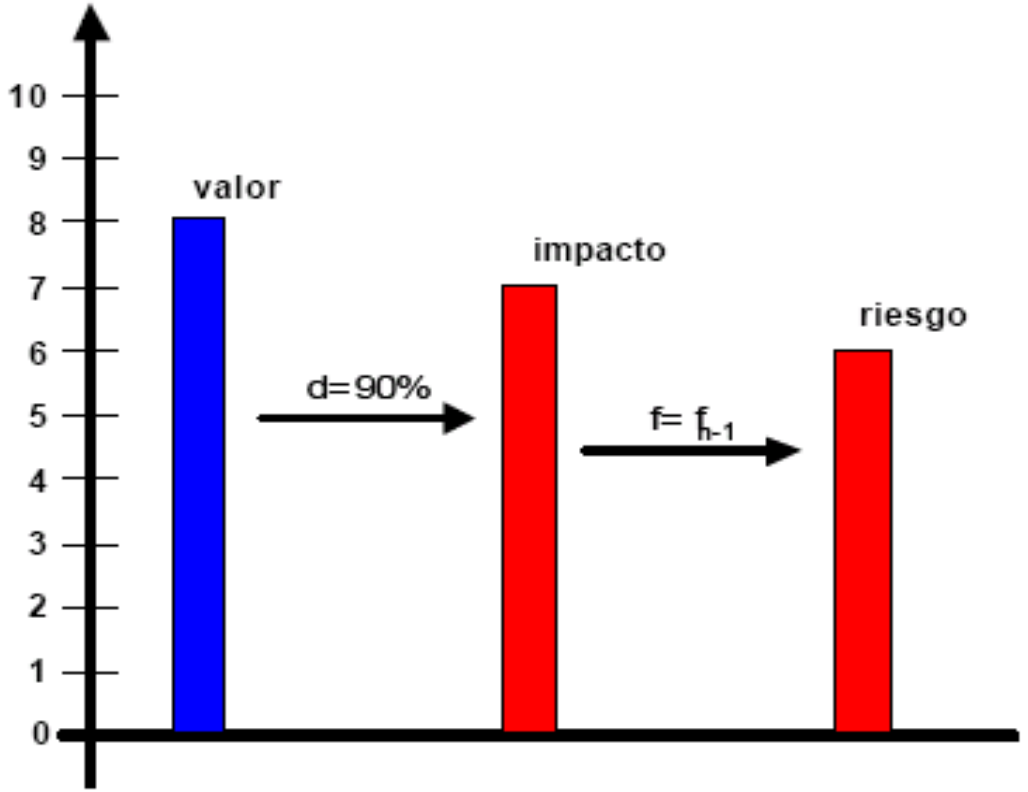
impacto		*degradación*		
		1%	10%	100%
valor	MA	M	A	MA
	A	B	M	A
	M	MB	B	M
	B	MB	MB	B
	MB	MB	MB	MB

Estimación del riesgo

riesgo		*frecuencia*			
		PF	FN	F	MF
impacto	MA	A	MA	MA	MA
	A	M	A	MA	MA
	M	B	M	A	MA
	B	MB	B	M	A
	MB	MB	MB	B	M

2. Análisis algorítmico.

Un modelo cualitativo



2. Análisis algorítmico. Un modelo cuantitativo

Ejemplo.

Sea un activo valorado en 1.000.000, que es víctima de una amenaza que lo degrada un 90%. El impacto es de cuantía

1.000.000 x 90% = 900.000

Si la frecuencia estimada es de 0,1, el riesgo es de cuantía

900.000 x 0,1 = 90.000

Si las salvaguardas tienen un 90% de eficacia sobre el impacto, el impacto residual es

900.000 x (1 – 0,9) = 90.000

Si las salvaguardas tienen un 50% de eficacia sobre la frecuencia, la frecuencia residual queda en

0,1 x (1 – 0,5) = 0,05

El riesgo residual queda en

90.000 x 0,05 = 4.500

La eficacia combinada de las salvaguardas es

1 – (1 – 90%) x (1 – 50%) = 95%

Si las cantidades son euros y las frecuencias anuales, la pérdida posible es de 90.000 euros y la pérdida anual se estima en 4.500 euros.

3. Árboles de ataque

1. **Objetivo**: usar sin pagar (OR)
    1. suplantar la identidad de un usuario legítimo
    2. soslayar la identificación de acceso al servicio
    3. abusar del contrato (AND)
        1. ser un usuario legítimo
        2. conseguir que no se facture el servicio (OR)
            1. que no queden trazas de uso
            2. que se destruyan las trazas antes de facturación (OR)
                1. las destruyo yo
                2. engaño al operador para que las borre
                3. manipulo del sw para que no las sume
            3. repudiar las trazas
            4. dar datos de cargo falsos

Técnicas generales

1. análisis coste beneficio
2. diagramas de flujo de datos (DFD)
3. diagramas de procesos (SADT)
4. técnicas gráficas: GANTT, histogramas, diagramas de Pareto y de tarta
5. técnicas de planificación y gestión de proyectos (PERT)
6. sesiones de trabajo: entrevistas, reuniones y presentaciones
7. valoraciones Delphi

Calificación según los Criterios de Seguridad del CSAE