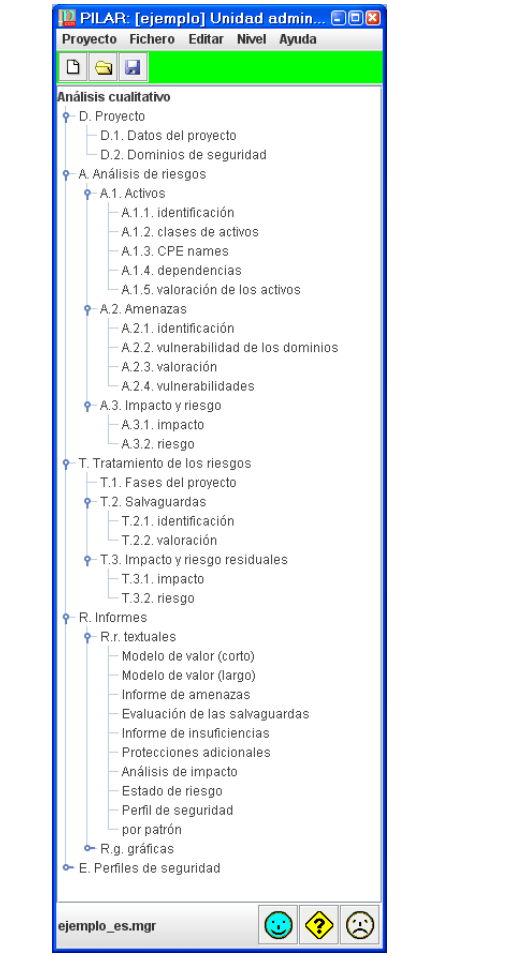
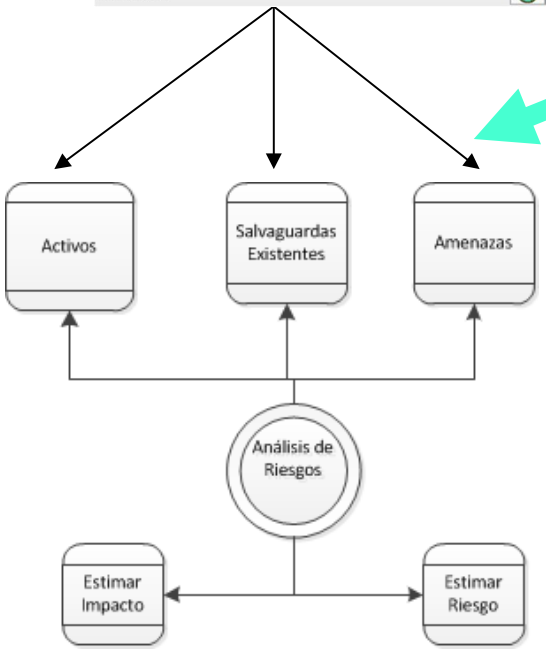
El método MAGERIT

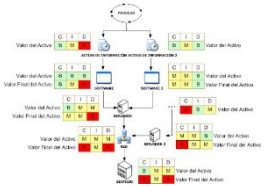
Índice

MAGERIT – versión 3.0
Metodología de Análisis y Gestión
de Riesgos de los Sistemas de Información



Proyecto



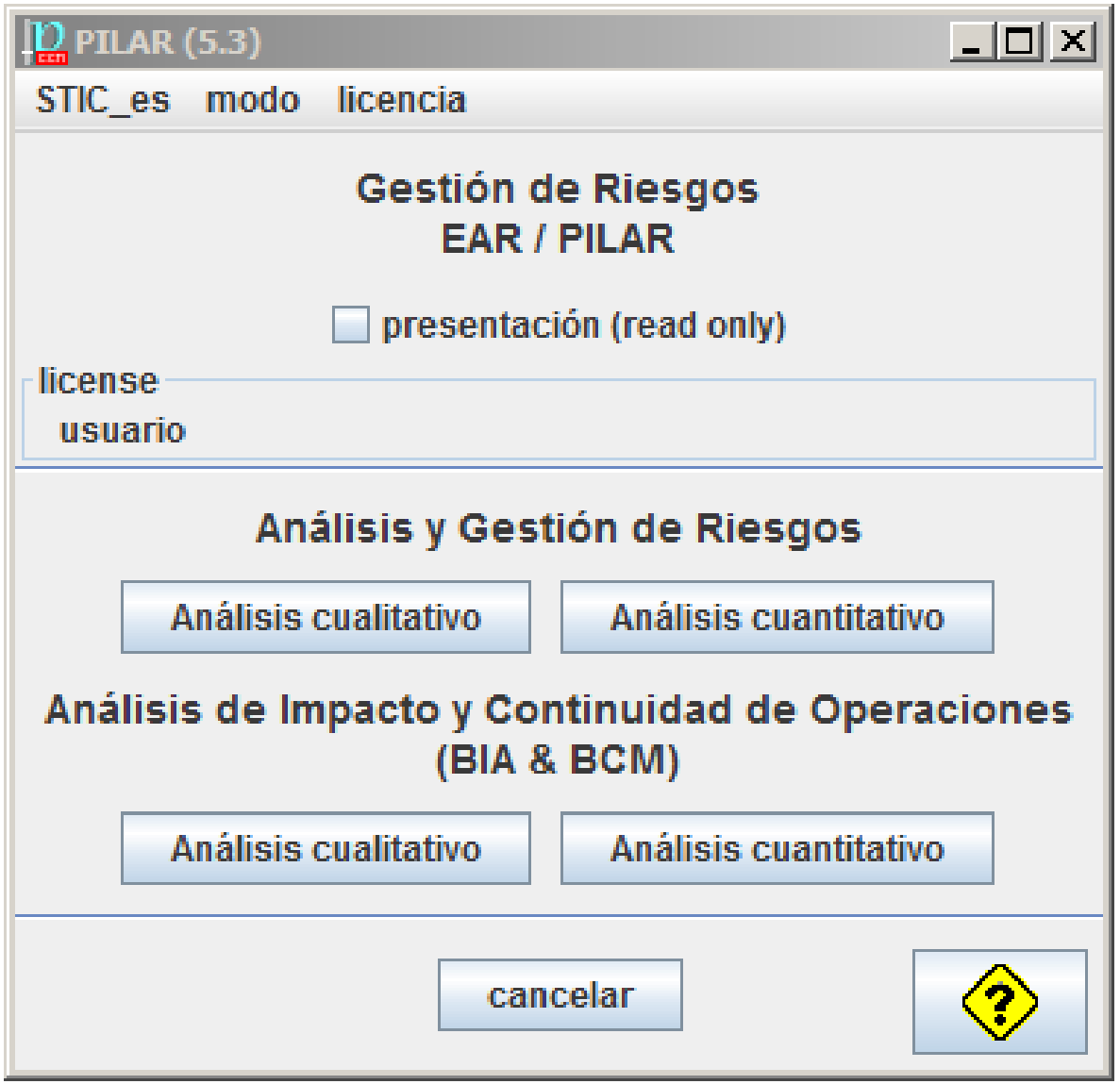


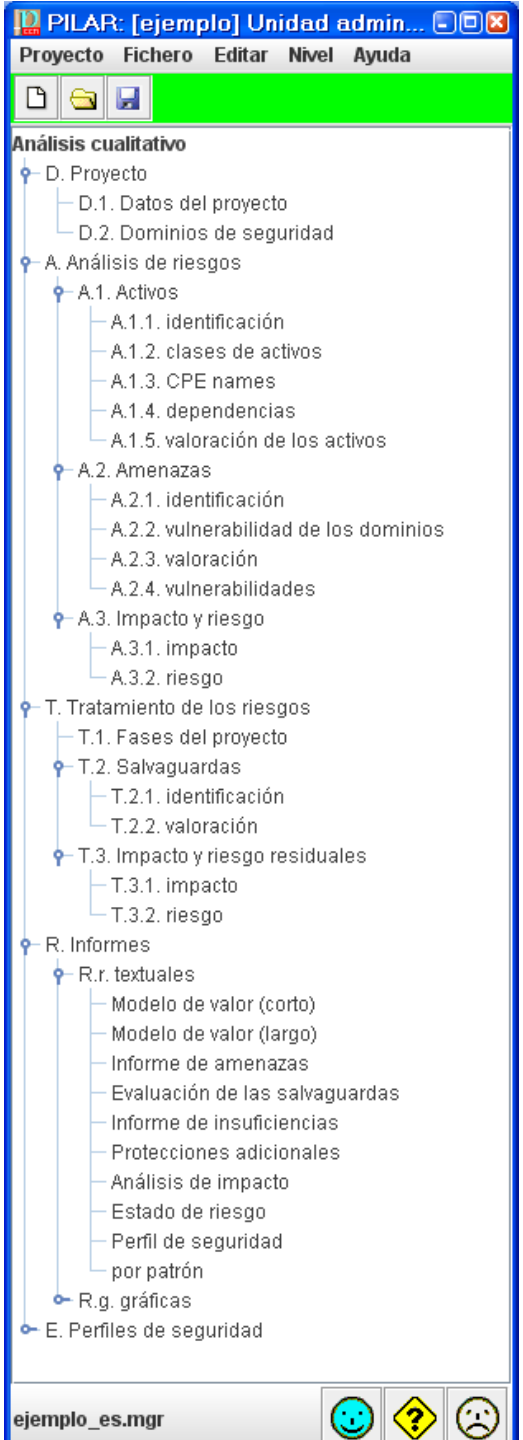
Informes

MAGERIT – versión 3.0
Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información

- Metodología elaborada y promovida por el Consejo Superior de Administración Electrónica (CSAE).
- Respuesta a la percepción de que la sociedad depende de forma creciente de las Tecnologías de la Información (TI) para la consecución de sus objetivos de servicio.
- Razón de ser de MAGERIT: la generalización del uso de los medios electrónicos, informáticos y telemáticos (MEIT) supone beneficios para los ciudadanos.

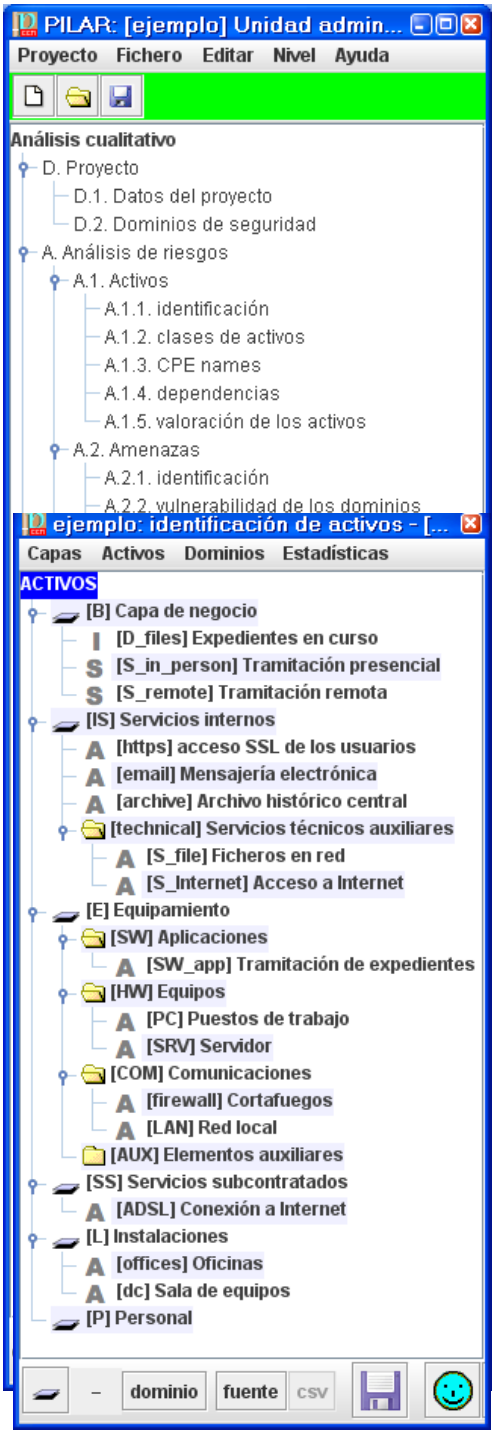
  Pero también da lugar a ciertos riesgos que deben minimizarse con medidas de seguridad que generen confianza en el uso de los MEIT.


PILAR (5.3)
STIC_es modo licencia
Gestión de Riesgos
EAR / PILAR
presentación (read only)
license
usuario
Análisis y Gestión de Riesgos
Análisis cualitativo
Análisis cuantitativo
Análisis de Impacto y Continuidad de Operaciones
(BIA & BCM)
Análisis cualitativo
Análisis cuantitativo
cancelar


PILAR: [ejemplo] Unidad admin...
Proyecto Fichero Editar Nivel Ayuda
Análisis cualitativo
D. Proyecto
D.1. Datos del proyecto
D.2. Dominios de seguridad
A. Análisis de riesgos
A.1. Activos
A.1.1. identificación
A.1.2. clases de activos
A.1.3. CPE names
A.1.4. dependencias
A.1.5. valoración de los activos
A.2. Amenazas
A.2.1. identificación
A.2.2. vulnerabilidad de los dominios
A.2.3. valoración
A.2.4. vulnerabilidades
A.3. Impacto y riesgo
A.3.1. impacto
A.3.2. riesgo
T. Tratamiento de los riesgos
T.1. Fases del proyecto
T.2. Salvaguardas
T.2.1. identificación
T.2.2. valoración
T.3. Impacto y riesgo residuales
T.3.1. impacto
T.3.2. riesgo
R. Informes
R.r. textuales
Modelo de valor (corto)
Modelo de valor (largo)
Informe de amenazas
Evaluación de las salvaguardas
Informe de insuficiencias
Protecciones adicionales
Análisis de impacto
Estado de riesgo
Perfil de seguridad
por patrón
R.g. gráficas
E. Perfiles de seguridad
ejemplo_es.mgr

Herramienta de AGR: PILAR

✓ La Herramienta **PILAR (Procedimiento Informático y Lógico de Análisis de Riesgos)**, desarrollada por el Centro Nacional de Inteligencia – Centro Criptológico Nacional, con la colaboración del MAP, tiene librerías que permiten aplicar Magerit versión 3 y realizar el análisis y la gestión de los riesgos en el marco de los Criterios.



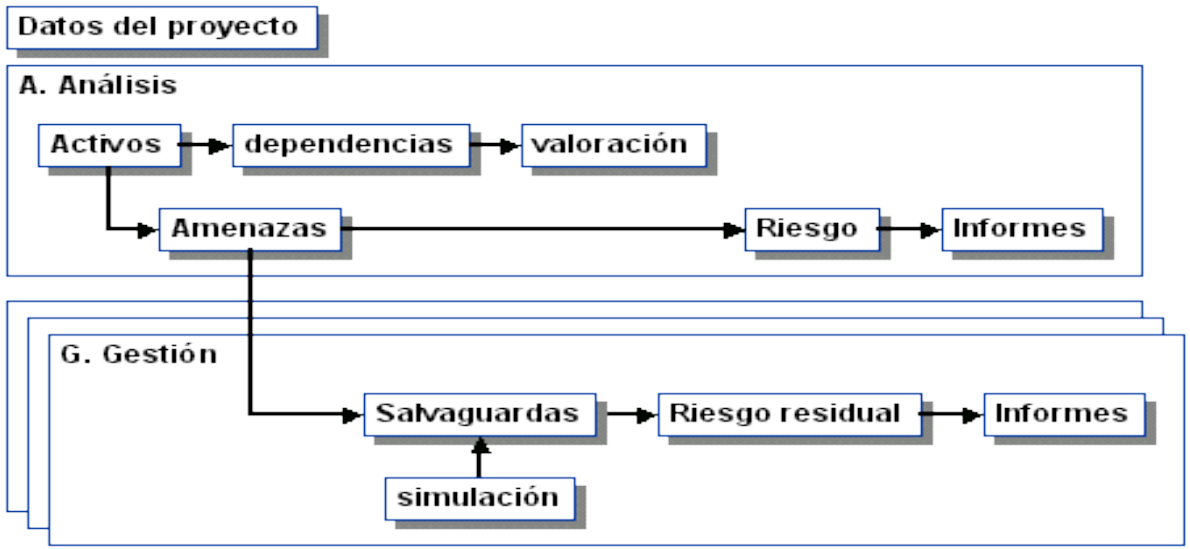
Herramienta PILAR:
PROCEDIMIENTO INFORMÁTICO Y LÓGICO DE ANÁLISIS DE RIESGOS

- **FACILIDAD DE USO.** Realización asistida del análisis y la gestión de los riesgos, de manera intuitiva y rápida.

- **FLEXIBILIDAD.** Utilizable a diferentes niveles de profundidad y de conocimiento de los usuarios.

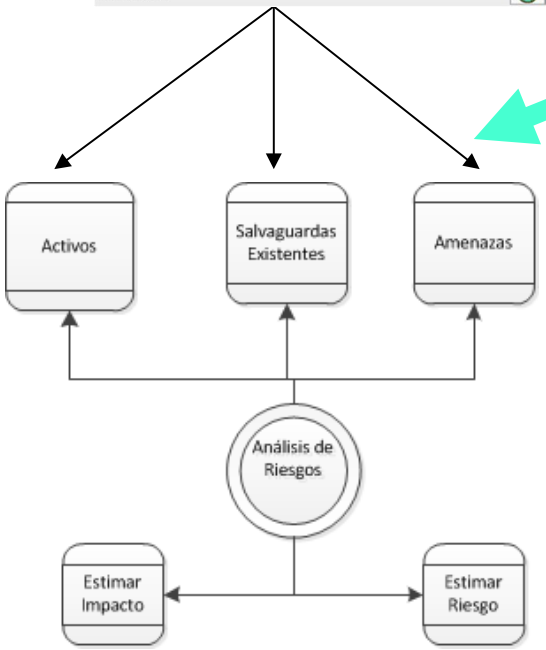
- **ADAPTACIÓN ENTORNO.** Posibilidad de generación y adaptación de bibliotecas (AAPP, OTAN, EMPRESAS).

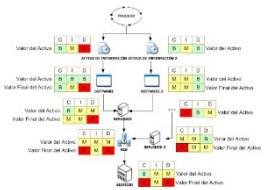
- **PRIORIZACIÓN SELECCIÓN SALVAGUARDAS.**



MAGERIT – versión 3.0
Metodología de Análisis y Gestión
de Riesgos de los Sistemas de Información

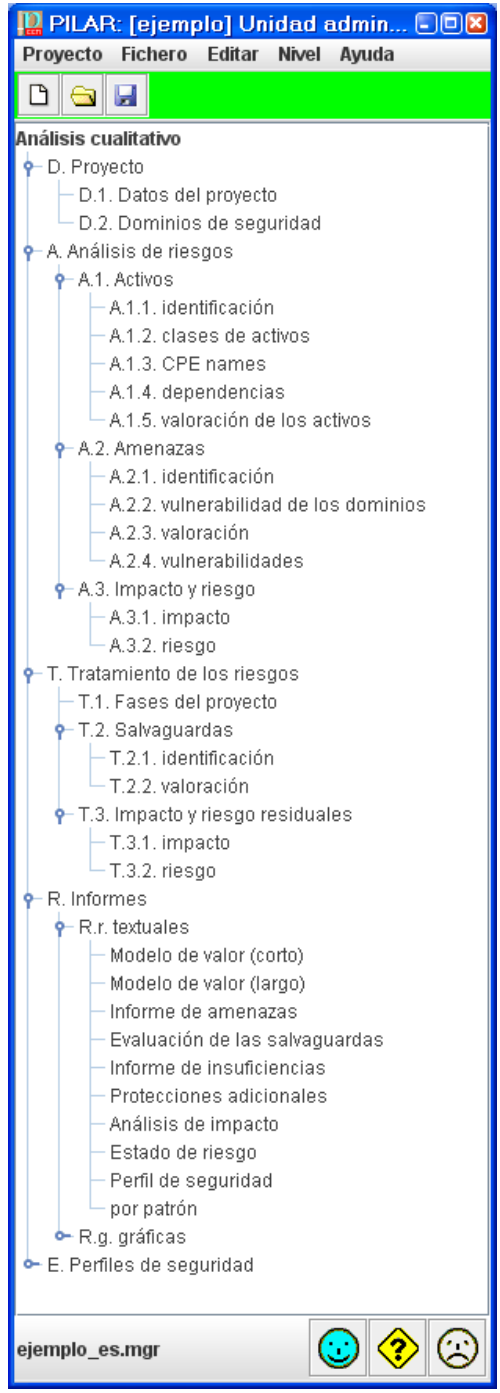
Proyecto





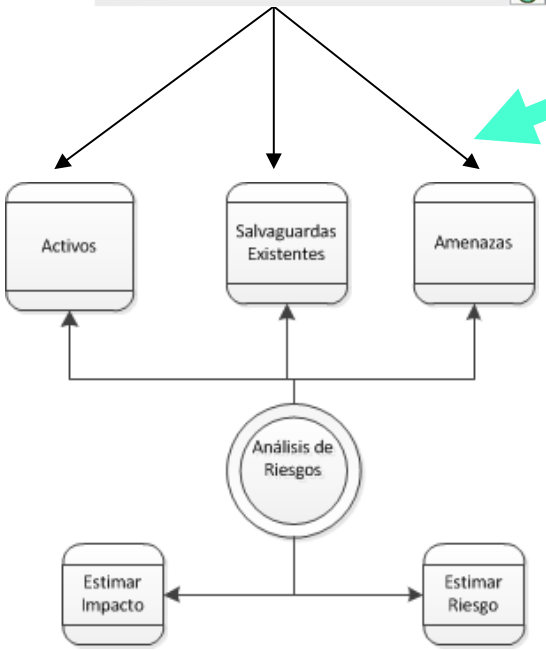
Informes

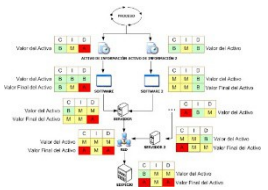

Datos del proyecto: ejemplo – usuario
1
2
3
4
biblioteca [std] Bib ca INFOSEC (23.3.2011) (std_52.pl5)
código ejemplo
nombre Unidad administrativa
informes - clasificación DIFUSIÓN LIMITADA
descripción Pequeña oficina de atención al ciudadano
propietario Juan García Iturriaga
organización MAP
versión 5.2
fecha 4.1.2012
arriba abajo nueva eliminar estándar limpiar
descripción


PILAR: [ejemplo] Unidad admin...
Proyecto Fichero Editar Nivel Ayuda
Análisis cualitativo
D. Proyecto
D.1. Datos del proyecto
D.2. Dominios de seguridad
A. Análisis de riesgos
A.1. Activos
A.1.1. identificación
A.1.2. clases de activos
A.1.3. CPE names
A.1.4. dependencias
A.1.5. valoración de los activos
A.2. Amenazas
A.2.1. identificación
A.2.2. vulnerabilidad de los dominios
A.2.3. valoración
A.2.4. vulnerabilidades
A.3. Impacto y riesgo
A.3.1. impacto
A.3.2. riesgo
T. Tratamiento de los riesgos
T.1. Fases del proyecto
T.2. Salvaguardas
T.2.1. identificación
T.2.2. valoración
T.3. Impacto y riesgo residuales
T.3.1. impacto
T.3.2. riesgo
R. Informes
R.r. textuales
Modelo de valor (corto)
Modelo de valor (largo)
Informe de amenazas
Evaluación de las salvaguardas
Informe de insuficiencias
Protecciones adicionales
Análisis de impacto
Estado de riesgo
Perfil de seguridad
por patrón
R.g. gráficas
E. Perfiles de seguridad
ejemplo_es.mgr

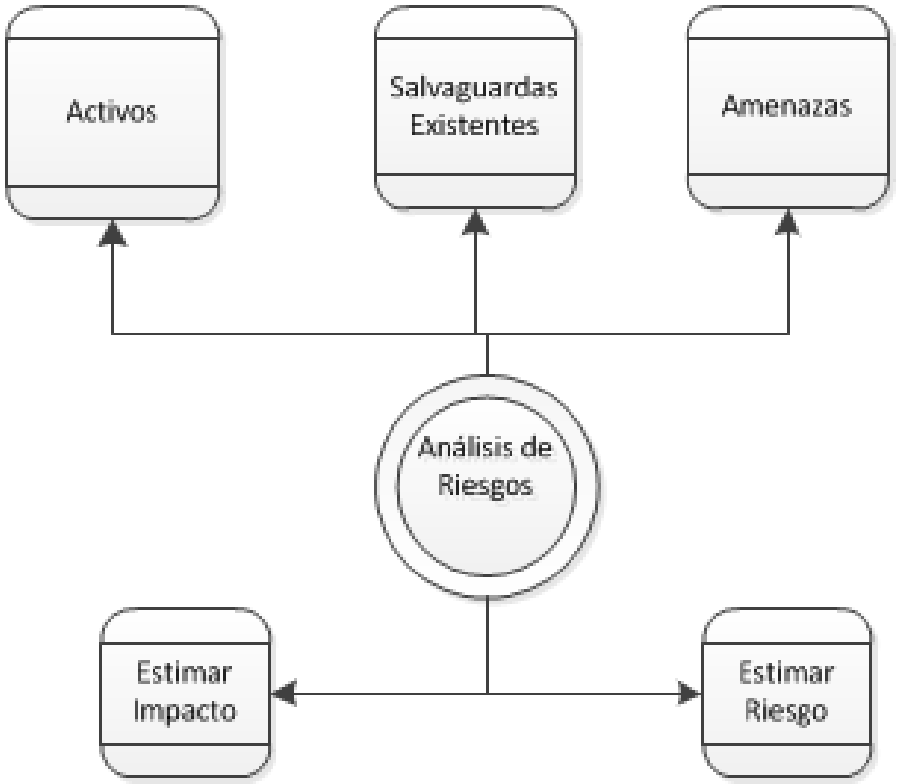
MAGERIT – versión 3.0
Metodología de Análisis y Gestión
de Riesgos de los Sistemas de Información

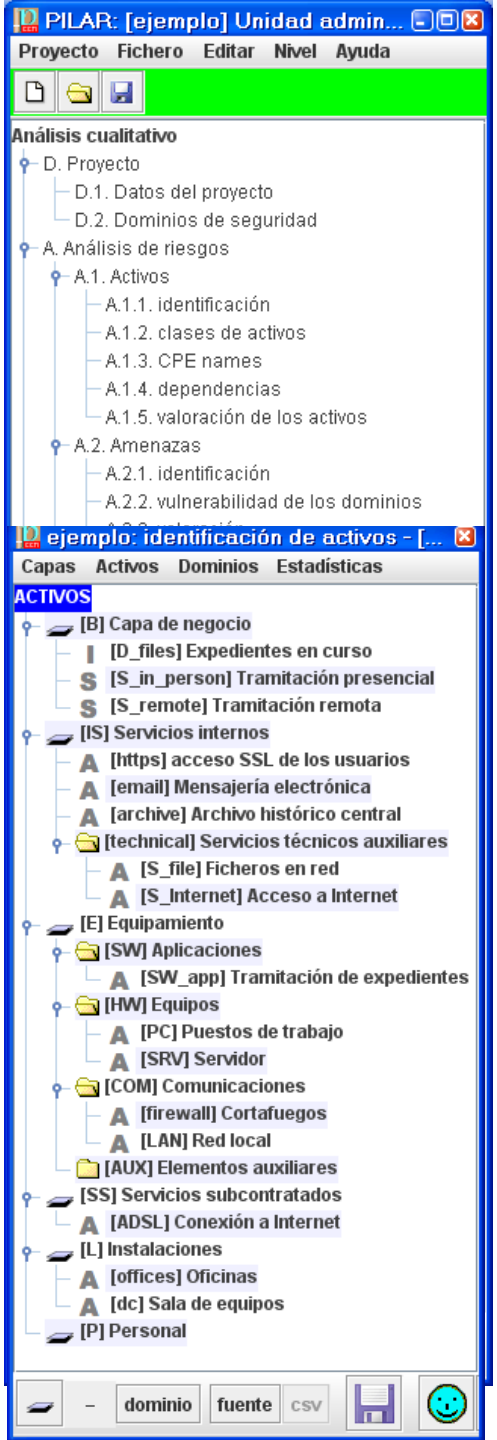
Proyecto





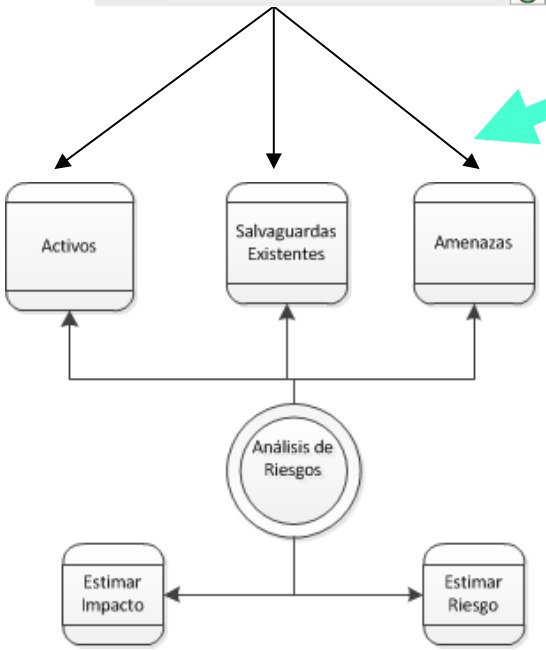
Informes

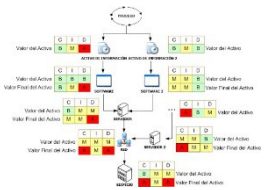

Activos
Salvaguardas Existentes
Amenazas
Análisis de Riesgos
Estimar Impacto
Estimar Riesgo


PILAR: [ejemplo] Unidad admin...
Proyecto Fichero Editar Nivel Ayuda
Análisis cualitativo
D. Proyecto
D.1. Datos del proyecto
D.2. Dominios de seguridad
A. Análisis de riesgos
A.1. Activos
A.1.1. identificación
A.1.2. clases de activos
A.1.3. CPE names
A.1.4. dependencias
A.1.5. valoración de los activos
A.2. Amenazas
A.2.1. identificación
A.2.2. vulnerabilidad de los dominios
ejemplo: identificación de activos - [...
Capas Activos Dominios Estadísticas
ACTIVOS
[B] Capa de negocio
[D_files] Expedientes en curso
[S_in_person] Tramitación presencial
[S_remote] Tramitación remota
[IS] Servicios internos
[https] acceso SSL de los usuarios
[email] Mensajería electrónica
[archive] Archivo histórico central
[technical] Servicios técnicos auxiliares
[S_file] Ficheros en red
[S_Internet] Acceso a Internet
[E] Equipamiento
[SW] Aplicaciones
[SW_app] Tramitación de expedientes
[HW] Equipos
[PC] Puestos de trabajo
[SRV] Servidor
[COM] Comunicaciones
[firewall] Cortafuegos
[LAN] Red local
[AUX] Elementos auxiliares
[SS] Servicios subcontratados
[ADSL] Conexión a Internet
[L] Instalaciones
[offices] Oficinas
[dc] Sala de equipos
[P] Personal
dominio
fuente
csv

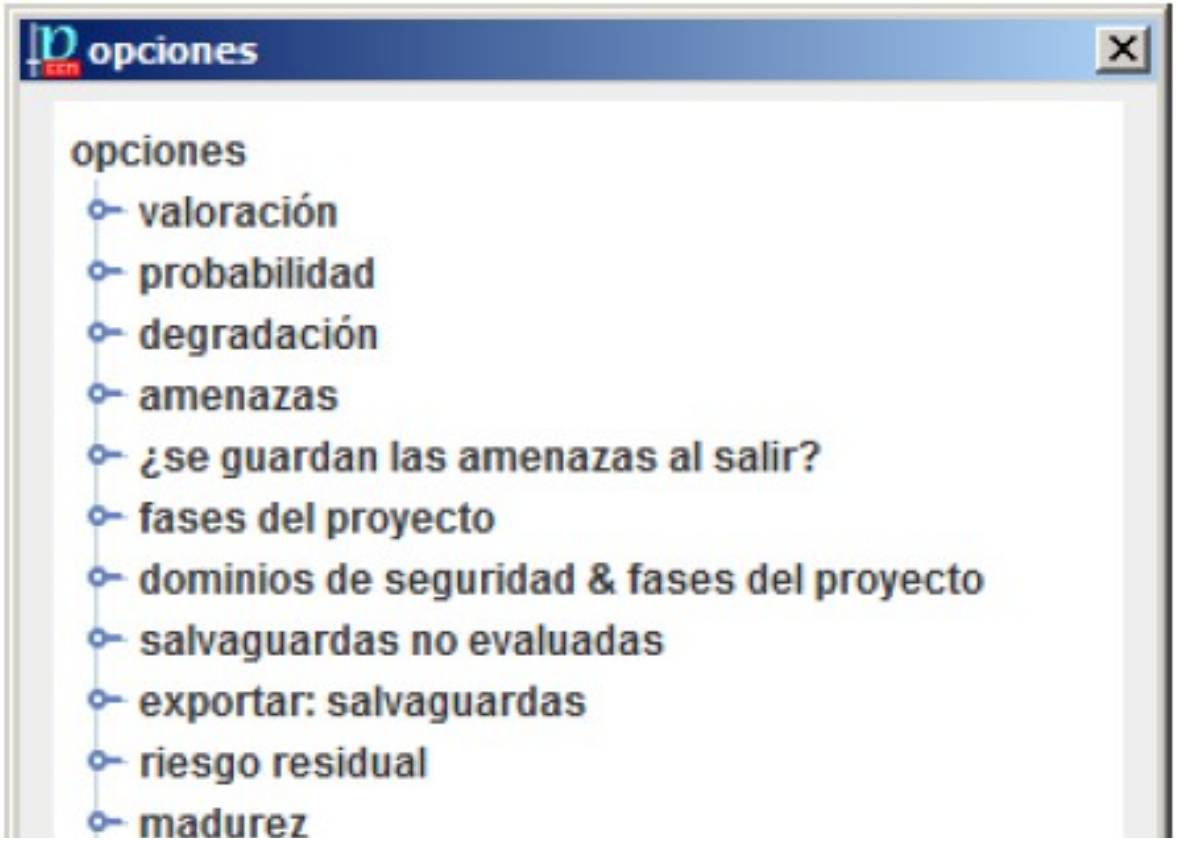
MAGERIT – versión 3.0
Metodología de Análisis y Gestión
de Riesgos de los Sistemas de Información

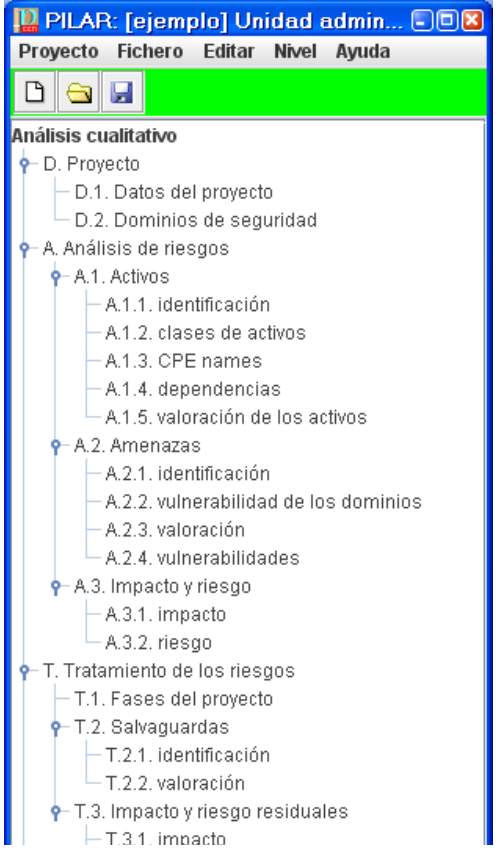
Proyecto





Informes





Opciones / Valoración

El sistema de información se puede valorar activo por activo (más dependencias) o por dominios de seguridad.

En ambos casos, se valoran los activos esenciales.

valoración / activos + dependencias

el valor de los activos esenciales se aplica a todos los activos del dominio de seguridad

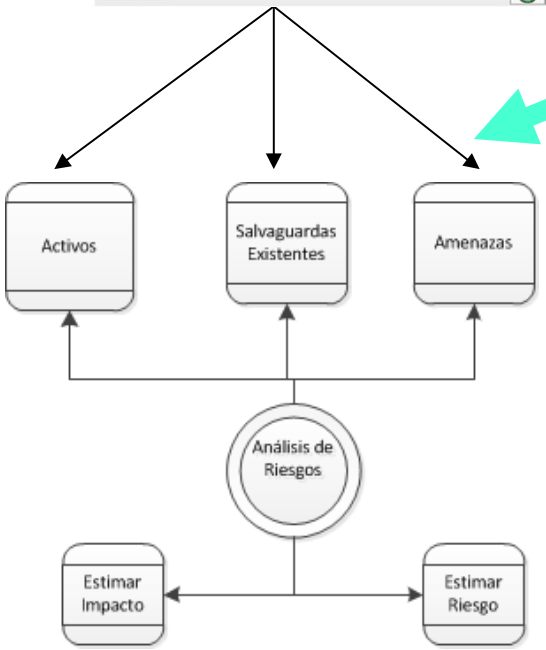
valoración / dominios

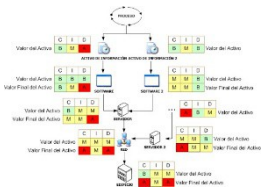
el valor se propaga siguiendo las dependencias entre activos

La valoración por dominios es más rápida, mientras que la valoración por dependencias es más precisa.

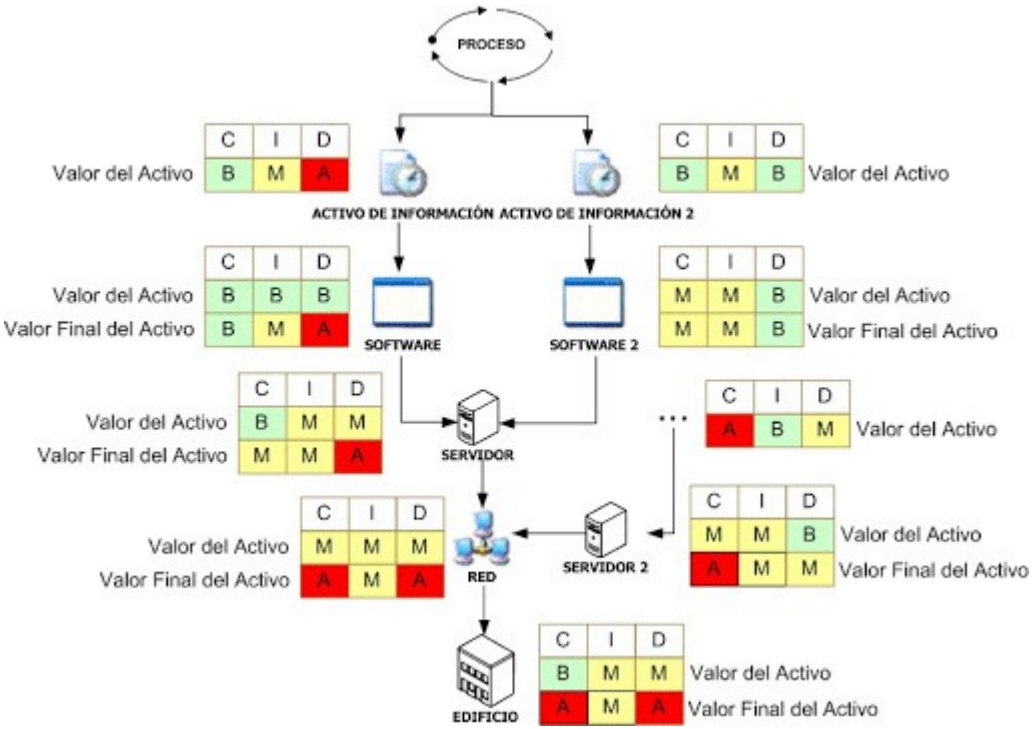
MAGERIT – versión 3.0
Metodología de Análisis y Gestión
de Riesgos de los Sistemas de Información

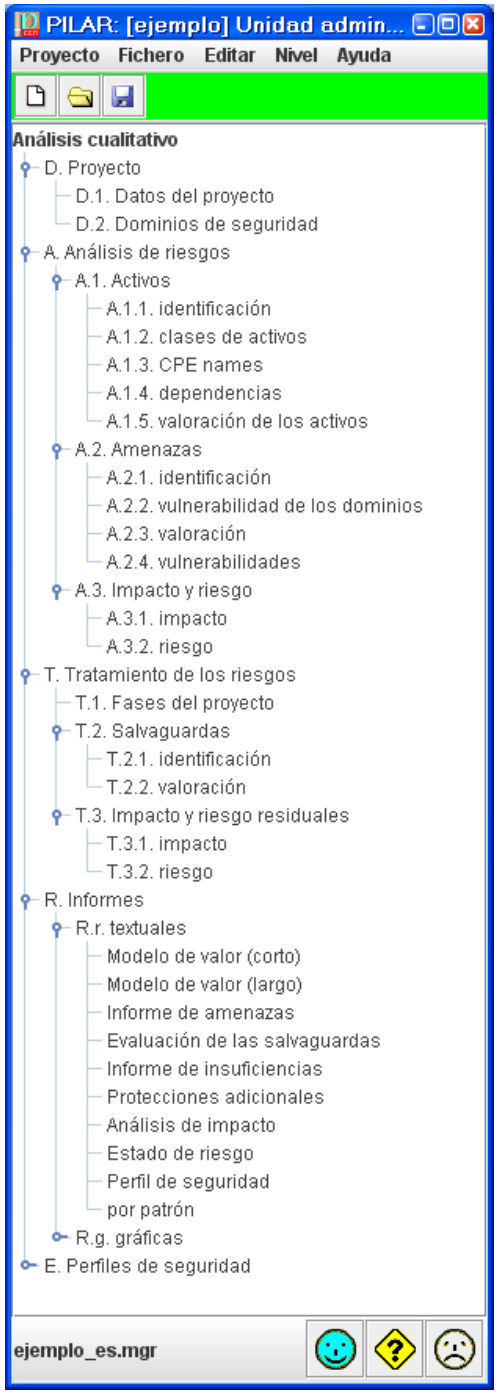
Proyecto





Informes

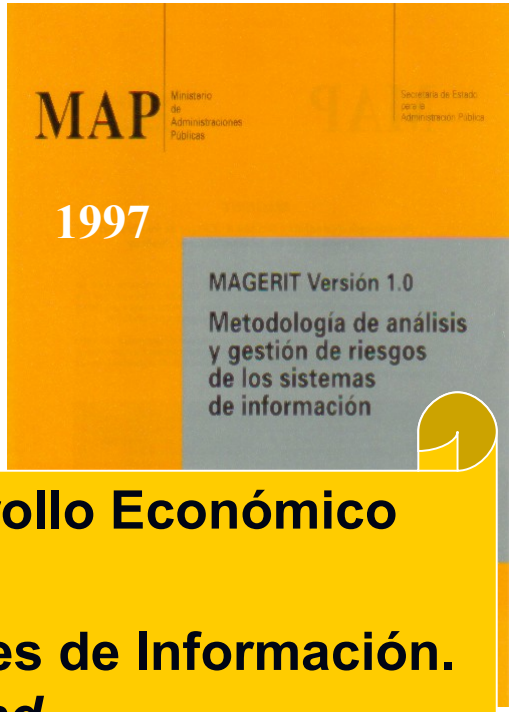

PROCESO
C I D
B M A
Valor del Activo
ACTIVO DE INFORMACIÓN
C I D
B M B
Valor del Activo
ACTIVO DE INFORMACIÓN 2
C I D
B B B
Valor del Activo
B M A
Valor Final del Activo
SOFTWARE
SOFTWARE 2
C I D
M M B
Valor del Activo
M M B
Valor Final del Activo
C I D
B M M
Valor del Activo
M M A
Valor Final del Activo
SERVIDOR
C I D
A B M
Valor del Activo
SERVIDOR 2
C I D
M M M
Valor del Activo
A M A
Valor Final del Activo
RED
C I D
M M B
Valor del Activo
A M M
Valor Final del Activo
EDIFICIO
C I D
B M M
Valor del Activo
A M A
Valor Final del Activo


PILAR: [ejemplo] Unidad admin...
Proyecto Fichero Editar Nivel Ayuda
Análisis cualitativo
D. Proyecto
D.1. Datos del proyecto
D.2. Dominios de seguridad
A. Análisis de riesgos
A.1. Activos
A.1.1. identificación
A.1.2. clases de activos
A.1.3. CPE names
A.1.4. dependencias
A.1.5. valoración de los activos
A.2. Amenazas
A.2.1. identificación
A.2.2. vulnerabilidad de los dominios
A.2.3. valoración
A.2.4. vulnerabilidades
A.3. Impacto y riesgo
A.3.1. impacto
A.3.2. riesgo
T. Tratamiento de los riesgos
T.1. Fases del proyecto
T.2. Salvaguardas
T.2.1. identificación
T.2.2. valoración
T.3. Impacto y riesgo residuales
T.3.1. impacto
T.3.2. riesgo
R. Informes
R.r. textuales
Modelo de valor (corto)
Modelo de valor (largo)
Informe de amenazas
Evaluación de las salvaguardas
Informe de insuficiencias
Protecciones adicionales
Análisis de impacto
Estado de riesgo
Perfil de seguridad
por patrón
R.g. gráficas
E. Perfiles de seguridad
ejemplo_es.mgr

Magerit v.3: Introducción

- Método
- Catálogo de Elementos
- Guía de Técnicas

Magerit
Versión 2
2005



Organización para la Cooperación y el Desarrollo Económico (OCDE)

Directrices para la seguridad de sistemas y redes de Información.
***Hacia una cultura de la seguridad*.**
Junio 2002
Principio 6: *Evaluación del riesgo.*
Los participantes deben llevar a cabo evaluaciones de riesgo.

Magerit v.3: Introducción

- Metodología que interesa a los que trabajan con sistemas de información para tratar información y prestar servicios.
- Como **conocer su riesgo** es imprescindible y por ello han aparecido multitud de guías informales, aproximaciones metódicas y herramientas de soporte que buscan objetivar el análisis para saber cuán seguros (o inseguros) están.
- El **gran reto** de estas aproximaciones: la **complejidad** del problema. Hay muchos elementos que considerar y hay que ser riguroso.
- MAGERIT persigue una **aproximación metódica** que no deje lugar a la improvisación, ni dependa de la arbitrariedad del analista.

Magerit v.3: Introducción

• **Inquietud por la seguridad de los SI** en los que descansan graves responsabilidades para cumplir los objetivos de las organizaciones.

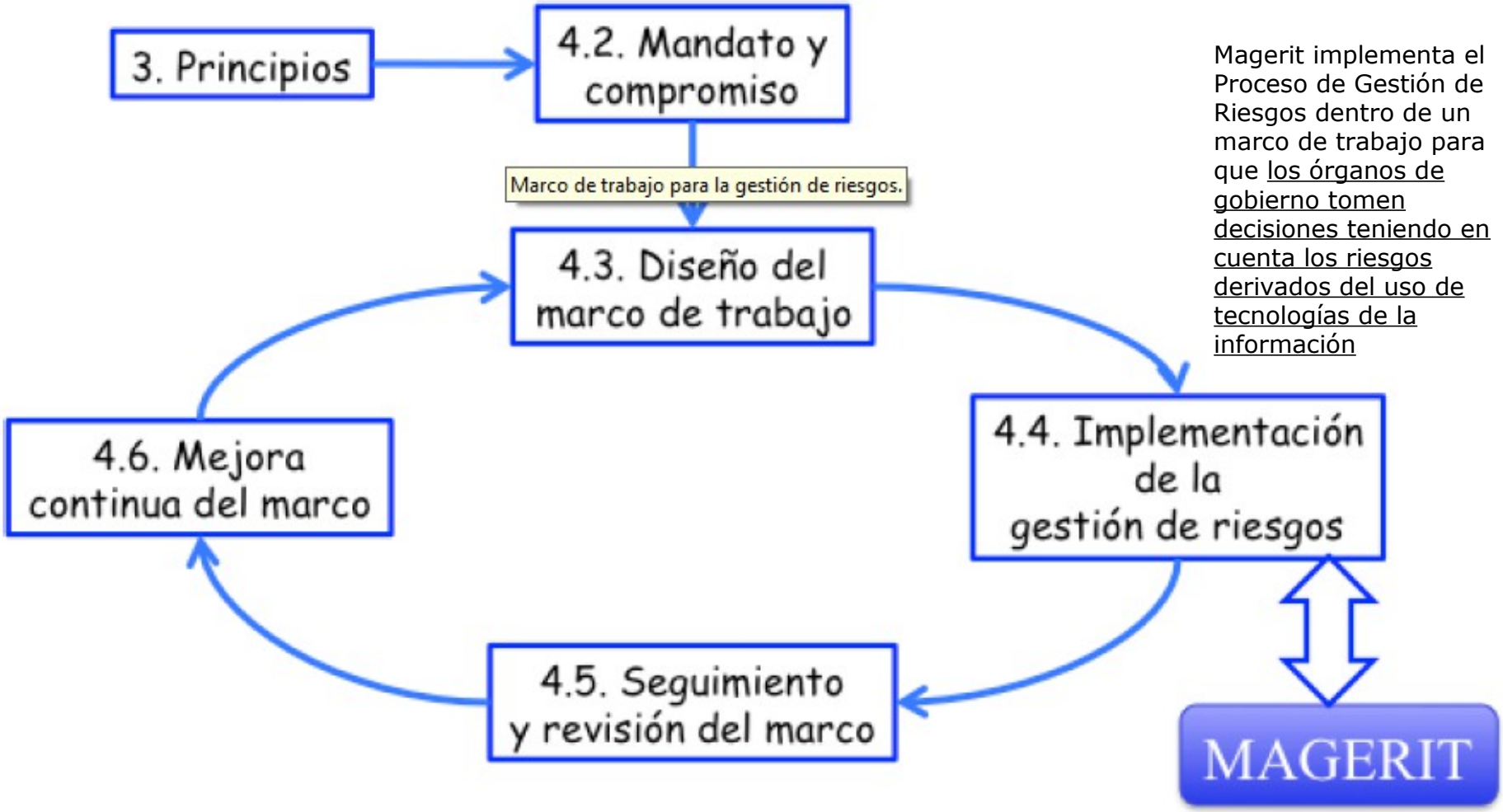
• Los **usuarios** (que no son técnicos) se preguntan **si estos sistemas merecen su confianza**, que se ve mermada por cada fallo, y más cuando las inversiones no se traducen en ausencia de fallos.

• **Se acepta convivir con sistemas que fallan.**

• *El asunto no es la ausencia de incidentes sino la* ***confianza de que están bajo control****: saber qué puede pasar y saber qué hacer cuando pasa.*

• El temor a lo desconocido es el principal origen de la desconfianza. Conocer para confiar: **conocer los riesgos** para poder afrontarlos y controlarlos.

Magerit v.3: Introducción



Magerit implementa el Proceso de Gestión de Riesgos dentro de un marco de trabajo para que los órganos de gobierno tomen decisiones teniendo en cuenta los riesgos derivados del uso de tecnologías de la información

Ilustración 1. ISO 31000 - Marco de trabajo para la gestión de riesgos

Magerit: Objetivos

Directos

- **Concienciar** a los responsables de los sistemas de información de la existencia de riesgos y de la necesidad de gestionarlos
- Ofrecer un **método sistemático** para analizar tales riesgos
- Ayudar a descubrir y planificar las medidas oportunas para **mantener los riesgos bajo control**

Indirectos

- Preparar a la Organización para procesos de **evaluación, auditoría, certificación o acreditación,** según corresponda en cada caso

Magerit: Objetivos

Uniformidad de los informes que recogen los hallazgos y conclusiones de un proyecto de Análisis y Gestión de Riesgos

Modelo de valor

Caracterización del valor que representan los activos para la Organización así como de las dependencias entre los diferentes activos.

Mapa de riesgos

Relación de las amenazas a que están expuestos los activos.

Evaluación de salvaguardas

Evaluación de la eficacia de las salvaguardas existentes en relación al riesgo que afrontan.

Estado de riesgo

Caracterización de los activos por su riesgo residual; es decir, por lo que puede pasar tomando en consideración las salvaguardas desplegadas.

Informe de insuficiencias

Ausencia o debilidad de las salvaguardas que aparecen como oportunas para reducir los riesgos sobre el sistema.

Plan de seguridad

Conjunto de programas de seguridad que permiten materializar las decisiones de gestión de riesgos

Dimensiones

De un activo puede interesar calibrar diferentes dimensiones:

- su **autenticidad:** ¿qué perjuicio causaría no saber exactamente quien hace o ha hecho cada cosa?

  Esta valoración es típica de servicios (autenticidad del usuario) y de los datos (autenticidad de quien accede a los datos para escribir o, simplemente, consultar)

- su **confidencialidad**: ¿qué daño causaría que lo conociera quien no debe?

  Esta valoración es típica de datos.

- su **integridad**: ¿qué perjuicio causaría que estuviera dañado o corrupto?

  Esta valoración es típica de los datos, que pueden estar manipulados, ser total o parcialmente falsos o, incluso, faltar datos.

- su **disponibilidad**: ¿qué perjuicio causaría no tenerlo o no poder utilizarlo?

  Esta valoración es típica de los servicios[13].

En sistemas dedicados a la administración electrónica o al comercio electrónico, el conocimiento de los actores es fundamental para poder prestar el servicio correctamente y poder perseguir los fallos (accidentales o deliberados) que pudieran darse. En estos activos, además de la autenticidad, interesa calibrar la:

- la **trazabilidad** del uso del servicio: ¿qué daño causaría no saber a quién se le presta tal servicio? O sea, ¿quién hace qué y cuándo?
- la **trazabilidad** del acceso a los datos: ¿qué daño causaría no saber quién accede a qué datos y qué hace con ellos?

Dimensiones de la seguridad

Dimensión (de seguridad): Un aspecto, diferenciado de otros posibles aspectos, respecto del que podemos medir el valor de un activo en el sentido del perjuicio que nos causaría su pérdida de valor.

Disponibilidad: o disposición a ser usados cuando sea necesario. La carencia de disponibilidad supone una interrupción del servicio. **La disponibilidad afecta directamente a la productividad de las organizaciones**.

Integridad: o mantenimiento de las características de completitud y corrección de los datos. Contra la integridad podemos encontrarnos información manipulada, corrupta o incompleta. **La integridad afecta directamente al correcto desempeño de las funciones de una Organización**.

Confidencialidad: o que la información llegue solamente a las personas autorizadas. Contra la confidencialidad o secreto nos encontraremos con fugas y filtraciones de información, así como con accesos no autorizados. La confidencialidad es una **propiedad de difícil recuperación**, pudiendo minar la confianza de los demás en la organización que no es diligente en el mantenimiento del secreto, y pudiendo suponer el incumplimiento de leyes y compromisos contractuales relativos a la custodia de los datos.

Dimensiones de la seguridad

Autenticidad (de quién hace uso de los datos o servicios): o que no haya duda de quién se hace responsable de una información o prestación de un servicio, tanto a fin de confiar en él como de poder perseguir posteriormente los incumplimientos o errores.

- Contra la autenticidad nos encontramos con suplantaciones y engaños que buscan realizar un fraude.
- La autenticidad es la base para poder luchar contra el **repudio** y, como tal, se convierte en una dimensión básica para fundamentar el llamado **comercio electrónico** o la **administración electrónica**, permitiendo confiar sin papeles ni presencia física.

Trazabilidad. Aseguramiento de que en todo momento se podrá determinar quién hizo qué y en qué momento.

- La trazabilidad es esencial para analizar los incidentes,
- Perseguir a los atacantes y
- Aprender de la experiencia.
- La trazabilidad se materializa en la integridad de los registros de actividad.

Introducción al AGR

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

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

Tratamiento de los riesgos: proceso destinado a modificar el riesgo.

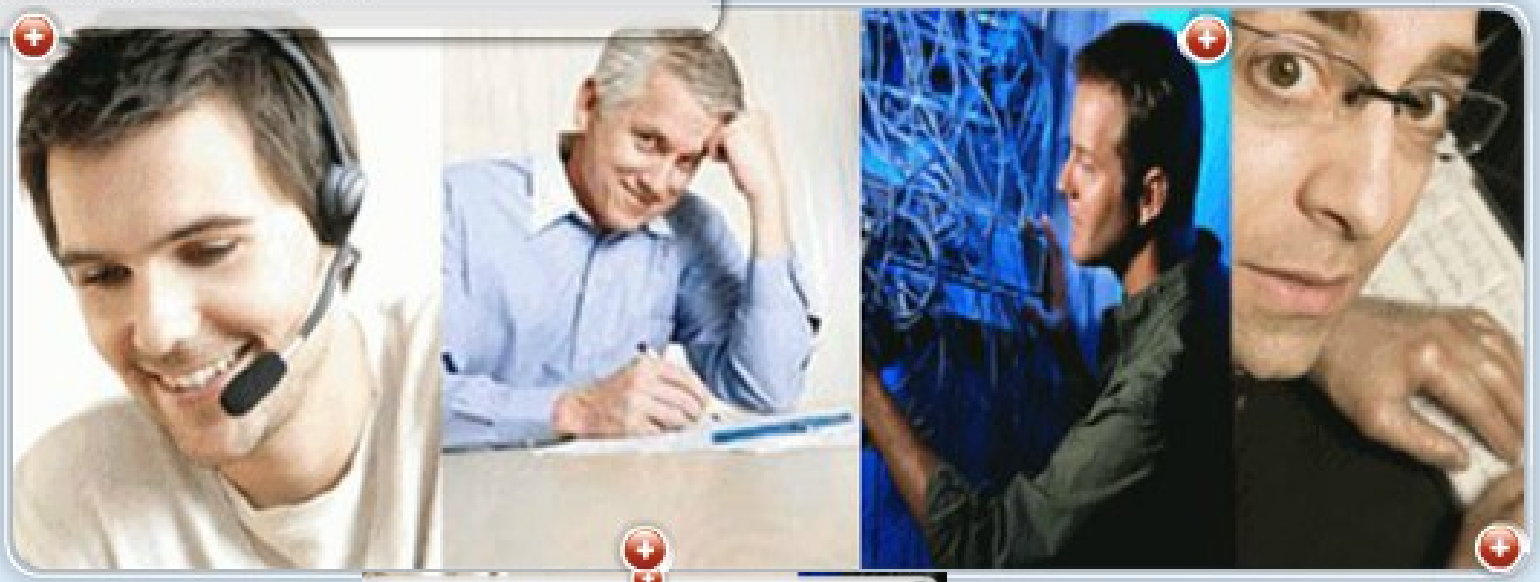
Percepción del riesgo

Usuario

Los **usuarios** del sistema informático ven la **seguridad como confianza.**

Tecnicos

Los **técnicos** ven la seguridad como **componentes, dispositivos, software, ...**



Gestores

Los **gestores** ven la seguridad como **gestión de riesgos.**

Atacantes

Los **atacantes** ven la seguridad como **aquello que impide sus objetivos.**

Organización de la guía

- **Método**
- **Catálogo de Elementos**
- **Guía de Técnicas**

- MAGERIT – versión 3.0. Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. Libro I - Método
  - Créditos
  - Índice
  - 1. Introducción
  - 2. Visión de conjunto
  - 3. Método de análisis de riesgos
  - 4. Proceso de gestión de riesgos
  - 5. Proyectos de análisis de riesgos
  - 6. Plan de seguridad
  - 7. Desarrollo de sistemas de información
  - 8. Consejos prácticos
  - Apéndice 1. Glosario
  - Apéndice 2. Referencias
  - Apéndice 3. Marco legal
  - Apéndice 4. Marco de evaluación y certificación
  - Apéndice 5. Herramientas
  - Apéndice 6. Evolución de Magerit

El capítulo 2 presenta los conceptos informalmente. En particular se enmarcan las actividades de análisis y tratamiento dentro de un proceso integral de gestión de riesgos.

El capítulo 3 concreta los pasos y formaliza las actividades de análisis de los riesgos.

El capítulo 4 describe opciones y criterios de tratamiento de los riesgos y formaliza las actividades de gestión de riesgos.

El capítulo 5 se centra en los proyectos de análisis de riesgos, proyectos en los que nos veremos inmersos para realizar el primer análisis de riesgos de un sistema y eventualmente cuando hay cambios sustanciales y hay que rehacer el modelo ampliamente.

- MAGERIT – versión 3.0. Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. Libro I - Método
  - Créditos
  - Índice
  - 1. Introducción
  - 2. Visión de conjunto
  - 3. Método de análisis de riesgos
  - 4. Proceso de gestión de riesgos
  - 5. Proyectos de análisis de riesgos
  - 6. Plan de seguridad
  - 7. Desarrollo de sistemas de información
  - 8. Consejos prácticos
  - Apéndice 1. Glosario
  - Apéndice 2. Referencias
  - Apéndice 3. Marco legal
  - Apéndice 4. Marco de evaluación y certificación
  - Apéndice 5. Herramientas
  - Apéndice 6. Evolución de Magerit

El capítulo 6 formaliza las actividades de los planes de seguridad, a veces denominados planes directores o planes estratégicos.

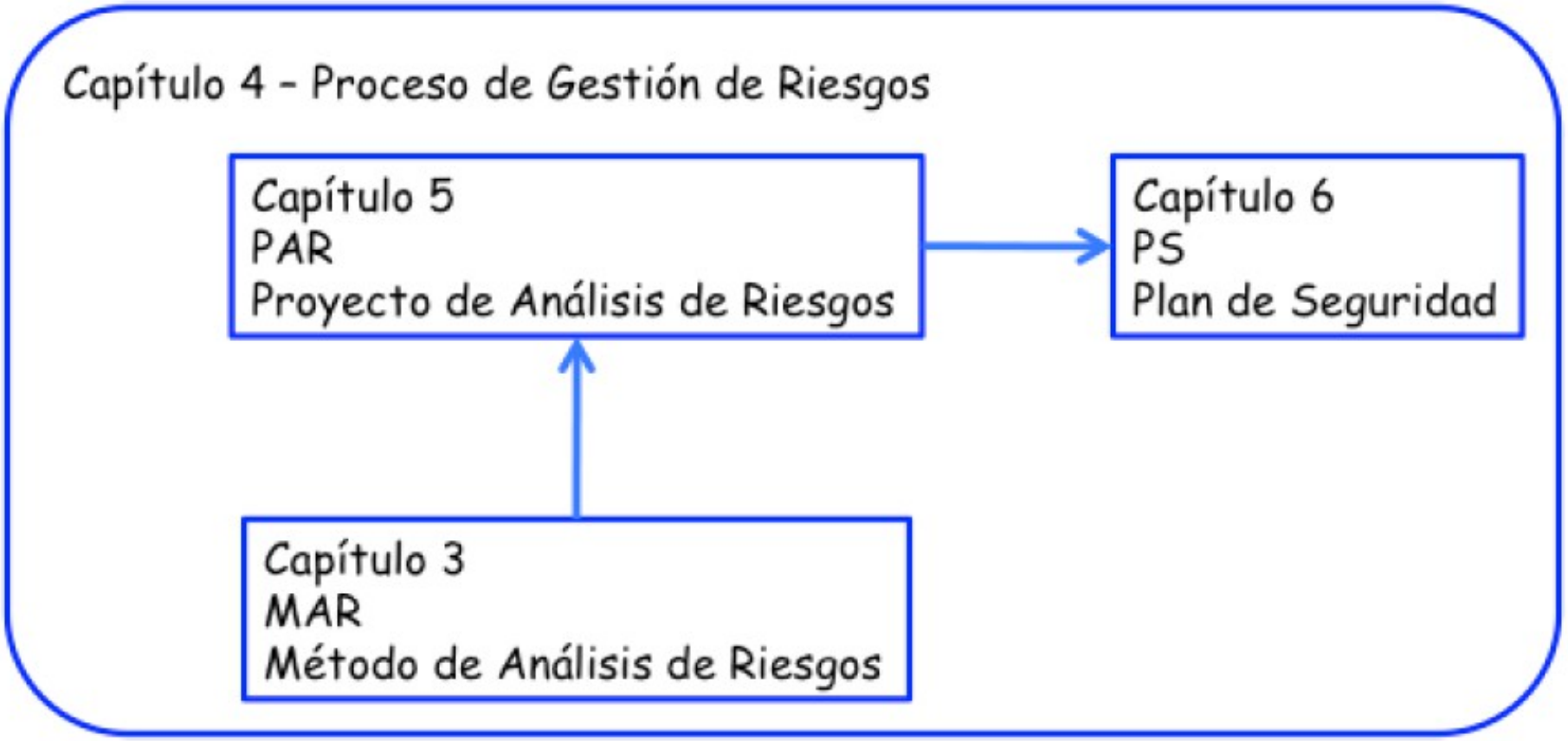
El capítulo 7 se centra en el desarrollo de sistemas de información y cómo el análisis de riesgos sirve para gestionar la seguridad del producto final desde su concepción inicial hasta su puesta en producción, así como a la protección del propio proceso de desarrollo.

El capítulo 8 se anticipa a algunos problemas que aparecen recurrentemente cuando se realizan análisis de riesgos.

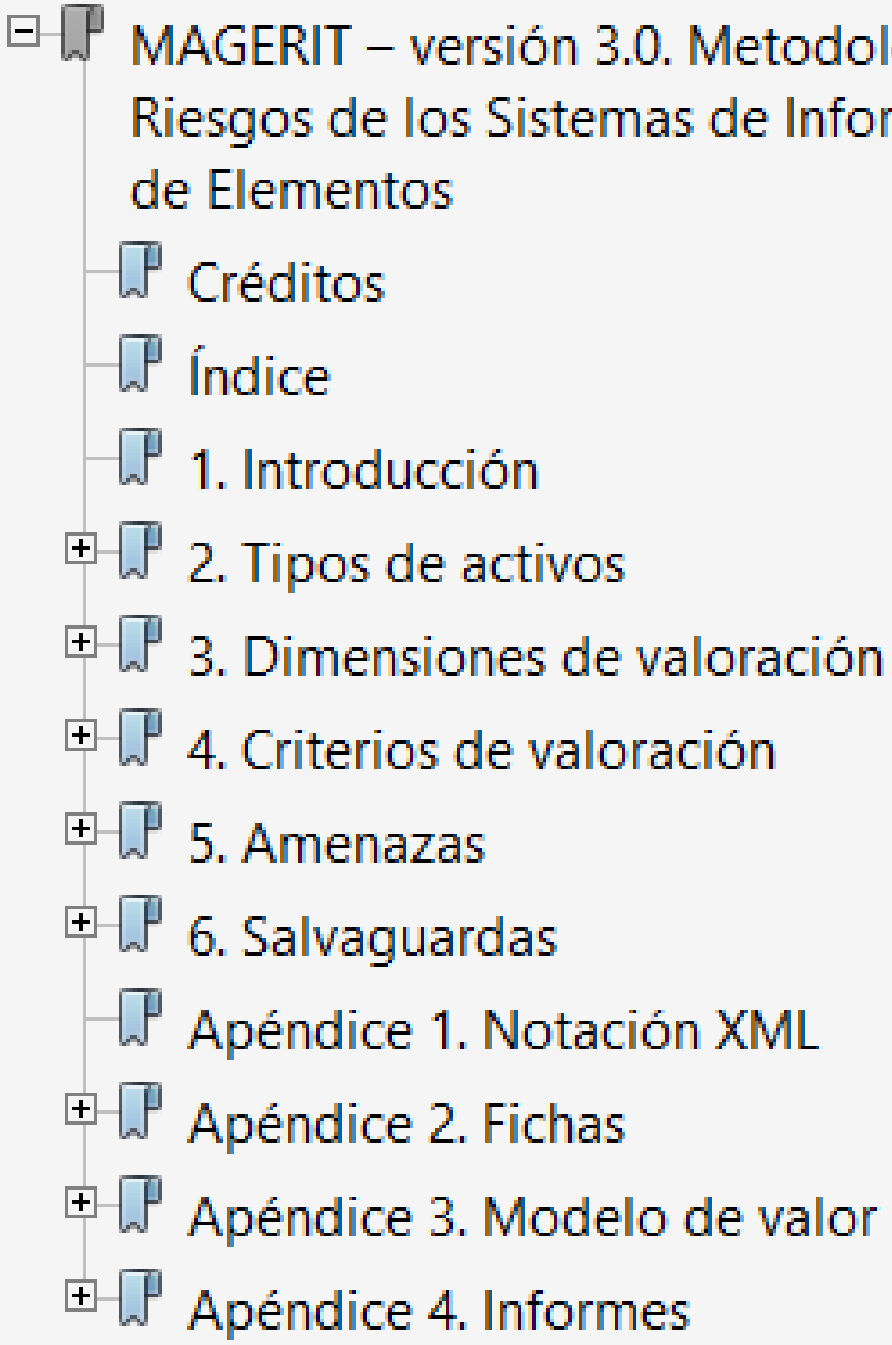
- MAGERIT – versión 3.0. Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. Libro I - Método
  - Créditos
  - Índice
  - 1. Introducción
  - 2. Visión de conjunto
  - 3. Método de análisis de riesgos
  - 4. Proceso de gestión de riesgos
  - 5. Proyectos de análisis de riesgos
  - 6. Plan de seguridad
  - 7. Desarrollo de sistemas de información
  - 8. Consejos prácticos
  - Apéndice 1. Glosario
  - Apéndice 2. Referencias
  - Apéndice 3. Marco legal
  - Apéndice 4. Marco de evaluación y certificación
  - Apéndice 5. Herramientas
  - Apéndice 6. Evolución de Magerit

- Apéndice:
  - 1. un glosario
  - 2. referencias bibliográficas consideradas para el desarrollo de esta metodología,
  - 3. referencias al marco legal que encuadra las tareas de análisis y gestión en la Administración Pública Española,
  - 4. el marco normativo de evaluación y certificación
  - 5. las características que se requieren de las herramientas, presentes o futuras, para soportar el proceso de análisis y gestión de riesgos,
  - 6. una guía comparativa de cómo Magerit versión 1 ha evolucionado a la versión 2 y a esta versión 3.

Modo de empleo

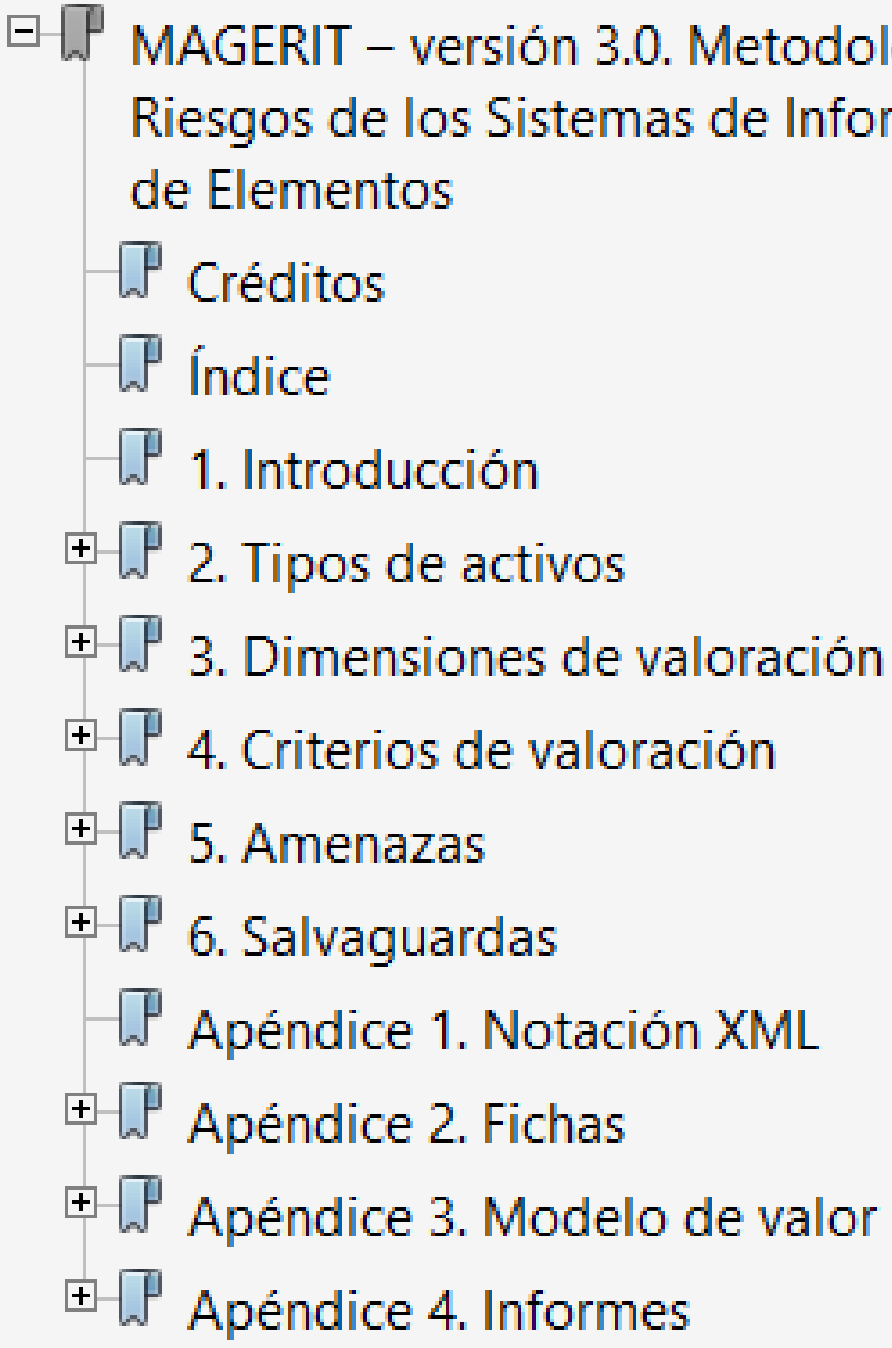


Actividades formalizadas



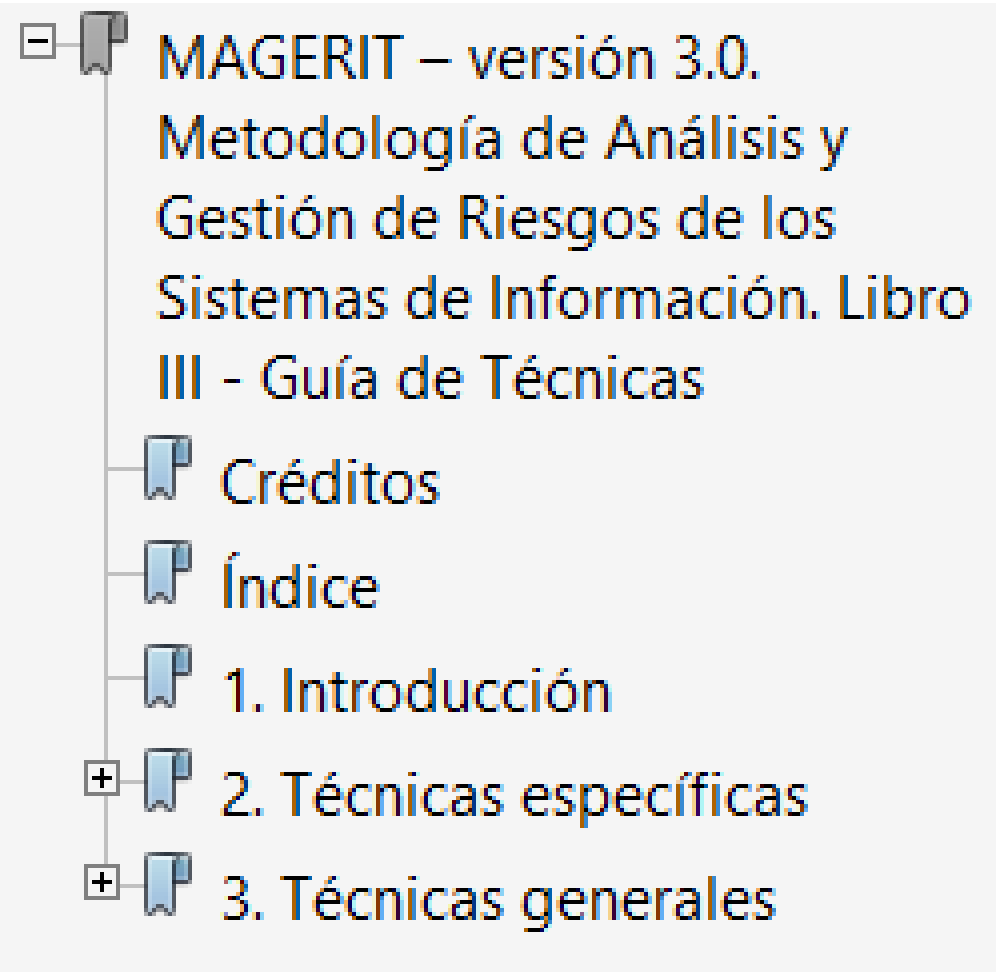
Se ocupa de los tipos de **activos**, dimensiones de **valoración** de los activos, criterios de valoración de los activos, **amenazas** típicas sobre los sistemas de información y **salvaguardas** para proteger sistemas de información, con el doble objetivo de:

- Facilitar la labor, ofreciendo elementos estándar a los que puedan adscribirse rápidamente, para así centrarse en lo específico del sistema objeto del análisis.
- Homogeneizar los resultados de los análisis, promoviendo una terminología y unos criterios uniformes que permitan comparar e incluso integrar análisis realizados por diferentes equipos.



- Cada sección incluye una **notación XML** que se empleará para publicar regularmente los elementos en un formato estándar capaz de ser procesado automáticamente por herramientas de análisis y gestión.
- El catálogo proporciona una extensa **referencia de los objetos** del AGR, lo cual facilita avanzar con rapidez, evitando distracciones u olvidos.
- El catálogo forma **parte de las herramientas** de apoyo del AGR
- **Abierto** a futuras actualizaciones o ampliaciones

Magerit versión 3: La guía de técnicas



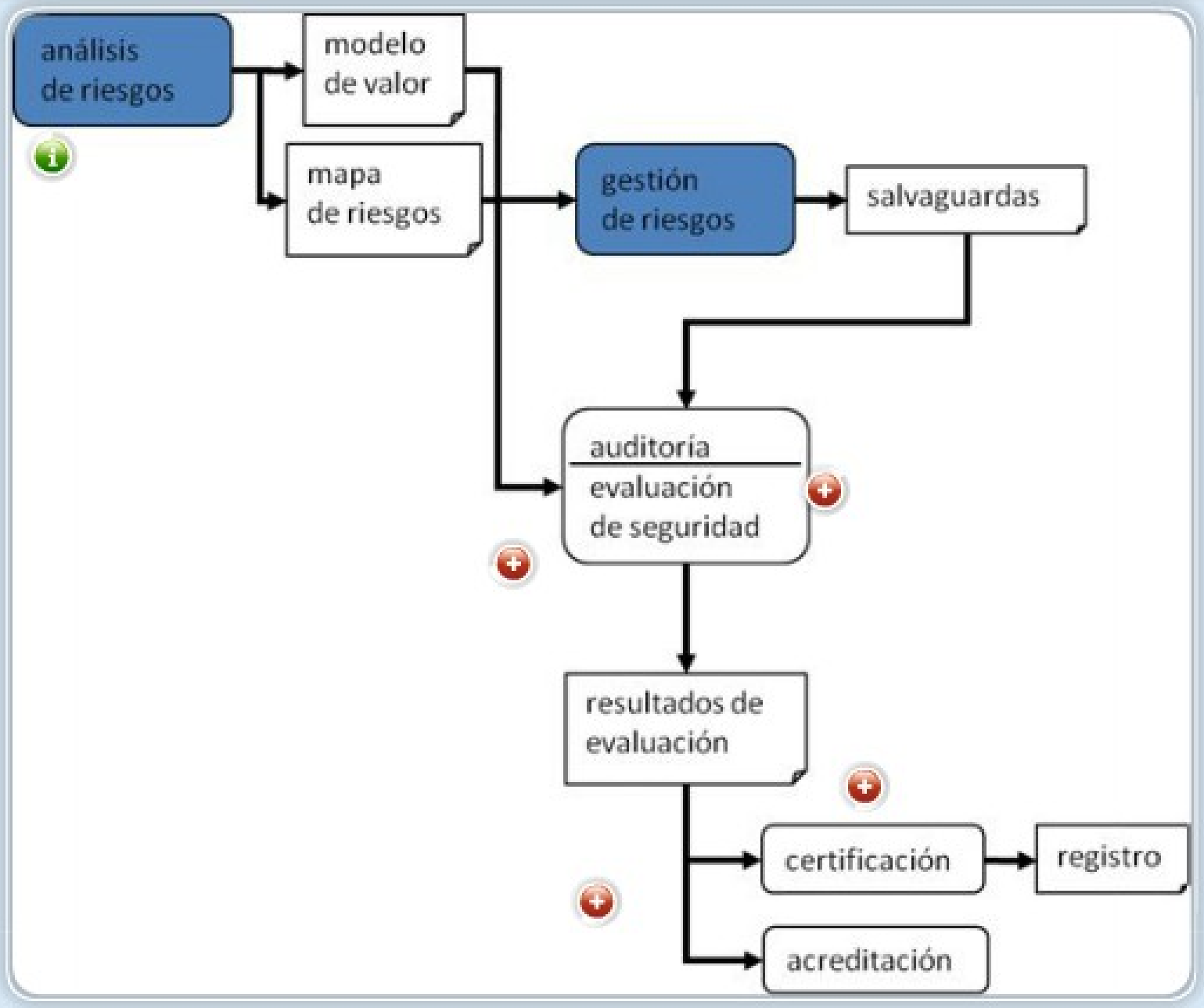
Técnicas específicas para el análisis de riesgos

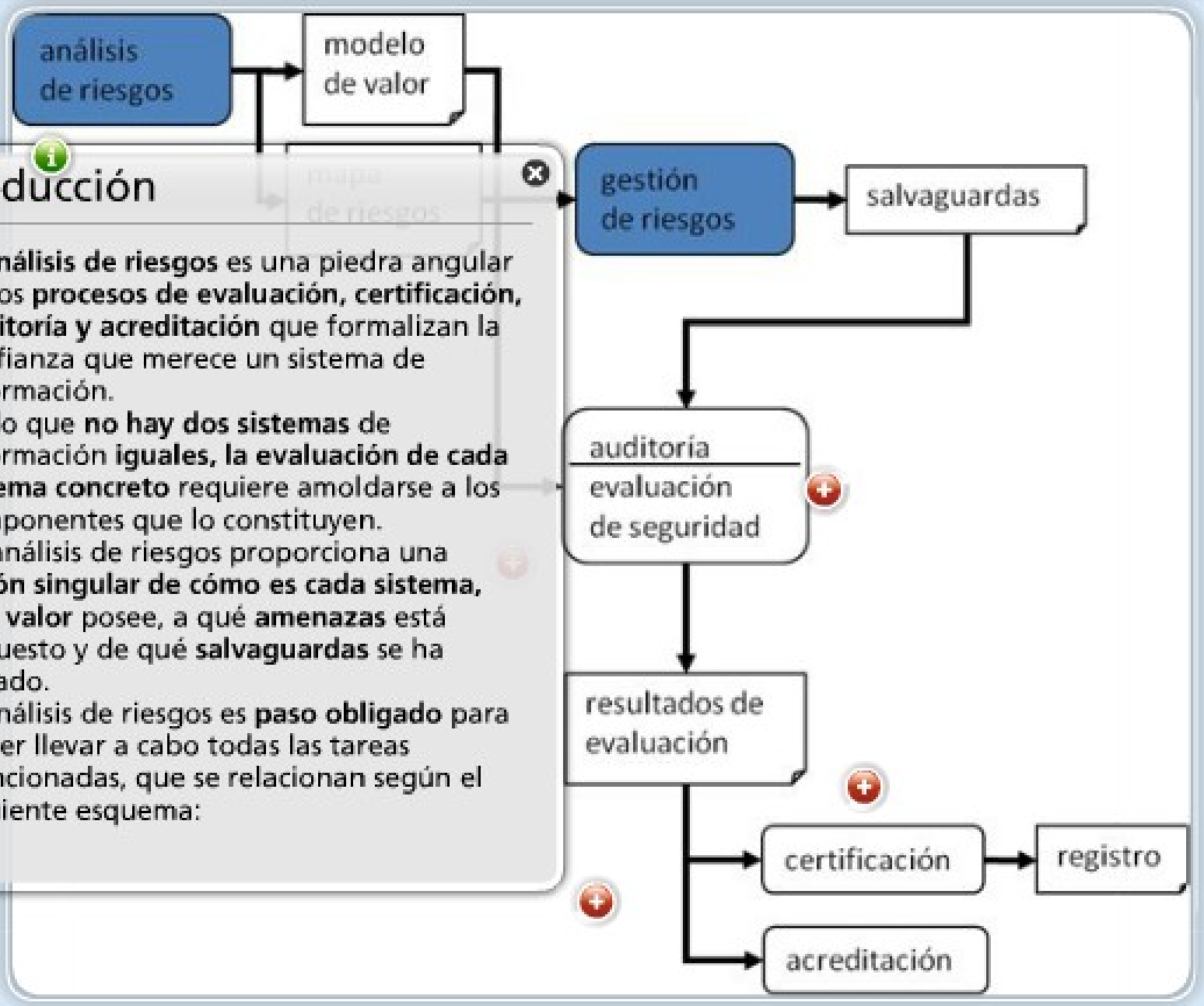
- análisis mediante tablas
- análisis algorítmico
- árboles de ataque

Técnicas generales

- técnicas gráficas
- planificación de proyectos
- sesiones de trabajo: entrevistas, reuniones y presentaciones
- valoración Delphi

Certificación y acreditación

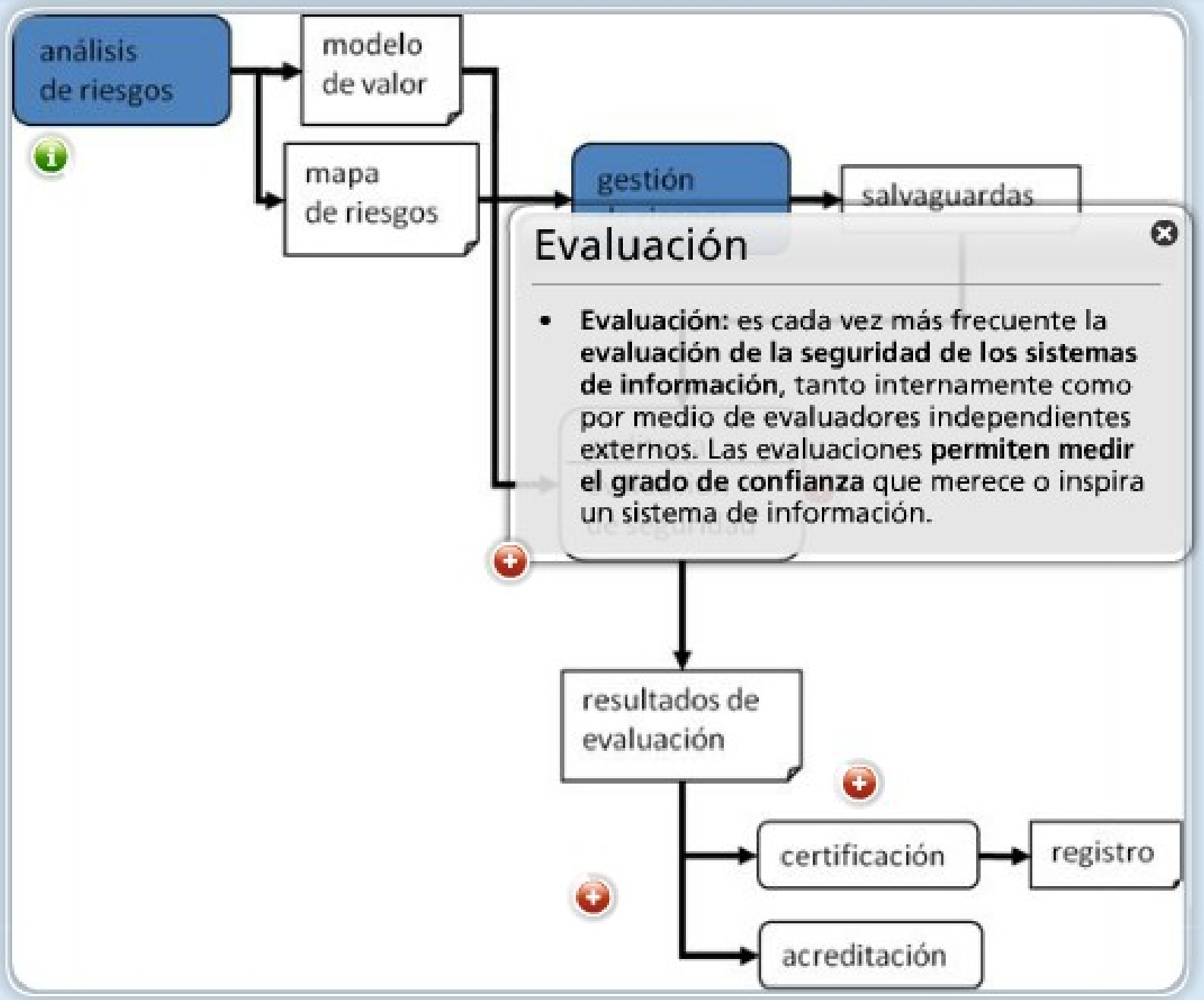




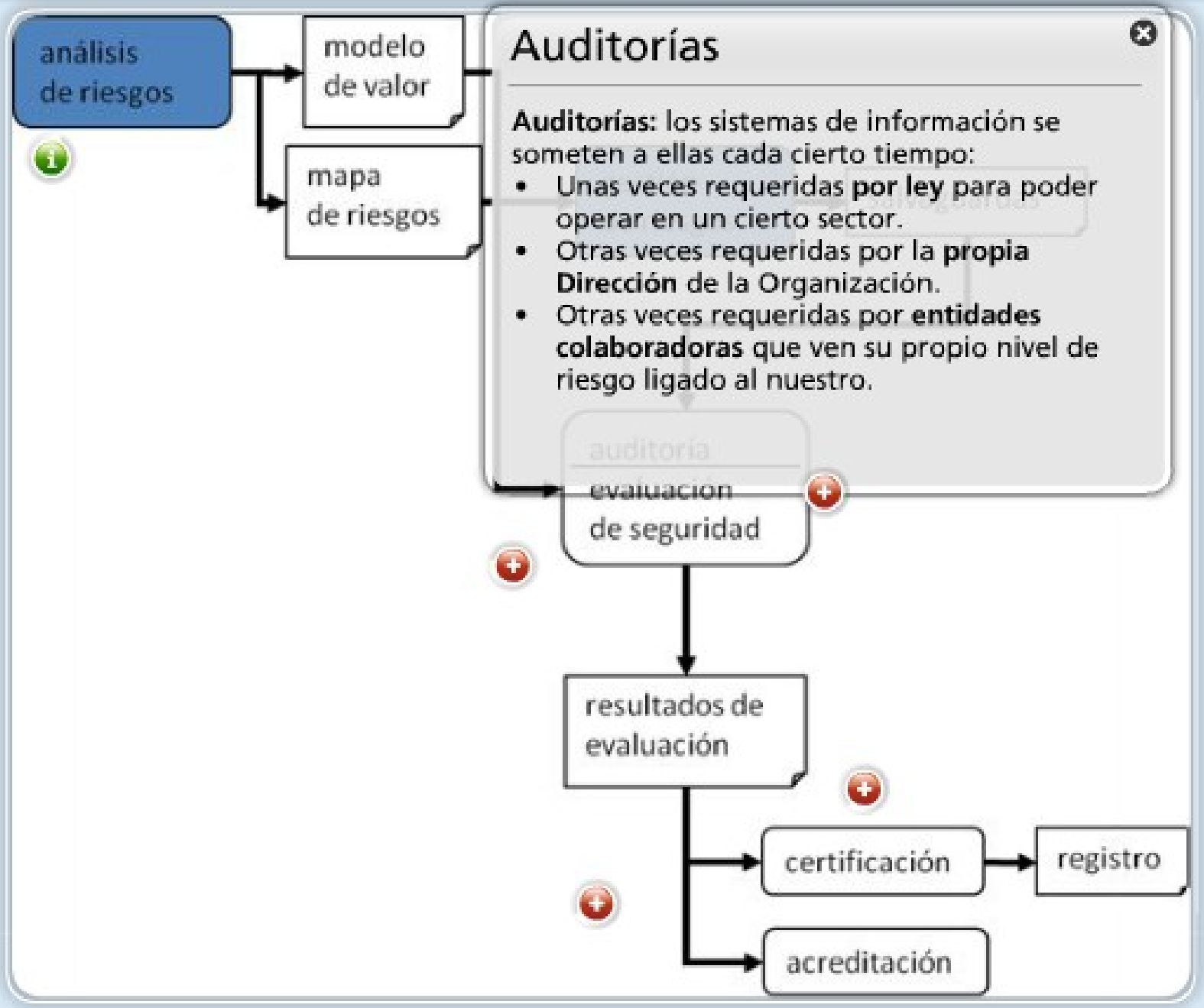
Introducción

- El **análisis de riesgos** es una piedra angular de los **procesos de evaluación, certificación, auditoría y acreditación** que formalizan la confianza que merece un sistema de información.
- Dado que **no hay dos sistemas** de información **iguales, la evaluación de cada sistema concreto** requiere amoldarse a los componentes que lo constituyen.
- En análisis de riesgos proporciona una **visión singular de cómo es cada sistema,** qué **valor** posee, a qué **amenazas** está expuesto y de qué **salvaguardas** se ha dotado.
- El análisis de riesgos es **paso obligado** para poder llevar a cabo todas las tareas mencionadas, que se relacionan según el siguiente esquema:

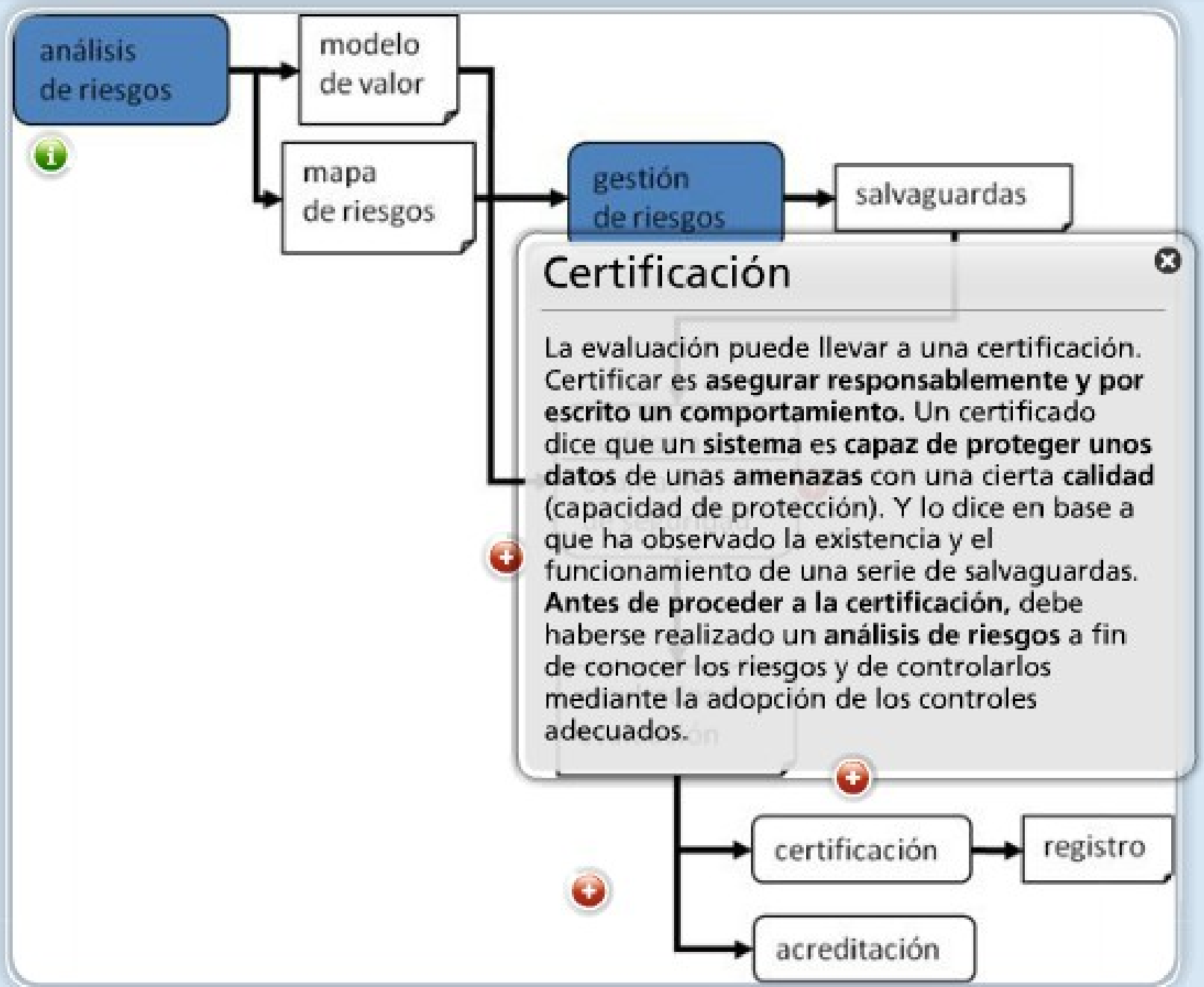
Certificación y acreditación

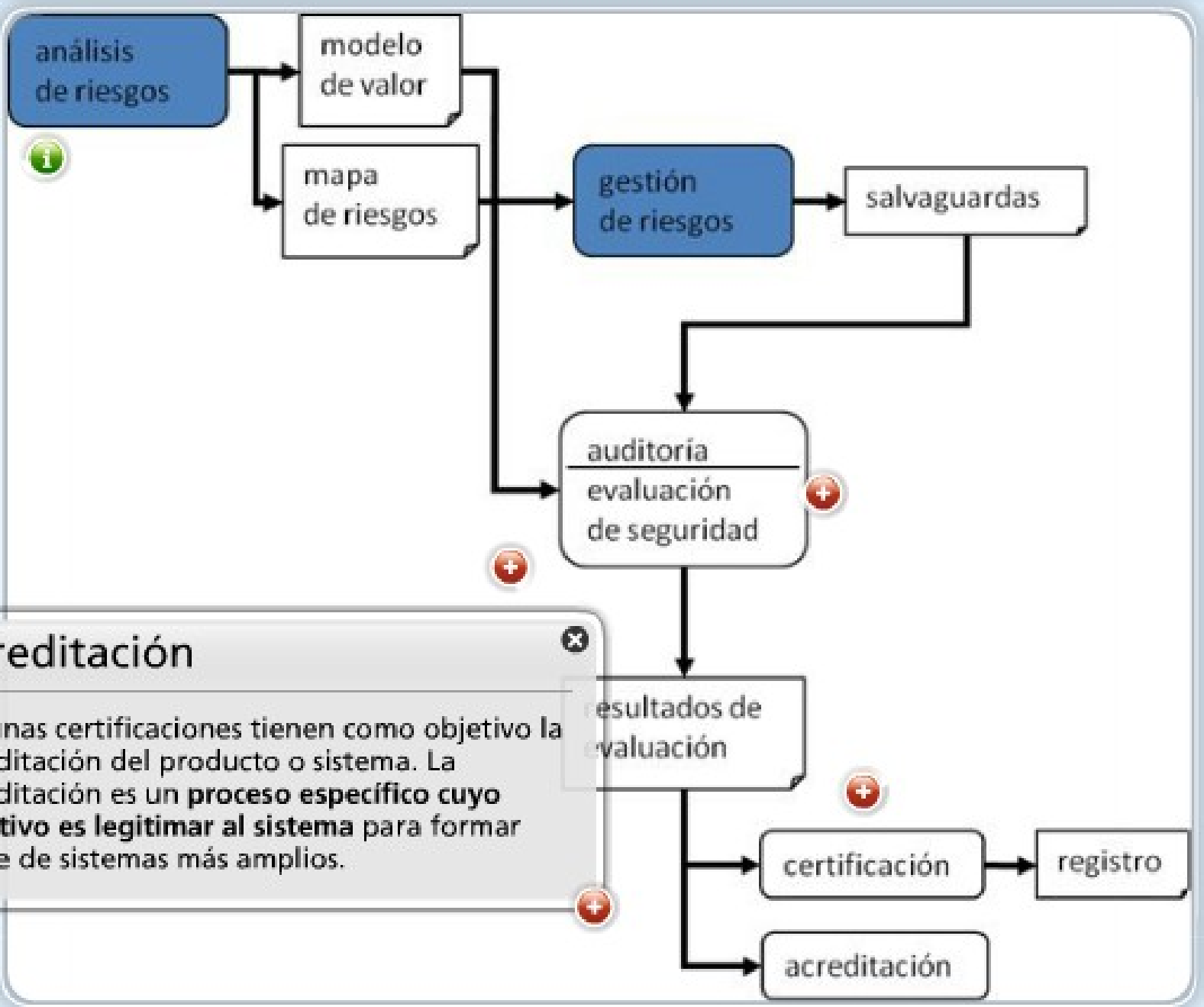


Certificación y acreditación



Certificación y acreditación



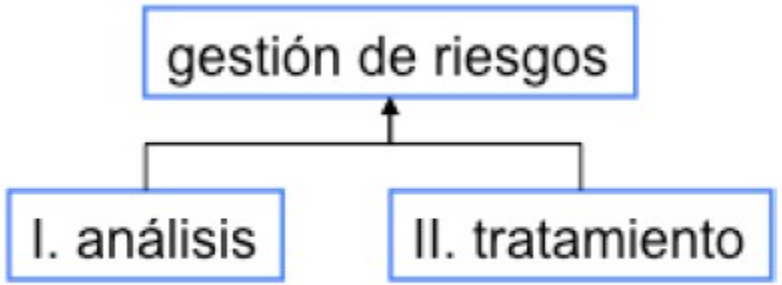


Acreditación

Algunas certificaciones tienen como objetivo la acreditación del producto o sistema. La acreditación es un **proceso específico cuyo objetivo es legitimar al sistema** para formar parte de sistemas más amplios.

Magerit v.3

- **I. análisis de riesgos,**
  - que permite determinar qué tiene la Organización y estimar lo que podría pasar.
- **II. tratamiento de los riesgos,**
  - que permite organizar la defensa concienzuda y prudente, defendiendo para que no pase nada malo y al tiempo estando preparados para atajar las emergencias, sobrevivir a los incidentes y seguir operando en las mejores condiciones; como nada es perfecto, se dice que el riesgo se reduce a un nivel residual que la Dirección asume.
- Ambas actividades, análisis y tratamiento se combinan en el proceso denominado **Gestión de Riesgos.**



Gestión de riesgos

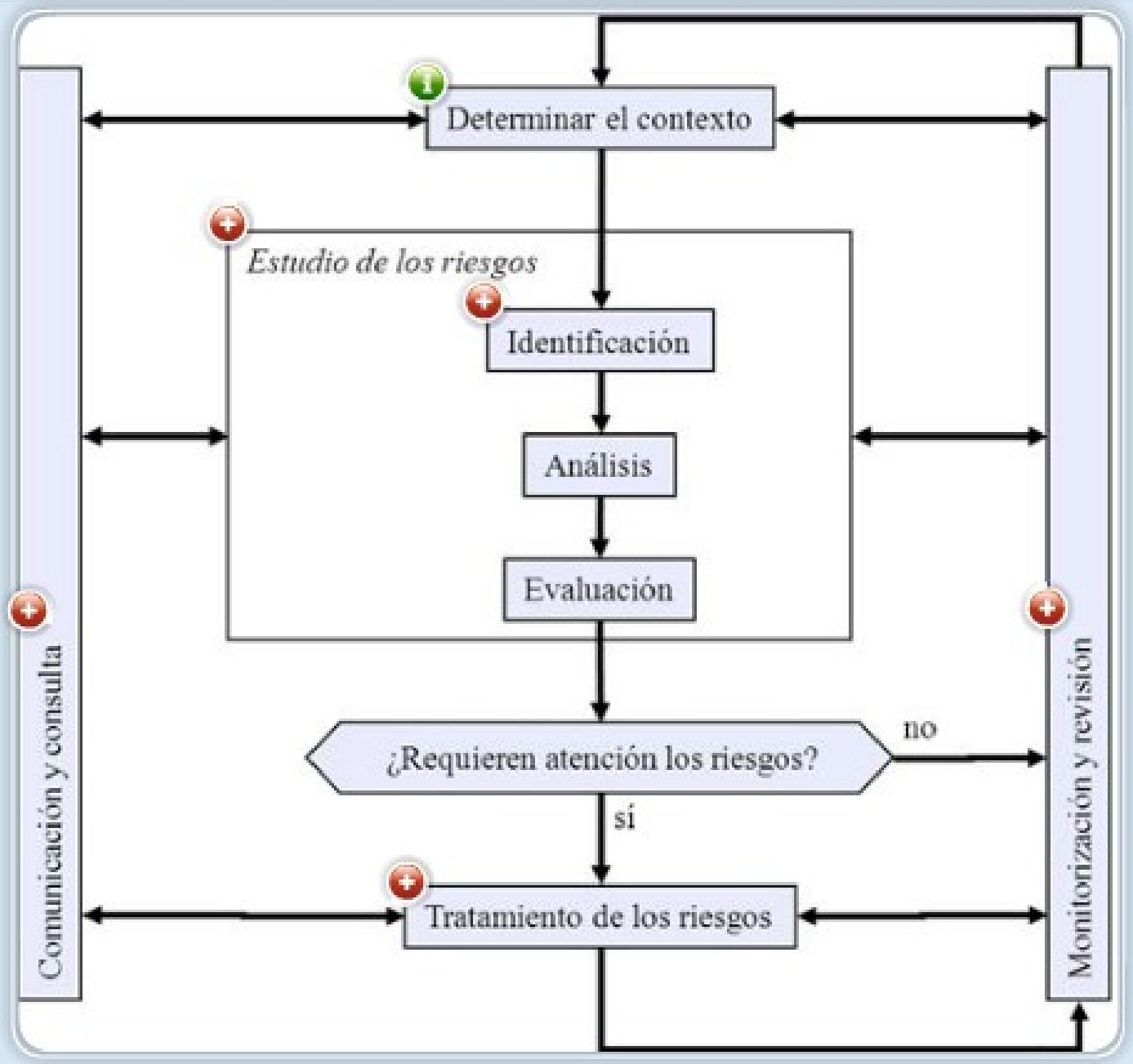
Análisis de Riesgos

- El análisis de riesgos considera los siguientes elementos:
  - activos, que son los elementos del sistema de información (o estrechamente relacionados con este) que soportan la misión de la Organización
  - amenazas, que son cosas que les pueden pasar a los activos causando un perjuicio a la Organización
  - salvaguardas (o contra medidas), que son medidas de protección desplegadas para que aquellas amenazas no causen [tanto] daño.
- Con estos elementos se puede estimar:
  - el impacto: lo que podría pasar
  - el riesgo: lo que probablemente pase

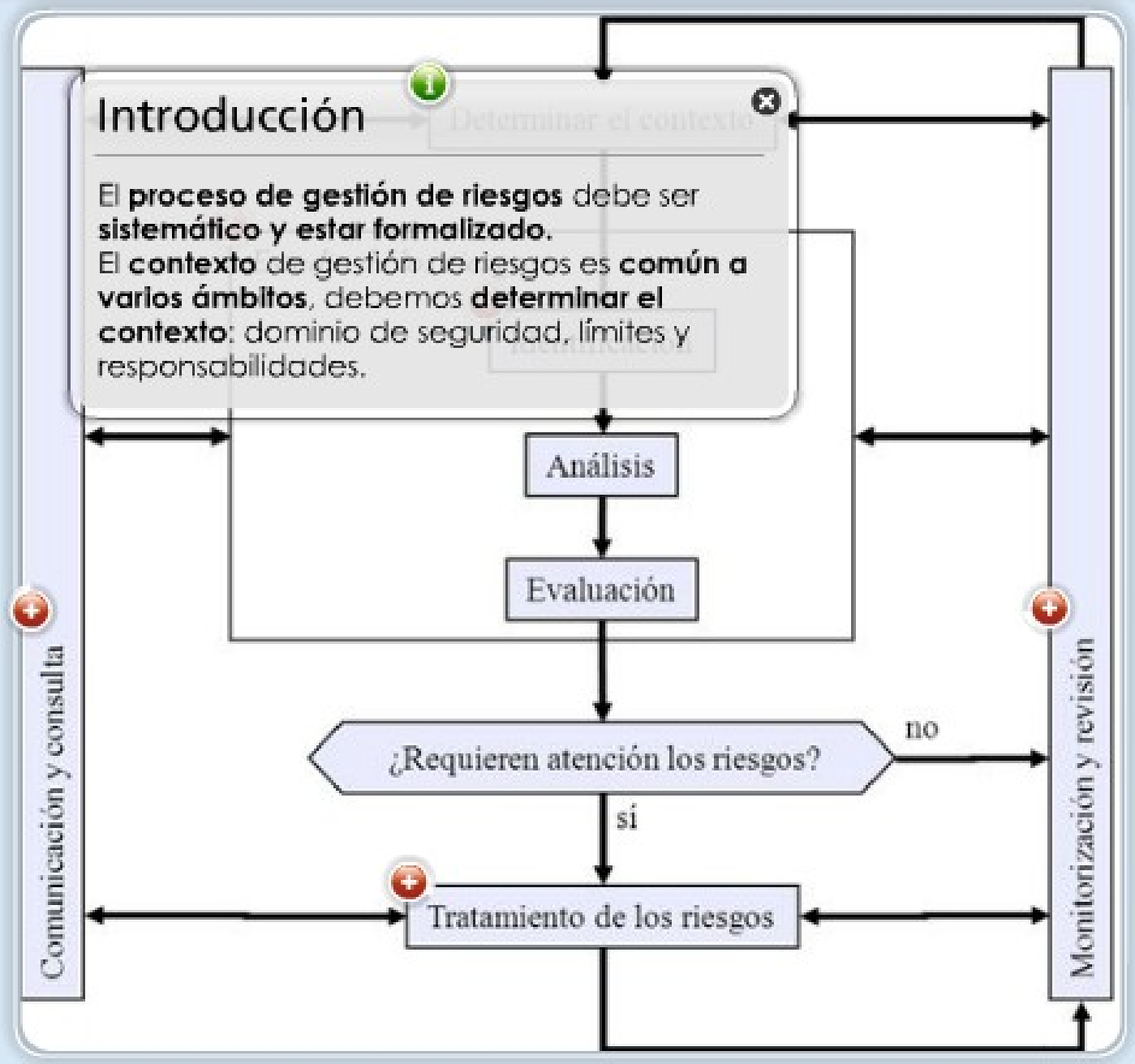
El análisis de riesgos permite analizar estos elementos de forma metódica para llegar a conclusiones con fundamento y proceder a la fase de tratamiento.

Informalmente, se puede decir que la gestión de la seguridad de un sistema de información es la gestión de sus riesgos y que el análisis permite racionalizar dicha gestión.

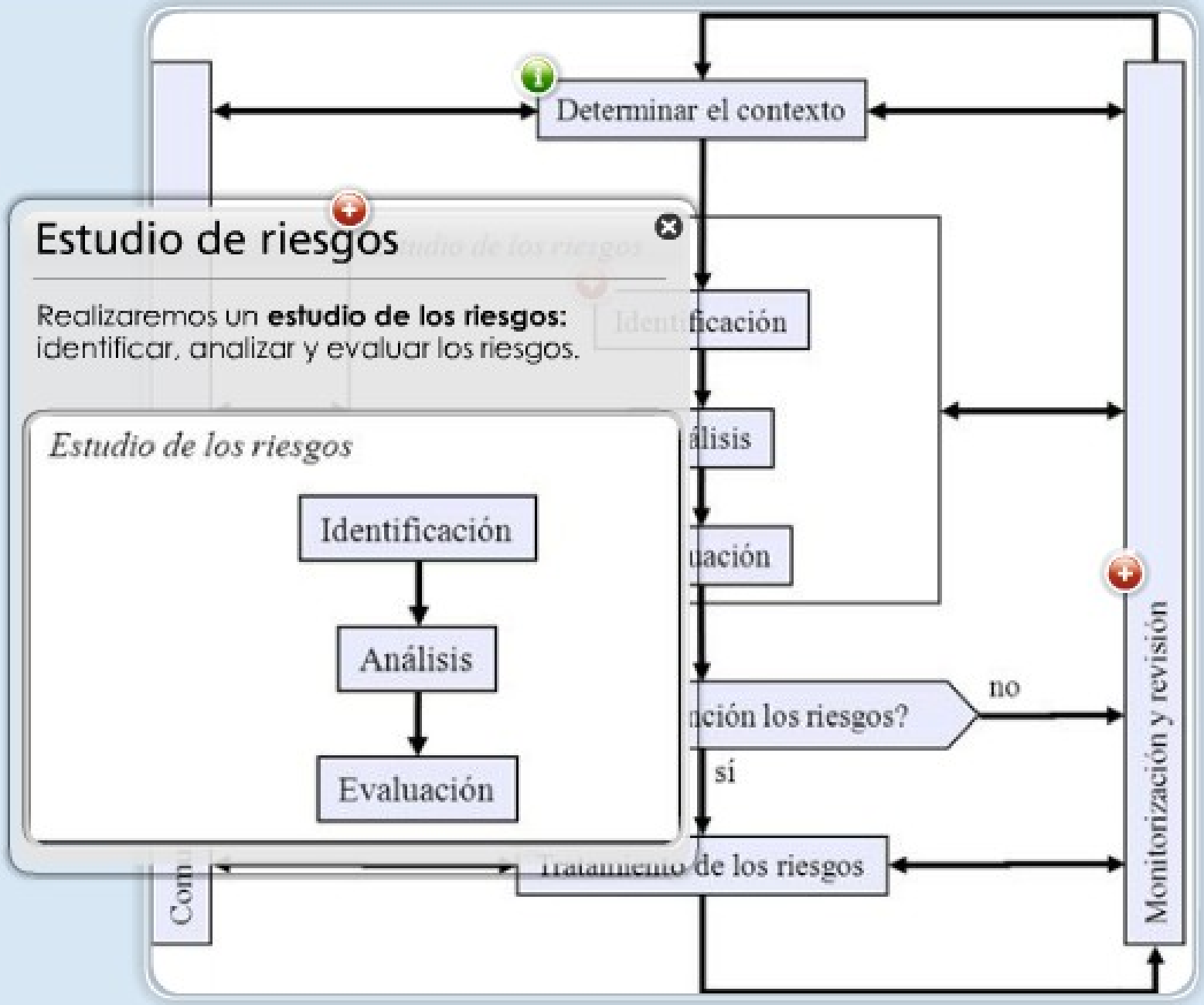
Proceso de gestión de riesgos



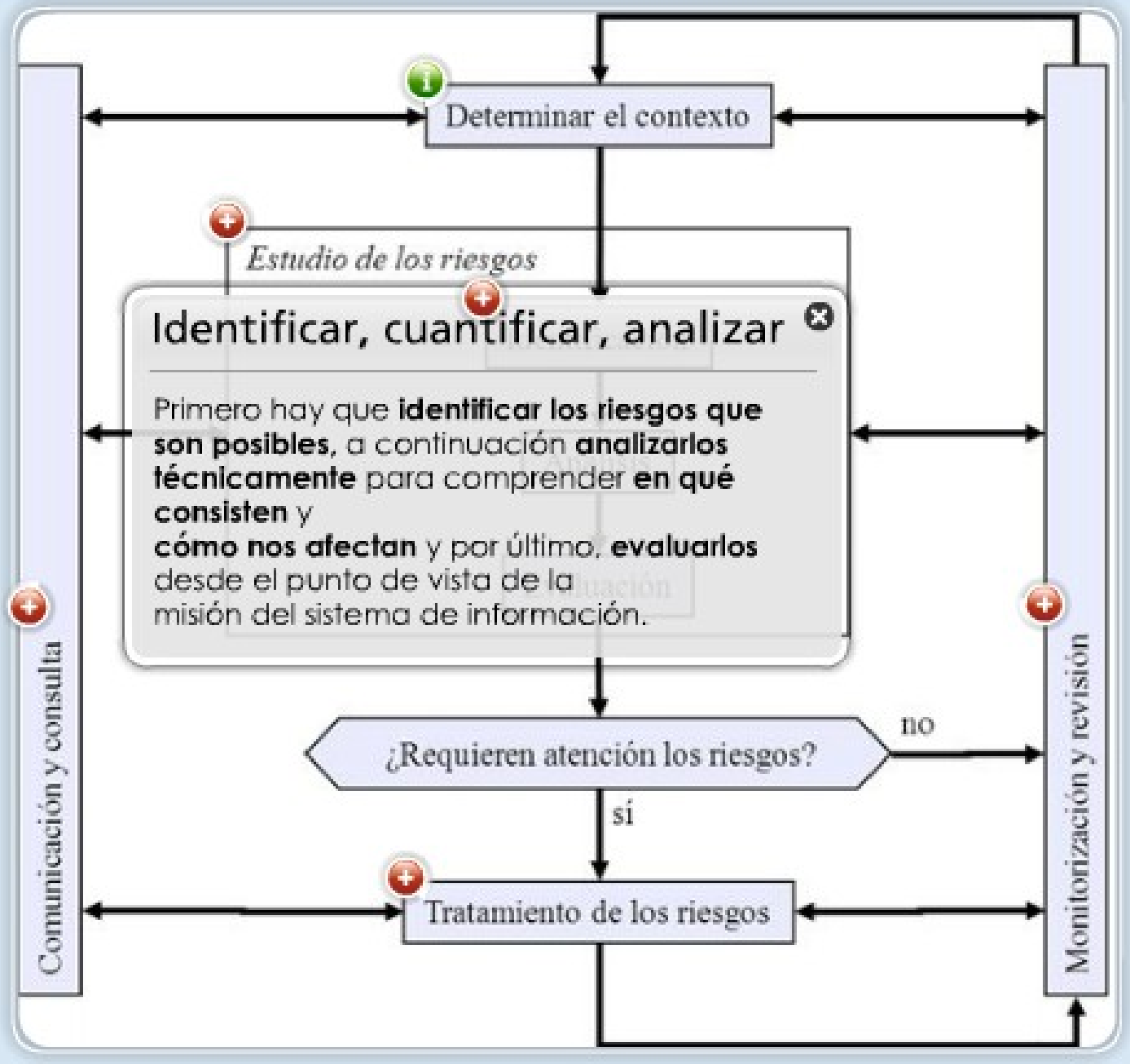
Proceso de gestión de riesgos



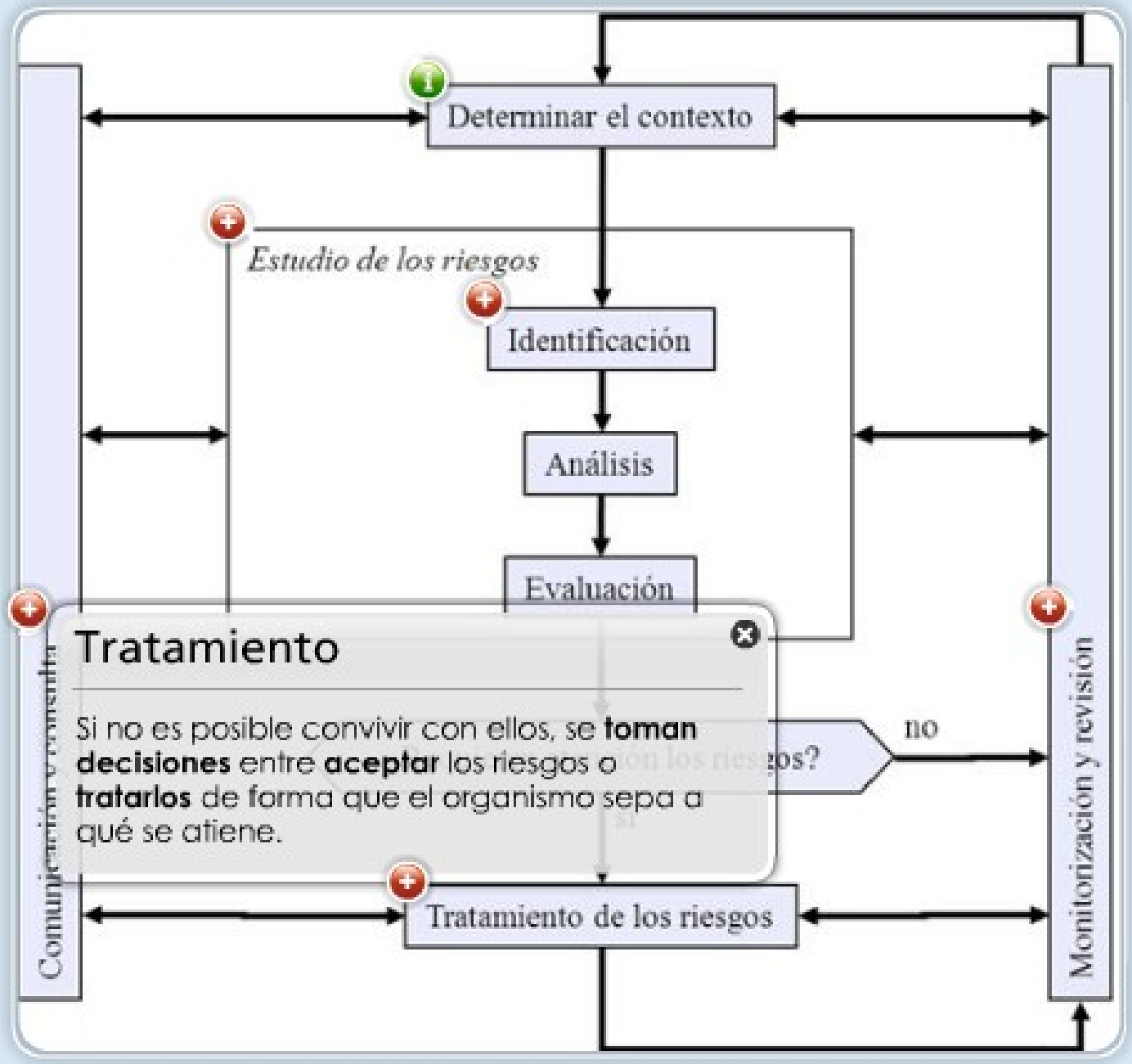
Proceso de gestión de riesgos



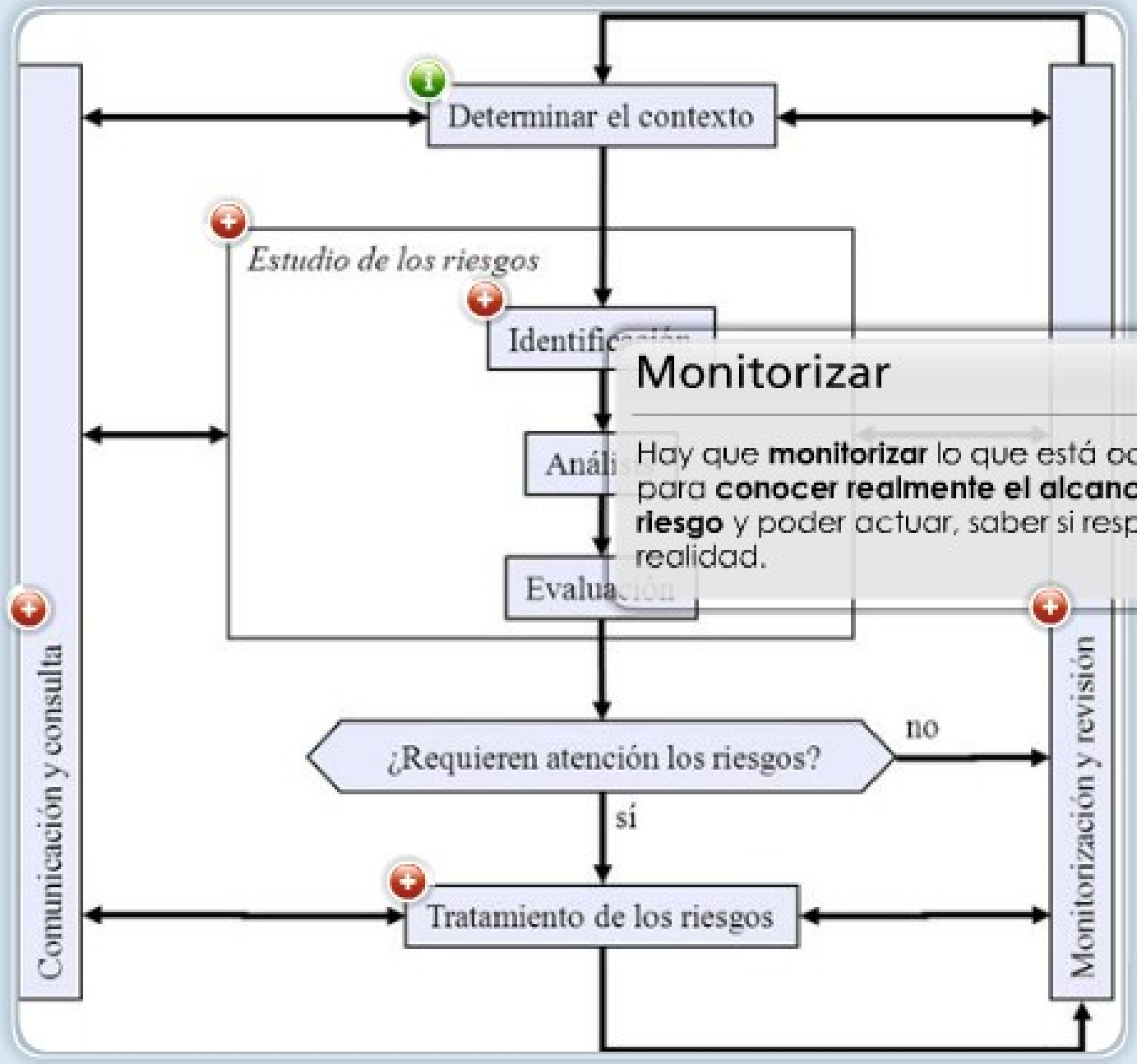
Proceso de gestión de riesgos



Proceso de gestión de riesgos

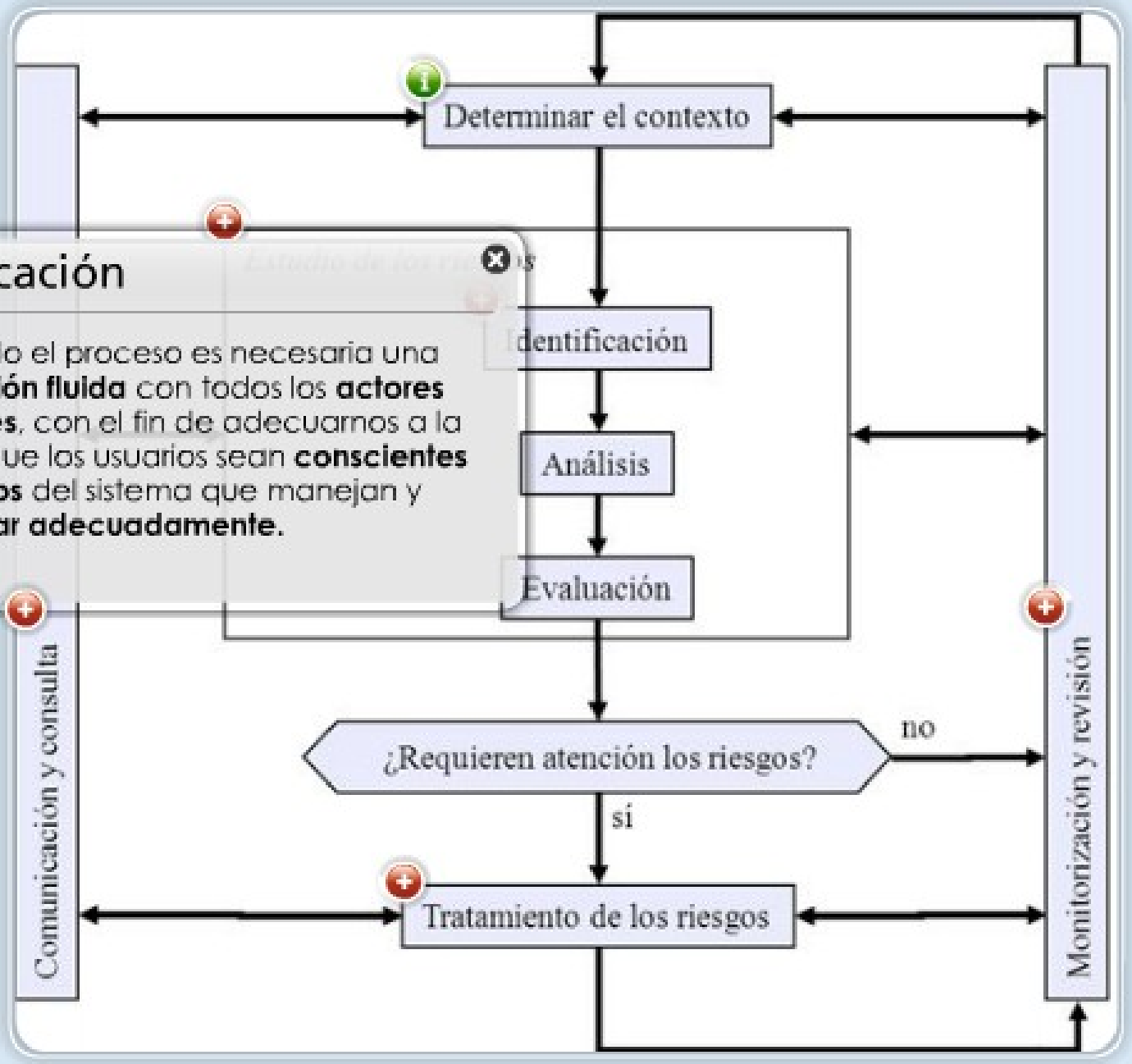


Proceso de gestión de riesgos



Proceso de gestión de riesgos

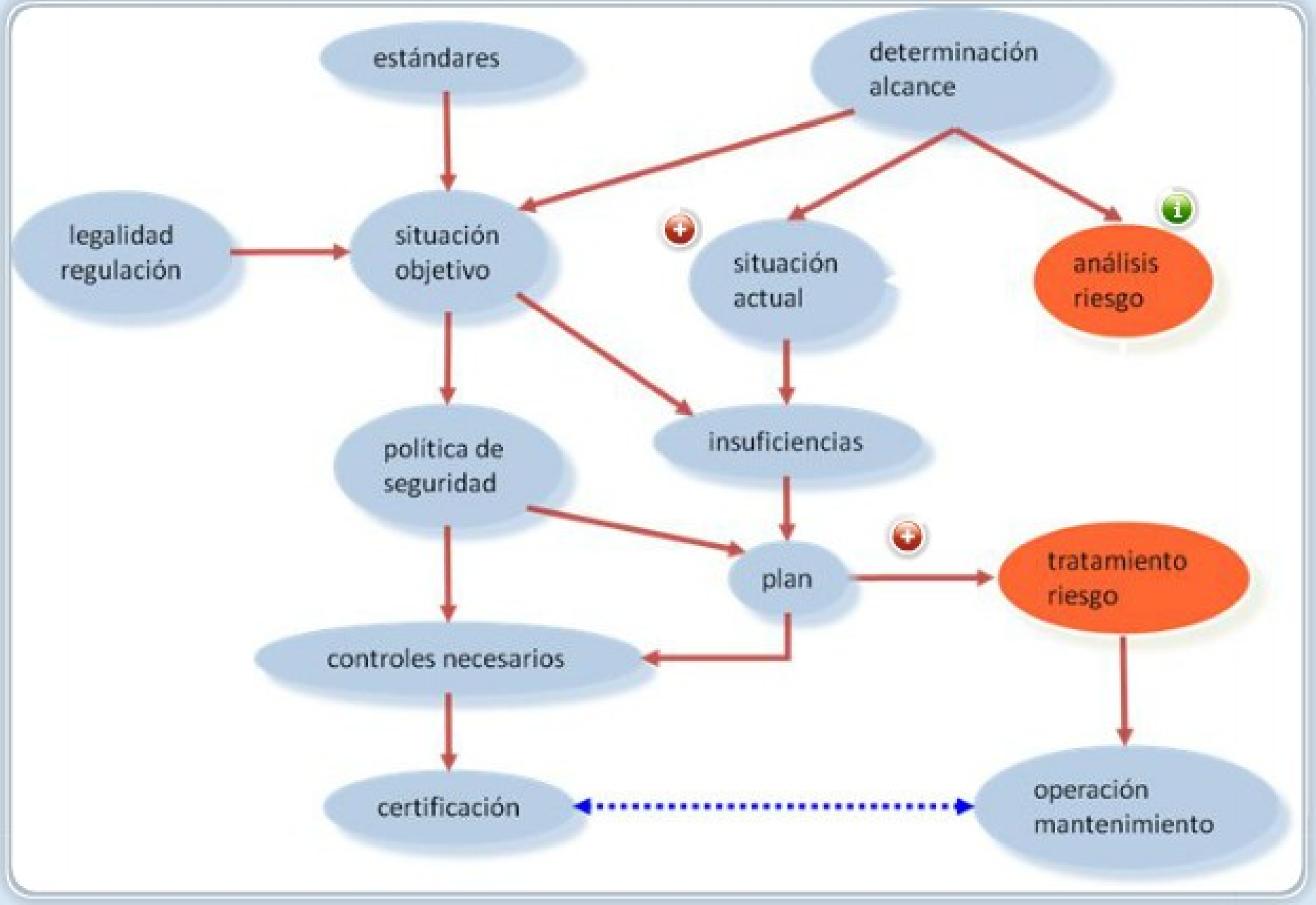
Siguiente



Comunicación

Durante todo el proceso es necesaria una **comunicación fluida** con todos los **actores intervinientes**, con el fin de adecuarnos a la realidad y que los usuarios sean **conscientes de los riesgos** del sistema que manejan y **sepan actuar adecuadamente.**

Mapa de ruta


estándares
determinación alcance
legalidad regulación
situación objetivo
situación actual
análisis riesgo
política de seguridad
insuficiencias
plan
tratamiento riesgo
controles necesarios
certificación
operación mantenimiento

Mapa de ruta

Análisis de Riesgos

Determinamos el **alcance del riesgo:** hacemos un **análisis de riesgos** y obtenemos **una fotografía de la situación actual.**

Mapa de ruta

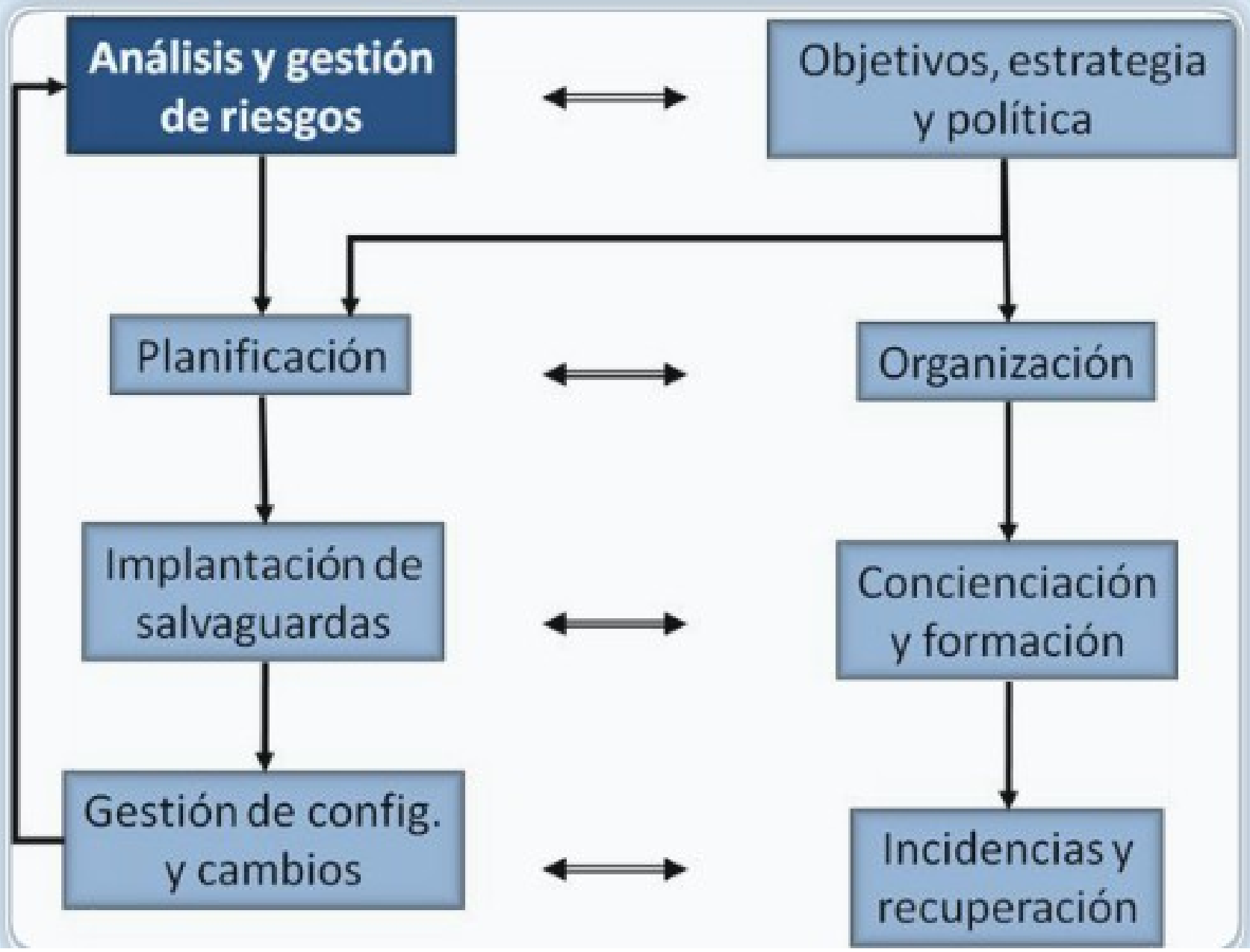

estándares
determinación alcance
legalidad regulación
Situación
La **decisión** de si el análisis que hemos realizado nos sirve o no hay que ponerla en un **contexto:**
• Ver que **estándares** manejamos, con qué **normas y obligaciones** nos regimos.
• Qué **situación objetivo** queremos alcanzar, y cual es la **diferencia con la situación actual.**
análisis riesgo
plan
tratamiento riesgo
controles necesarios
certificación
operación mantenimiento

Plan y Tratamiento

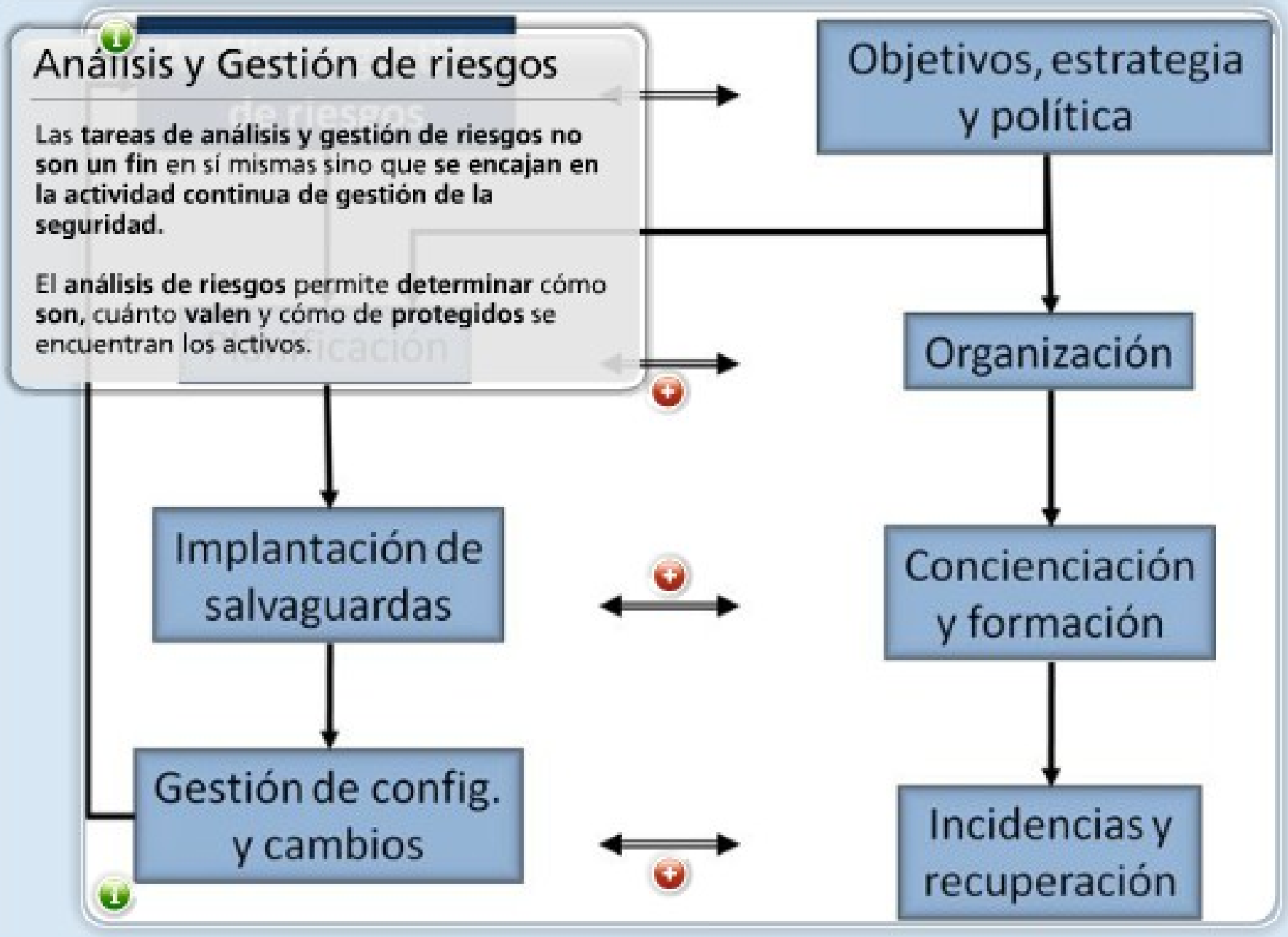
A continuación hay que **establecer un plan,** un cierto **tratamiento** para alcanzar la situación que queremos.

- Se establecen unas **políticas de seguridad.**
- Se elabora un plan en el cual se establecen las **acciones de tratamiento** del riesgo.
- Se establecen **controles.**
- Se **toman decisiones** para tratar el riesgo y mantenerlo bajo control.

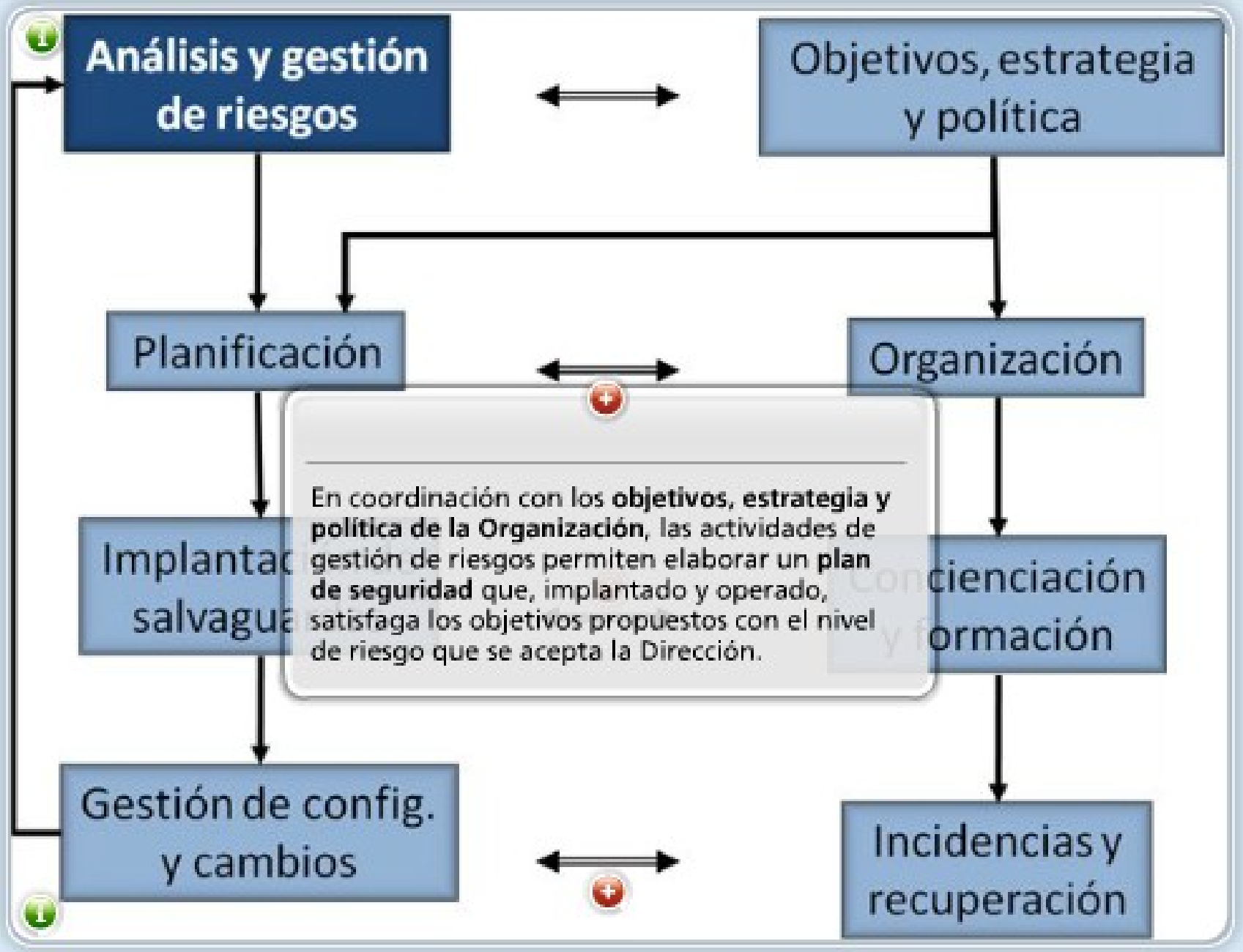
Ciclo continuo en la gestión de riesgos



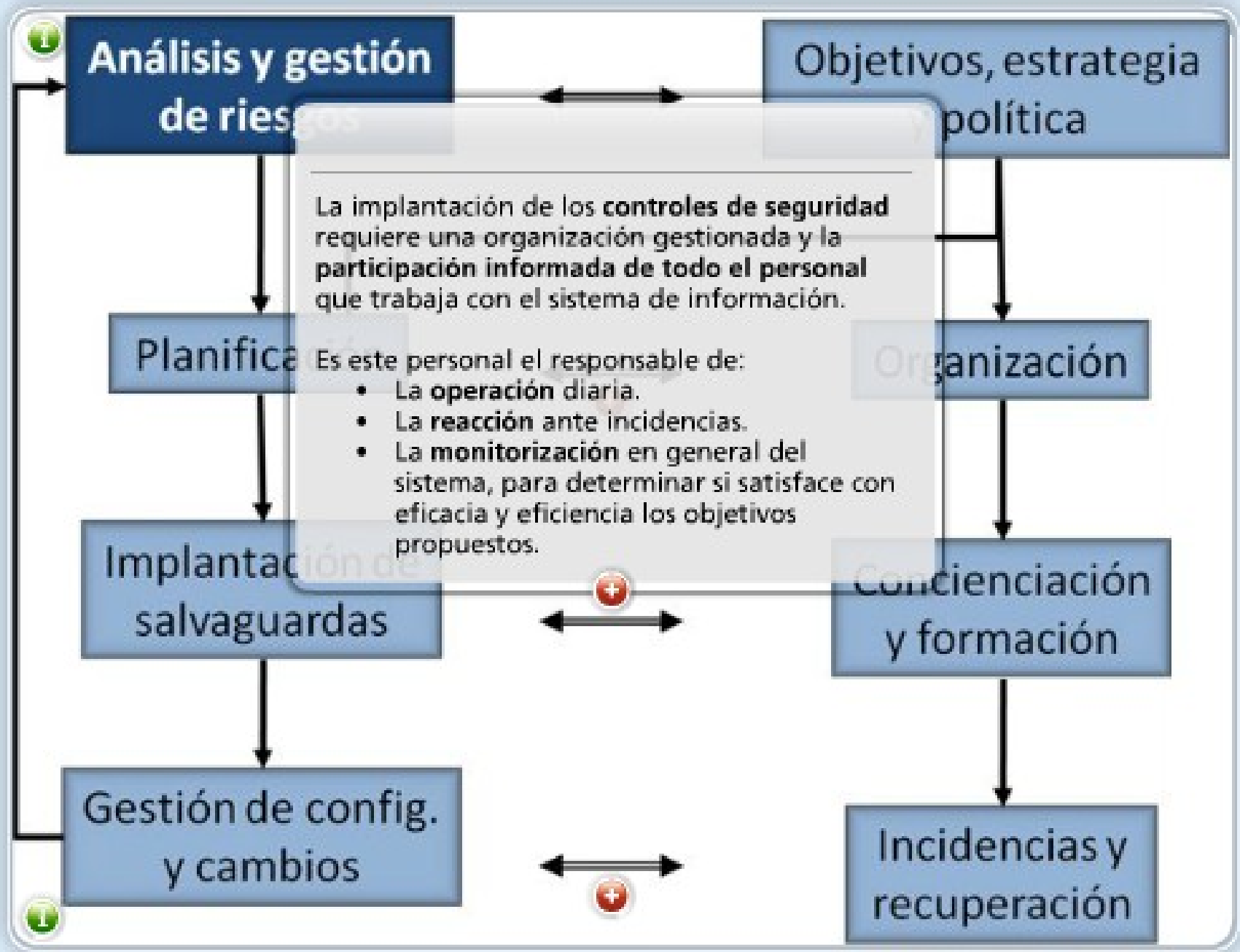
Ciclo continuo en la gestión de riesgos



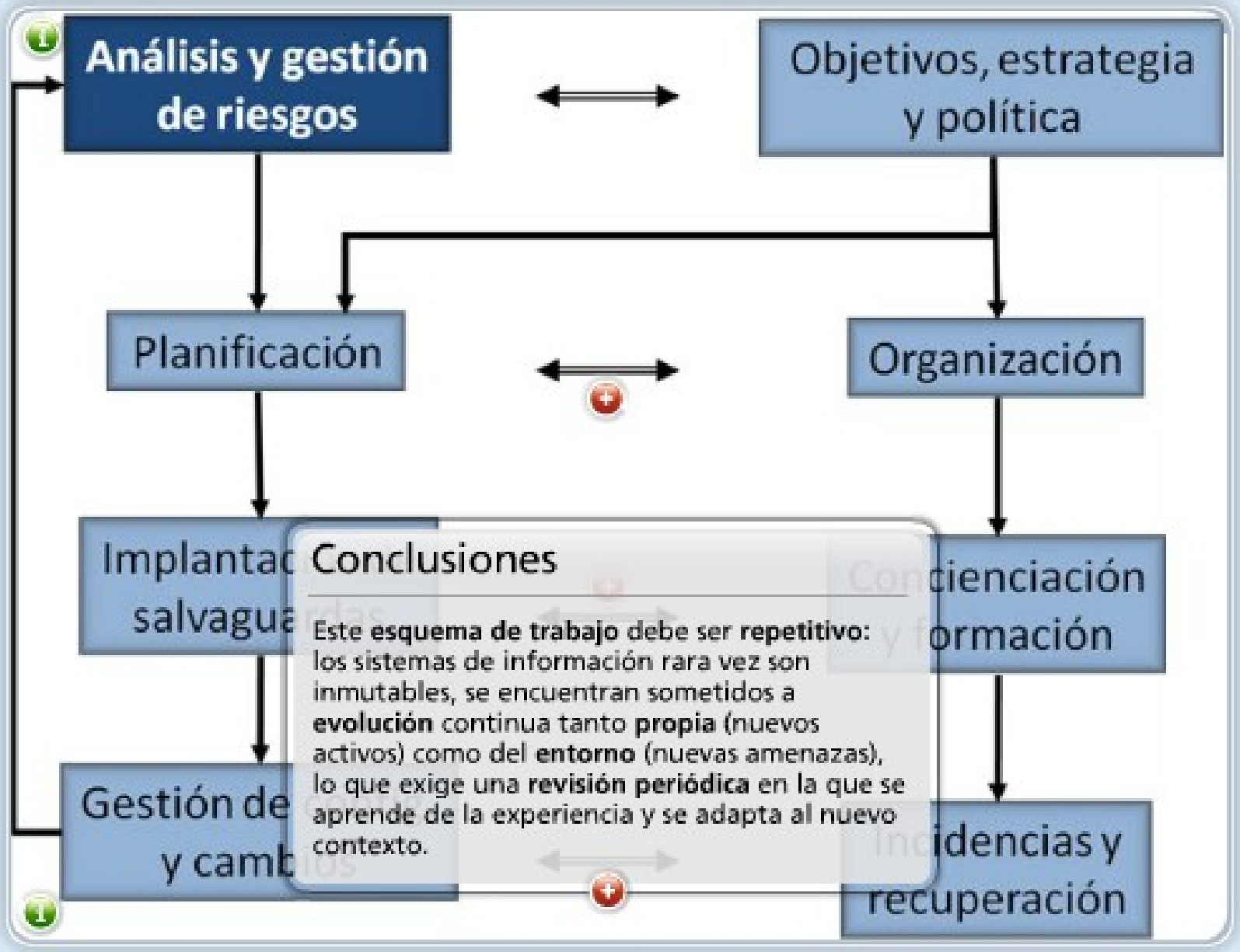
Ciclo continuo en la gestión de riesgos



Ciclo continuo en la gestión de riesgos



Ciclo continuo en la gestión de riesgos



Ciclo continuo en la gestión de riesgos

Siguiente

SGSI.

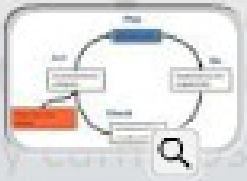
Sistema General de Gestión de la Información.

La gestión de la seguridad es un ciclo continuo:

- Planificar (Plan)
- Hacer (Do)
- Chequear (Check)
- Actuar (Act)

Este esquema se ha aplicado desde hace años en los procesos de producción industrial (ISO 9001), lo trasladamos a la gestión de riesgos en los sistemas informáticos.

En los **sistemas de información prácticamente** todo el mundo trabaja con los **mismos componentes**, las **diferencias** están en **cómo se vertebran los sistemas**. Conociendo lo que le ocurre a los demás, podemos adoptar medidas.

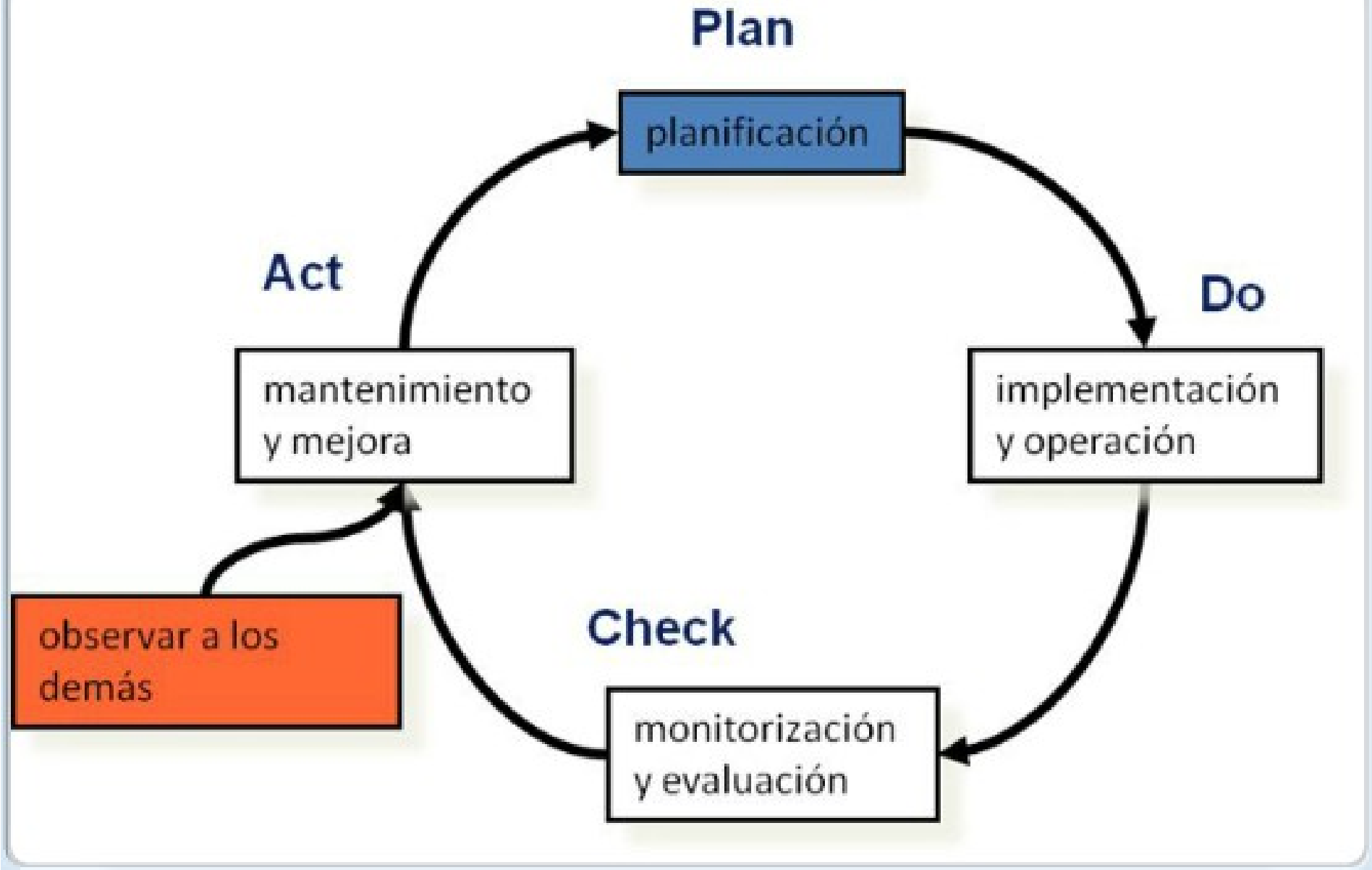


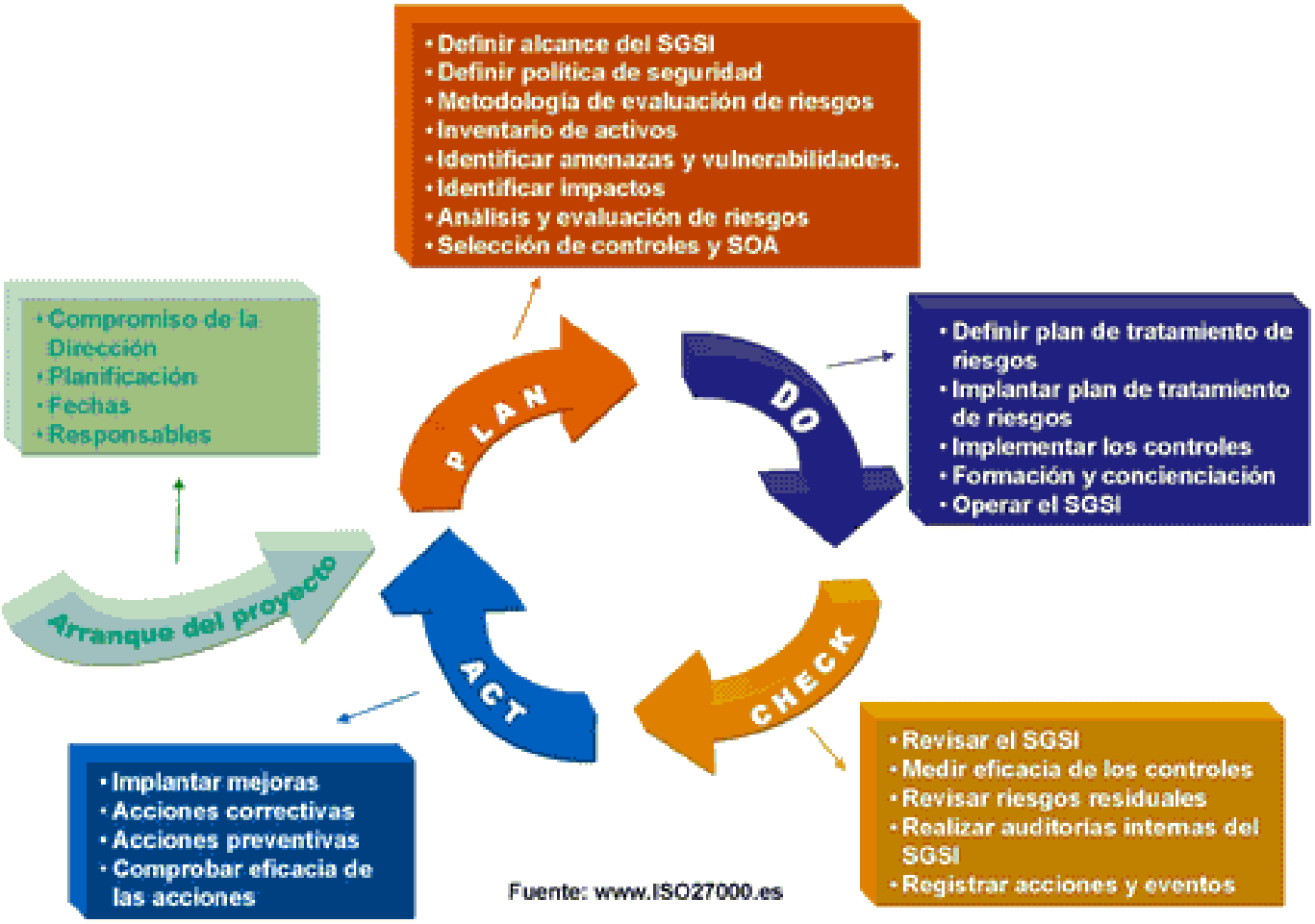
Objetivos, estrategia y política

Organización

Concienciación y formación

Incidencias y recuperación


Plan
planificación
Do
implementación
y operación
Check
monitorización
y evaluación
Act
mantenimiento
y mejora
observar a los
demás


• Definir alcance del SGSI
• Definir política de seguridad
• Metodología de evaluación de riesgos
• Inventario de activos
• Identificar amenazas y vulnerabilidades.
• Identificar impactos
• Análisis y evaluación de riesgos
• Selección de controles y SOA
PLAN
DO
• Definir plan de tratamiento de riesgos
• Implantar plan de tratamiento de riesgos
• Implementar los controles
• Formación y concienciación
• Operar el SGSI
CHECK
• Revisar el SGSI
• Medir eficacia de los controles
• Revisar riesgos residuales
• Realizar auditorías internas del SGSI
• Registrar acciones y eventos
ACT
• Implantar mejoras
• Acciones correctivas
• Acciones preventivas
• Comprobar eficacia de las acciones
Arranque del proyecto
• Compromiso de la Dirección
• Planificación
• Fechas
• Responsables
Fuente: www.ISO27000.es

¿Cuándo procede analizar y gestionar los riesgos?

Realizar un análisis de riesgos es laborioso y costoso

- hacer un **mapa de activos y valorarlos** requiere involucrar a muchas personas y perfiles dentro de la Organización
- hay que lograr una unidad de criterio entre ellos
- en un análisis de riesgos aparecen multitud de datos que han de estar bien ordenados para poder interpretarlos
- es una tarea mayor que requiere esfuerzo y coordinación, debe ser planificada y justificada

¿Cuándo procede analizar y gestionar los riesgos?

Un análisis de riesgos es recomendable:

- en cualquier Organización que dependa de las TIC para el cumplimento de su misión
- en cualquier entorno (público o privado) donde se practique la tramitación electrónica de bienes y servicios
- para tomar decisiones de inversión en tecnología: equipos de producción, salvaguardas técnicas, selección y capacitación del personal, centros alternativos de respaldo,…
- antes de desplegar un servicio para que las medidas se incorporen en su diseño: elección de componentes, desarrollo de aplicaciones, manuales de usuario,… (mejor prevenir que curar)

¿Cuándo procede analizar y gestionar los riesgos?

Un análisis de riesgos puede requerirse:

- Por precepto legal

De forma similar, en la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal, en su artículo 9 (Seguridad de los datos) dice así:

1. El responsable del fichero, y, en su caso, el encargado del tratamiento, deberán adoptar las medidas de índole técnica y organizativas necesarias que garanticen la seguridad de los datos de carácter personal y eviten su alteración, pérdida, tratamiento o acceso no autorizado, habida cuenta del estado de la tecnología, la naturaleza de los datos almacenados y *los riesgos a que están expuestos*, ya provengan de la acción humana o del medio físico o natural.

REAL DECRETO 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal.

Artículo 88. *El documento de seguridad*.
1. El responsable del fichero o tratamiento elaborará un documento de seguridad que recogerá las medidas de índole técnica y organizativa acordes a la normativa de seguridad vigente que será de obligado cumplimiento para el personal con acceso a los sistemas de información.

- Para una certificación o acreditación
- Siempre que lo requiera la Organización

Invitación para utilizar Magerit versión 3

Magerit versión 3 interesa a todos aquellos que trabajan con la información y los sistemas informáticos que la tratan.

Si dicha información o los servicios que la explotan son valiosos, esta metodología permíte saber cuánto de este valor está en juego y ayudará a protegerlo.

El texto completo de Magerit versión 3 se puede encontrar en

https://www.ccn-cert.cni.es/herramientas-de-ciberseguridad/ear-pilar/metodologia.html

Índice

Seguridad de los Sistemas de Información.
Algunas preguntas clave

¿Dónde estoy?

¿Dónde quiero / puedo llegar?

¿Qué pasos voy a dar?

¿Por qué?

¿Cómo?

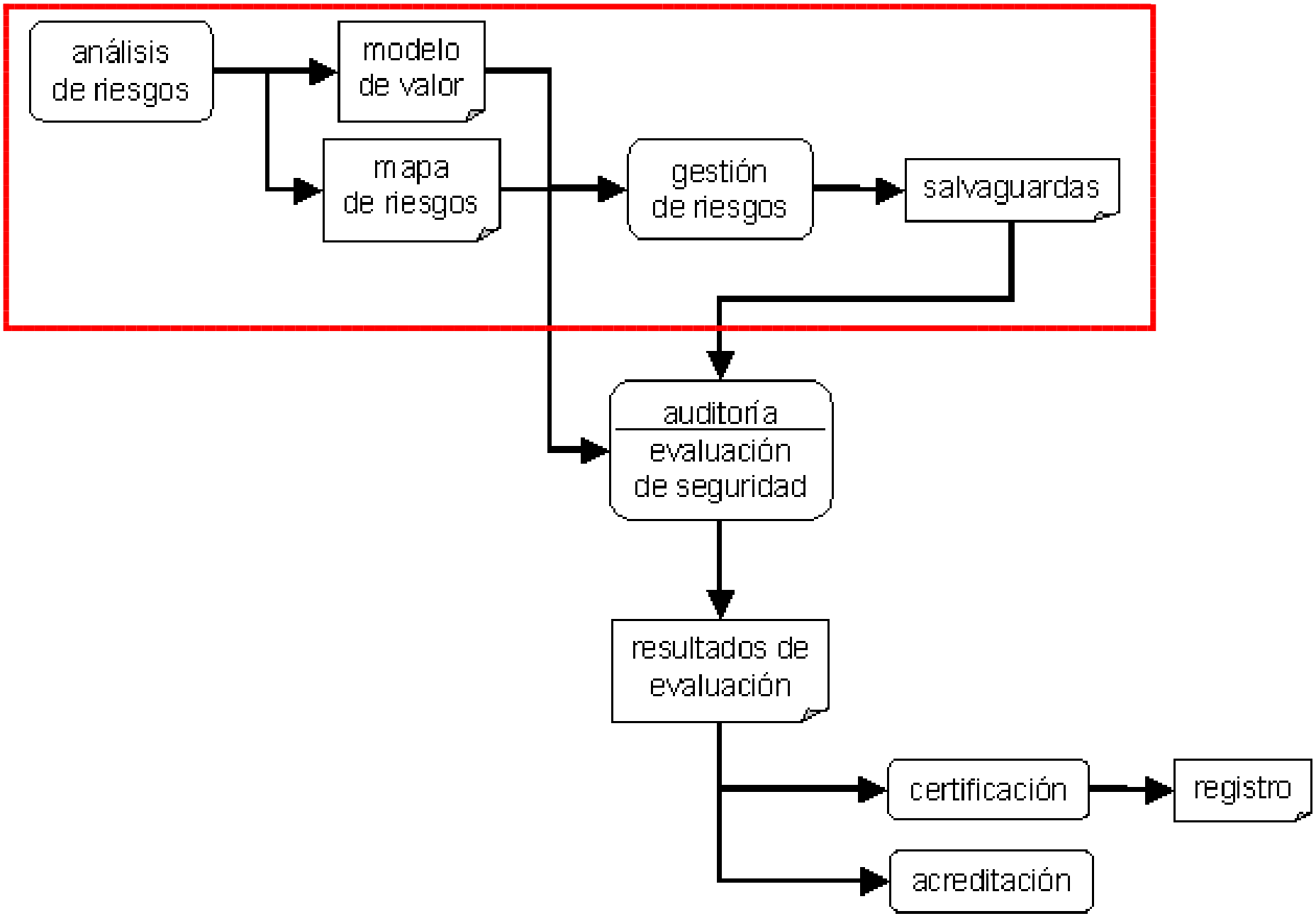
o ¿*Por dónde empiezo*?

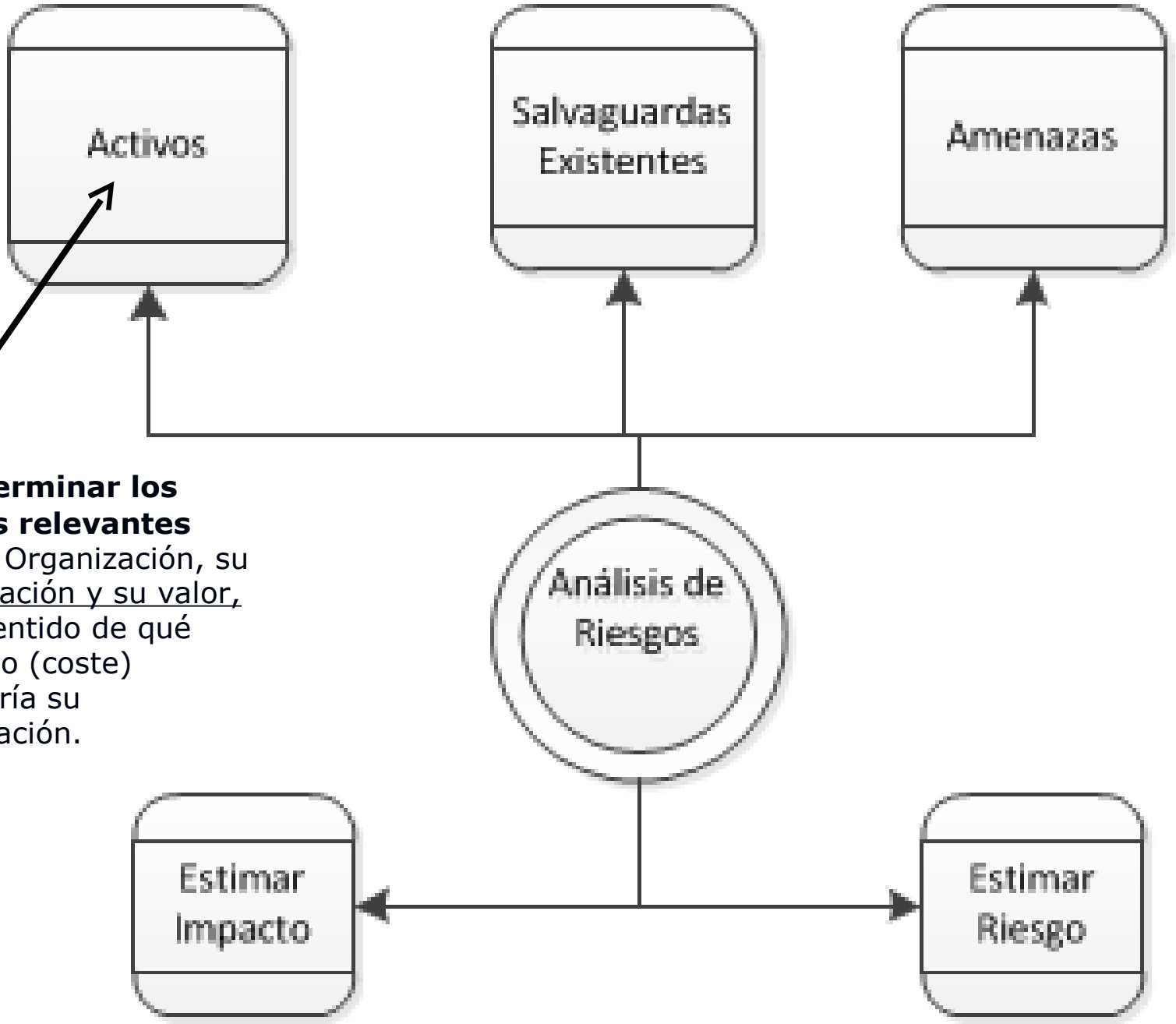
Análisis y gestión de riesgos
MAGERIT

"**método:** manera ordenada y sistemática de hacer cierta cosa."

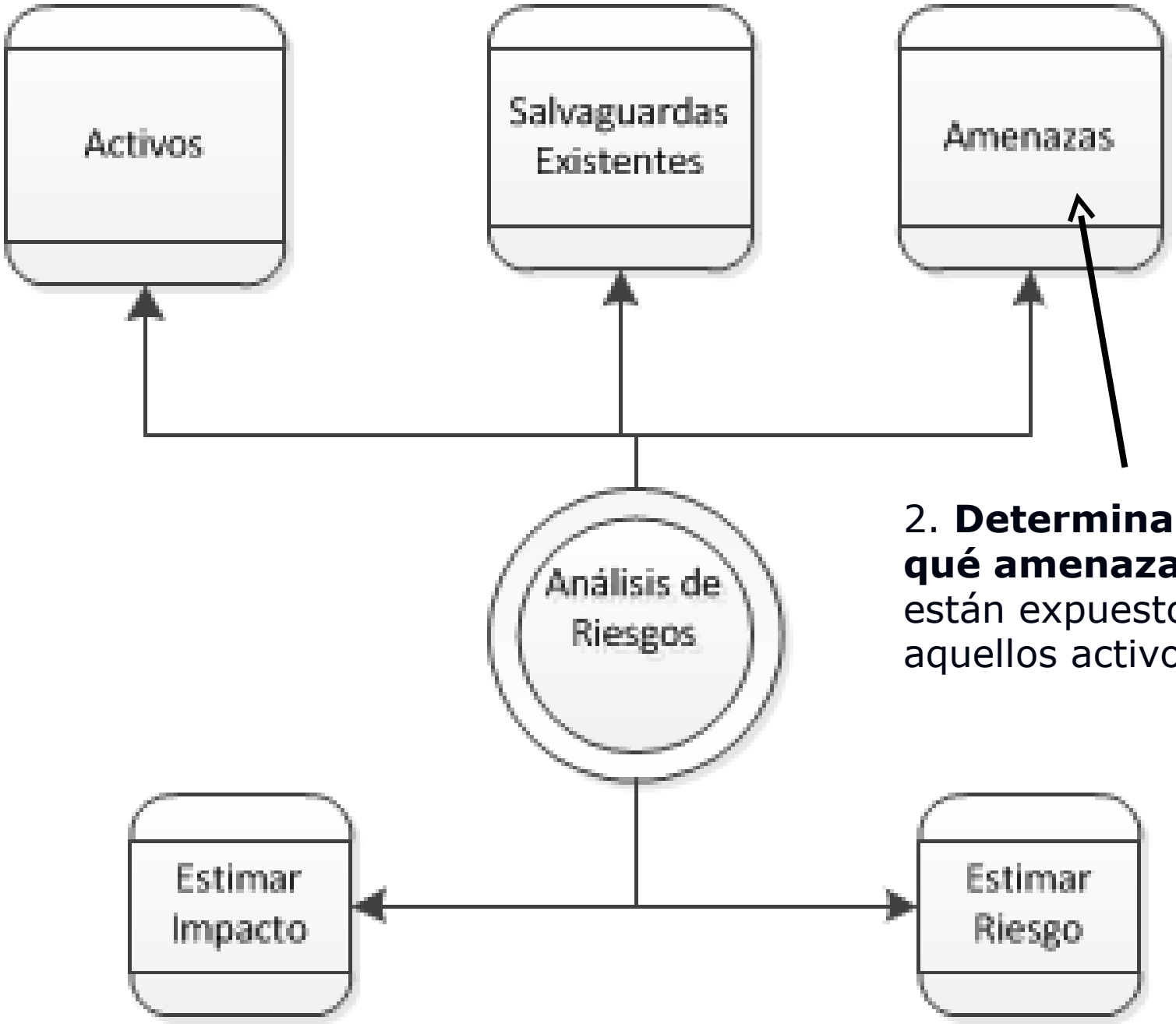
Diccionario María Moliner

Aplicaciones del AGR

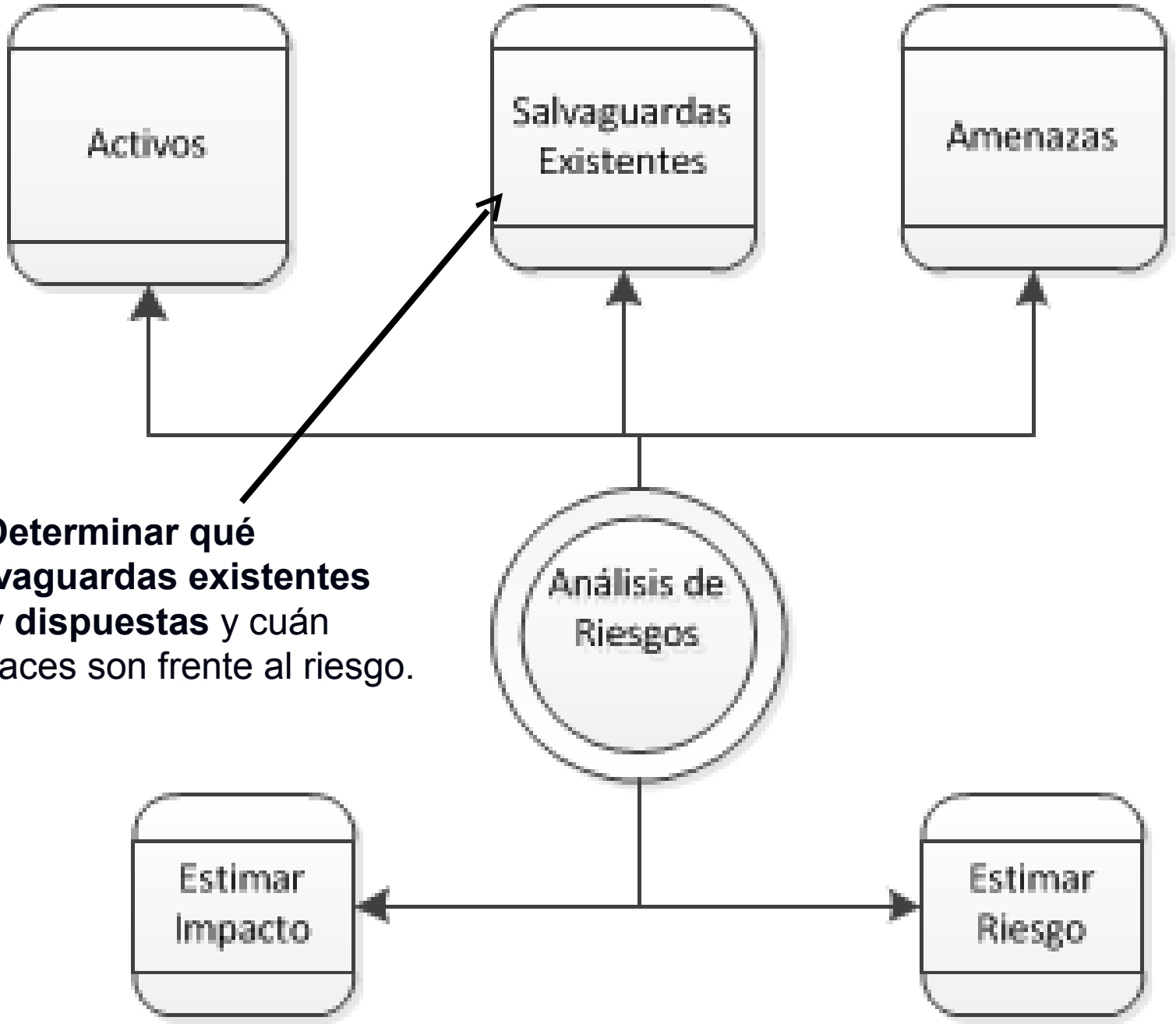




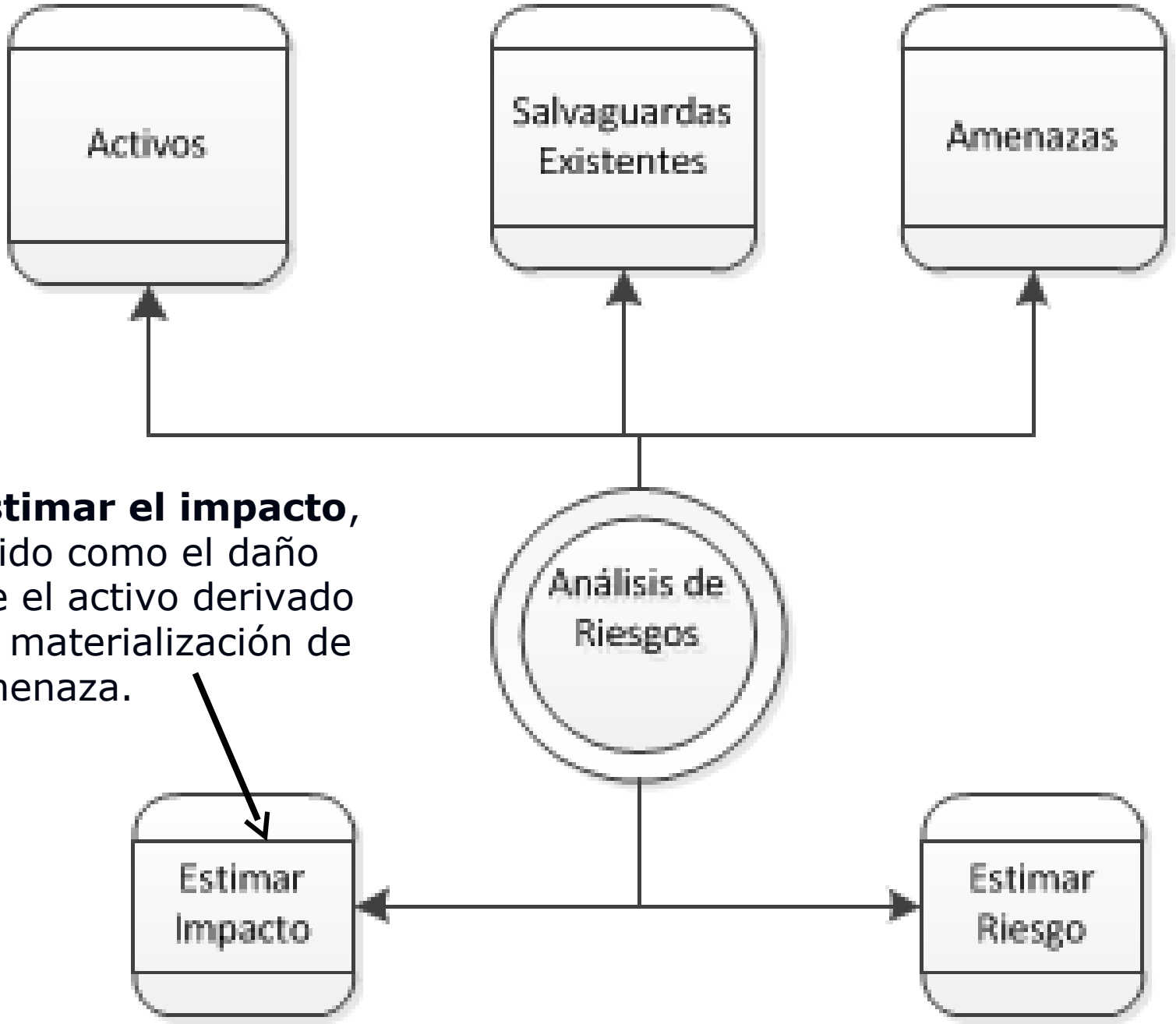
1. **Determinar los activos relevantes** para la Organización, su interrelación y su valor, en el sentido de qué perjuicio (coste) supondría su degradación.



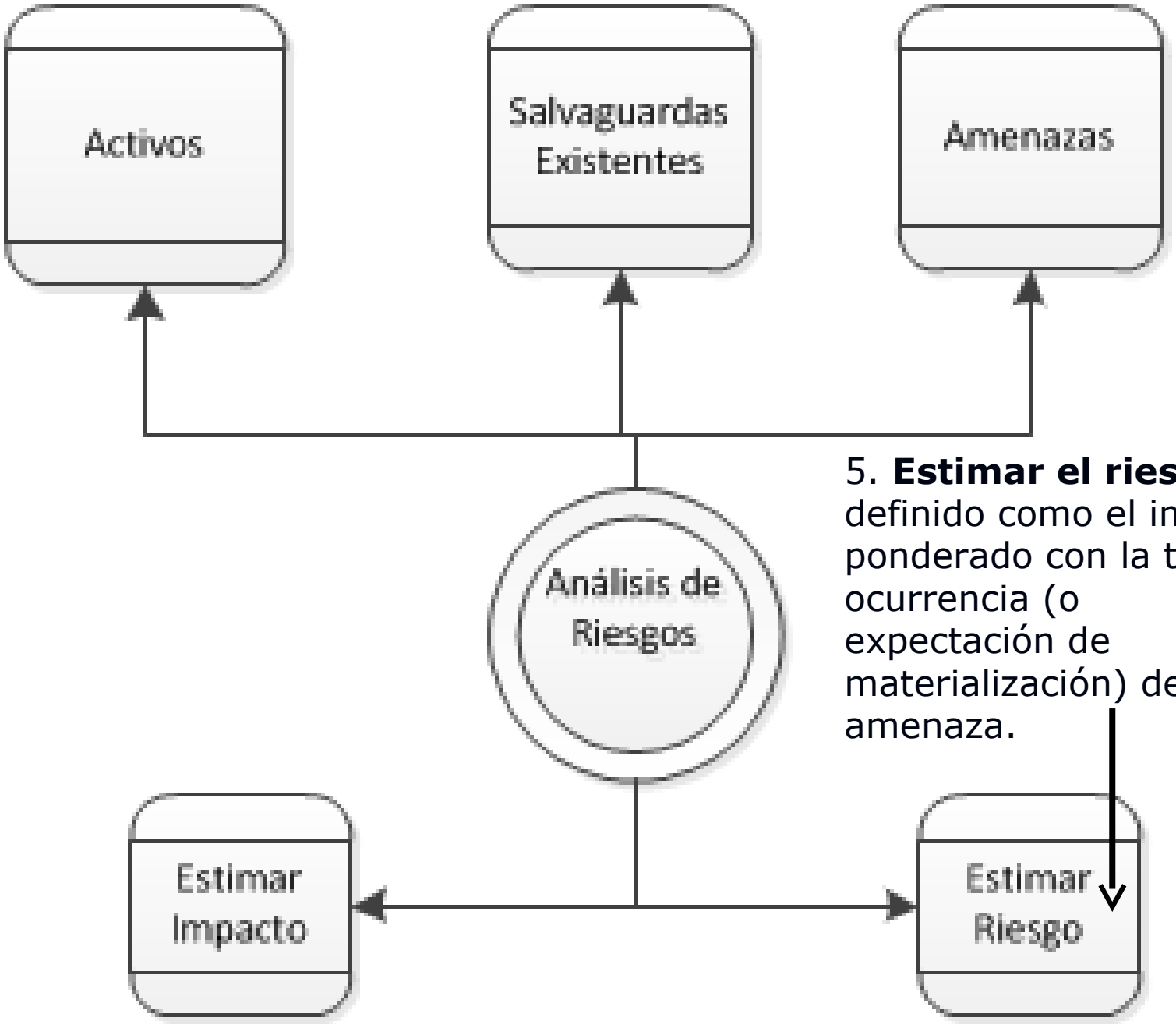
2. **Determinar a qué amenazas** están expuestos aquellos activos.



3. **Determinar qué salvaguardas existentes hay dispuestas** y cuán eficaces son frente al riesgo.

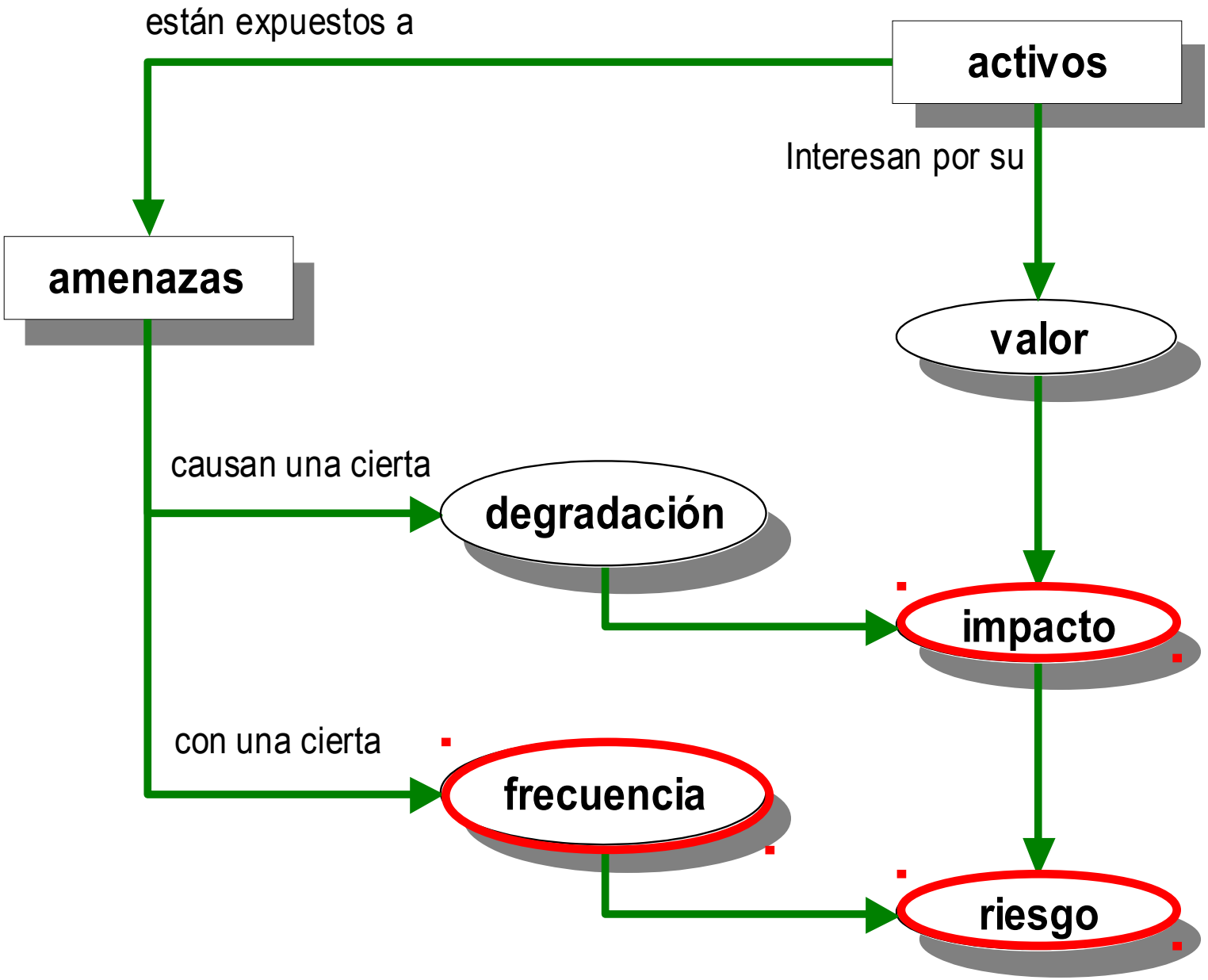


4. **Estimar el impacto**, definido como el daño sobre el activo derivado de la materialización de la amenaza.



5. **Estimar el riesgo**, definido como el impacto ponderado con la tasa de ocurrencia (o expectación de materialización) de la amenaza.

Análisis de riesgos

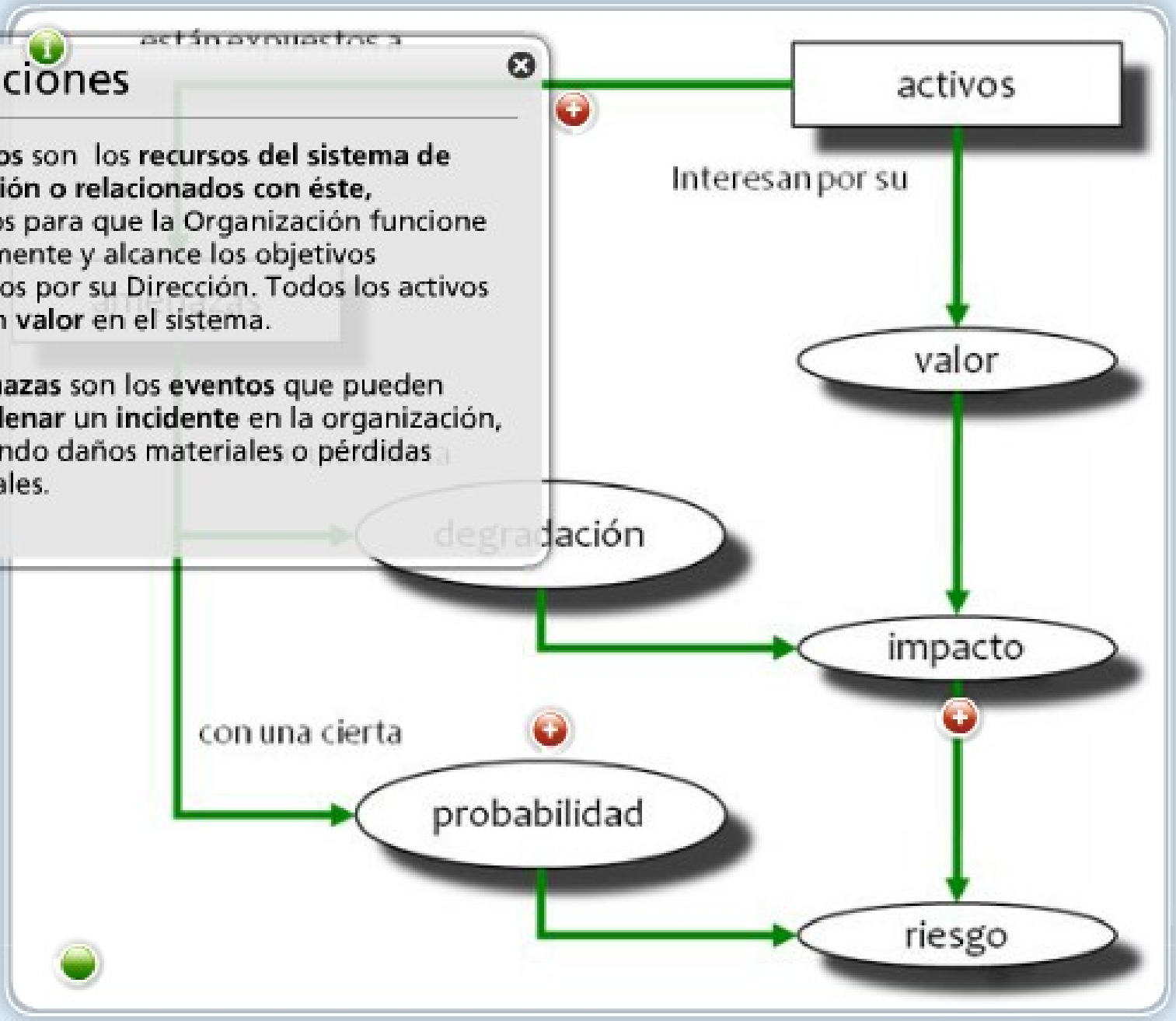


Activos y amenazas

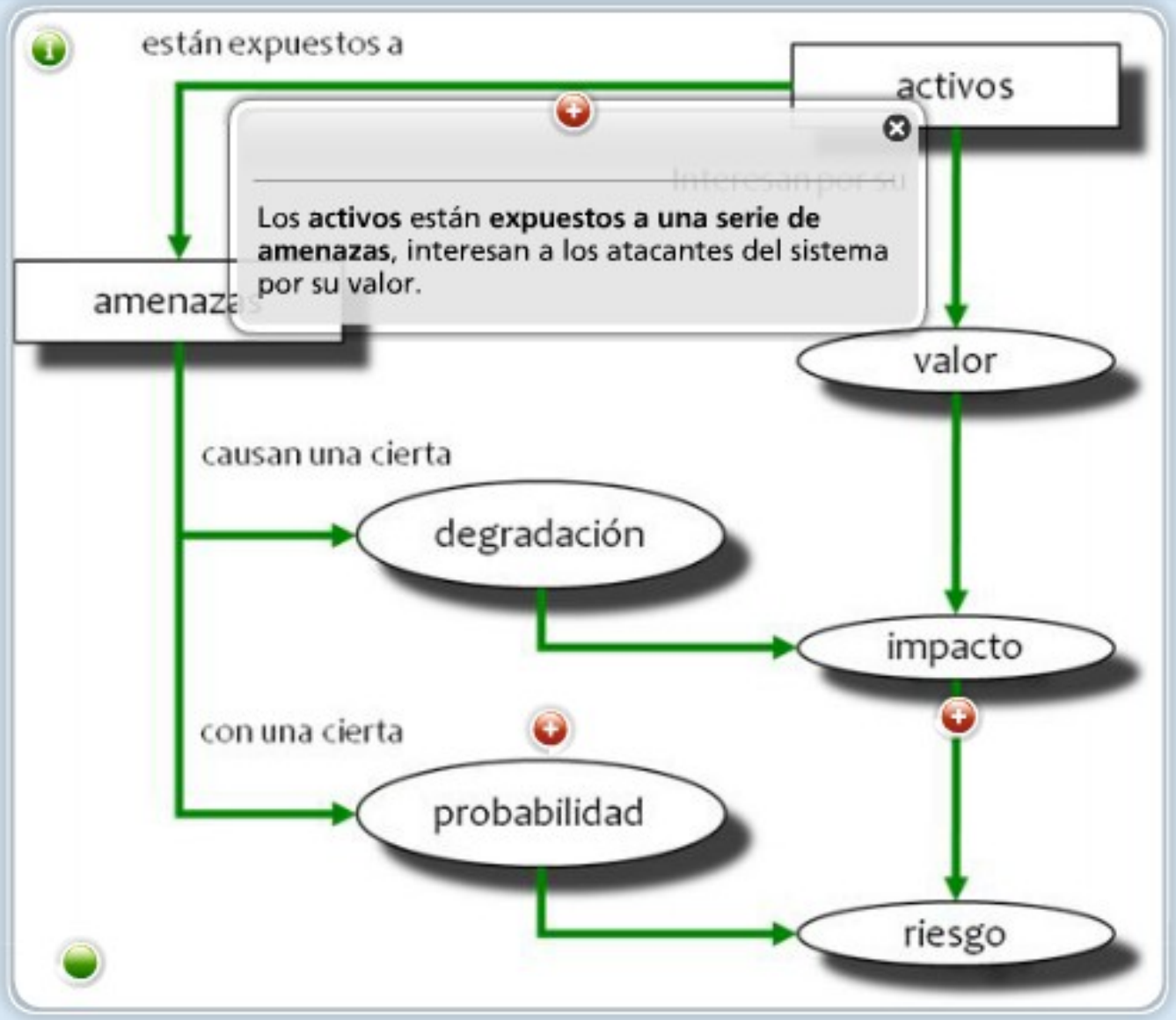
Definiciones

Los **activos** son los **recursos del sistema de información o relacionados con éste,** necesarios para que la Organización funcione correctamente y alcance los objetivos propuestos por su Dirección. Todos los activos tienen un **valor** en el sistema.

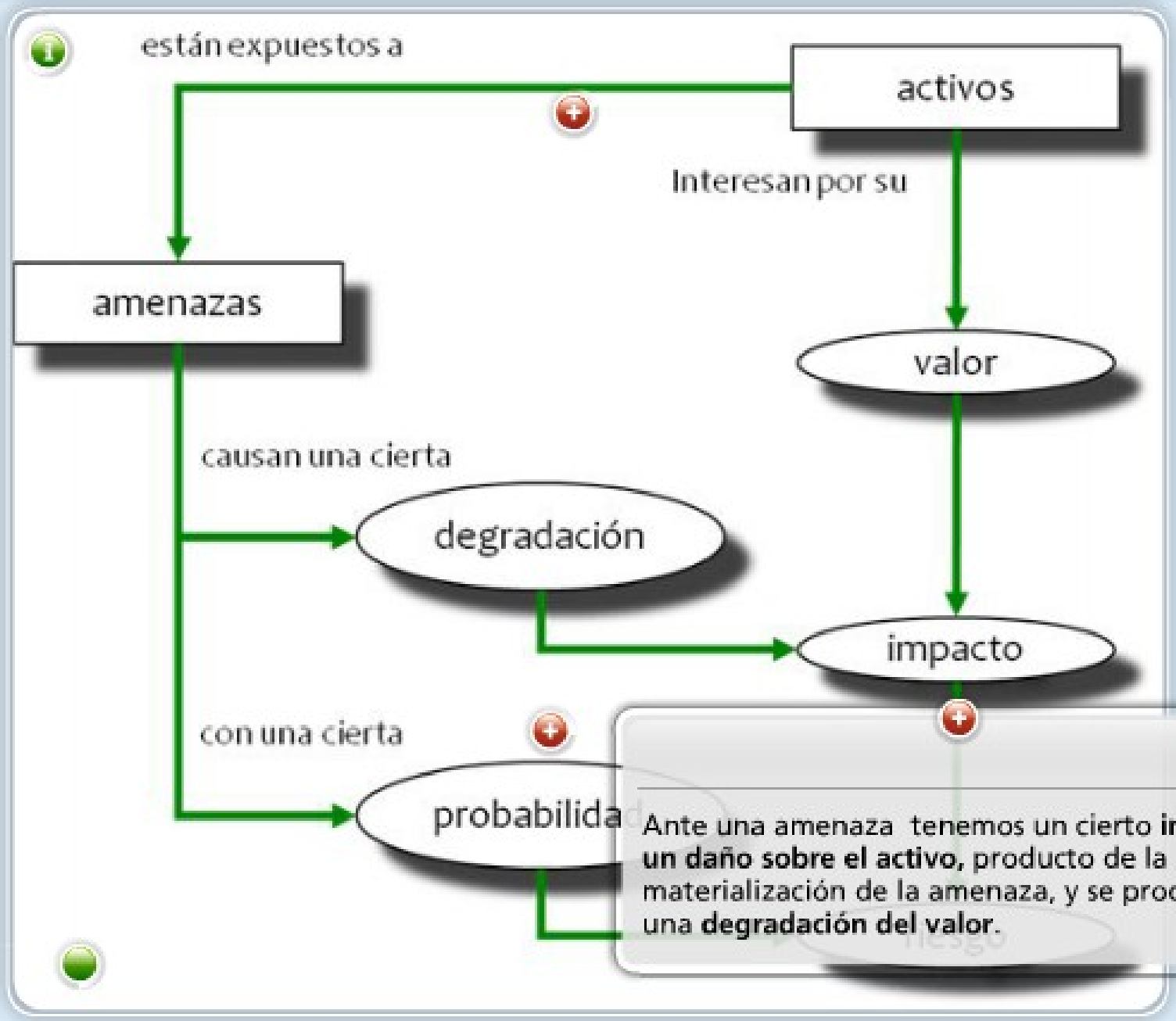
Las **amenazas** son los **eventos** que pueden **desencadenar** un **incidente** en la organización, produciendo daños materiales o pérdidas inmateriales.



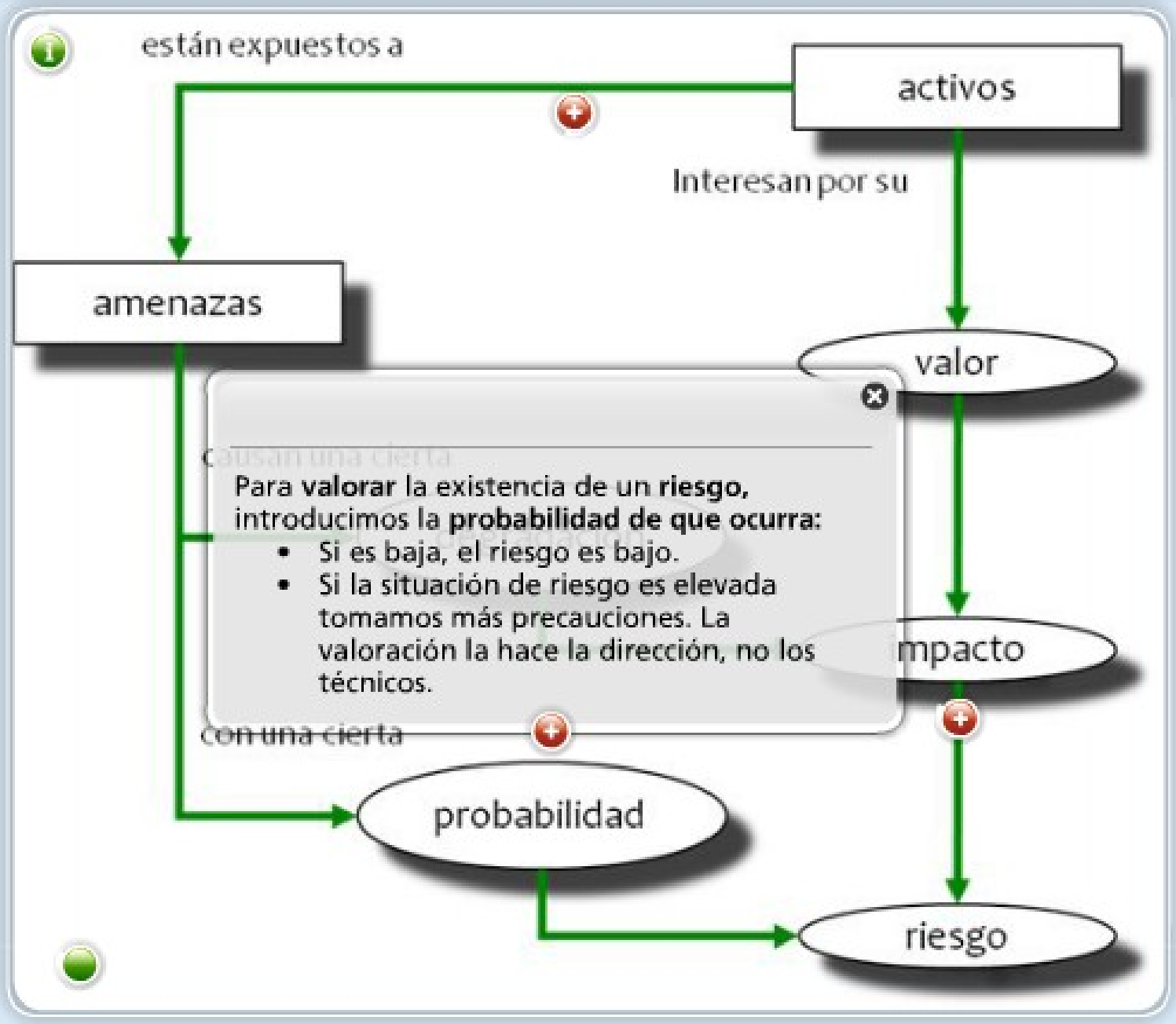
Activos y amenazas



Activos y amenazas

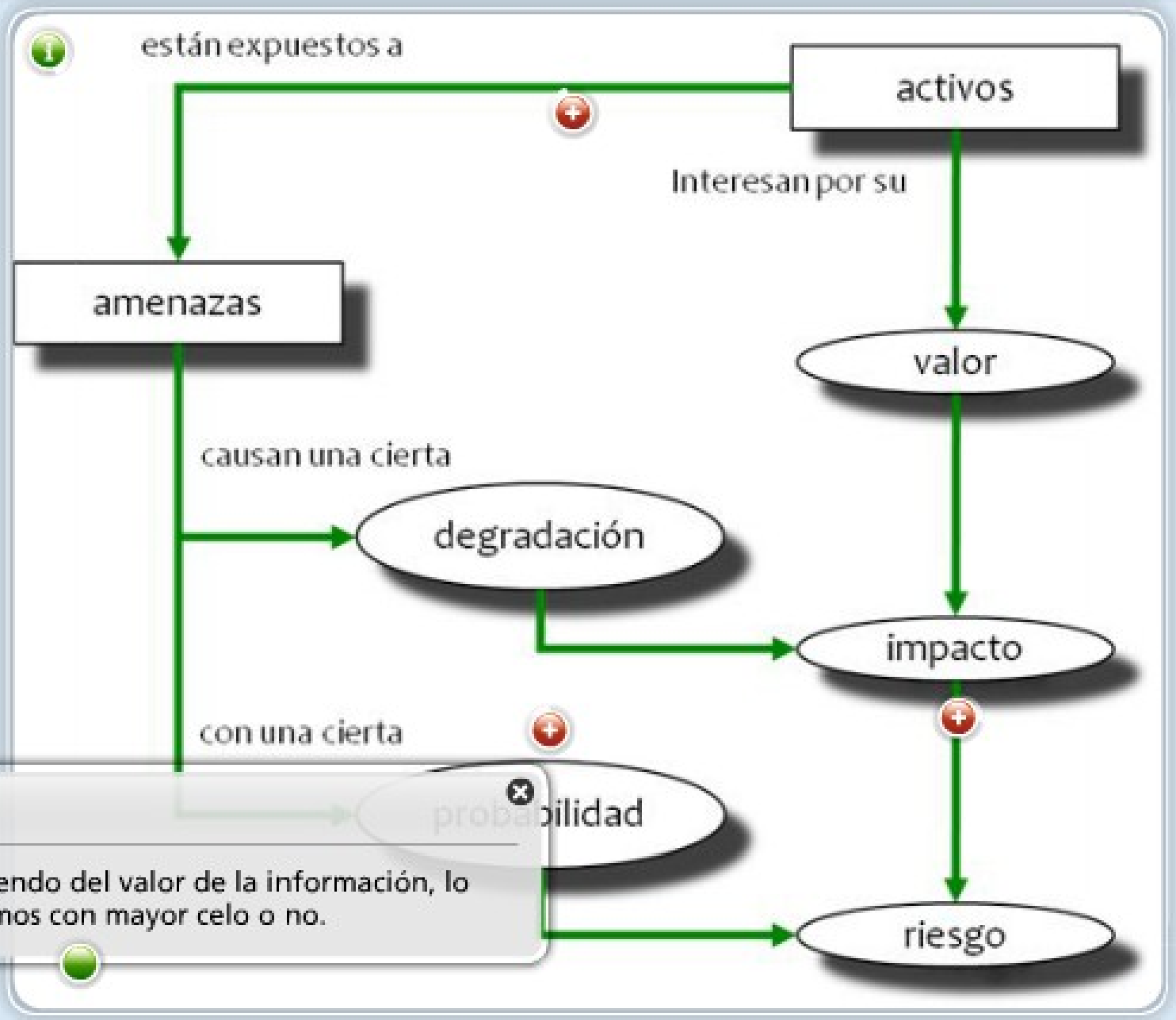


Activos y amenazas



Activos y amenazas

Siguiente

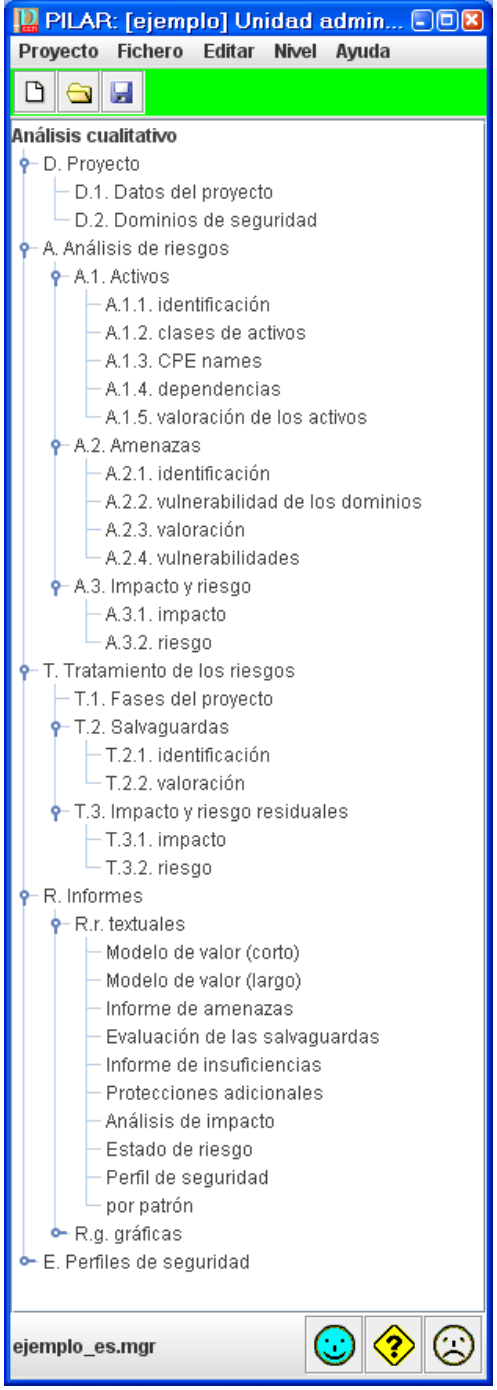


Dependiendo del valor de la información, lo protegemos con mayor celo o no.

El análisis de los riesgos se lleva a cabo por medio de las siguientes tareas:

MAR – Método de Análisis de Riesgos

- MAR.1 – Caracterización de los activos
  - MAR.11 – Identificación de los activos
  - MAR.12 – Dependencias entre activos
  - MAR.13 – Valoración de los activos
- MAR.2 – Caracterización de las amenazas
  - MAR.21 – Identificación de las amenazas
  - MAR.22 – Valoración de las amenazas
- MAR.3 – Caracterización de las salvaguardas
  - MAR.31 – Identificación de las salvaguardas pertinentes
  - MAR.32 – Valoración de las salvaguardas
- MAR.4 – Estimación del estado de riesgo
  - MAR.41 – Estimación del impacto
  - MAR.42 – Estimación del riesgo



Paso 1: Determinar los Activos relevantes para la organización

Definición: Componente o funcionalidad de un sistema de información susceptible de ser atacado deliberada o accidentalmente con consecuencias para la organización.

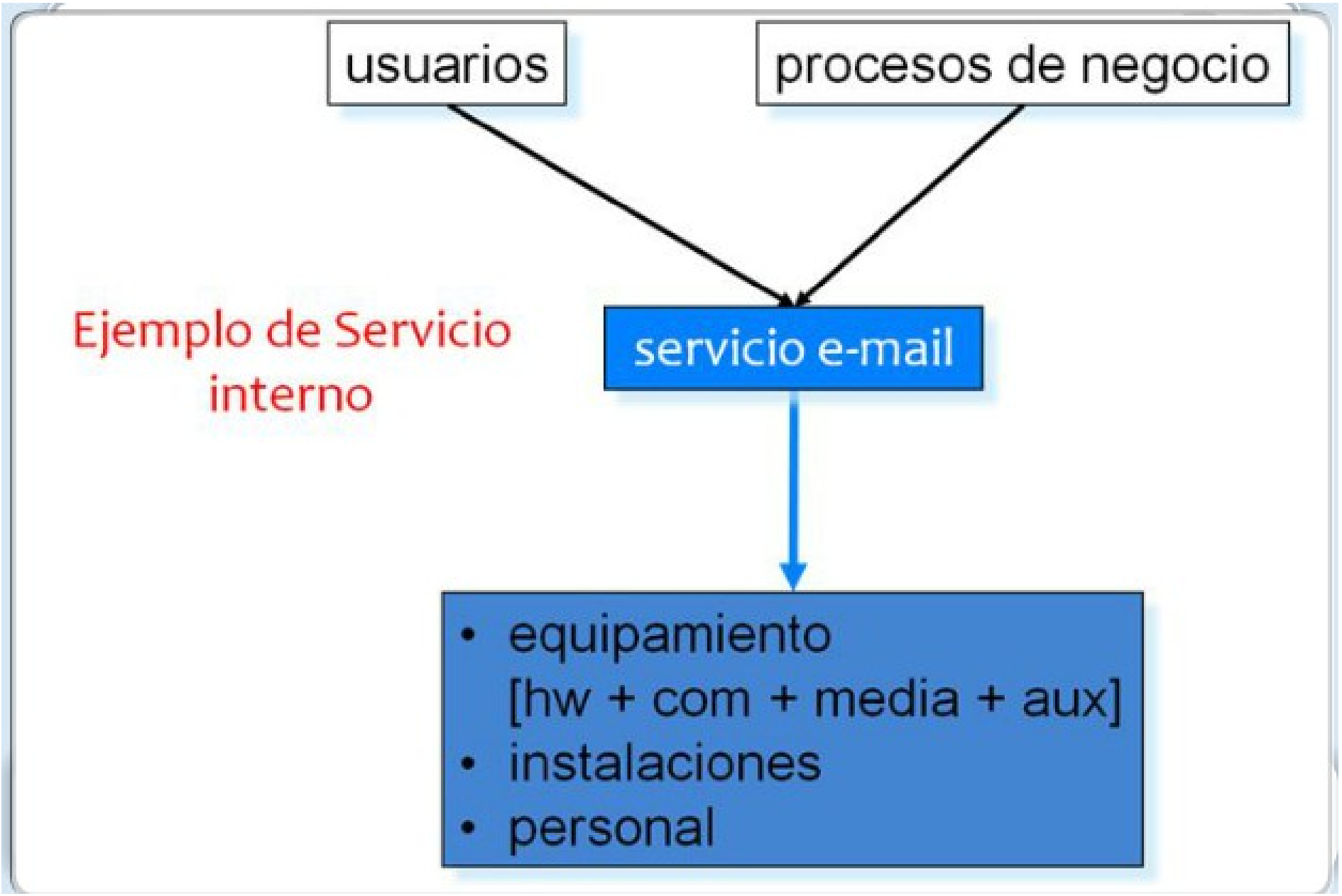
En un sistema de información hay 2 cosas esenciales:

- **La información** que maneja.
- **Los servicios** prestados gracias a los datos, y los servicios necesarios para gestionar los datos.

Subordinados a dicha esencia se pueden identificar otros activos relevantes:

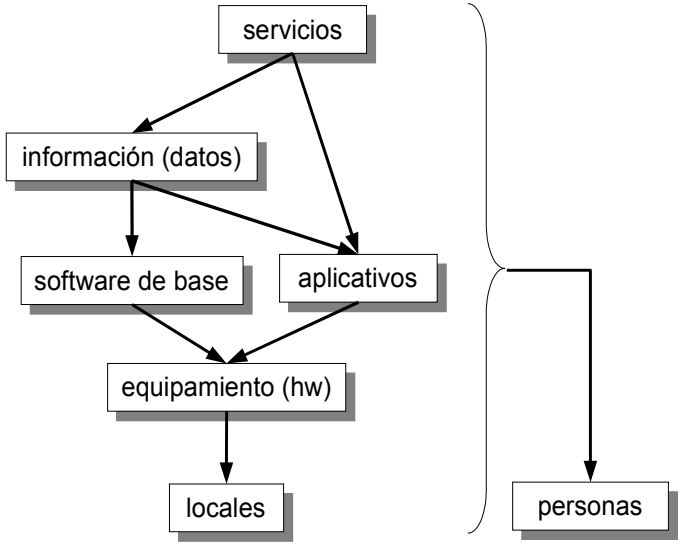
- **Datos** que materializan la información.
- **Servicios** auxiliares que se necesitan para poder organizar el sistema.
- **Las aplicaciones informáticas** (software) que permiten manejar los datos.
- **Los equipos informáticos** (hardware) que permite hospedar datos, aplicaciones y servicios.
- **Los soportes de información** que son dispositivos de almacenamiento de datos.
- **Las redes de comunicaciones** que permiten intercambiar datos.
- **Las instalaciones** que acogen equipos informáticos y de comunicaciones.
- **Las personas** que explotan u operan todos los elementos anteriormente citados.

- Capítulo 2 del "Catálogo de Elementos"


usuarios
procesos de negocio
Ejemplo de Servicio interno
servicio e-mail
• equipamiento [hw + com + media + aux]
• instalaciones
• personal

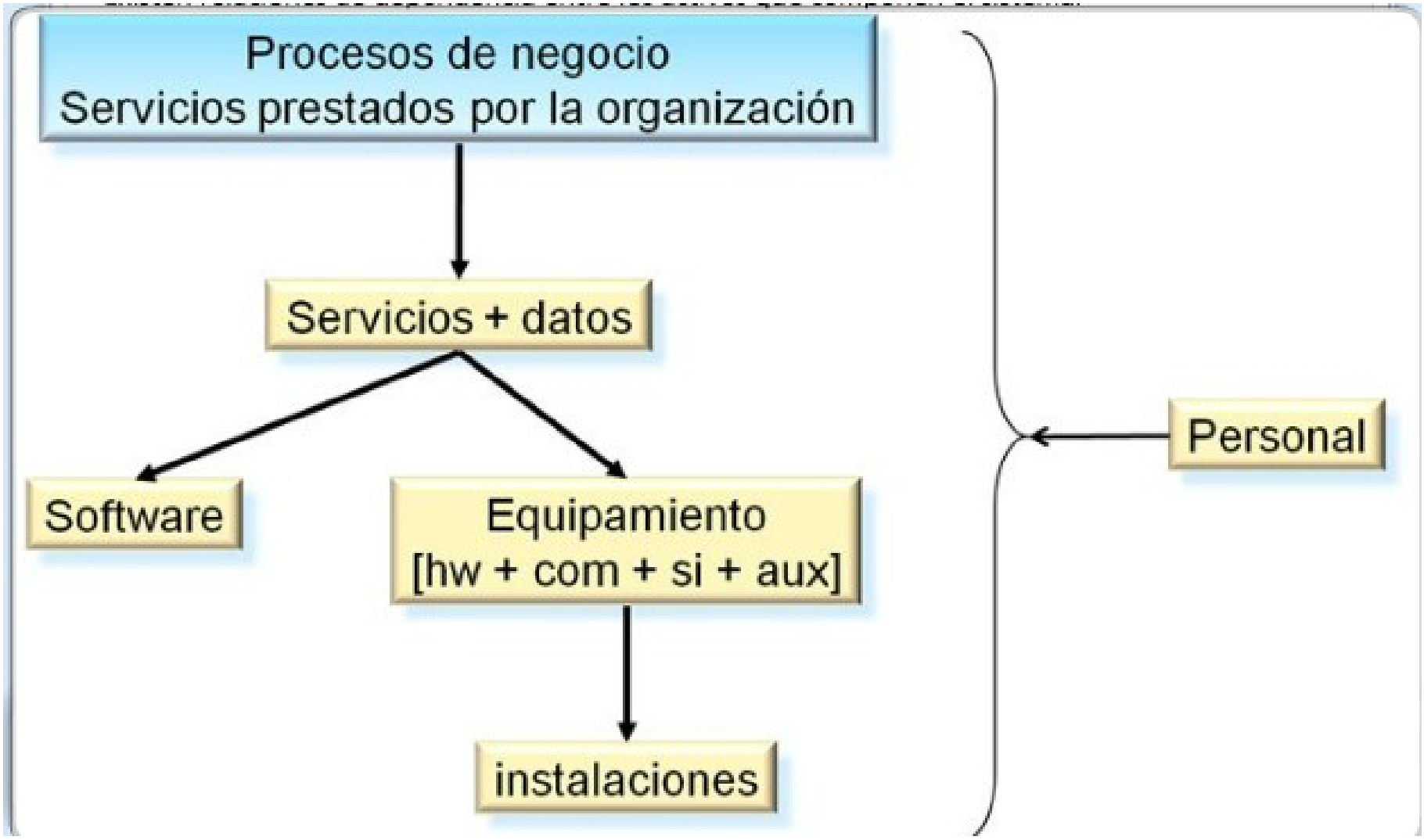
Paso 1: Determinar los Activos relevantes para la organización

Dependencias



Valoración. ¿Cuánto vale la “salud” de los activos?

Dimensiones


Procesos de negocio
Servicios prestados por la organización
Servicios + datos
Software
Equipamiento
[hw + com + si + aux]
instalaciones
Personal

Determinar los Activos relevantes para la organización

- 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 cifra, 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


OTROS
FUNCIONALIDADES
INFORMACIÓN
SISTEMA INFORMACIÓN
ENTORNO
Credibilidad (ética, jurídica)
Conocimiento acumulado
Intimidad de una persona física
Integridad material de personas
Objetivos y misión de la organización
Bienes y servicios producidos
Personal usuario y/o destinatario de los bienes o servicios producidos
Datos (concurrentes al o resultantes del SI)
Meta-información (estructuración, índices, claves de cifrado)
Soportes (tratables informáticamente, no tratables)
Hardware (de proceso, almacenamiento, servidores, firmware)
Software (de base, paquetes, producción de aplicaciones)
Comunicaciones (redes propias, servicios, conexiones)
Equipamientos y suministros (energía, climatización, comunicaciones)
Personal (de dirección, de operación, de desarrollo)
Otros tangibles (edificaciones, mobiliario, instalación física)

Paso 1. Determinar los Activos relevantes para la organización

La **valoración** es la determinación del coste que supondría salir de una incidencia que destrozara el activo. **Factores a considerar**:

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

Paso 1. Determinar los Activos relevantes para la organización

La **valoración** puede ser **cuantitativa** (con una cantidad numérica) o **cualitativa** (en alguna escala de niveles). Los **criterios más importantes a respetar** son:

la **homogeneidad**: es importante poder comparar valores aunque sean de diferentes dimensiones a fin de poder combinar valores propios y valores acumulados, así como poder determinar si es más grave el daño en una dimensión o en otra.

la **relatividad**: es importante poder relativizar el valor de un activo en comparación con otros.

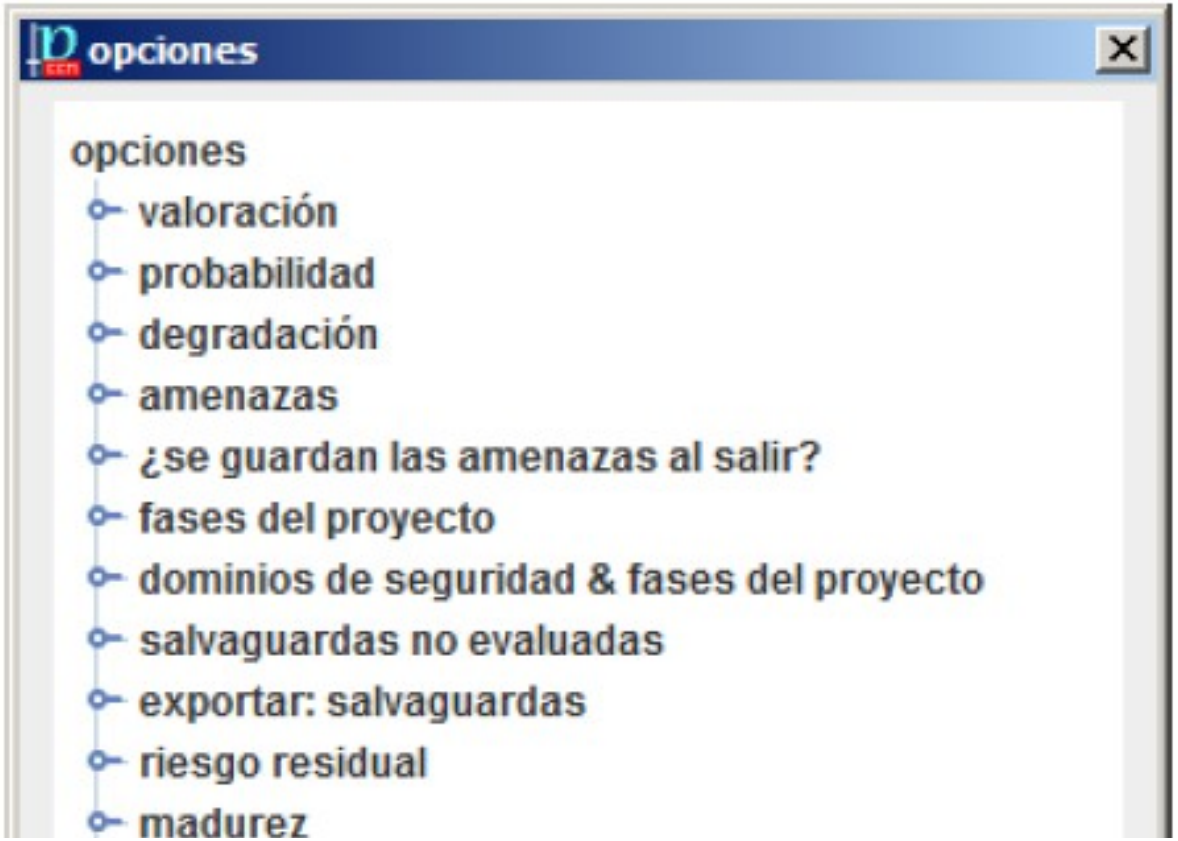
Valoración cualitativa

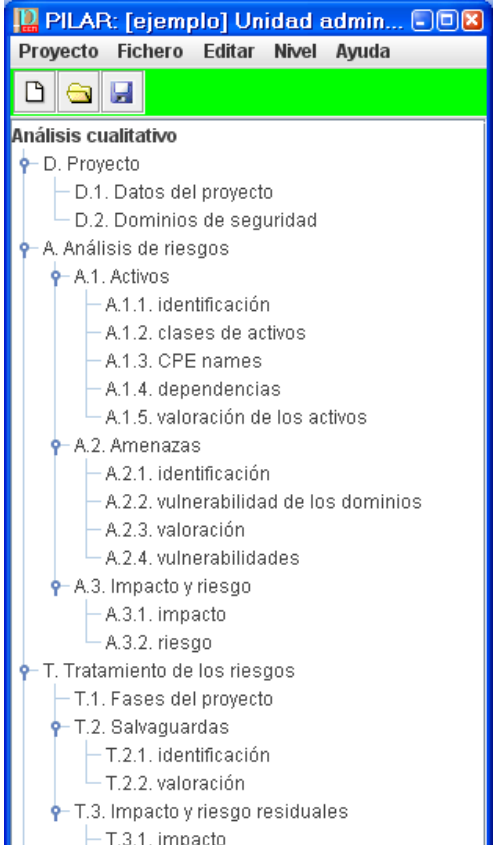
Las escalas cualitativas permiten avanzar con rapidez, posicionando el valor de cada activo en un orden relativo respecto de los demás. Es frecuente plantear estas escalas como "órdenes de magnitud" y, en consecuencia, derivar estimaciones del orden de magnitud del riesgo.

Valoración cuantitativa

Si la valoración es dineraria, además podemos hacer estudios económicos comparando lo que arriesgamos con lo que cuesta la solución respondiendo a las preguntas:

- ¿Vale la pena invertir tanto dinero en esta salvaguarda?
- ¿Qué conjunto de salvaguardas optimizan la inversión?
- ¿En qué plazo de tiempo se recupera la inversión?
- ¿Cuánto es razonable que cueste la prima de un seguro?





Opciones / Valoración

El sistema de información se puede valorar activo por activo (más dependencias) o por dominios de seguridad.

En ambos casos, se valoran los activos esenciales.

valoración / activos + dependencias

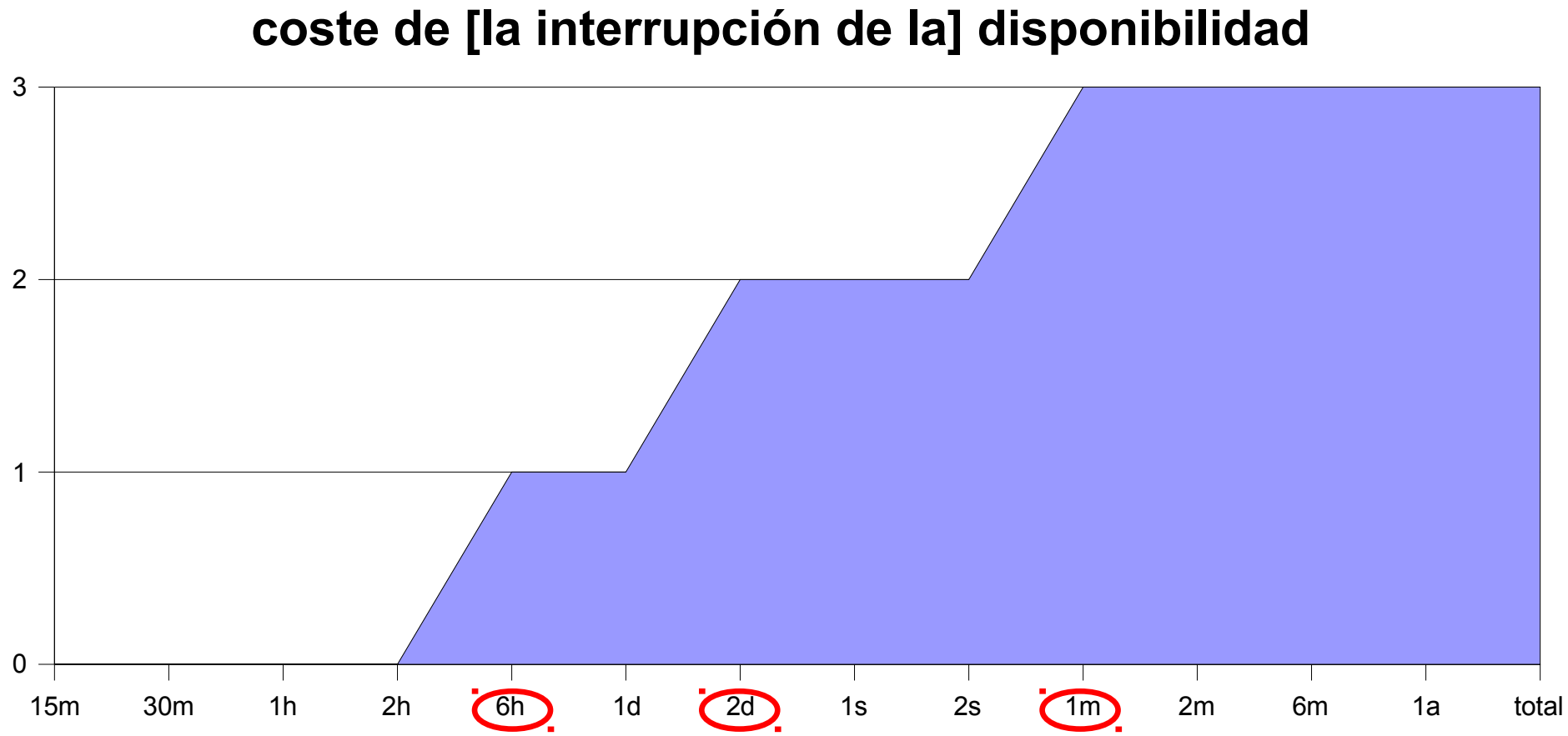
el valor de los activos esenciales se aplica a todos los activos del dominio de seguridad

valoración / dominios

el valor se propaga siguiendo las dependencias entre activos

La valoración por dominios es más rápida, mientras que la valoración por dependencias es más precisa.

El valor de la interrupción del servicio



En el ejemplo, paradas de hasta 6 horas se pueden asumir sin consecuencias. Pero a las 6 horas se disparan las alarmas que aumentan si la parada supera los 2 días. Y si la parada supera el mes, se puede decir que la Organización ha perdido su capacidad de operar: ha muerto.

Paso 2: Determinar las Amenazas a las que están sometidos los Activos

Definición: Causa potencial de un incidente que puede causar daños a un sistema de información o a una organización.

Tipos: *Grupos de Amenazas (de origen natural, del entorno, defectos de las aplicaciones, causadas por personas de forma accidental, causadas por las personas de forma deliberada)*

Degradación: cuán perjudicado resultaría el activo

Probabilidad: cuán probable o improbable es que se materialice la amenaza

La degradación mide el daño causado por un incidente en el supuesto de que ocurriera.

Valoración:
Frecuencia estimada de materialización de la amenaza.

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

Catálogo de elementos
Capítulo 5

Tipos de amenazas:

- accidentales
  - industriales
    - electricidad, emanaciones, ...
  - humanas: errores y omisiones
- deliberadas (intencionales)
  - intercepción pasiva o activa
  - intrusión, espionaje, ...
  - robo, fraude, ...

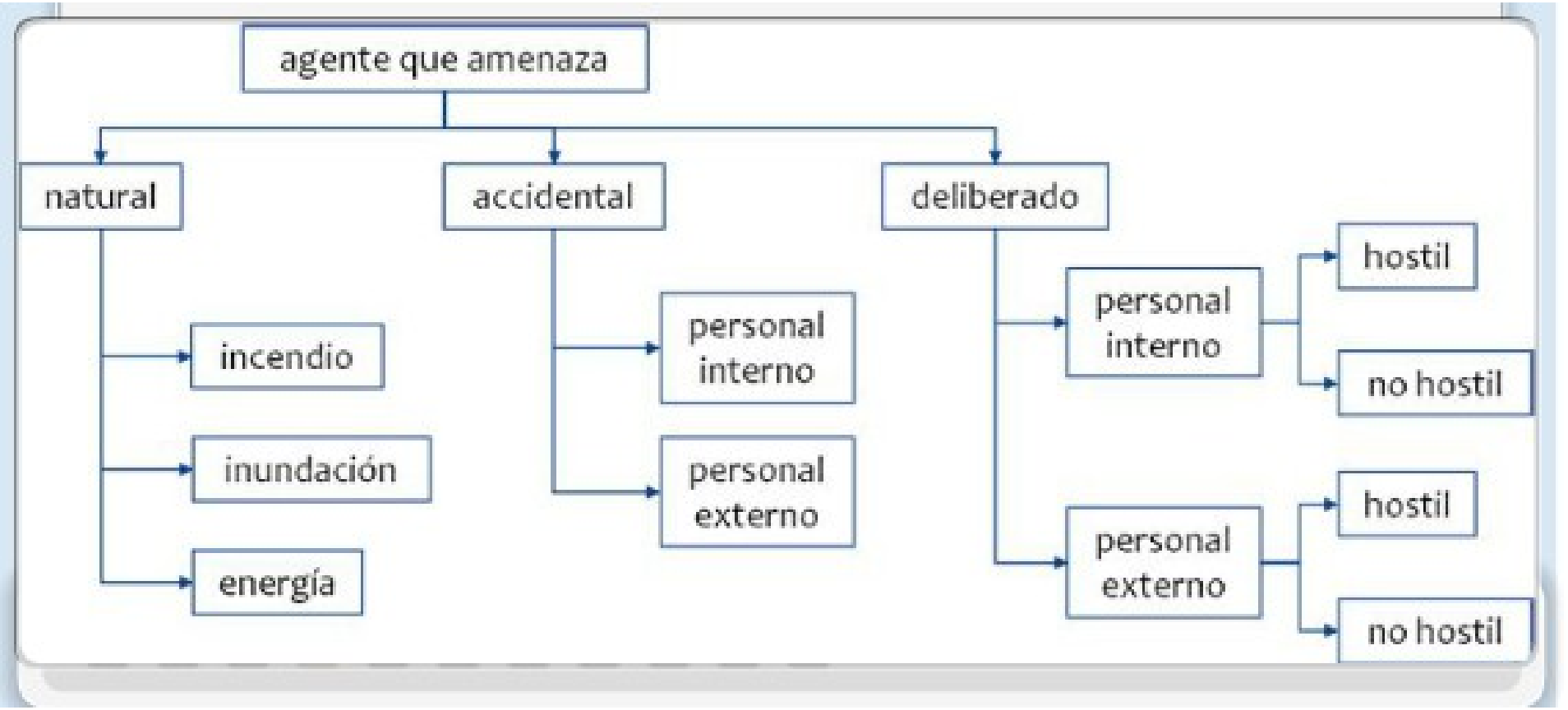
Clasificación de las amenazas por grupos de activos

	Accidente natural o industrial	origen humano directo	origen humano indirecto
personas			
hardware	Inundación		
software			Propagación no intencionada de virus

Clasificación de las amenazas por tipo de impacto

	accidentales	deliberadas
Autenticidad		
Confidencialidad		
Integridad		Virus informático
Disponibilidad	fuego	
otras ...		

Clasificación de las amenazas por agente causante



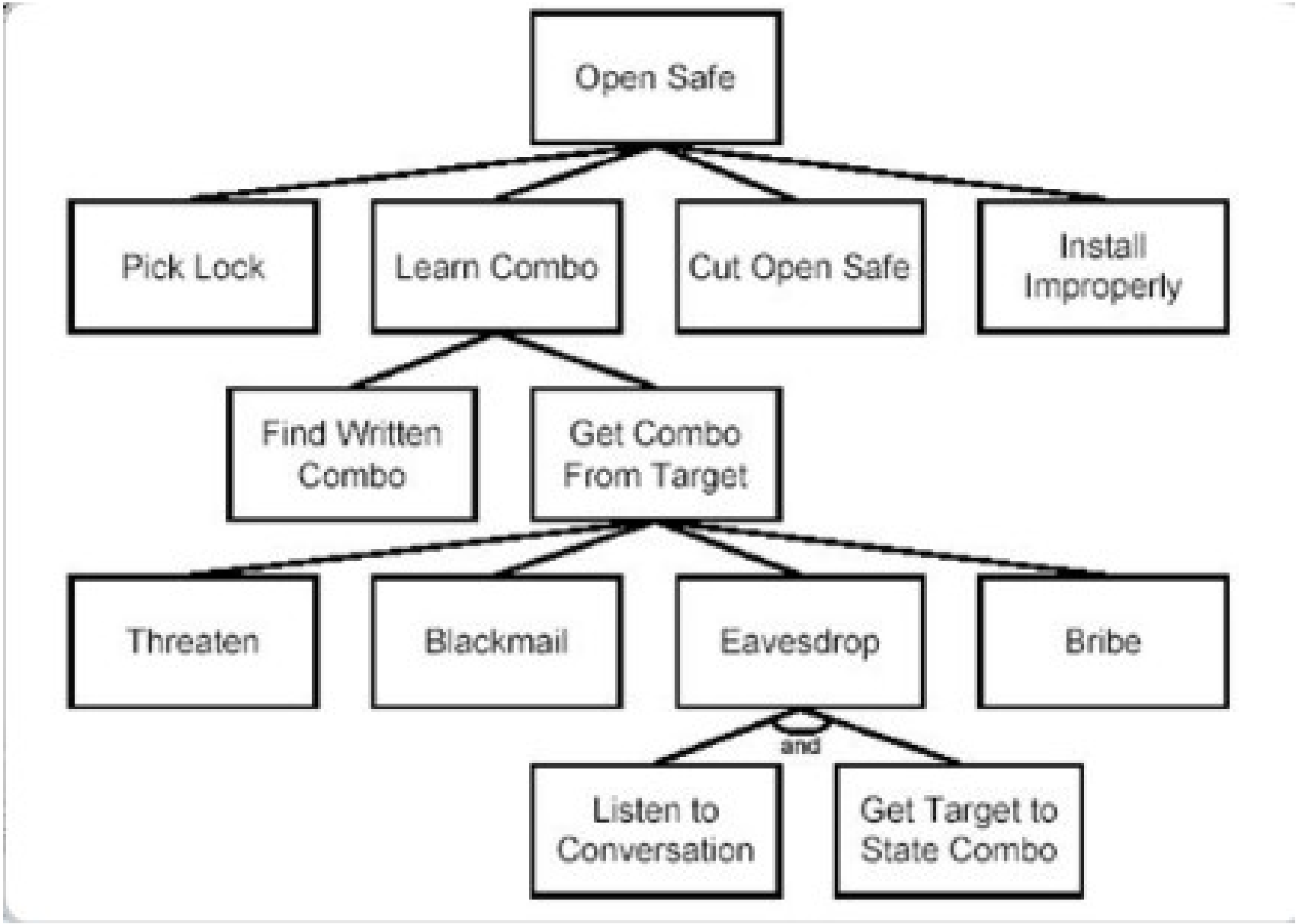
Clasificación por agente causante

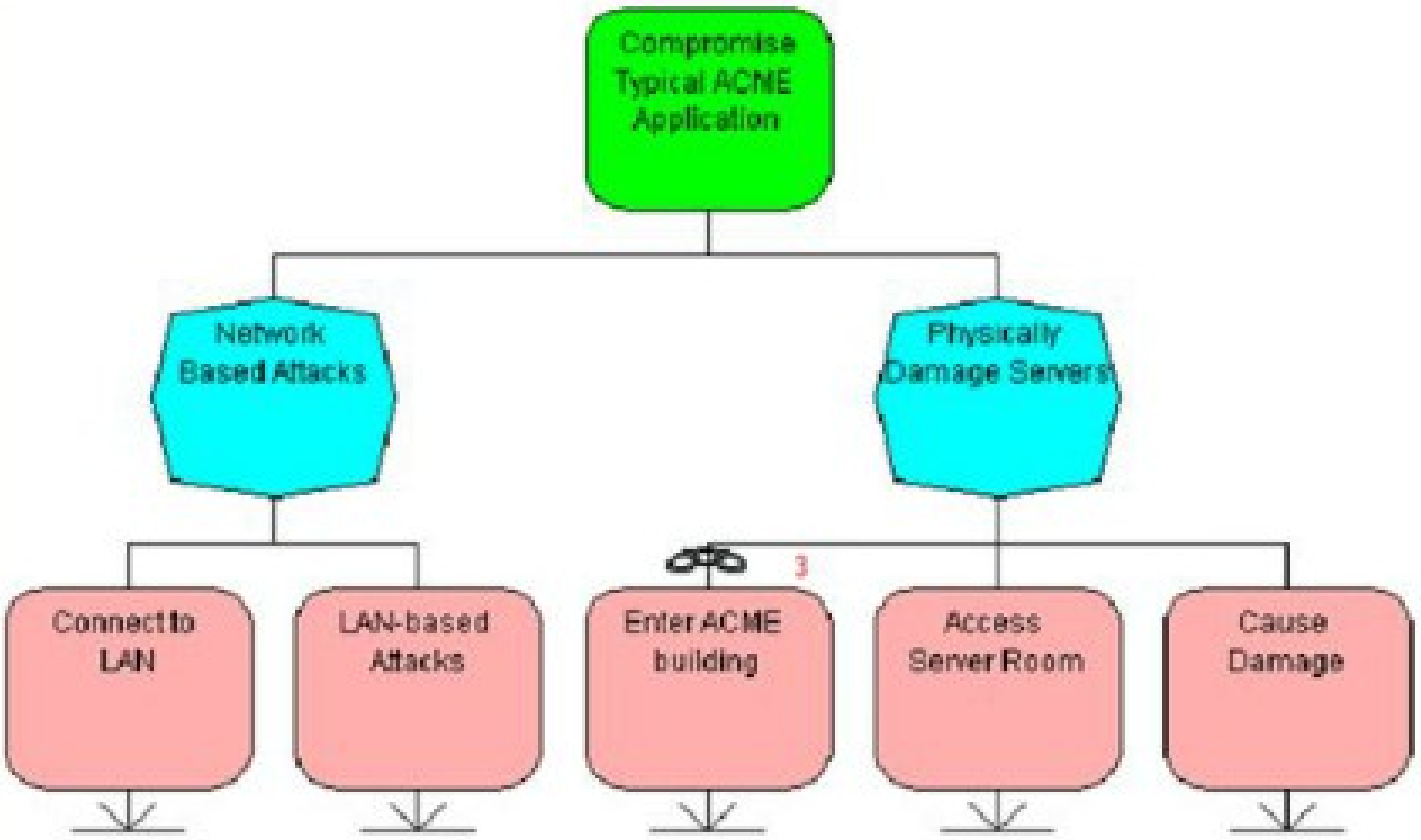
Threat-Source	Motivation	Threat Actions
Hacker, cracker	Challenge Ego Rebellion	• Hacking • Social engineering • System intrusion, break-ins • Unauthorized system access
Computer criminal	Destruction of information Illegal information disclosure Monetary gain Unauthorized data alteration	• Computer crime (e.g., cyber stalking) • Fraudulent act (e.g., replay, impersonation, interception) • Information bribery • Spoofing • System intrusion
Terrorist	Blackmail Destruction Exploitation Revenge	• Bomb/Terrorism • Information warfare • System attack (e.g., distributed denial of service) • System penetration • System tampering
Industrial espionage (companies, foreign governments, other government interests)	Competitive advantage Economic espionage	• Economic exploitation • Information theft • Intrusion on personal privacy • Social engineering • System penetration • Unauthorized system access (access to classified, proprietary, and/or technology-related information)

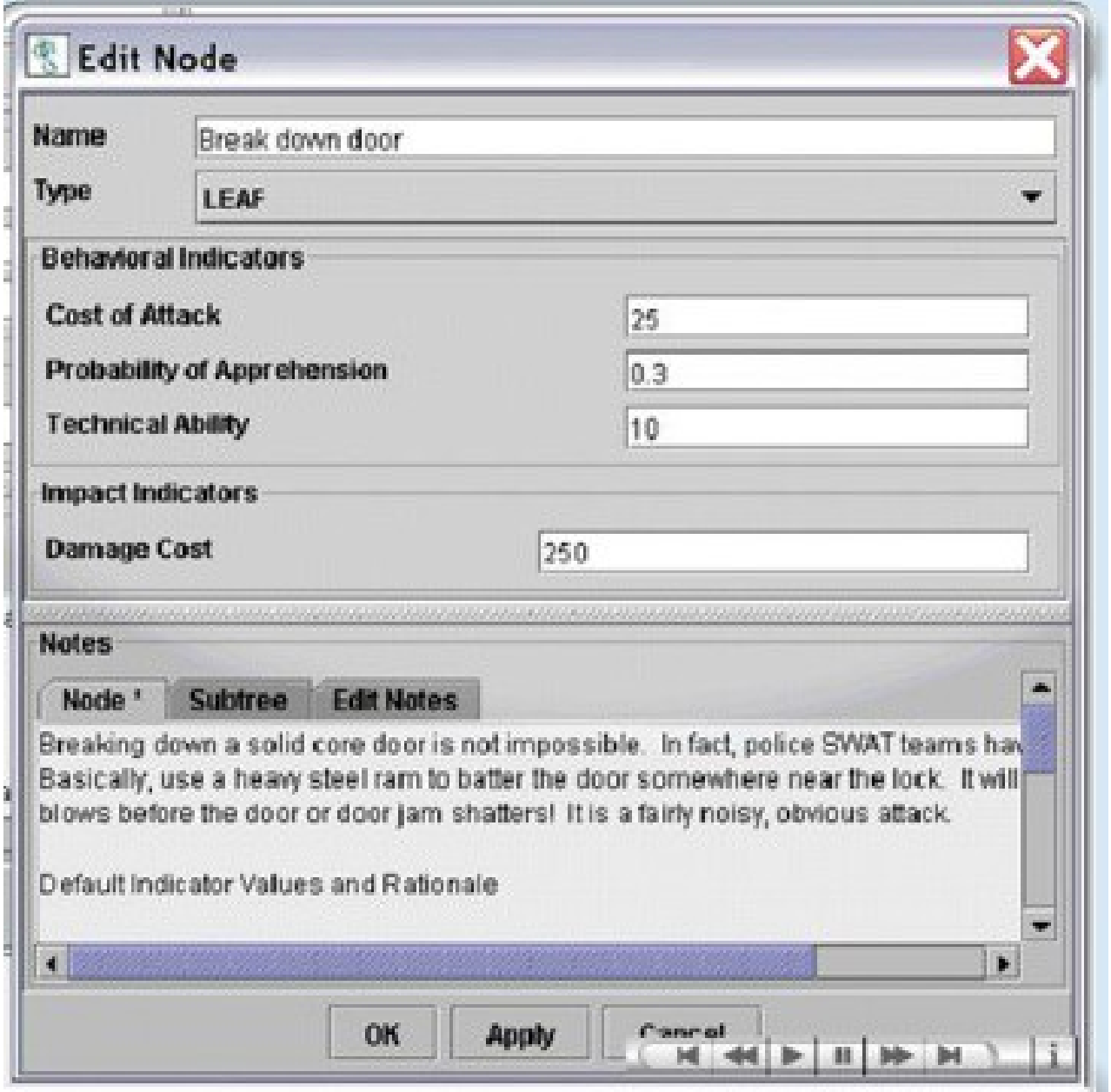
Árboles de ataque

Se utilizan en análisis más completos y formales. Se realiza una construcción con los diferentes componentes de donde puede venir la amenaza y a qué afecta. Conociendo al atacante, podemos poner las medidas.

- Existen amenazas que actúan directamente sobre los activos.
- Existen amenazas que actúan indirectamente sobre los activos habilitando otras amenazas.
- Pueden requerirse la conjunción de desastres para que se materialice una amenaza: AND.
- Una amenaza funcional puede ocurrir por diferentes vías prácticas: OR.
- No es acumulativa: no se puede destruir lo destruido.


Open Safe
Pick Lock
Learn Combo
Cut Open Safe
Install Improperly
Find Written Combo
Get Combo From Target
Threaten
Blackmail
Eavesdrop
Bribe
and
Listen to Conversation
Get Target to State Combo


Compromise Typical ACME Application
Network Based Attacks
Physically Damage Servers
Connect to LAN
LAN-based Attacks
Enter ACME building
Access Server Room
Cause Damage



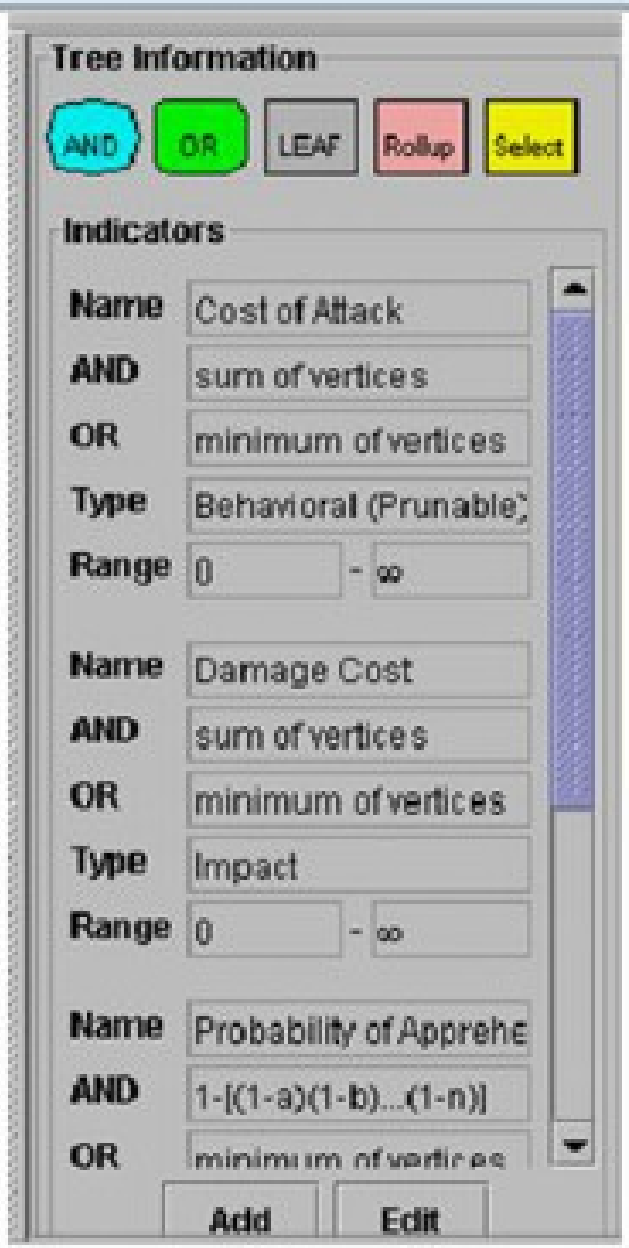
9 Árboles de ataque

Se califican los nodos del árbol:

- Coste del ataque.
- Impacto.
- Miedo del atacante.

Se pueden modelar escenarios:

- Coste X.
- Inversión Y.
- Interés Z.



[código] descripción sucinta de lo que puede pasar	
Tipos de activos: ▯ que se pueden ver afectados por este tipo de amenazas	**Dimensiones:** 1. de seguridad que se pueden ver afectadas por este tipo de amenaza, ordenadas de más a menos relevante
Descripción: complementaria o más detallada de la amenaza: lo que le puede ocurrir a activos del tipo indicado con las consecuencias indicadas	

[N.º] Desastres naturales	
Tipos de activos: ▯ [HW] equipos informáticos (hardware) ▯ [COM] redes de comunicaciones ▯ [SI] soportes de información ▯ [AUX] equipamiento auxiliar ▯ [L] instalaciones	**Dimensiones:** 1. [D] disponibilidad 2. [T_S] trazabilidad de los servicios 3. [T_D] trazabilidad de los datos

1 Probabilidad

Problemas de la probabilidad.

- La probabilidad es **"fácil"** de estimar:
  - En ataques no deliberados: naturales / industriales / fallos humanos.
  - Basado en series históricas: análisis estadístico.

- Es **"difícil"** de estimar:
  - En ataques deliberados.
  - En sistemas nuevos.
  - ¿Cómo de sensibles somos al criterio del que estima?
  - Introduce una cierta incertidumbre en detrimento de la credibilidad del análisis de riesgos (se piensa que la probabilidad es subjetiva).

2 Probabilidad

Agravantes que afectan a la determinación de la probabilidad:

- El **deseo de poseer** del atacante (trofeos, ego, reconocimiento social, ...).
- La oportunidad de **ganar dinero "fácil"**.
- **Espionaje** industrial / militar / personal.
- **Baja expertise técnica** requerida para ejecutar el ataque: ataques enlatados.
- **Bajo coste** del ataque.
- **Impunidad del atacante** (¿es perseguible? ¿castigable?).
- El hecho de que el **atacante** sea **interno**.

Razonamiento: conoce a tu enemigo.

3 Degradación

- La degradación se suele caracterizar como una **fracción del valor del activo** y así aparecen expresiones como que un activo se ha visto "totalmente degradado", o "degradado en una pequeña fracción".

- Cuando las **amenazas no son intencionadas**, probablemente baste **conocer la fracción físicamente perjudicada** de un activo para **calcular la parte proporcional de valor** que se pierde.

- Pero **cuando la amenaza es intencionada**, no se puede pensar en proporcionalidad alguna pues el **atacante puede causar muchísimo daño de forma selectiva**.

- Es **más fácil de estimar que la probabilidad:**
  - Resultados creíbles.
  - Se traslada a los indicadores de impacto y riesgo.

4 Degradación

Agravantes (aumentan la degradación):

- Activos reducidos o compactos.
- Efecto dominó o pólvora.
- Personal desmotivado o incompetente.

Atenuantes (disminuyen la degradación):

- Información dispersa.
- Equipamiento redundante.
- Compartimentación (física, lógica, segregación de tareas, ...)
- Personal motivado y con habilidades técnicas reactivas.

Vulnerabilidades

Se denomina vulnerabilidad a toda debilidad que puede ser aprovechada por una amenaza, o más detalladamente a las debilidades de los activos o de sus medidas de protección que facilitan el éxito de una amenaza potencial.

Son vulnerabilidades todas las ausencias o ineficacias de las salvaguardas pertinentes para salvaguardar el valor propio o acumulado de un activo.

5 Vulnerabilidades

- **Incidente = amenaza * vulnerabilidad.**
- La **amenaza** tiene un cierto nivel que **depende de:**
  - Las características del atacante.
  - Las características del activo.
- Si un **activo es vulnerable**, la **amenaza** lleva a un **incidente.**
  - Defectos de software : anunciados ... hasta que se reparen.
  - Carencia de contramedidas: no existen ... hasta que se implanten.
- El resultado es siempre una **probabilidad** mayor o menor **de materialización.**

6 Aspectos prácticos

- La ley de Murphy asegura que "si algo puede ir mal, irá mal", pero hay que distinguir entre:
  - **Posibilidad (si/no)**, que debe existir para que tenga sentido el resto.
  - **Probabilidad** , que hemos de cuantificar.

- El daño podría ser **tremendo (gran impacto)**, pero una **baja frecuencia** puede convertirlo en **"riesgo teórico".**

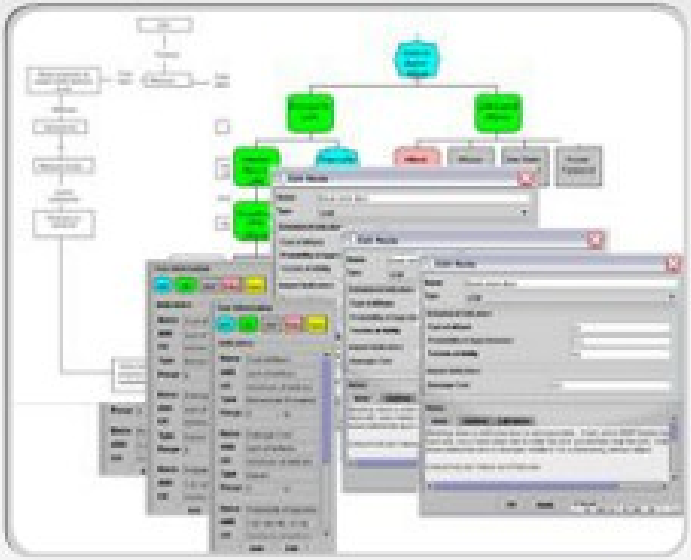
- El daño puede ser **mínimo (impacto ridículo)**, pero una **alta frecuencia** puede convertirlo en un **problema**.

- **La estimación de amenazas es difícil**, porque los interlocutores viven en una situación en la que ya existen controles: hay que imaginar lo que podría ocurrir si no ...

7 Mapa de amenazas

Es el **producto final del análisis de amenazas**, un **informe** que recoge la relación de:

- Amenazas por activo.
- Daño que causarían.
- Frecuencia esperada.



Impacto. Conceptos

Definición de impacto

El impacto se define como la medida del daño sobre un activo derivado de la materialización de una amenaza.

- Conociendo el **valor de los activos** en varias dimensiones y la **degradación que causan las amenazas**, derivamos el **impacto** que éstas tendrian **sobre el sistema.**

- Es frecuente que **el valor del sistema de información se centre en los servicios** que presta y los **datos** que maneja, al tiempo que las **amenazas suelen materializarse en los medios.**

Definición de impacto

Valoración del impacto

Impacto acumulado

Cálculo del impacto acumulado

Impacto repercutido

Cálculo del impacto repercutido

Valoración del impacto

La valoración del impacto de una amenaza en nuestro sistema de información **se puede realizar de las siguientes maneras:**

- Valoración **cualitativa / subjetiva:** calificación del impacto como irrelevante … grave … intolerable.
- Valoración **cuantitativa / económica:** coste dinerario.

Métodos

- **Directos:** ¿qué impacto tendría …?
- **Indirectos:** valor x degradación.

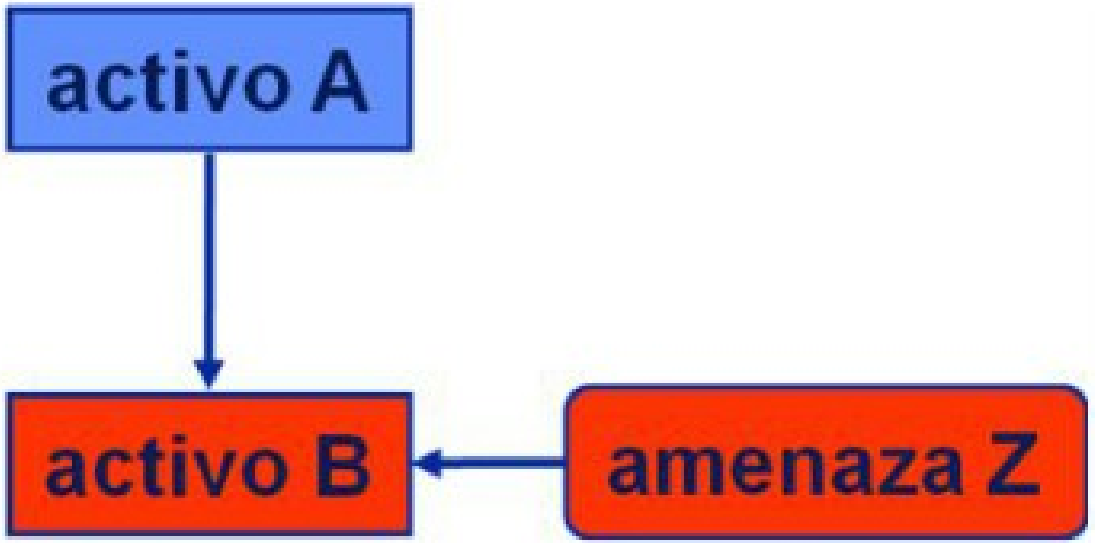
Impacto acumulado

- Es el **calculado sobre un activo teniendo en cuenta:**
  - Su **valor acumulado** (el propio más el acumulado de los activos que dependen de él.
  - Las **amenazas** a que está expuesto.
- El impacto acumulado **se calcula para cada activo, por cada amenaza y en cada dimensión de valoración**,siendo una función del **valor acumulado** y de la **degradación** causada.
- El impacto es **tanto mayor cuanto mayor** es el **valor propio o acumulado** sobre un activo.
- El impacto es **tanto mayor cuanto mayor** sea la **degradación** del activo atacado.
- El impacto acumulado, al calcularse sobre los activos que soportan el peso del sistema de información, **permite determinar las salvaguardas** de que hay que dotar a los medios de trabajo: protección de los equipos, copias de respaldo, etc.

Cálculo del impacto acumulado

Si el activo A depende del activo B, el valor de A se acumula en B en la proporción en que A depende de B

Impacto_acumulado = valor_acumulado_B * degradación_B



Impacto repercutido

Es el calculado sobre un activo teniendo en cuenta:

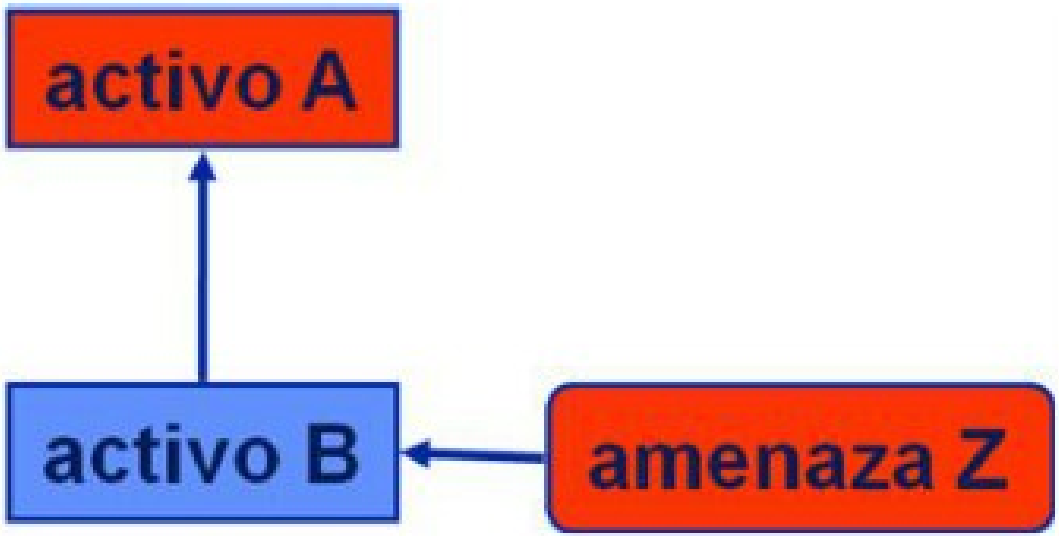
- Su **valor propio.**
- Las **amenazas** a que están expuestos los **activos de los que depende.**

- El impacto repercutido se **calcula para cada activo,** por cada **amenaza** y en cada **dimensión de valoración**, siendo una función del **valor propio** y de la **degradación** causada.
- El impacto es **tanto mayor cuanto mayor** es el **valor propio** de un activo.
- El impacto es **tanto mayor cuanto mayor** sea la **degradación** del activo atacado.
- El impacto es **tanto mayor cuanto mayor** sea la **dependencia** del activo atacado.
- El impacto repercutido, al calcularse sobre los activos que tienen valor propio, **permite determinar las consecuencias de las incidencias técnicas** sobre la misión del sistema de información. Es pues una presentación gerencial que ayuda a tomar una de las decisiones críticas de un análisis de riesgos: aceptar un cierto nivel de riesgo.

Cálculo del impacto repercutido

Si el activo A depende del activo B, el daño en B repercute en A en la proporción en que A depende de B.

Impacto_repercutido = valor_A * dependencia * degradación_B



Definición de riesgo

Medida del daño probable sobre un sistema. Estimación del grado de exposición a que una amenaza se materialice sobre uno o más activos causando daños o perjuicios a la organización.

- Conociendo el impacto de las amenazas sobre los activos, es directo derivar el riesgo sin más que tener en cuenta la frecuencia de ocurrencia.
- El riesgo crece con el impacto y con la frecuencia.

Definición de riesgo
Riesgo acumulado
Riesgo repercutido
Estimación del riesgo
Estimación cualitativa
Estimación cuantitativa

Riesgo acumulado

- Es el calculado sobre un activo teniendo en cuenta:
  - El **impacto acumulado** sobre un activo debido a una amenaza.
  - La **frecuencia** de la amenaza.

- Se calcula **para cada activo**, por **cada amenaza** y en cada **dimensión de valoración**, siendo una función del valor acumulado, la degradación causada y la frecuencia de la amenaza.

- Al calcularse sobre los activos que soportan el peso del sistema de información, **permite determinar las salvaguardas** de que hay que dotar a los medios de trabajo: protección de los equipos, copias de respaldo, etc.

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.
- Se calcula **para cada activo**, por cada **amenaza** y en cada dimensión de valoración, siendo una **función del valor propio**, la **degradación** causada y la **frecuencia** de la amenaza.
- Al calcularse **sobre los activos que tienen valor propio**, permite **determinar las consecuencias de las incidencias** técnicas sobre la **misión del sistema de información.** Es pues una presentación gerencial que ayuda a tomar una de las decisiones críticas de un análisis de riesgos: aceptar un cierto nivel de riesgo.

Definición de riesgo
Riesgo acumulado
Riesgo repercutido
Estimación del riesgo
Estimación cualitativa
Estimación cuantitativa

Estimación del riesgo

Conociendo el impacto de las **amenazas sobre los activos,** es directo derivar el riesgo sin más que tener en cuenta la **frecuencia de ocurrencia.**

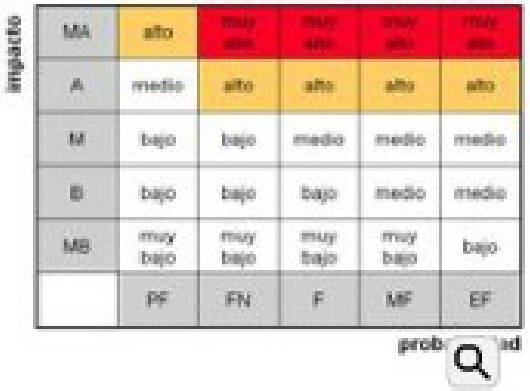
Valoración:

- **Cualitativa / subjetiva:** irrelevante ... grave ... intolerable.
- **Cuantitativa / económica:** coste dinerario.

Estimación cualitativa

Estimación Tabular:

- Para **estimar el riesgo** hay que darle más peso al impacto que a la probabilidad.
- Para estimar **riesgos cualitativos**, percepción del riesgo. El riesgo tiene que ser **creciente con el impacto o valor**, y **también con la frecuencia.**
- Se utiliza **en todas las metodologías de análisis de riesgo**, y para **todos los ámbitos** (riesgos naturales, industriales, financieros, etc.).



impacto

MA	alto	muy alto	muy alto	muy alto	muy alto
A	medio	alto	alto	alto	alto
M	bajo	bajo	medio	medio	medio
B	bajo	bajo	bajo	medio	medio
MB	muy bajo	muy bajo	muy bajo	muy bajo	bajo
	PF	FN	F	MF	EF

probabilidad

Estimación cuantitativa

Conociendo el valor del impacto sobre un activo y la frecuencia de ocurrencia, calculamos el riesgo de amenaza sobre un activo.

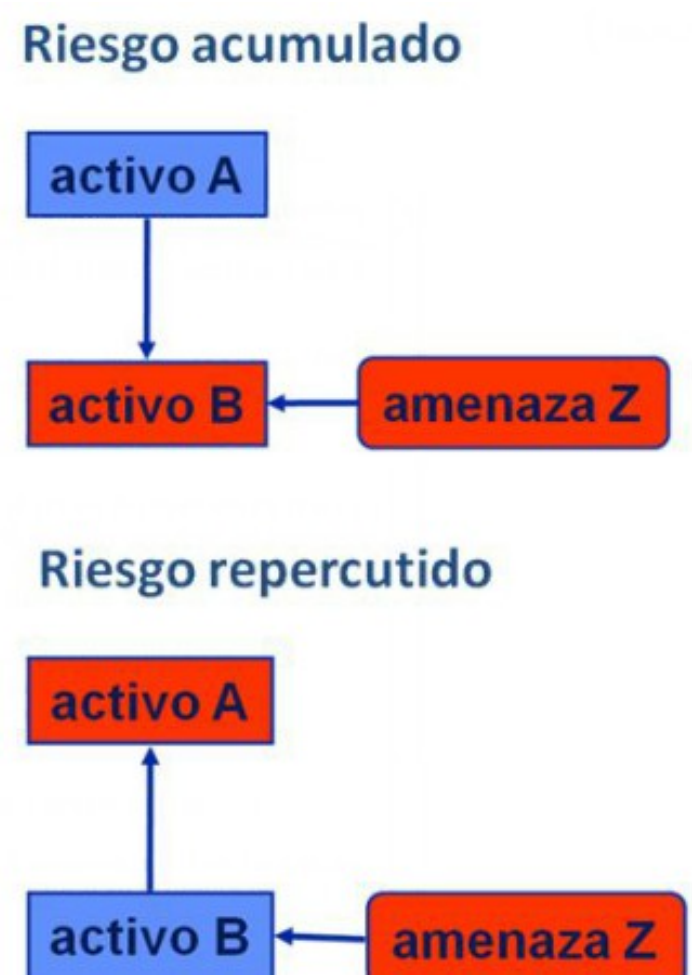
- Impacto = valor * degradación
- Riesgo = impacto * frecuencia

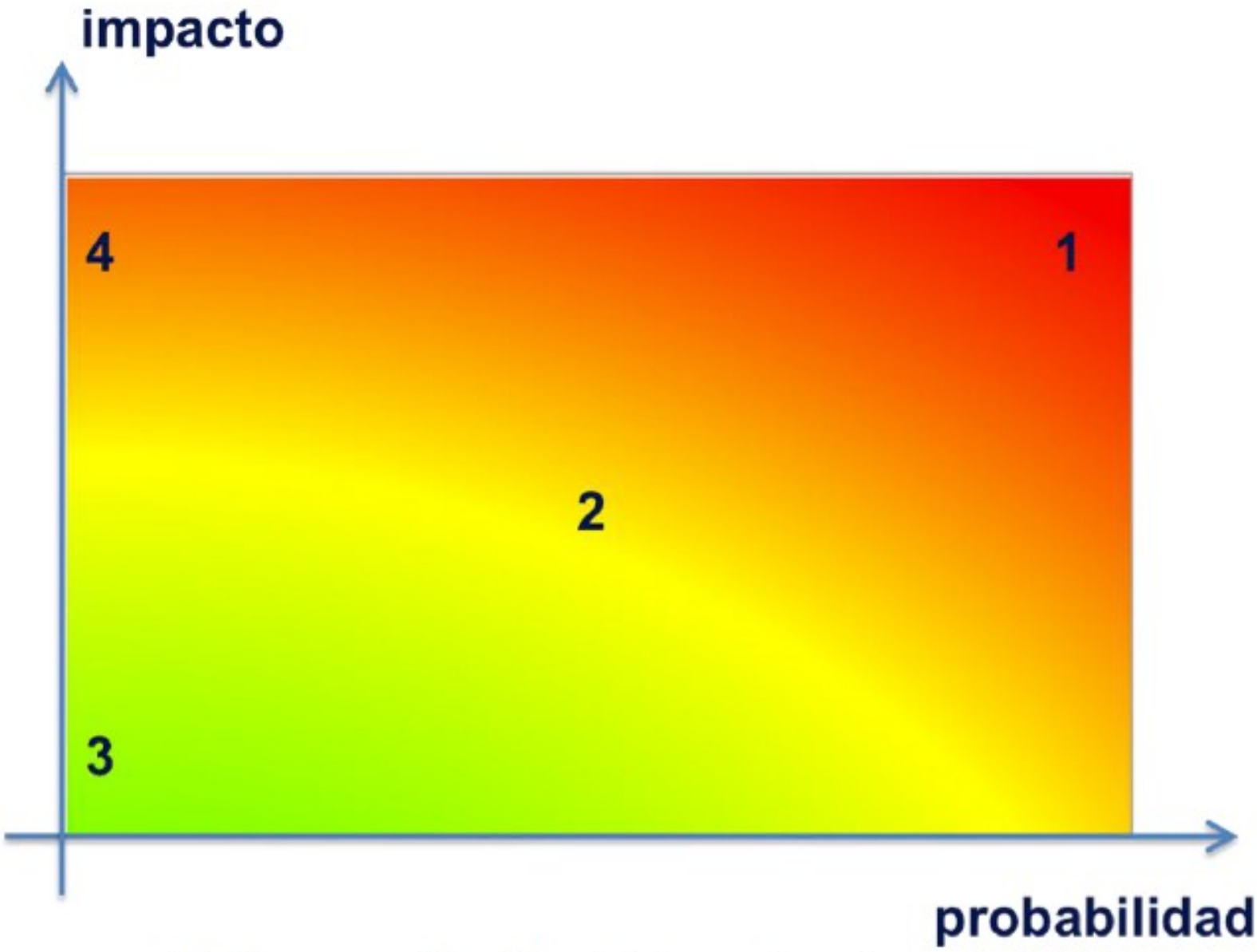
Cálculo del riesgo acumulado:

- Sí el activo A depende de B en un x %, el valor de A se acumula en B en la proporción en que depende.
- **Riesgo_acumulado_B =** impacto_acumulado_B x frecuencia

Cálculo del riesgo repercutido:

- Si A depende de B en un g%, la degradación de B repercute en A en la proporción en que depende.
- **Riesgo_repercutido_A =** impacto_repercutido_A x frecuencia





El riesgo en función del impacto y la probabilidad

El análisis de los riesgos se lleva a cabo por medio de las siguientes tareas:

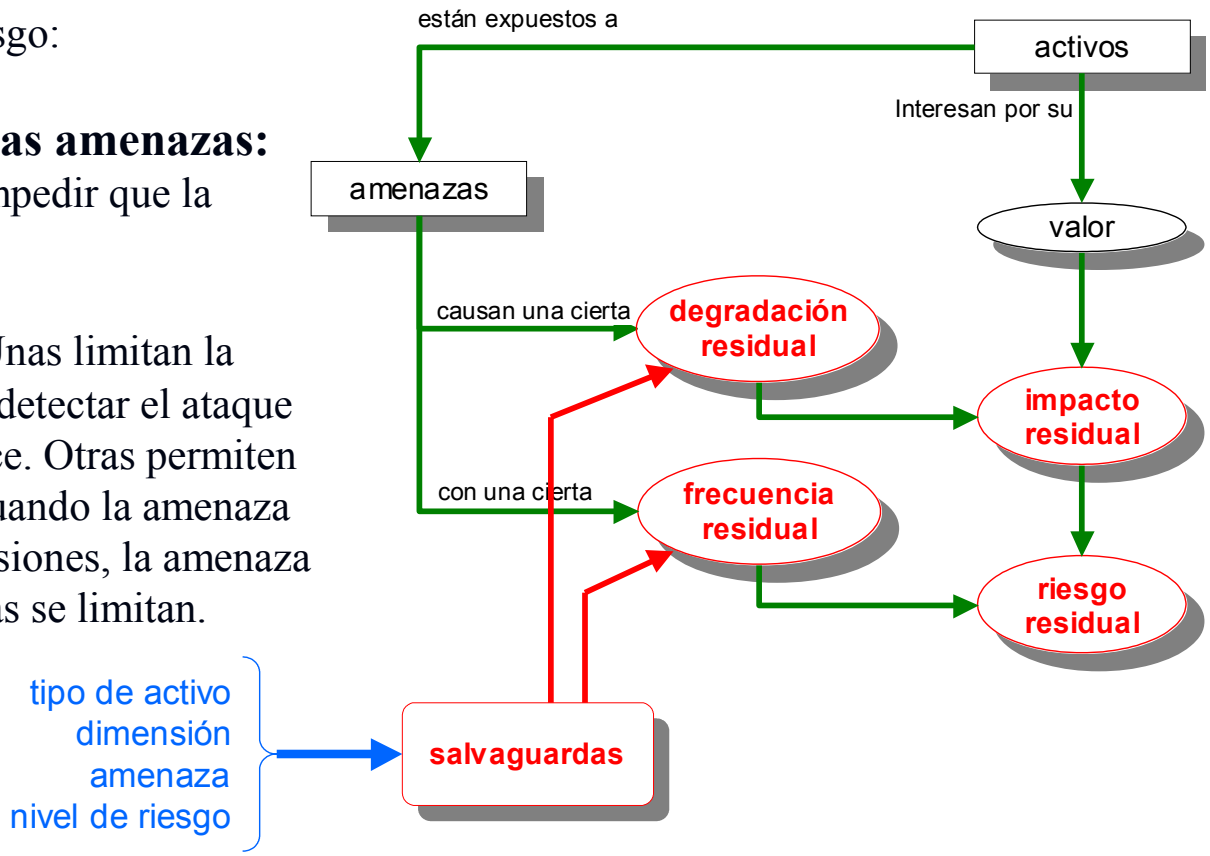
MAR – Método de Análisis de Riesgos
MAR.1 – Caracterización de los activos
MAR.11 – Identificación de los activos
MAR.12 – Dependencias entre activos
MAR.13 – Valoración de los activos
MAR.2 – Caracterización de las amenazas
MAR.21 – Identificación de las amenazas
MAR.22 – Valoración de las amenazas
MAR.3 – Caracterización de las salvaguardas
MAR.31 – Identificación de las salvaguardas pertinentes
MAR.32 – Valoración de las salvaguardas
MAR.4 – Estimación del estado de riesgo
MAR.41 – Estimación del impacto
MAR.42 – Estimación del riesgo

Definición: Procedimiento o mecanismo tecnológico que reduce el riesgo.

Las salvaguardas actúan sobre el riesgo:

· **Reduciendo la frecuencia de las amenazas:** (preventivas). Las ideales llegan a impedir que la amenaza se materialice.

· **Limitando el daño causado:** Unas limitan la posible degradación; otras permiten detectar el ataque para frenar que la degradación avance. Otras permiten la pronta recuperación del sistema cuando la amenaza lo destruye. En cualquiera de las versiones, la amenaza se materializa; pero las consecuencias se limitan.



¿Qué salvaguardas se requieren?

Para implementar un conjunto de salvaguardas en nuestro sistema de información:

- En primer lugar necesitamos una **lista de posibles salvaguardas:**
  - Buscamos el **consejo de expertos.**
  - Existen **estándares** (ej. ENS, 27002, …)
  - El consejo de los expertos se traduce en **leyes, reglamentos, práctica sectorial**. Un ejemplo de salvaguardas lo encontramos en la documentación del **Esquema Nacional de Seguridad.**

- A continuación hay que **casar las salvaguardas con las amenazas identificadas:**
  - Se prepara una **Declaración de Aplicabilidad**

- Se **evalúa el despliegue** actual:
  - **Existencia** (o ausencia).
  - **Efectividad** del despliegue.

3 Cuantificación de la eficacia

Una vez evaluados activos y amenazas en nuestro análisis de riesgos, tenemos que hacer lo mismo con las salvaguardas del sistema. **Cuantificamos la eficacia:**

- **Eficacia (E):**
  - Medida en que la salvaguarda está implantada y es efectiva frente al riesgo al que se enfrenta.
  - Debemos recurrir a la opinión cualificada (de un experto).

- La eficacia **se reparte entre:**
  - La reducción de la probabilidad de amenaza.
  - Limitación del impacto.

4 Cuantificación de la eficacia

- Aplicamos un **modelo de madurez**. Se trata de una escala universal, diseñada en principio para medir los procesos de software.
- La escala hace referencia a la **cuantificación de la eficacia de las salvaguardas existentes** ante una amenaza determinada.

	Madurez	
• NA	L0	Por la naturaleza del sistema, no es necesaria ante esa amenaza.
• 0%		Inexistente.
• 10%	L1	Se actúa de forma "ad hoc" ante las amenazas.
• 50%	L2	Procedimiento reproducible, no hay sistemática.
• 90%	L3	Existe un proceso definido y sistemático.
• 95%	L4	Gestionado y medible, tenemos una métrica del proceso.
• 100%	L5	Optimizado, se buscan conseguir objetivos de calidad.

5 Combinación de salvaguardas. Eficacia

Cuando combinemos varias salvaguardas para responder ante una amenaza, la efectividad combinada de ambas salvaguardas depende de si son:

AND: Necesarias:

- Efectividad combinada: la peor (más baja, eslabón más débil).

OR: Acumulativas:

- Efectividad combinada: la suma de ambas(defensa en profundidad).

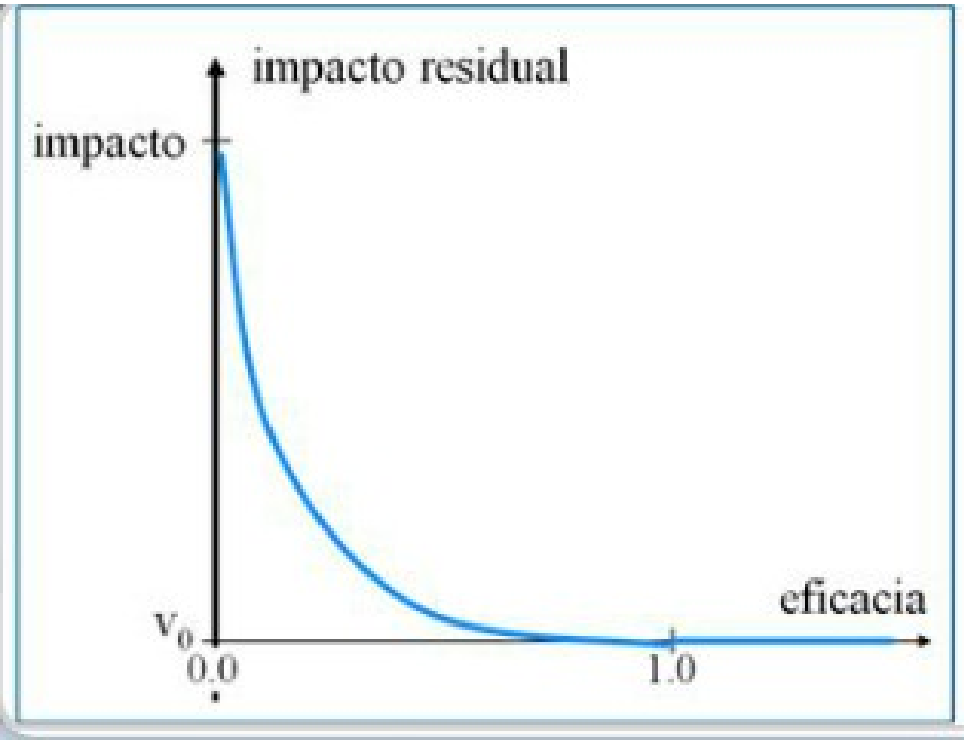
XOR: Alternativas:

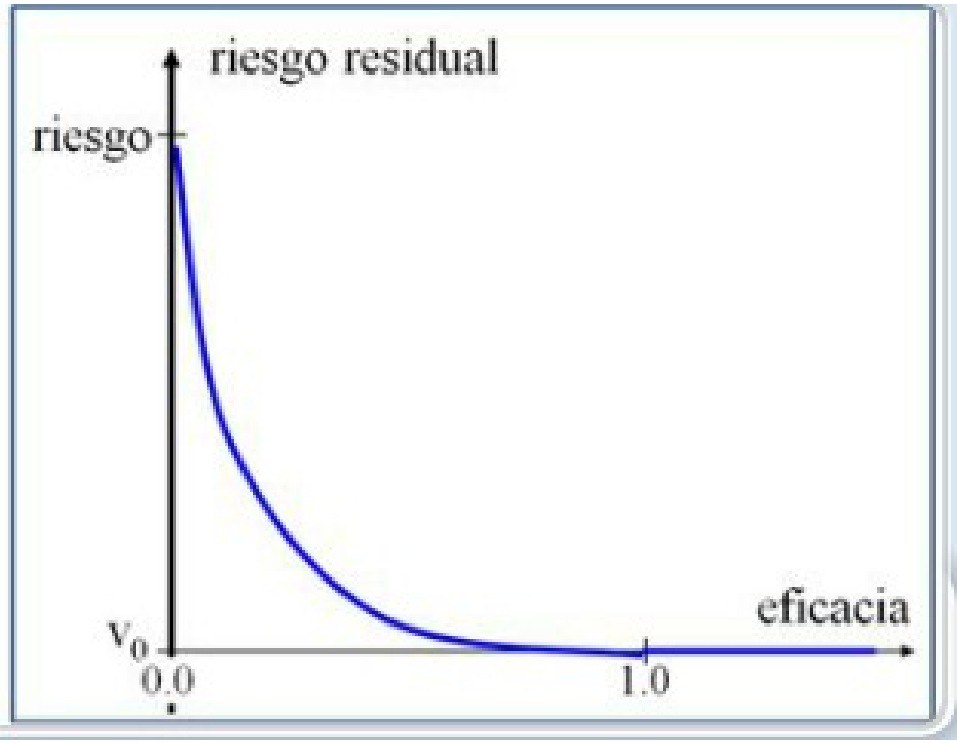
- Efectividad combinada: la mejor (la más altasalvaguardas redundantes).


MIDE EL INTERES DE LOS
Activos
SE MATERIALIZAN SOBRE LOS
Amenazas
SUFREN UNA
Valor
PERMITEN ESTIMAR EL
Degradación
CAUSAN UNA CIERTA
OCURREN CON
UNA CIERTA
Impacto
PERMITEN ESTIMAR EL
Frecuencias
Riesgo
LIMITAN
EL PERJUICIO
REDUCEN
LA OCURRENCIA
(Preventivas)
MITIGAN EL
Salvaguardas
LIMITAN EL RIESGO A UN VALOR
Riesgo residual

El análisis de los riesgos se lleva a cabo por medio de las siguientes tareas:

MAR – Método de Análisis de Riesgos
MAR.1 – Caracterización de los activos
MAR.11 – Identificación de los activos
MAR.12 – Dependencias entre activos
MAR.13 – Valoración de los activos
MAR.2 – Caracterización de las amenazas
MAR.21 – Identificación de las amenazas
MAR.22 – Valoración de las amenazas
MAR.3 – Caracterización de las salvaguardas
MAR.31 – Identificación de las salvaguardas pertinentes
MAR.32 – Valoración de las salvaguardas
MAR.4 – Estimación del estado de riesgo
MAR.41 – Estimación del impacto
MAR.42 – Estimación del riesgo


impacto residual
impacto
eficacia
v_0
0.0
1.0


riesgo residual
riesgo
eficacia
v_0
0.0
1.0

Paso 4: Impacto residual

- Dado un cierto conjunto de salvaguardas desplegadas y una medida de la madurez de su proceso de gestión, el sistema queda en una situación de posible impacto que se denomina residual. Se dice que hemos modificado el impacto, desde un valor potencial a un valor residual.
- El cálculo del impacto residual es sencillo. Como no han cambiado los activos, ni sus dependencias, sino solamente la magnitud de la degradación, se repiten los cálculos de impacto con este nuevo nivel de degradación.
- La magnitud de la degradación tomando en cuenta la eficacia de las salvaguardas, es la proporción que resta entre la eficacia perfecta y la eficacia real.
- El impacto residual puede calcularse acumulado sobre los activos inferiores, o repercutido sobre los activos superiores.

Paso 5: Riesgo residual

- Dado un cierto conjunto de salvaguardas desplegadas y una medida de la madurez de su proceso de gestión, el sistema queda en una situación de riesgo que se denomina residual. Se dice que hemos modificado el riesgo, desde un valor potencial a un valor residual.
- El cálculo del riesgo residual es sencillo. Como no han cambiado los activos, ni sus dependencias, sino solamente la magnitud de la degradación y la probabilidad de las amenazas, se repiten los cálculos de riesgo usando el impacto residual y la probabilidad residual de ocurrencia.
- La magnitud de la degradación se toma en consideración en el cálculo del impacto residual.
- La magnitud de la probabilidad residual tomando en cuenta la eficacia de las salvaguardas, es la proporción que resta entre la eficacia perfecta y la eficacia real.
- El riesgo residual puede calcularse acumulado sobre los activos inferiores, o repercutido sobre los activos superiores.

El análisis de los riesgos se lleva a cabo por medio de las siguientes tareas:

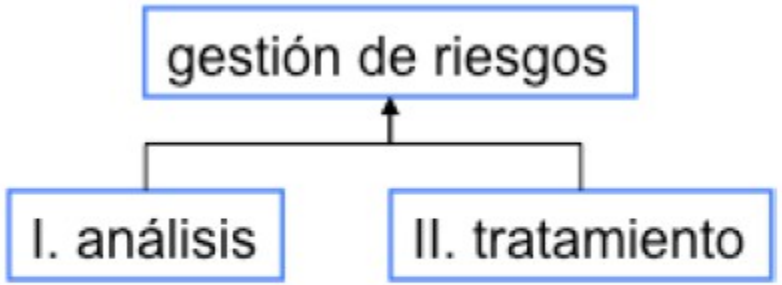
MAR – Método de Análisis de Riesgos
MAR.1 – Caracterización de los activos
MAR.11 – Identificación de los activos
MAR.12 – Dependencias entre activos
MAR.13 – Valoración de los activos
MAR.2 – Caracterización de las amenazas
MAR.21 – Identificación de las amenazas
MAR.22 – Valoración de las amenazas
MAR.3 – Caracterización de las salvaguardas
MAR.31 – Identificación de las salvaguardas pertinentes
MAR.32 – Valoración de las salvaguardas
MAR.4 – Estimación del estado de riesgo
MAR.41 – Estimación del impacto
MAR.42 – Estimación del riesgo

Lista de control

√	actividad	tarea
	Se han identificado los activos esenciales: información que se trata y servicios que se prestan	MAR.11
	Se han valorado las necesidades o niveles de seguridad requeridos por cada activo esencial en cada dimensión de seguridad	MAR.13
	Se han identificado los demás activos del sistema	MAR.11
	Se han establecido el valor (o nivel requerido de seguridad) de los demás activos en función de su relación con los activos esenciales (por ejemplo, mediante identificación de las dependencias)	MAR.12
	Se han identificado las amenazas posibles sobre los activos	MAR.21
	Se han estimado las consecuencias que se derivarían de la materialización de dichas amenazas	MAR.22
	Se ha estimado la probabilidad de que dichas amenazas se materialicen	MAR.23
	Se han estimado los impactos y riesgos potenciales, inherentes al sistema	MAR.4
	Se han identificado las salvaguardas apropiadas para atajar los impactos y riesgos potenciales	MAR.31
	Se ha valorado el despliegue de las salvaguardas identificadas	MAR.32
	Se han estimado los valores de impacto y riesgo residuales, que es el nivel de impacto y riesgo que aún soporta el sistema tras el despliegue de las salvaguardas	MAR.4

Magerit v.3

- **I. análisis de riesgos,**
  - que permite determinar qué tiene la Organización y estimar lo que podría pasar.
- **II. tratamiento de los riesgos,**
  - que permite organizar la defensa concienzuda y prudente, defendiendo para que no pase nada malo y al tiempo estando preparados para atajar las emergencias, sobrevivir a los incidentes y seguir operando en las mejores condiciones; como nada es perfecto, se dice que el riesgo se reduce a un nivel residual que la Dirección asume.
- Ambas actividades, análisis y tratamiento se combinan en el proceso denominado **Gestión de Riesgos.**



Gestión de riesgos

Proceso de gestión de riesgos

- Evaluación: interpretación de los valores de impacto y riesgo residuales
- Aceptación del riesgo
- Tratamiento
- Estudio cuantitativo de costes / beneficios
- Estudio cualitativo de costes / beneficios
- Estudio mixto de costes / beneficios
- Opciones de tratamiento del riesgo
  - Eliminación
  - Mitigación
  - Compartición
  - Financiación
- Formalización de las actividades
  - Roles y funciones
  - Contexto Criterios
  - Evaluación de los riesgos
  - Decisión de tratamiento
  - Comunicación y consulta
  - Seguimiento y revisión
- Documentación del proceso
- Indicadores de control del proceso de gestión de riesgos

Proceso de gestión de riesgos

A la vista de los impactos y riesgos a que está expuesto el sistema, hay que tomar una serie de decisiones condicionadas por diversos factores:

- la gravedad del impacto y/o del riesgo
- las obligaciones a las que por ley esté sometida la Organización
- las obligaciones a las que por reglamentos sectoriales esté sometida la Organización
- las obligaciones a las que por contrato esté sometida la Organización

Proceso de gestión de riesgos

Dentro del margen de maniobra que permita este marco, pueden aparecer consideraciones adicionales sobre la capacidad de la Organización para aceptar ciertos impactos de naturaleza intangible tales como:

- imagen pública de cara a la Sociedad (aspectos reputacionales)
- política interna: relaciones con los propios empleados, tales como capacidad de contratar al personal idóneo, capacidad de retener a los mejores, capacidad de soportar rotaciones de personas, capacidad de ofrecer una carrera profesional atractiva, etc.
- relaciones con los proveedores, tales como capacidad de llegar a acuerdos ventajosos a corto, medio o largo plazo, capacidad de obtener trato prioritario, etc.
- relaciones con los clientes o usuarios, tales como capacidad de retención, capacidad de incrementar la oferta, capacidad de diferenciarse frente a la competencia, ...
- relaciones con otras organizaciones, tales como capacidad de alcanzar acuerdos estratégicos, alianzas, etc.
- nuevas oportunidades de negocio, tales como formas de recuperar la inversión en seguridad
- acceso a sellos o calificaciones reconocidas de seguridad

Proceso de gestión de riesgos

Todas las consideraciones anteriores desembocan en una calificación de cada riesgo significativo, determinándose si ...

1. es crítico en el sentido de que requiere atención urgente
2. es grave en el sentido de que requiere atención
3. es apreciable en el sentido de que pueda ser objeto de estudio para su tratamiento
4. es asumible en el sentido de que no se van a tomar acciones para atajarlo

La opción 4, aceptación del riesgo, siempre es arriesgada y hay que tomarla con prudencia y justificación. Las razones que pueden llevar a esta aceptación son:

- cuando el impacto residual es asumible
- cuando el riesgo residual es asumible
- cuando el coste de las salvaguardas oportunas es desproporcionado en comparación al impacto y riesgo residuales

La calificación de los riesgos tendrá consecuencias en las tareas subsiguientes, siendo un factor básico para establecer la prioridad relativa de las diferentes actuaciones.

Proceso de gestión de riesgos

El análisis de riesgos determina impactos y riesgos.

Los impactos recogen daños absolutos, independientemente de que sea más o menos probable que se dé la circunstancia.

En cambio, el riesgo pondera la probabilidad de que ocurra.

El impacto refleja el daño posible (lo peor que puede ocurrir), mientras que el riesgo refleja el daño probable (lo que probablemente ocurra).

El resultado del análisis es sólo un análisis. A partir de el disponemos de información para tomar decisiones conociendo lo que queremos proteger (activos valorados), de qué lo queremos proteger (amenazas valoradas) y qué hemos hecho por protegerlo (salvaguardas valoradas). Todo ello sintetizado en los valores de impacto y riesgo.

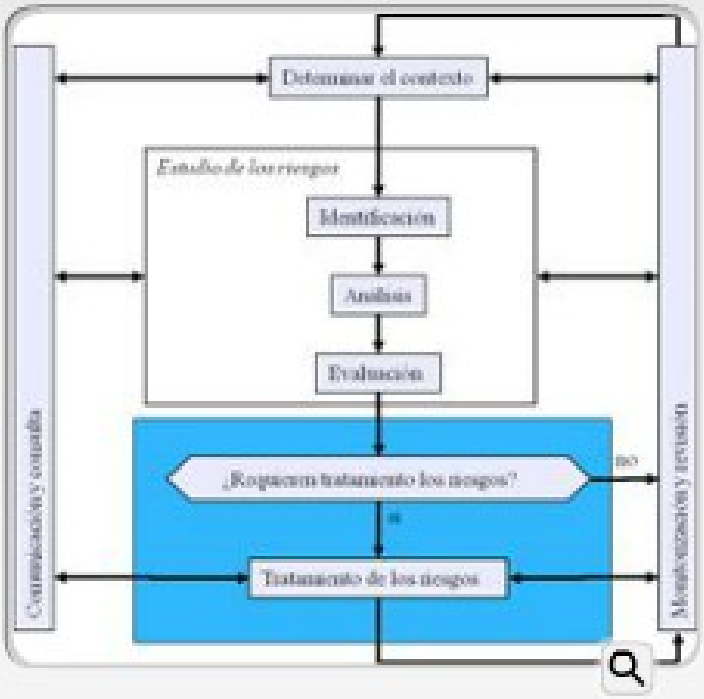
A partir de aquí, las decisiones son de los órganos de gobierno de la Organización que actuarán en 2 pasos:

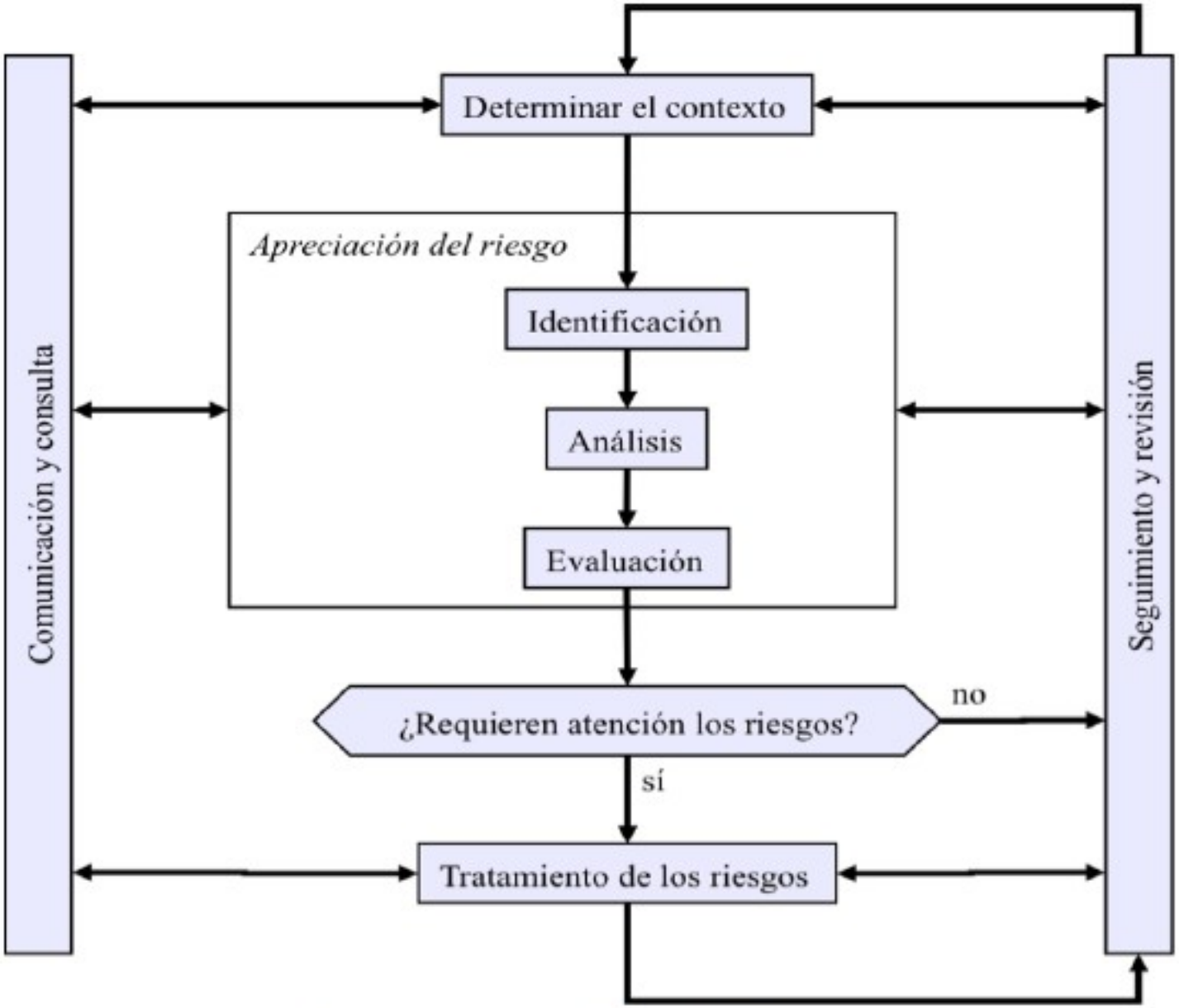
- paso 1: evaluación
- paso 2: tratamiento

Gestión de riesgos

- Hemos realizado un **estudio de los riesgos** a los que se encuentra sometido nuestro Sistema de Información, los hemos **identificado, analizado y cuantificado.**

- Iniciaríamos una **nueva fase** dentro del proceso de gestión de riesgos, la **toma de decisiones** y las acciones de tratamiento.





Proceso de gestión de riesgos

1 ¿Qué hacer con el riesgo?

Hemos detectado tras el análisis de riesgos la existencia de un riesgo determinado. ¿Qué podemos hacer con este riesgo?

- **Evitarlo:**
  - Si se puede ... es la solución ideal.
  - Lo hacemos prescindiendo de activos.
  - Reordenar el sistema.

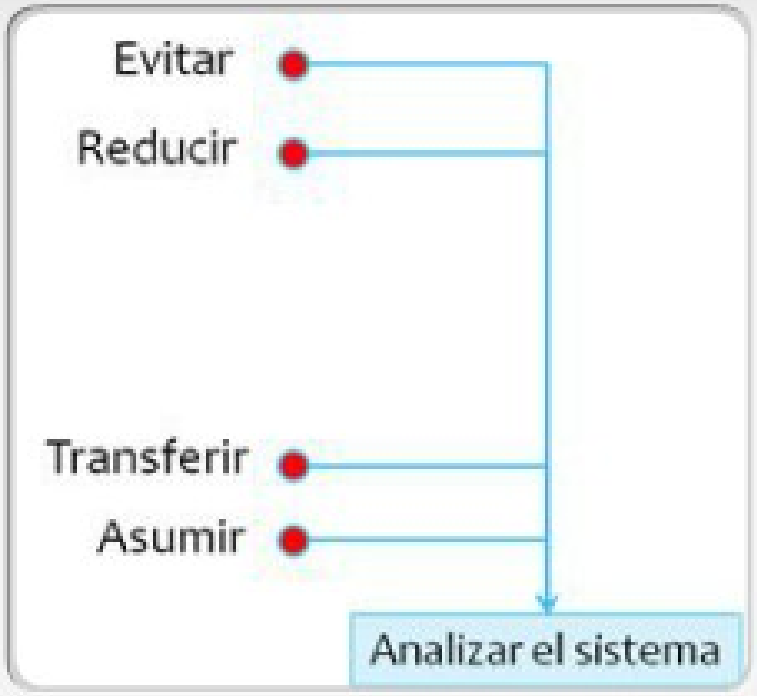
- **Reducirlo l mitigarlo:**
  - Es a lo que se suele tender.
  - Aplicamos salvaguardas para tratar y reducir el riesgo.
  - impacto limitado.

- **Transferirlo:**
  - Cuando hemos llegado al límite y no podemos mitigarlo.
  - Compartimos el riesgo con otra entidad, especialista en el tratamiento. Se suele reducir previamente el riesgo hasta que otra entidad acepta las condiciones.
  - Puede contratarse un seguro, esta acción afecta a la valoración del sistema.

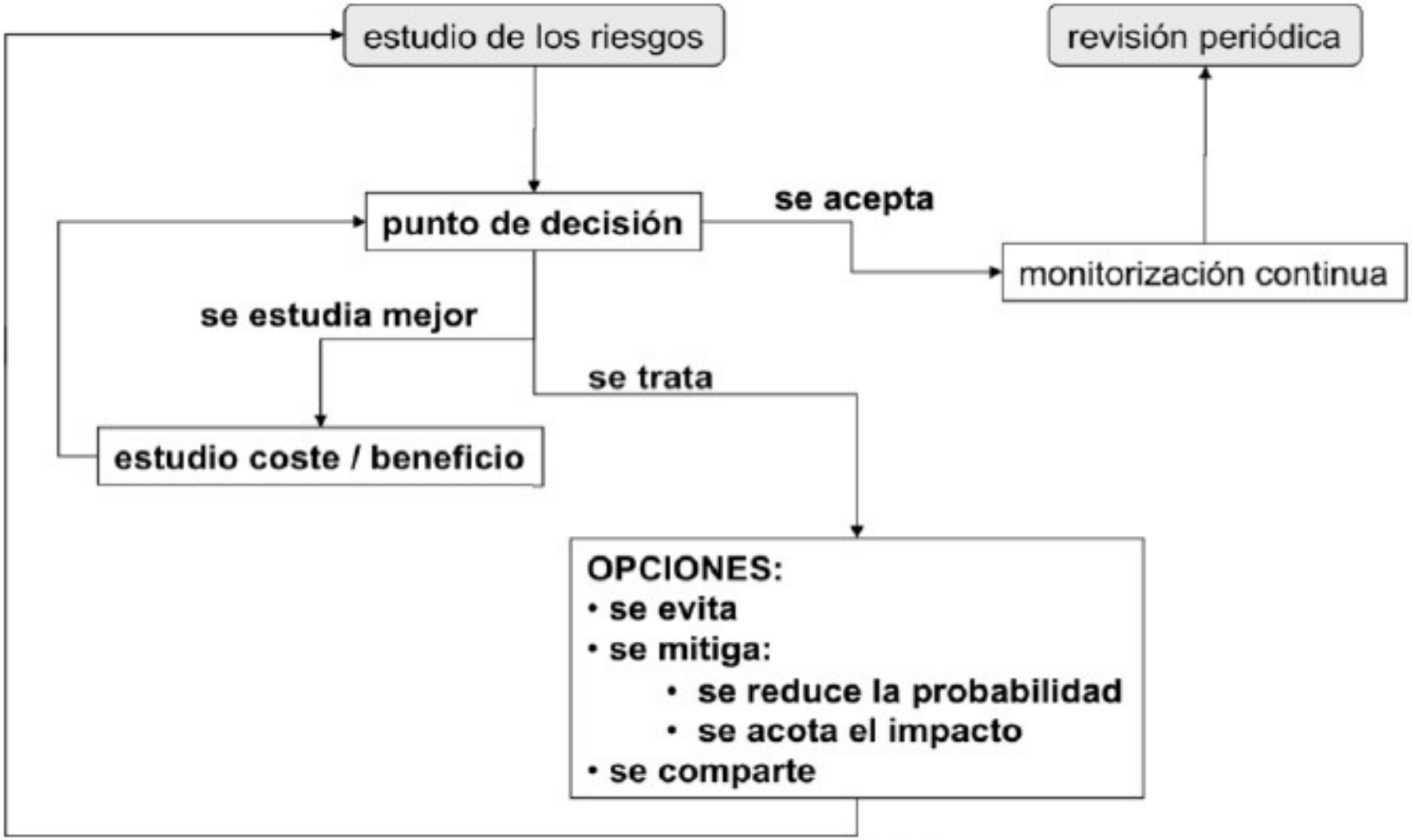
- **Asumirlo l aceptarlo:**
  - Es la última opción, no podemos adoptar las opciones anteriores.
  - Pasa a contabilizarse como gasto operacional.

2 ¿Qué hacer con el riesgo?

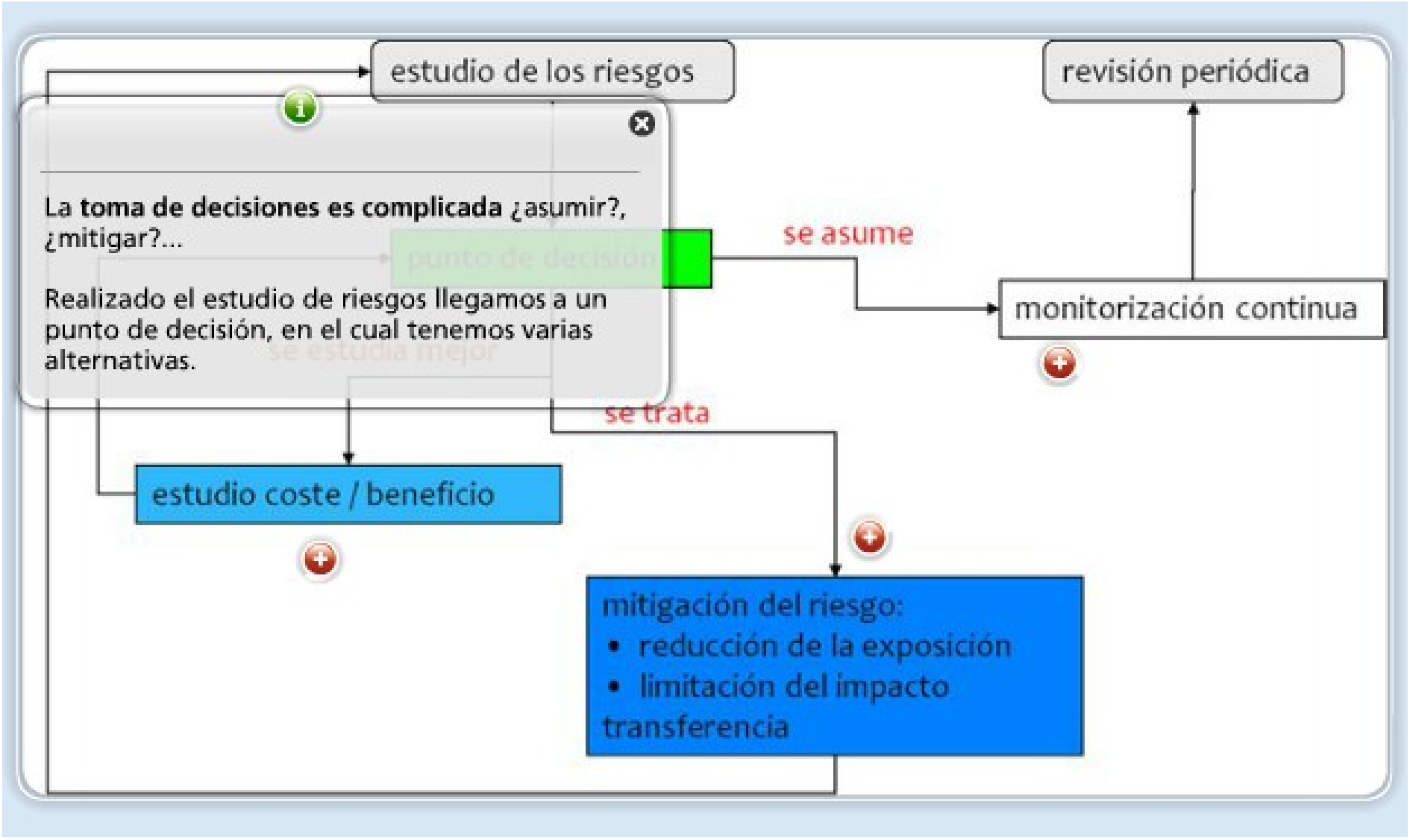
- Una vez realizado el tratamiento del riesgo, puede ser que haya cambiado nuestro sistema de Información. Es necesario realizar un nuevo análisis.
- Comparamos los resultados del nuevo análisis con el realizado en primer lugar.

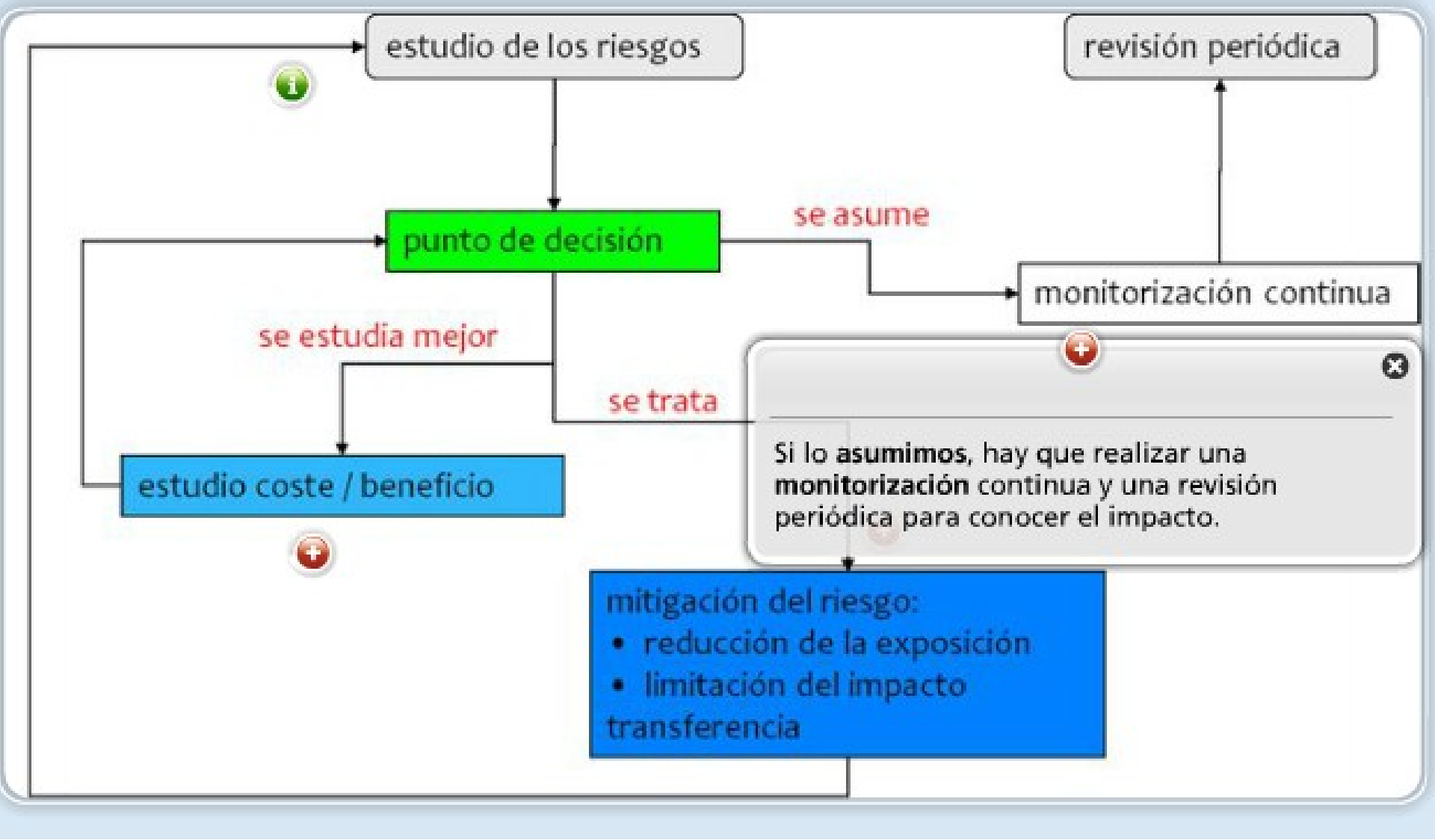


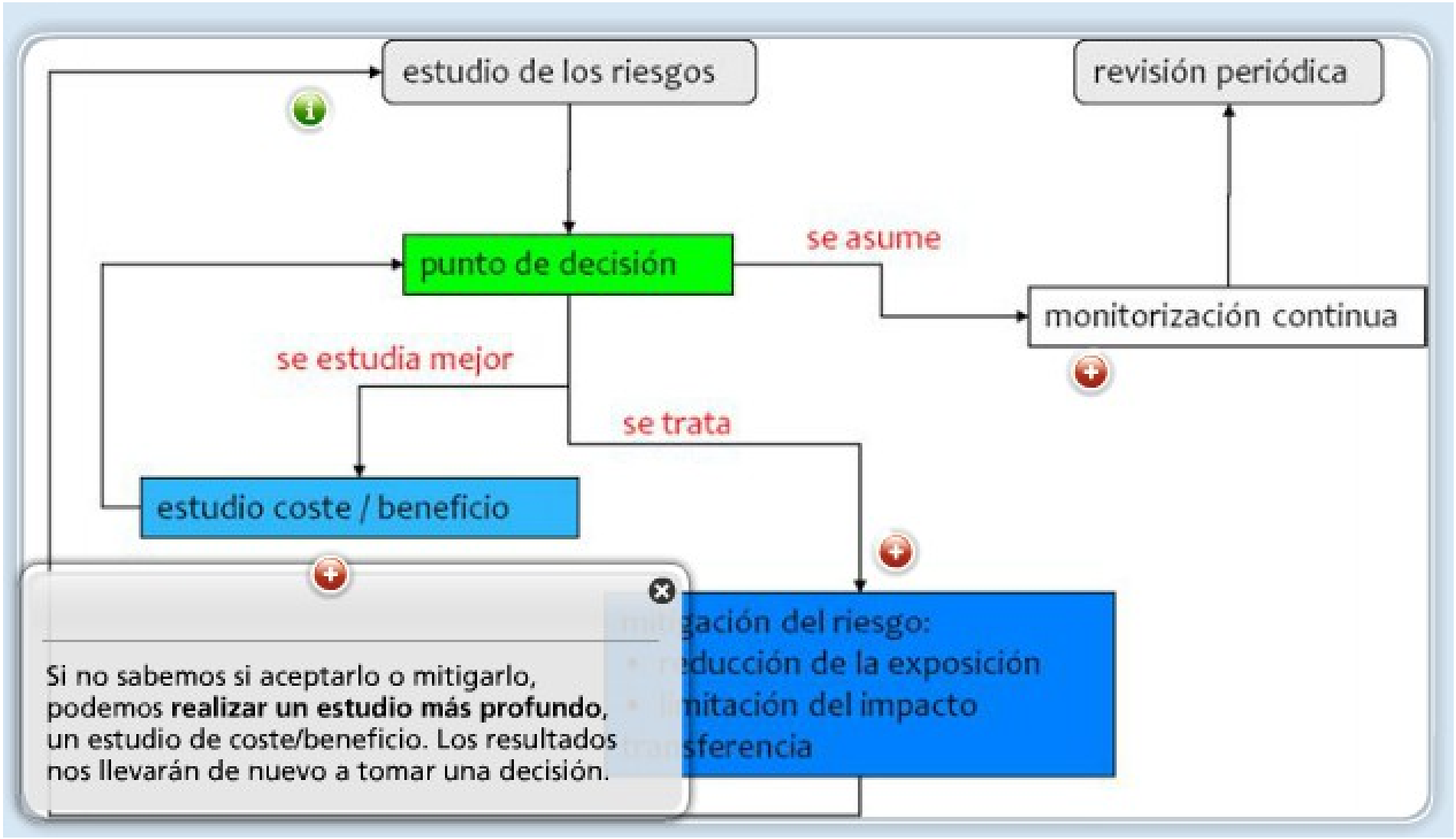
Proceso de gestión de riesgos

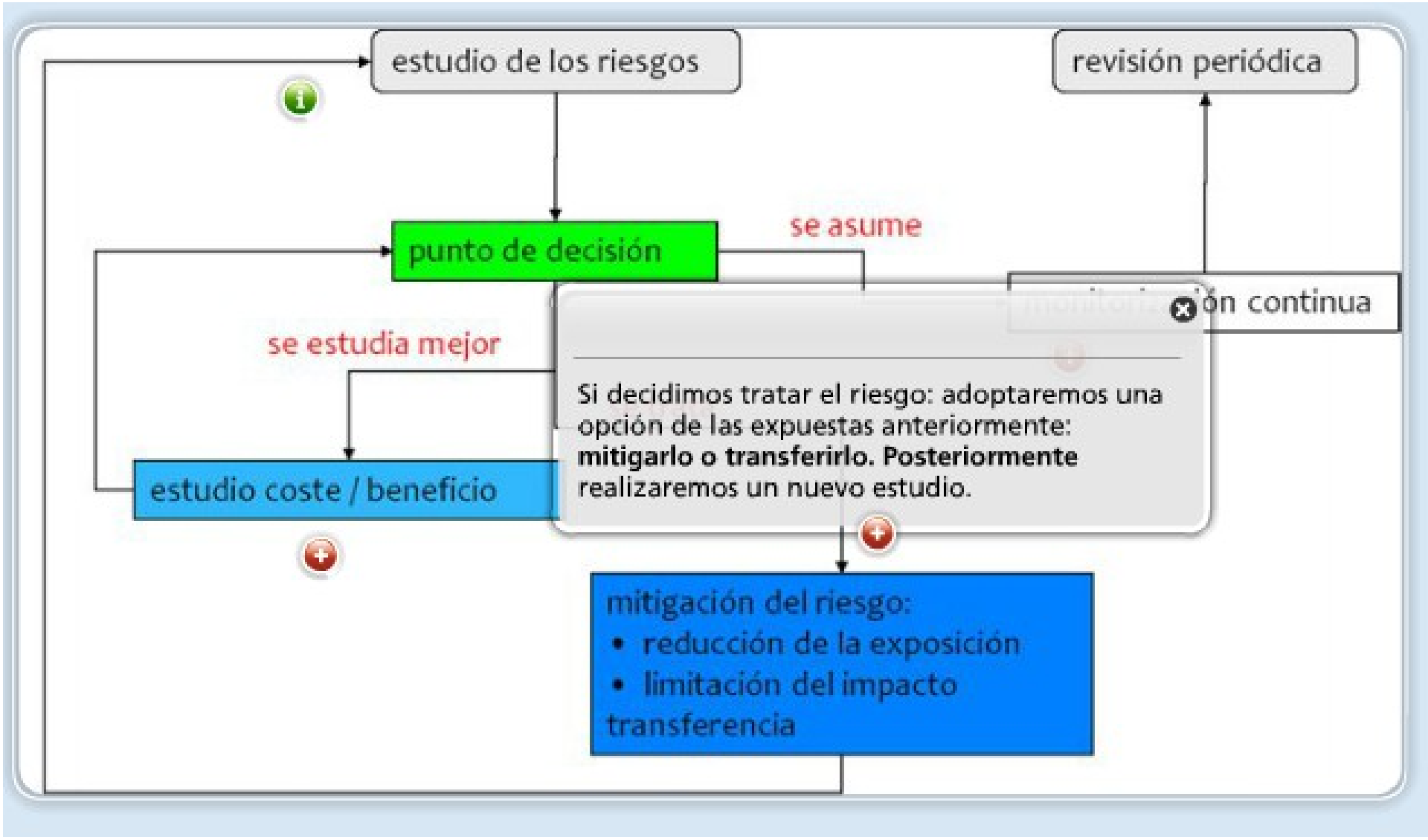


Decisiones de tratamiento de los riesgos


estudio de los riesgos
revisión periódica
La toma de decisiones es complicada ¿asumir?, ¿mitigar?...
Realizado el estudio de riesgos llegamos a un punto de decisión, en el cual tenemos varias alternativas.
se asume
monitorización continua
se trata
estudio coste / beneficio
mitigación del riesgo:
• reducción de la exposición
• limitación del impacto
transferencia


estudio de los riesgos
revisión periódica
punto de decisión
se asume
monitorización continua
se estudia mejor
se trata
Si lo **asumimos**, hay que realizar una **monitorización** continua y una revisión periódica para conocer el impacto.
estudio coste / beneficio
mitigación del riesgo:
• reducción de la exposición
• limitación del impacto
transferencia


estudio de los riesgos
revisión periódica
punto de decisión
se asume
monitorización continua
se estudia mejor
se trata
estudio coste / beneficio
gación del riesgo:
ducción de la exposición
itación del impacto
sferencia
Si no sabemos si aceptarlo o mitigarlo, podemos **realizar un estudio más profundo**, un estudio de coste/beneficio. Los resultados nos llevarán de nuevo a tomar una decisión.


estudio de los riesgos
revisión periódica
punto de decisión
se asume
ón continua
se estudia mejor
Si decidimos tratar el riesgo: adoptaremos una opción de las expuestas anteriormente: **mitigarlo o transferirlo. Posteriormente** realizaremos un nuevo estudio.
estudio coste / beneficio
mitigación del riesgo:
• reducción de la exposición
• limitación del impacto
transferencia

Proceso de gestión de riesgos

Evaluación: interpretación de los valores de impacto y riesgo residuales

- Impacto y riesgo residual son una medida del estado presente, entre la inseguridad potencial (sin salvaguarda alguna) y las medidas adecuadas que reducen impacto y riesgo a valores aceptables.
- 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.
- Es importante entender que un valor residual es sólo un número. Para su correcta interpretación debe venir acompañado de la relación de lo que se debería hacer y no se ha hecho; es decir, de las vulnerabilidades que presenta el sistema.
- Los responsables de la toma de decisiones deberán prestar cuidadosa atención a esta relación de tareas pendientes, que se denomina **Informe de Insuficiencias o de vulnerabilidades**.

Proceso de gestión de riesgos

Aceptación del riesgo

La Dirección de la Organización sometida al análisis de riesgos debe determinar el nivel de impacto y riesgo aceptable.

Más propiamente dicho, debe aceptar la responsabilidad de las insuficiencias.

Esta decisión no es técnica.

Puede ser una decisión política o gerencial o puede venir determinada por ley o por compromisos contractuales con proveedores o usuarios.

Estos niveles de aceptación se pueden establecer por activo o por agregación de activos (en un determinado departamento, en un determinado servicio, en una determinada dimensión, ...)

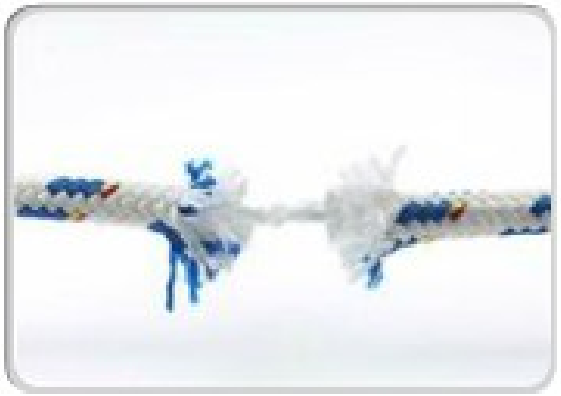
Cualquier nivel de impacto y/o riesgo es aceptable si lo conoce y acepta formalmente la Dirección.

Aceptación del riesgo
Elementos a valorar
Recurrencia
Ciclo de los riesgos

Aceptación del riesgo

Es una opción…

- **Honrada y necesaria**. En algún momento hay que aceptarlo.
- **Pero peligrosa:**
  - El análisis realizado nos dice cuán peligrosa es.
  - Debe ser tomada **EXPLÍCITAMENTE** por la Dirección, nunca puede ser una decisión técnica. La decisión la toman aquellos que tienen responsabilidad en la organización.



Aceptación del riesgo

Elementos a valorar

Recurrencia

Ciclo de los riesgos

Elementos a valorar

Que valoramos al analizar cada riesgo?

- La **gravedad** del impacto y del riesgo.
- **Obligaciones** por ley, reglamentos sectoriales o contratos.
- **Intangibles** (cómo afecta a):
  - Imagen pública de cara a la Sociedad.
  - Política interna.
  - Relaciones con los proveedores.
  - Relaciones con los usuarios.
  - Relaciones con otras organizaciones.
  - Nuevas oportunidades.
  - Acceso a sellos o calificaciones reconocidas de seguridad.
  - ...

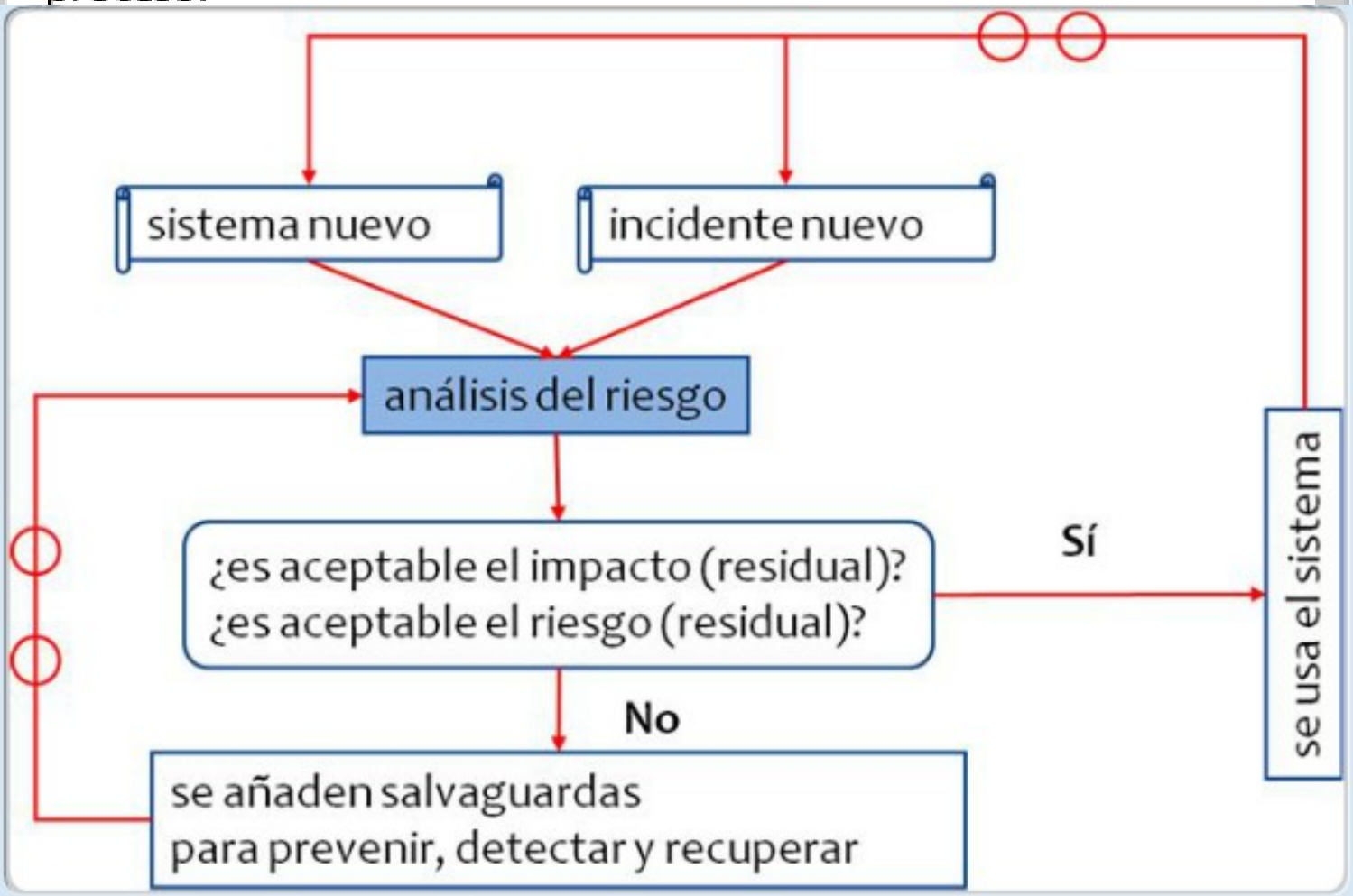
Recurrencia

La naturaleza cíclica del proceso de tratamiento de riesgos nos obliga a hacer un **uso recurrente de las herramientas de análisis de riesgos**. ¿Cuántas veces debemos realizar el análisis? Consideramos dos tipos de ciclo:

- **Micro ciclos:**
  - Hasta que nos quedemos satisfechos.
  - Hasta satisfacer leyes, reglamentos, acuerdos, contratos, ...
  - Hasta tener el certificado.
  - Mientras el coste compense el riesgo.
- **Macro ciclos:**
  - De acuerdo a la política de certificación o acreditación.
  - Como seguimiento de incidentes propios y ajenos.
  - Como seguimiento de cambios en el alcance del riesgo.

Ciclo de los riesgos

Ante sistemas o incidentes nuevos, seguimos el siguiente proceso:



Proceso de gestión de riesgos

Tratamiento

La Dirección puede decidir aplicar algún tratamiento al sistema de seguridad desplegado para proteger el sistema de información.

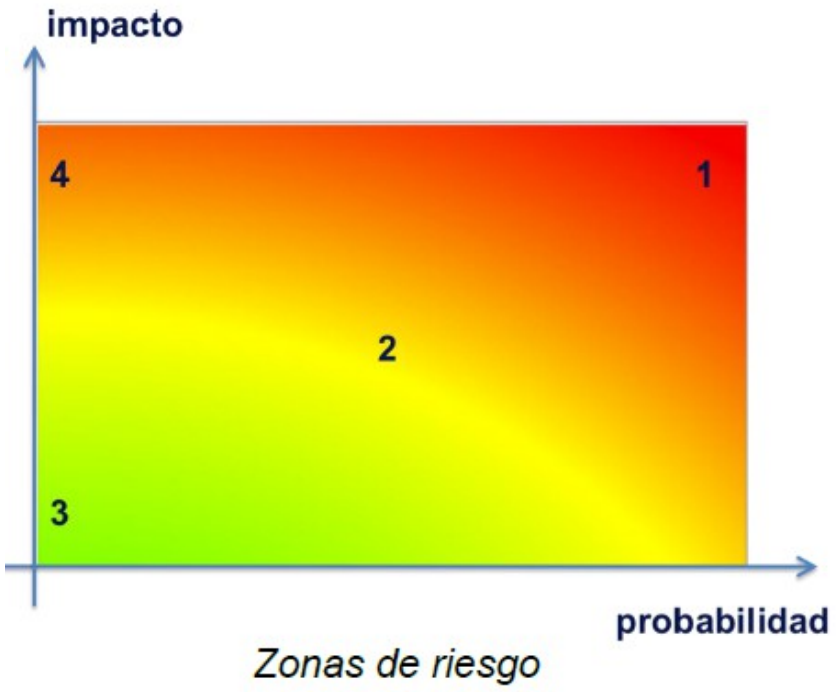
Hay dos grandes opciones:

- reducir el riesgo residual (aceptar un menor riesgo)
- ampliar el riesgo residual (aceptar un mayor riesgo)

Para tomar una u otra decisión hay que enmarcar los riesgos soportados por el sistema de información dentro de un contexto más amplio que cubre un amplio espectro de consideraciones de las que podemos apuntar algunas sin pretender ser exhaustivos:

- cumplimiento de obligaciones; sean legales, regulación pública o sectorial, compromisos internos, misión de la Organización, responsabilidad corporativa, etc.
- posibles beneficios derivados de una actividad que en sí entraña riesgos
- condicionantes técnicos, económicos, culturales, políticos, etc.
- equilibrio con otros tipos de riesgos: comerciales, financieros, regulatorios, medioambientales, laborales, …

Proceso de gestión de riesgos



Zonas de riesgo

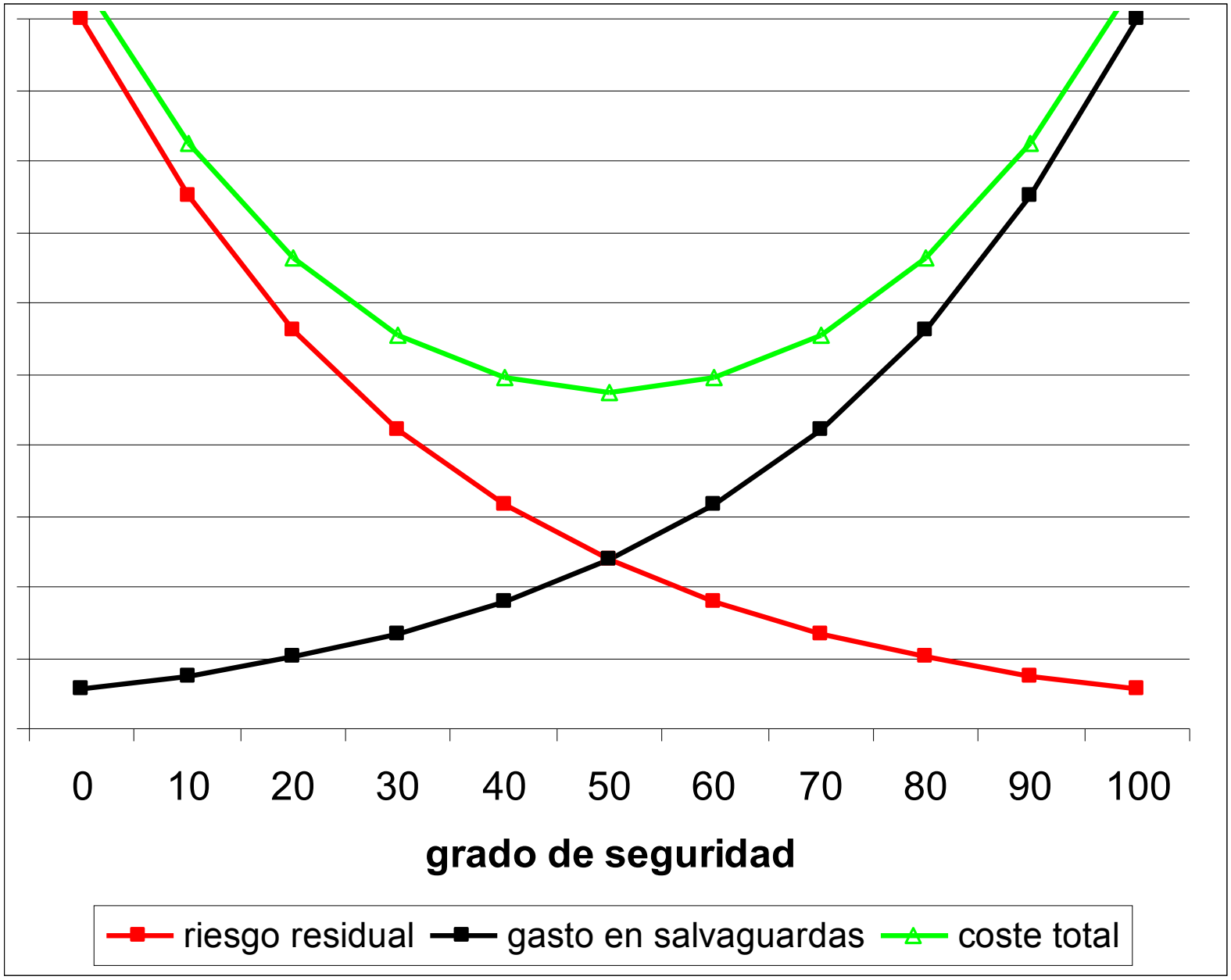
zona 1 – riesgos muy probables y de muy alto impacto; posiblemente nos planteemos sacarlos de esta zona

zona 2 – riesgos de probabilidad relativa e impacto medio; se pueden tomar varias opciones

zona 3 – riesgos improbables y de bajo impacto; o los dejamos como están, o permitimos que suban a mayores si ello nos ofreciera alguna ventaja o beneficio en otro terreno

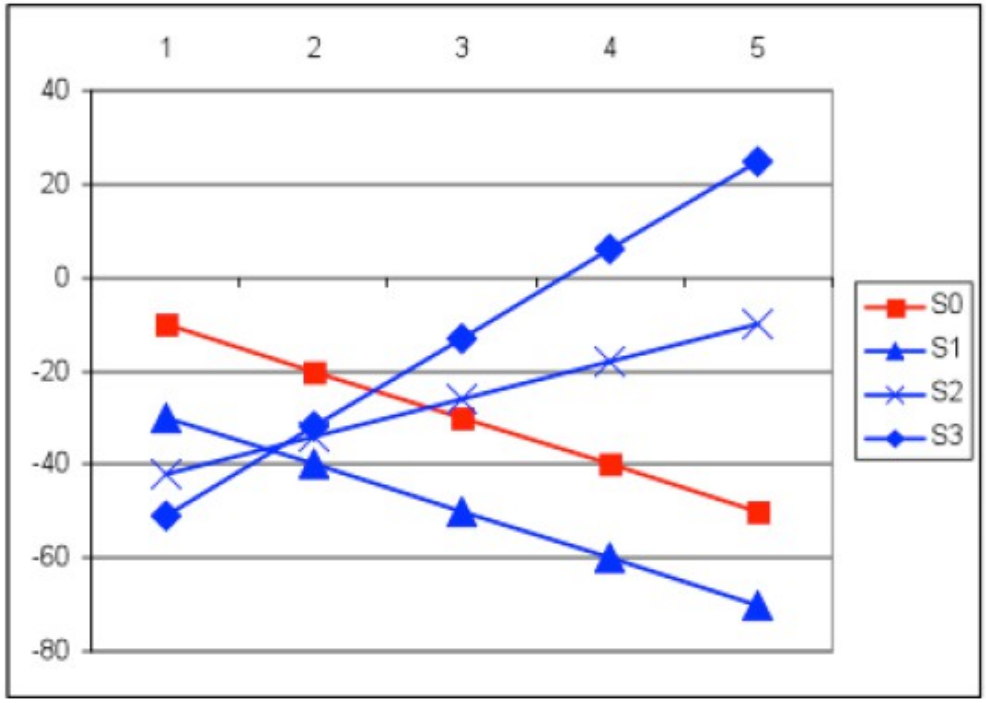
zona 4 – riesgos improbables pero de muy alto impacto; suponen un reto de decisión pues su improbabilidad no justifica que se tomen medidas preventivas, pero su elevado impacto exige que tengamos algo previsto para reaccionar; es decir, hay que poner el énfasis en medidas de reacción para limitar el daño y de recuperación del desastre si ocurriera.

Relación entre el gasto en seguridad y el riesgo residual



Proceso de gestión de riesgos

						año				
	riesgo (anual)	**coste (inicial)**	**coste (anual)**	**mejora (anual)**	**otros (anual)**	**1**	**2**	**3**	**4**	**5**
E0	10	0	0	0	0	-10	-20	-30	-40	-50
E1	5	20	5	0	0	-30	-40	-50	-60	-70
E2	2	50	10	20	0	-42	-34	-26	-18	-10
E3	1	70	15	35	0	-51	-32	-13	6	25



Proceso de gestión de riesgos

Estudio cualitativo de costes / beneficios

Cuando el análisis es cualitativo, en la balanza de costes beneficios aparecen aspectos intangibles que impiden el cálculo de un punto numérico de equilibrio.

Entre los aspectos intangibles se suelen contemplar:

- aspectos reputacionales o de imagen
- aspectos de competencia: comparación con otras organizaciones de mismo ámbito de actividad
- cumplimiento normativo, que puede ser obligatorio o voluntario
- capacidad de operar
- productividad

Estas consideraciones nos llevan a contemplar diversos escenarios para determinar el balance neto.

Por ejemplo, el no adoptar medidas puede exponernos a un cierto riesgo que causaría mala imagen; pero si la solución preventiva causa también mala imagen o supone un merma notable de oportunidades o de productividad, hay que buscar un punto de equilibrio, eligiendo una combinación de medidas que sea asumible.

Proceso de gestión de riesgos

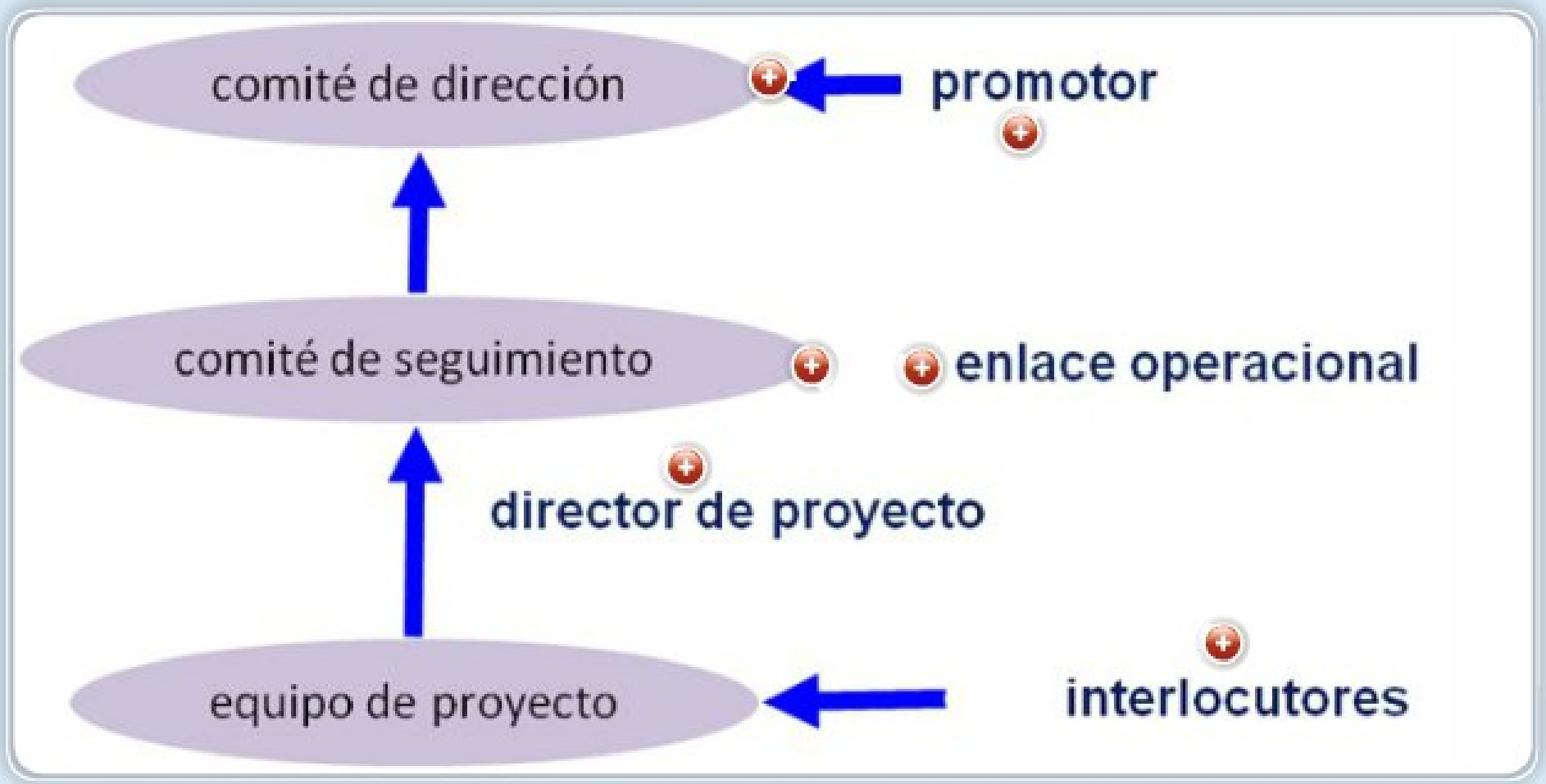
Estudio mixto de costes / beneficios

En análisis de riesgos meramente cualitativos, la decisión la marca el balance de costes y beneficios intangibles, si bien siempre hay que hacer un cálculo de lo que cuesta la solución y cerciorarse de que el gasto es asumible.

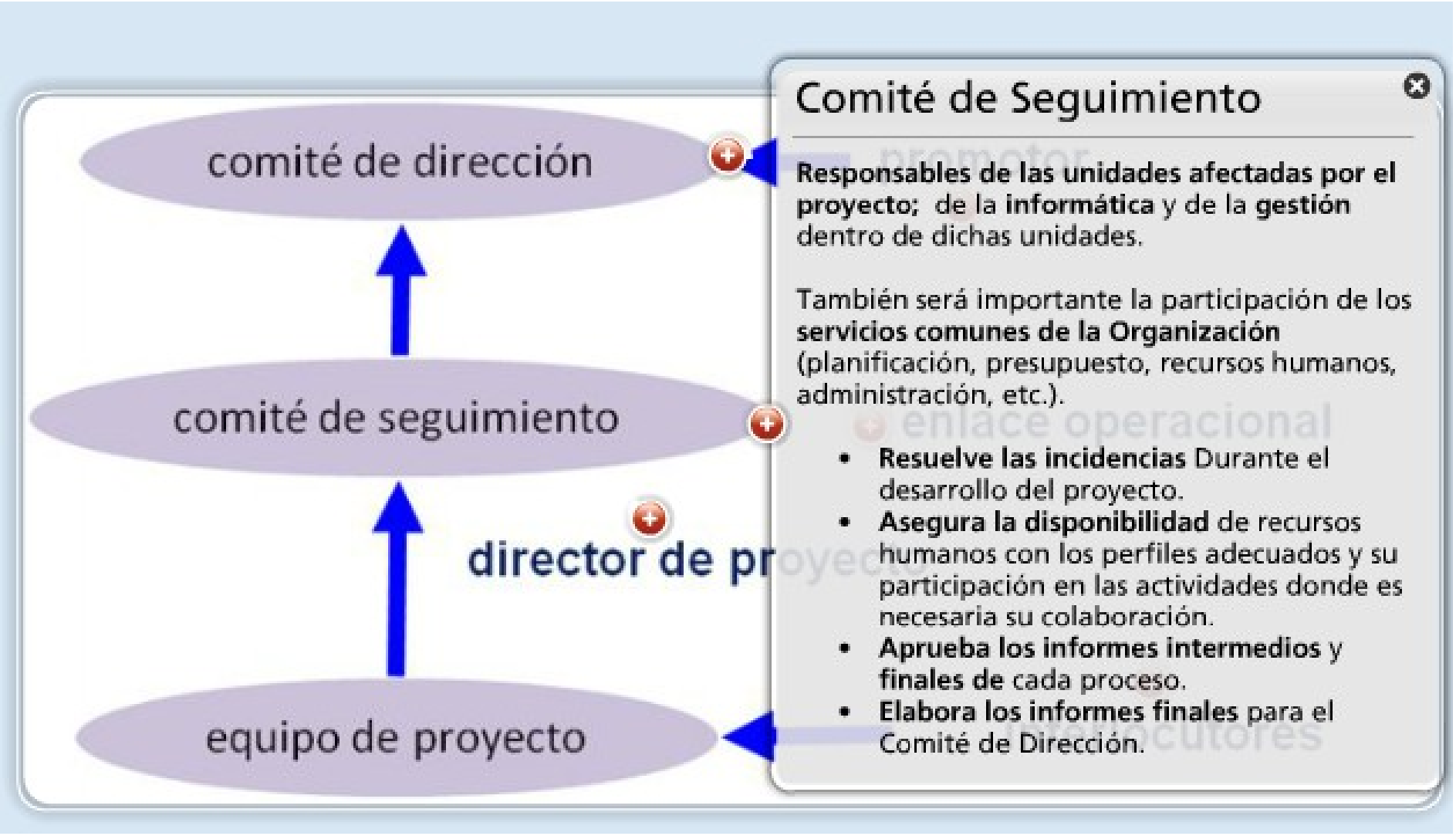
De lo contrario, la supuesta solución no es una opción. Es decir, primero hay que pasar el filtro económico y luego elegir la mejor de las soluciones factibles.

Roles y funciones

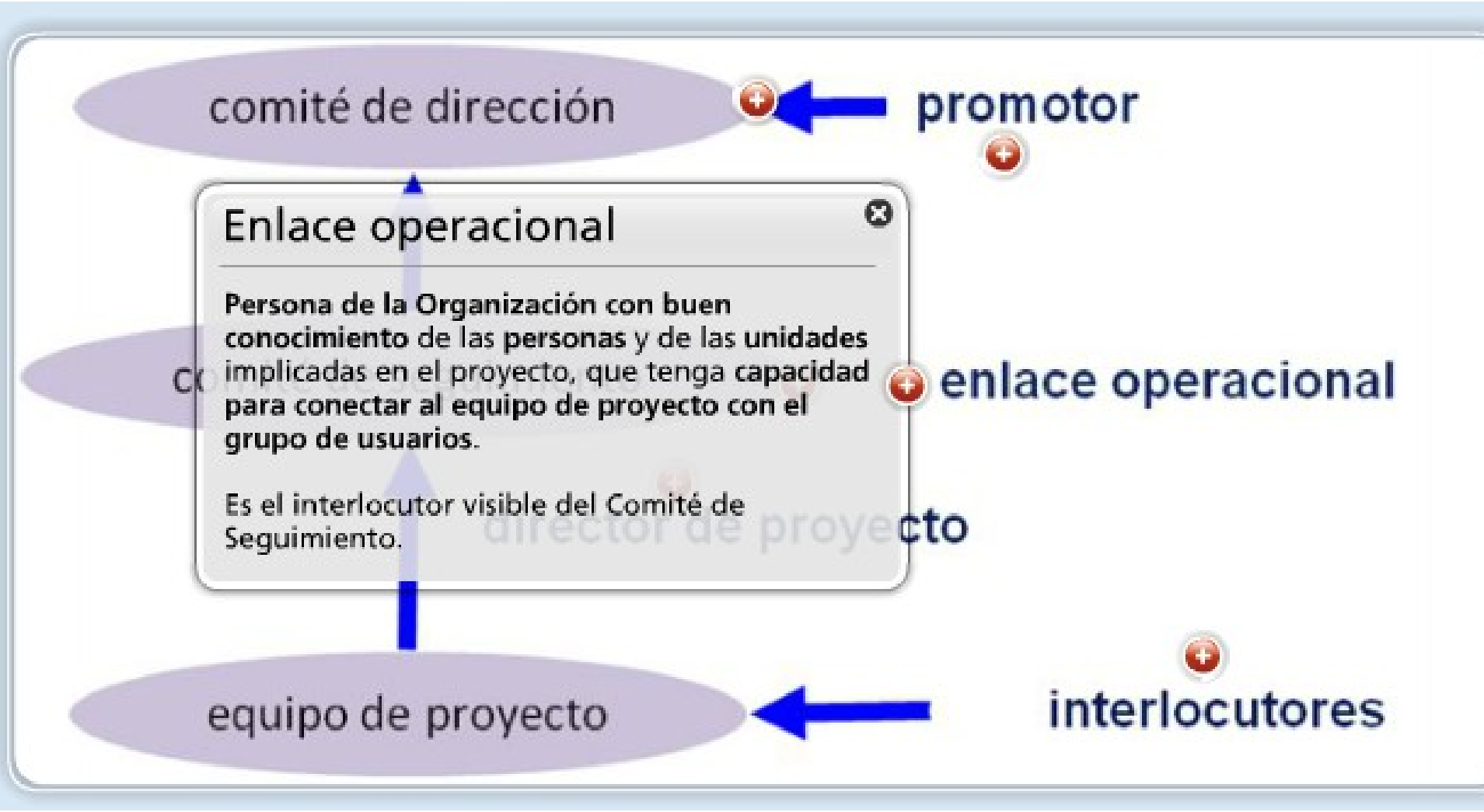
Actores del proceso

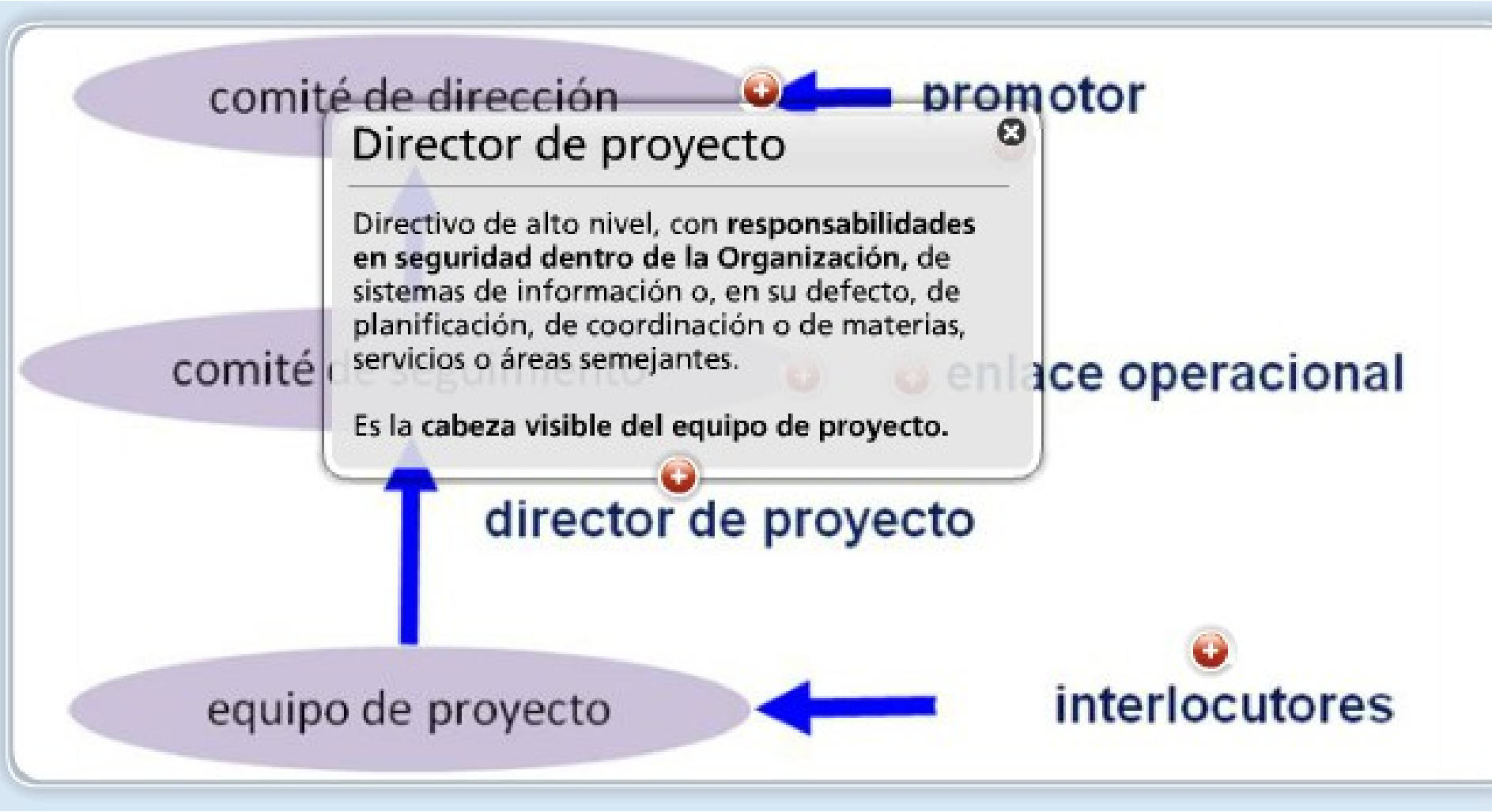


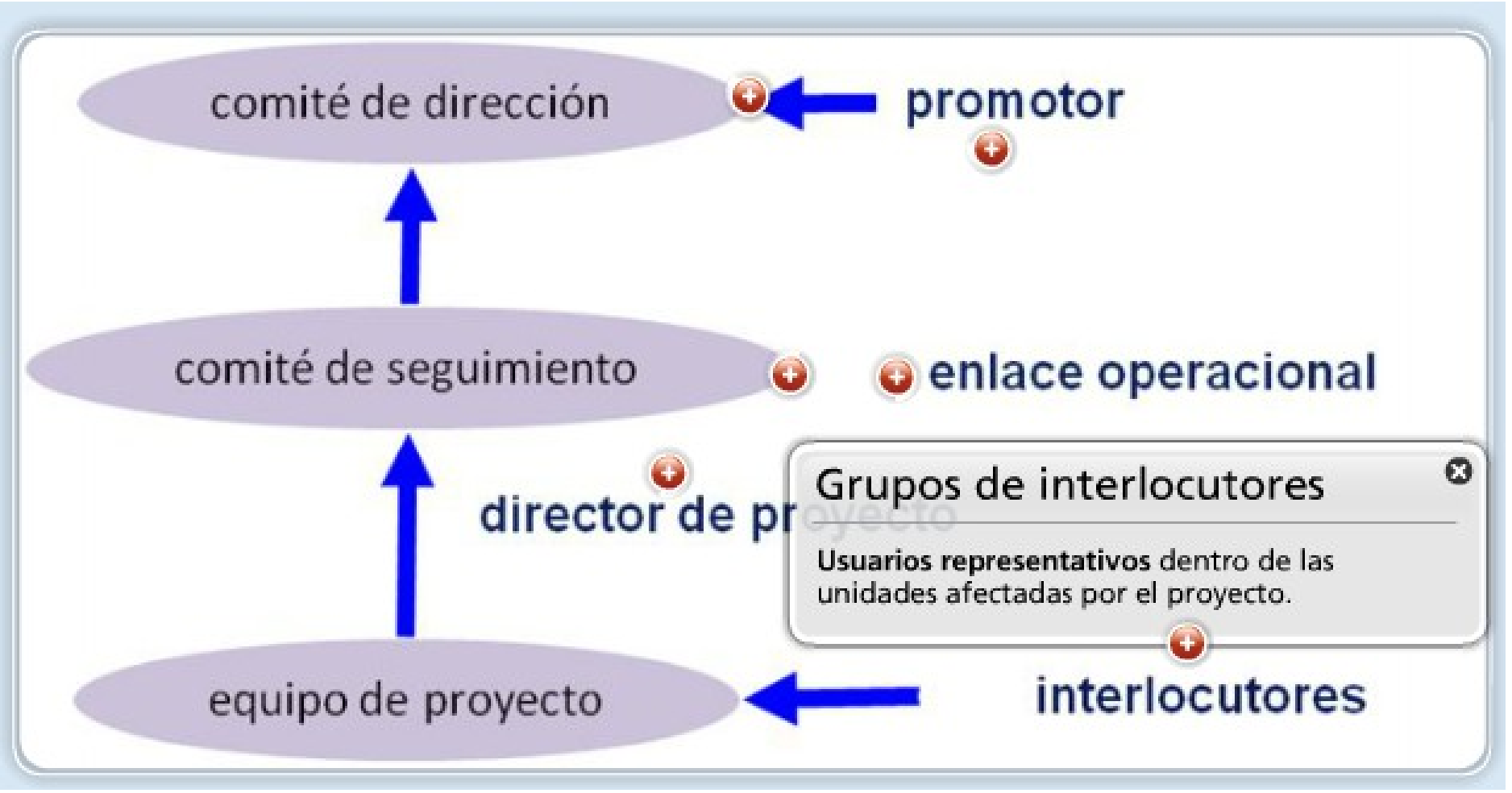

comité de dirección
comité de seguimiento
director de proyecto
equipo de proyecto
interlocutores
Comité de Dirección
Personas con un nivel alto en la **Dirección**, con **conocimiento de los objetivos estratégicos y de negocio** que se persiguen y autoridad para **validar y aprobar** cada uno de los procesos realizados durante el desarrollo del proyecto.
Asigna los recursos necesarios para la ejecución del proyecto.
Aprueba los resultados finales de cada proceso.


comité de dirección
comité de seguimiento
director de pr
equipo de proyecto
Comité de Seguimiento
Responsables de las unidades afectadas por el proyecto; de la informática y de la gestión dentro de dichas unidades.
También será importante la participación de los servicios comunes de la Organización (planificación, presupuesto, recursos humanos, administración, etc.).
Resuelve las incidencias Durante el desarrollo del proyecto.
Asegura la disponibilidad de recursos humanos con los perfiles adecuados y su participación en las actividades donde es necesaria su colaboración.
Aprueba los informes intermedios y finales de cada proceso.
Elabora los informes finales para el Comité de Dirección.

Actores del proceso


comité de dirección
promotor
Enlace operacional
Persona de la Organización con buen conocimiento de las personas y de las unidades implicadas en el proyecto, que tenga capacidad para conectar al equipo de proyecto con el grupo de usuarios.
Es el interlocutor visible del Comité de Seguimiento.
enlace operacional
director de proyecto
equipo de proyecto
interlocutores


comité de dirección
promotor
Director de proyecto
Directivo de alto nivel, con responsabilidades en seguridad dentro de la Organización, de sistemas de información o, en su defecto, de planificación, de coordinación o de materias, servicios o áreas semejantes.
Es la cabeza visible del equipo de proyecto.
comité
ace operacional
director de proyecto
equipo de proyecto
interlocutores

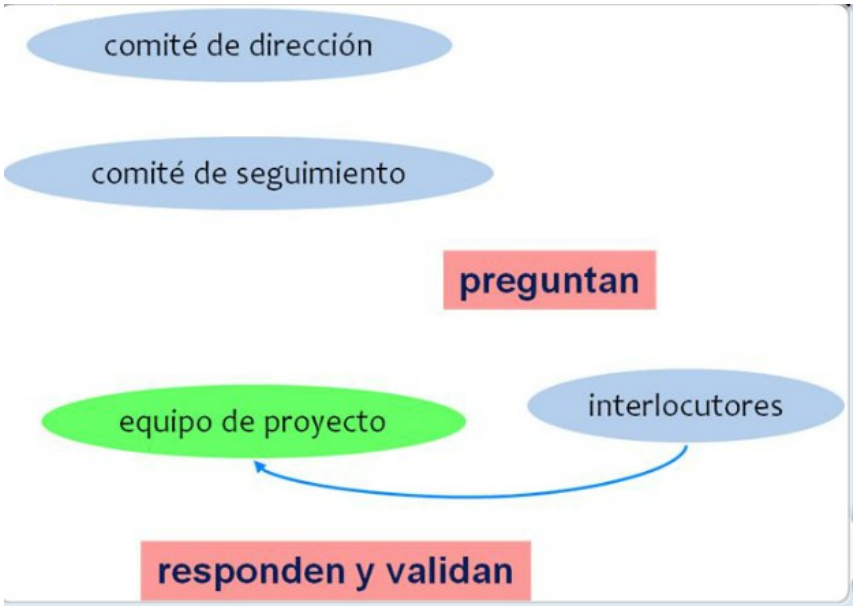

comité de dirección
promotor
comité de seguimiento
enlace operacional
director de proyecto
Grupos de interlocutores
Usuarios representativos dentro de las unidades afectadas por el proyecto.
equipo de proyecto
interlocutores

Pasos iniciales

- Se suele iniciar a partir de una persona que es el promotor, que conciencia a la Dirección de que es necesario actuar, bien por condicionamiento legal o por necesidad técnica.
- La Dirección crea un comité de seguimiento (nivel gerencial) para arrancar el proyecto de análisis de riesgos (interno o externo). Si el comité es externo, es importante que estas personas no sean propietarios del análisis de riesgos. Debe quedar en propiedad del que contrata, deben estar dentro del equipo de proyecto para poder actualizar el proceso.

Magerit. Proceso. Realización

El equipo del proyecto habla con los interlocutores, las personas que están trabajando en el día a día con el sistema, para conocer realmente los posibles riesgos y qué elementos del sistema es necesario proteger.



Magerit. Proceso. Reporting

El equipo de proyecto genera un informe (análisis técnico).

El comité de seguimiento lo convierte en términos de negocio y se lo muestra a la Dirección, que es quien toma decisiones.

Se establece un plan de seguridad, que el equipo de proyecto difunde entre los diferentes interlocutores de la organización para que lo pongan en práctica.

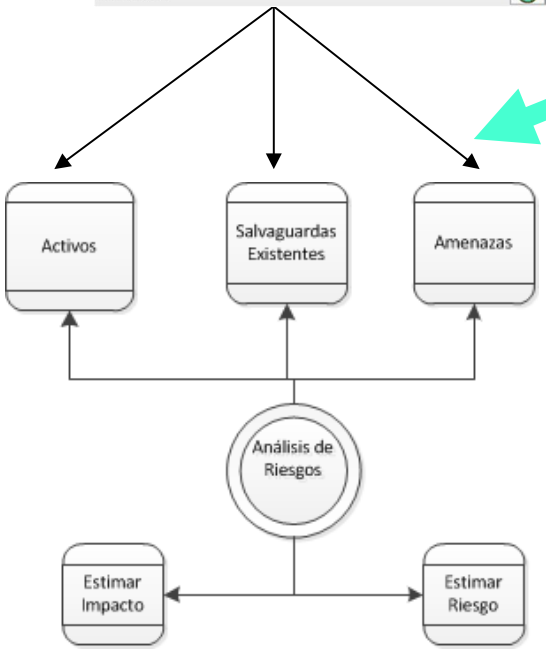
Indicadores de control del proceso de gestión de riesgos

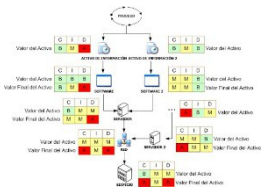
- Se han definido los roles y responsabilidades respecto de la gestión de riesgos
- Se ha establecido el contexto de gestión de riesgos
- Se han establecido los criterios de valoración de riesgos y toma de decisiones de tratamiento
- Se han interpretado los riesgos residuales en términos de impacto en el negocio o misión de la Organización
- Se han identificado y valorado opciones de tratamiento de los riesgos residuales (propuesta de programas de seguridad)
- Los órganos de gobierno han adoptado una propuesta de tratamiento
  - evitar el riesgo
  - prevenir: mitigar la probabilidad de que ocurra
  - mitigar el impacto si ocurriera
  - compartir el riesgo con un tercero
  - asumir el riesgo
- Se han previsto recursos para acometer el plan de seguridad
- Se han previsto recursos para atender a contingencias
- Se han comunicado las decisiones a las partes afectadas
- Se ha desplegado un sistema de monitorización constante para detectar modificaciones en los supuestos de análisis de riesgos
- Se han establecido las normas y procedimientos de actuación en caso de detectar desviaciones de los supuestos

Índice

MAGERIT – versión 3.0
Metodología de Análisis y Gestión
de Riesgos de los Sistemas de Información

Proyecto





Informes

Proyecto de Análisis de Riesgos

- Cuando se realiza un análisis de riesgos partiendo de cero, se consumen una serie de recursos apreciables y conviene planificar estas actividades dentro de un proyecto, sea interno o se subcontrate a una consultora externa.
- En esta sección se presentan las consideraciones que se deben tener en cuenta para que este proyecto llegue a buen término.
  - PAR.1 – Actividades preliminares
  - PAR.2 – Elaboración del análisis de riesgos
  - PAR.3 – Comunicación de resultados

El proyecto de análisis de los riesgos se lleva a cabo por medio de las siguientes tareas:

PAR – Proyecto de Análisis de Riesgos
PAR.1 – Actividades preliminares
PAR.11 – Estudio de oportunidad
PAR.12 – Determinación del alcance del proyecto
PAR.13 – Planificación del proyecto
PAR.14 – Lanzamiento del proyecto
PAR.2 – Elaboración del análisis de riesgos
PAR.3 – Comunicación de resultados

Documentación final

- Modelo de valor: identificación de activos junto con sus dependencias y valoración propia y acumulada
- Mapa de amenazas junto con sus consecuencias y probabilidad de ocurrencia.
- Documento de aplicabilidad de las salvaguardas.
- Informe de valoración de la efectividad de las salvaguardas presentes.
- Informe de insuficiencias o debilidades del sistema de salvaguardas.
- Indicadores de impacto y riesgo, potenciales y residuales.

Índice

Plan de Seguridad

- Son los proyectos para materializar las decisiones adoptadas para el tratamiento de los riesgos.
- Estos planes reciben diferentes nombres en diferentes contextos y circunstancias:
  - plan de mejora de la seguridad
  - plan director de seguridad
  - plan estratégico de seguridad
  - plan de adecuación (en concreto es el nombre que se usa en el ENS)
- Se identifican 3 tareas:
  - PS.1 – Identificación de proyectos de seguridad
  - PS.2 – Plan de Ejecución
  - PS.3 - Ejecución

Listas de control Planes de Seguridad

- Se han definido los proyectos constituyentes
- Se han definido las interdependencias entre proyectos (necesidades de que uno avance para que progrese otro)
- Se han asignado recursos
- — disponibles para los proyectos en curso
- — previstos para los proyectos que seguirán en el futuro
- Se han definido roles y responsabilidades
- Se ha establecido un calendario de ejecución
- Se han definido indicadores de progreso
- Se han previsto necesidades de concienciación y formación
- Se han previsto necesidades de documentación:
  - normativa de seguridad y
  - procedimientos operativos de seguridad

Índice

Desarrollo de sistemas de información

Las aplicaciones (software) constituyen un tipo de activos frecuente y nuclear para el tratamiento de la información en general y para la prestación de servicios basados en aquella información.

La presencia de aplicaciones en un sistema de información es siempre una fuente de riesgo en el sentido de que constituyen un punto donde se pueden materializar amenazas.

A veces, además, las aplicaciones son parte de la solución en el sentido de que constituyen una salvaguarda frente a riesgos potenciales.

En cualquier caso es necesario que el riesgo derivado de la presencia de aplicaciones esté bajo control.

El análisis de los riesgos constituye una pieza fundamental en el diseño y desarrollo de sistemas de información seguros.

Es posible, e imperativo, incorporar durante la fase de desarrollo las funciones y mecanismos que refuerzan la seguridad del nuevo sistema y del propio proceso de desarrollo, asegurando su consistencia y seguridad, completando el plan de seguridad vigente en la Organización.

Es un hecho reconocido que tomar en consideración la seguridad del sistema antes y durante su desarrollo es más efectivo y económico que tomarla en consideración a posteriori.

La seguridad debe estar embebida en el sistema desde su primera concepción.

Desarrollo de sistemas de información

El Esquema Nacional de Seguridad recoge el riesgo como pieza fundamental de la seguridad de los sistemas en varios de sus principios básicos:

Artículo 5. La seguridad como un proceso integral.

1. La seguridad se entenderá como un proceso integral constituido por todos los elementos técnicos, humanos, materiales y organizativos, relacionados con el sistema. La aplicación del Esquema Nacional de Seguridad estará presidida por este principio, que excluye cualquier actuación puntual o tratamiento coyuntural.

2. Se prestará la máxima atención a la concienciación de las personas que intervienen en el proceso y a sus responsables jerárquicos, para que, ni la ignorancia, ni la falta de organización y coordinación, ni instrucciones inadecuadas, sean fuentes de riesgo para la seguridad.

Artículo 6. Gestión de la seguridad basada en los riesgos.

1. El análisis y gestión de riesgos será parte esencial del proceso de seguridad y deberá mantenerse permanentemente actualizado.

2. La gestión de riesgos permitirá el mantenimiento de un entorno controlado, minimizando los riesgos hasta niveles aceptables. La reducción de estos niveles se realizará mediante el despliegue de medidas de seguridad, que establecerá un equilibrio entre la naturaleza de los datos y los tratamientos, los riesgos a los que estén expuestos y las medidas de seguridad.

Artículo 9. Reevaluación periódica.

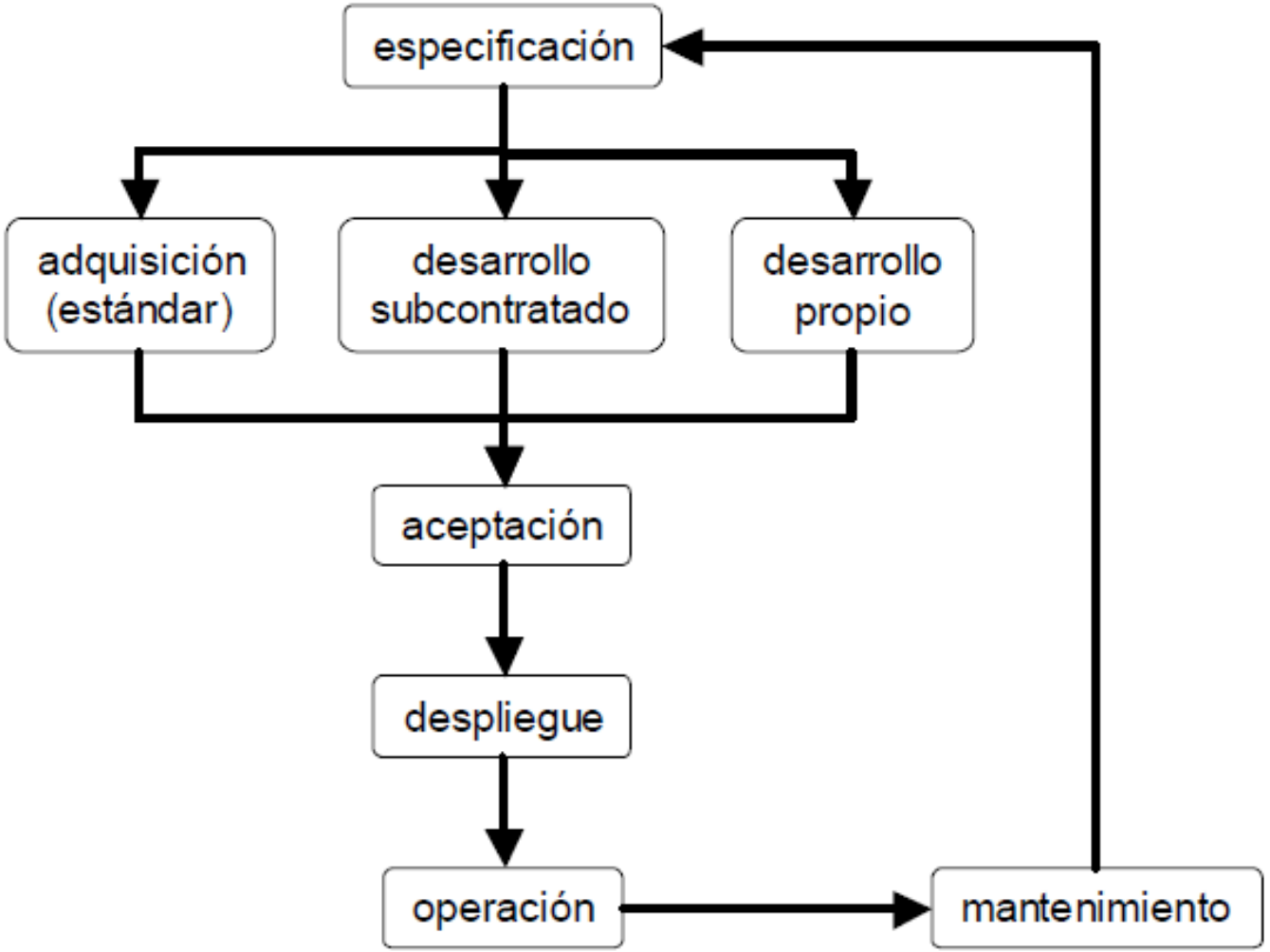
Las medidas de seguridad se reevaluarán y actualizarán periódicamente, para adecuar su eficacia a la constante evolución de los riesgos y sistemas de protección, llegando incluso a un replanteamiento de la seguridad, si fuese necesario.

Desarrollo de sistemas de información

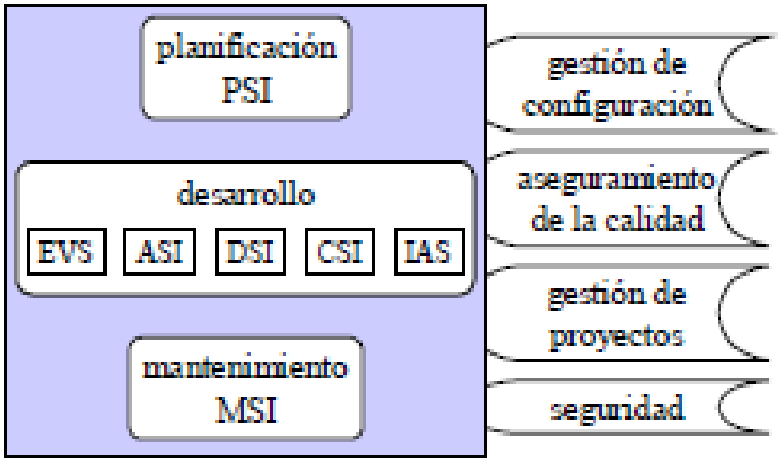
Durante el desarrollo de un sistema de información, se pueden identificar dos tipos de actividades diferenciadas:

- SSI: actividades relacionadas con la propia seguridad del sistema de información que se está desarrollando.
- SPD: actividades que velan por la seguridad del proceso de desarrollo del sistema de información.

Desarrollo de sistemas de información. SSI



Ciclo de vida de las aplicaciones



Métrica 3 - Actividades

Métrica 3

especificación	PSI – Planificación del sistema de información EVS – Estudio de viabilidad del sistema ASI – Análisis del sistema de información
adquisición o desarrollo	DSI – Diseño del sistema de información. CSI – Construcción del sistema de información
aceptación	IAS – Implantación y aceptación del sistema
despliegue	
operación	
mantenimiento	MSI – Mantenimiento del sistema de información

Ciclo de vida y actividades en Métrica 3

Desarrollo de sistemas de información. SSI

Contexto

Se debe determinar el contexto general:

— política de seguridad y normas

— requisitos de cumplimiento normativo

— obligaciones contractuales

— roles y funciones

— criterios de valoración de información y servicios

— criterios de valoración de riesgos

— criterios de aceptación de riesgos

En particular, hay que establecer unos procedimientos operativos que instrumenten la comunicación entre las tareas de desarrollo y las tareas de análisis y tratamiento de riesgos.

La Dirección aporta los servicios necesarios y la calidad de la seguridad deseada.

El equipo de desarrollo aporta los elementos técnicos que materializan la aplicación.

El equipo de análisis de riesgos aporta un juicio crítico sobre la seguridad del sistema.

La misma Dirección aprueba el riesgo residual.

Desarrollo de sistemas de información. SSI

Fase de especificación: adquisición de datos

Se debe recopilar información sobre

— la información esencial y sus requisitos de seguridad

— los servicios esenciales y sus requisitos de seguridad

— el contexto en el que se va a desarrollar y explotar el sistema

En particular se debe establecer un perfil de amenazas, sean naturales, del entorno o de origen humano, sean accidentales o deliberadas.

La caracterización del potencial del atacante debe formar parte de las especificaciones del diseño y su modificación más adelante.

Desarrollo de sistemas de información. SSI

Fase de diseño: estudio de opciones

La toma de decisiones de tratamiento de los riesgos puede recomendar salvaguardas evaluando su efecto en los indicadores de impacto y riesgo.

Las decisiones que se adopten dependerán de los criterios establecidos en la política de seguridad de la Organización y de otras consideraciones específicas de cada caso.

Si bien la política de seguridad establece un marco de referencia que no puede violentarse, es habitual que no prevea todos los detalles técnicos y coyunturales del servicio para tomar decisiones precisas.

Debido a la interrelación entre los elementos que constituyen un sistema, no es suficiente proteger un cierto tipo de activos para proteger el conjunto.

> Por ello, la toma de decisiones de tratamiento es local sobre una parte del sistema, pero siempre con un análisis global sobre la seguridad del conjunto.

Desarrollo de sistemas de información. SSI

Análisis y tratamiento de los riesgos

La seguridad requerida para la información que se maneja y los servicios que se prestan quedó fijada en la fase de especificación y no se puede modificar ahora.

El equipo de desarrollo y el equipo de análisis de riesgos trabajan de forma iterativa hasta encontrar una solución que satisfaga a ambas partes.

Normalmente la iniciativa la toma el equipo de desarrollo proponiendo una solución técnica que responda a los requisitos funcionales del sistema.

El equipo de seguridad analiza la propuesta informando de los riesgos asociados y, en su caso, proponiendo salvaguardas que pudieran dejar el riesgo en niveles aceptables.

En la medida en que las salvaguardas propuestas afecten al diseño, el equipo rehará su propuesta para un nuevo análisis.

La especificación de salvaguardas debe incorporar tanto los mecanismos de actuación como los mecanismos de configuración, monitorización y control de su eficacia y eficiencia.

Es frecuente que aparezcan algunos desarrollos específicamente destinados a configurar el conjunto de salvaguardas y a monitorizar su operación.

Es posible que el equipo de desarrollo pueda presentar dos o más opciones, en cuyo todas ellas serán evaluadas en lo que respecta a riesgo y salvaguardas requeridas.

El informe de riesgos será un elemento más de decisión entre las diferentes opciones.

Cuando ambos equipos lleguen a una situación estable, con un diseño técnicamente viable, con un riesgo aceptable y unos requisitos aceptables de recursos, la propuesta se eleva para su aprobación.

Como resultado de esta fase, dispondremos de especificaciones técnicas de desarrollo acompañadas de un análisis de los riesgos y sus decisiones de tratamiento.

Desarrollo de sistemas de información. SSI

Soporte al desarrollo: puntos críticos

Durante el desarrollo hay que incorporar las salvaguardas aprobadas en la fase de diseño, así como controles que permitan monitorizar su eficacia.

Estos requisitos de monitorización se suelen concretar en los siguientes aspectos:

— registros de actividad

— mecanismos para procesar estos registros e informar de la efectividad del sistema de protección

— disparo de alarmas cuando los hecho evidencian un problema de seguridad

El despliegue de estos elementos viene modulado por el nivel de riesgo potencial que se soporta en cada componente del sistema de información.

Desarrollo de sistemas de información. SSI

Aceptación y puesta en marcha: puntos críticos

Cuando el sistema se prueba antes de ponerlo en funcionamiento, debe revisarse que todos los registros de actividad funcionan correctamente, así como los sistemas de procesamiento y de alarma incorporados al sistema.

También debe comprobarse que el sistema responde al diseño previsto, concretamente que las salvaguardas están desplegadas, que su despliegue es efectivo y que no existen formas de circunvalarlas u obviarlas: es decir que el sistema no permite puertas traseras fuera de control.

Sistema(s) de identificación y autenticación:

— todo acceso al sistema requiere que el usuario se identifique y se autentique según lo previsto, bloqueando cualquier otra forma de acceso

— los mecanismos de identificación y autenticación están protegidos para evitar que un atacante pueda acceder a información o mecanismos que pongan en peligro su efectividad

Desarrollo de sistemas de información. SSI

Aceptación y puesta en marcha: puntos críticos

Sistema(s) de control de acceso:

— todo acceso a la información y a los servicios verifica previamente que el usuario tiene las autorizaciones pertinentes

Servicios externalizados: cuando parte de la operación del sistema está delegada en un tercero:

— hay que revisar los contratos de prestación del servicio

— hay que revisar la completitud de los procedimientos de reporte y gestión de incidencias

Si el sistema no refleja el modelo cuyos riesgos han sido analizados, será rechazado sin pasar a producción.

Hay que verificar que la **documentación de seguridad es clara y precisa**. Esto incluye normativa, procedimientos operacionales, material de concienciación y de formación.

Desarrollo de sistemas de información. SSI

Aceptación y puesta en marcha: puntos críticos

Sin poder ser exhaustivos, las siguientes líneas muestran pruebas de aceptación que conviene realizar:

- datos de prueba
  - si no son reales, deben ser realistas
  - si no se puede evitar que sean reales, hay que controlar copias y acceso
- pruebas funcionales (de los servicios de seguridad)
  - simulación de ataques: verificando que se detectan y reportan
  - pruebas en carga: verificando que no se obvian las medidas de protección
  - intrusión controlada (*hacking ético)*
- inspección de servicios / inspección de código
  - fugas de información: canales encubiertos, a través de los registros, etc.
  - puertas traseras de acceso
  - escalado de privilegios
  - problemas de desbordamiento de registros *(buffer overflow)*

Desarrollo de sistemas de información. SSI

Operación: análisis y gestión dinámicos

Durante la vida operativa del sistema podemos encontrarnos con cambios en el escenario que invalidan el análisis de riesgos realizado anteriormente. En entornos formales, el sistema requiere una re-acreditación para seguir operando bajo las nuevas condiciones.

Nuevas amenazas

Bien porque se descubren nuevas formas de ataque, bien porque la valoración de la capacidad del atacante se modifica. En estos casos hay que rehacer el análisis y decidir cómo tratar los nuevos resultados.

Vulnerabilidades sobrevenidas

Por ejemplo, defectos reportados por los fabricantes. En estos casos hay que analizar la nueva situación de riesgo y determinar cual es su tratamiento adecuado para seguir operando. Lo ideal es parchear el sistema; pero bien porque el parche no existe o porque su aplicación requiere unos recursos de los que no disponemos, podemos encontrarnos en una situación nueva ante la cual hay que decidir cómo tratar el riesgo.

Desarrollo de sistemas de información. SSI

Operación: análisis y gestión dinámicos

Incidentes de seguridad

Los incidentes de seguridad pueden indicarnos un fallo en nuestra identificación de amenazas o en su valoración, obligando a revisar el análisis.

Un incidente de seguridad también puede suponer un cambio en el sistema. Por ejemplo, una intrusión significa que no podemos contar con la defensa perimetral: tenemos un nuevo sistema, con el atacante en un nuevo lugar y con unas opciones nuevas.

Cambios en la utilización del sistema

A veces un sistema ya operacional no se utiliza como estaba previsto:

— nueva información con diferentes requisitos de seguridad

— nuevos servicios con diferentes requisitos de seguridad

— nuevos procedimientos operativos

En términos del análisis de riesgos, esto significa una diferente valoración de los activos o de las salvaguardas desplegadas.

Es posible que la alteración del sistema en alguna de las facetas contempladas en los puntos anteriores lleve a unos niveles de riesgo que no sean aceptables, obligando a un ciclo de mantenimiento que rediseñe el sistema o parte de él.

Desarrollo de sistemas de información. SSI

Ciclos de mantenimiento: análisis marginal

Cuando se propone una modificación del sistema, los nuevos elementos deben llevar a un nuevo análisis de riesgos, regresando a los ciclos iterativos de propuestas y soluciones de la fase de diseño.

Terminación

Cuando un sistema de información se retira del servicio, hay que realizar una serie de tareas de seguridad proporcionadas al riesgo al que están sometidos los componentes del sistema a retirar. En concreto:

— proteger el valor de la información manejada: retención y control de acceso

— proteger las claves criptográficas de cifra y de autenticación: retención y control de acceso

Todo lo que no sea necesario retener se destruirá de forma segura:

— datos operacionales

— copias de seguridad

— configuración de los sistemas

Desarrollo de sistemas de información. SSI

Documentación de seguridad

La documentación de seguridad evoluciona con el ciclo de vida del sistema:

fase	documentación de seguridad
contexto	se revisa la política de seguridad se revisa la normativa de seguridad
especificación	se amplia la normativa de seguridad
diseño	se prepara el índice de procedimientos operacionales de seguridad
desarrollo	se elaboran los procedimientos operacionales de seguridad
aceptación y puesta en operación	se validan los procedimientos operacionales de seguridad
operación	se actualizan los procedimientos operacionales de seguridad
mantenimiento	se actualizan los procedimientos operacionales de seguridad

Documentación de seguridad a lo largo del ciclo de vida de las aplicaciones

Desarrollo de sistemas de información. SPD

Lo que se comenta en esta sección afecta a todas y cada uno de los procesos y subprocesos de Métrica: PSI, EVS, ASI, DSI, CSI, IAS y MSI.

La interfaz de seguridad de Métrica identifica hasta 4 tareas que se repiten en cada proceso. Aquí se tratan de forma compacta:

Activos a considerar

En cada proceso se requiere un análisis de riesgos específico que contemple:

- los datos que se manejan:
  - especificaciones y documentación de los sistemas
  - código fuente
  - manuales del operador y del usuario
  - datos de prueba
- el entorno *software de desarrollo:*
  - herramientas de tratamiento de la documentación: generación, publicación, control de documentación, etc.
  - herramientas de tratamiento del código: generación, compilación, control de versiones, etc.
- el entorno *hardware de desarrollo: equipos centrales, puestos de trabajo, equipos de archivo, etc.*
- el entorno de comunicaciones de desarrollo
- las instalaciones
- el personal involucrado: desarrolladores, personal de mantenimiento y usuarios (de pruebas)

Desarrollo de sistemas de información. SPD

Actividades

Se siguen los siguientes pasos

1. el equipo de desarrollo expone a través del jefe de proyecto los elementos involucrados
2. el equipo de análisis de riesgos recibe a través del director de seguridad la información de los activos involucrados
3. el equipo de análisis de riesgos realiza el análisis
4. el equipo de análisis de riesgos expone a través de su director el estado de riesgo, proponiendo una serie de medidas a tomar
5. el equipo de desarrollo elabora un informe del coste que supondrían las medidas recomendadas, incluyendo costes de desarrollo y desviaciones en los plazos de entrega
6. la dirección califica el riesgo y decide las salvaguardas a implantar oyendo el informe conjunto de análisis de riesgos y coste de las soluciones propuestas
7. el equipo de análisis de riesgos elabora los informes correspondientes a las soluciones adoptadas
8. el equipo de seguridad elabora la normativa de seguridad pertinente
9. la dirección aprueba el plan para ejecutar el proceso con la seguridad requerida

Resultados del análisis y gestión de riesgos

En todos los casos

- salvaguardas recomendadas
- normas y procedimientos de tratamiento de la información

Desarrollo de sistemas de información. SPD

Otras consideraciones

Aunque cada proceso requiere su análisis de riesgos específico, es cierto que se trata de modelos tremendamente similares por lo que el mayor esfuerzo lo llevará el primero que se haga, siendo los demás adaptaciones de aquel primero.

En los primeros procesos, notablemente en PSI, pueden aparecer contribuciones de alto nivel que afecten a la normativa de seguridad de la Organización e incluso a la propia política de seguridad corporativa.

Entre las normas y procedimientos generados es de destacar la necesidad de una normativa de clasificación de la documentación y procedimientos para su tratamiento.

En todos los procesos hay que prestar una especial atención al personal involucrado. Como reglas básicas conviene:

- identificar los roles y las personas
- determinar los requisitos de seguridad de cada puesto e incorporarlos a los criterios de selección y condiciones de contratación
- limitar el acceso a la información: sólo por necesidad
- segregar tareas; en particular evitar la concentración en una sola persona de aquellas aplicaciones o partes de una aplicación que soporten un alto riesgo

Índice

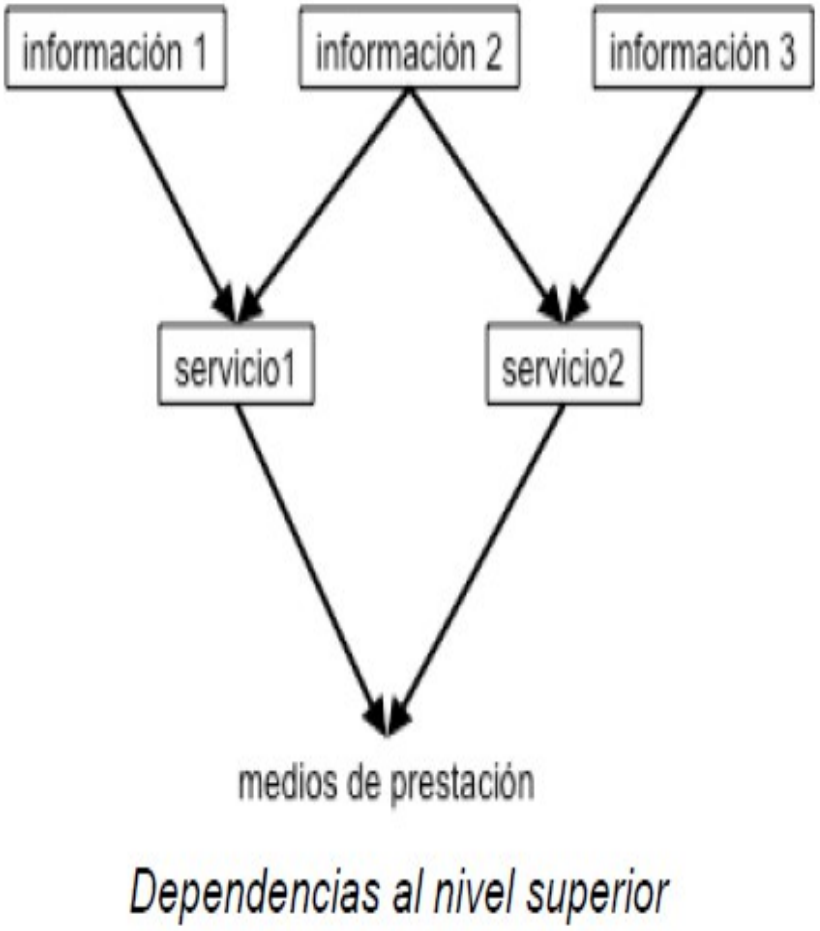
Consejos prácticos

- Alcance y profundidad
  - sólo se requiere un estudio de los ficheros afectos a la legislación de datos de carácter personal
  - sólo se requiere un estudio de las garantías de confidencialidad de la información
  - sólo se requiere un estudio de la seguridad de las comunicaciones
  - sólo se requiere un estudio de la seguridad perimetral
  - sólo se requiere un estudio de la disponibilidad de los servicios (típicamente porque se busca el desarrollo de un plan de contingencia)
  - se busca una homologación o acreditación del sistema o de un producto
  - se busca lanzar un proyecto de métricas de seguridad, debiendo identificar qué puntos interesa controlar y con qué grado de periodicidad y detalle

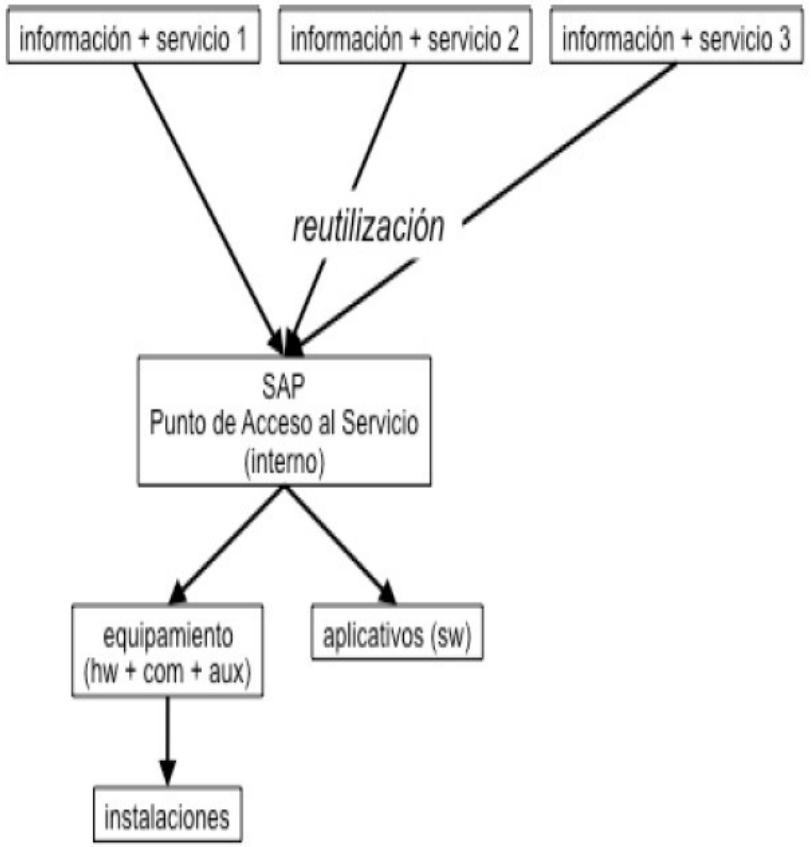
Consejos prácticos

- Identificación de activos:
  - Quizás la mejor aproximación para identificar los activos sea preguntar directamente:
    - ¿Qué activos son esenciales para que usted consiga sus objetivos?
    - ¿Hay más activos que tenga que proteger por obligación legal?
    - ¿Hay activos relacionados con los anteriores?

Consejos prácticos: Para descubrir y modelar las dependencias entre activos



Dependencias al nivel superior



Servicios internos

Consejos prácticos: Para descubrir y modelar las dependencias entre activo

mal	***bien***
aplicación → información	información → aplicación

Dependencias de la información y las aplicaciones

No es correcto decir que una aplicación depende de la información que maneja. El razonamiento de quien tal afirma es que "la aplicación no funcionaría sin datos", lo que es correcto; pero no es lo que interesa reflejar.

Más bien es todo lo contrario: la [seguridad de la] información depende de la aplicación que la maneja. En términos de servicio, se puede decir que la aplicación no vale para nada sin datos. Pero como el valor es una propiedad de la información, y la información es alcanzable por medio de la aplicación, son los requisitos de seguridad de la información los que hereda la aplicación. Luego la información depende de la aplicación. En otras palabras: a través de la aplicación puede accederse a la información, convirtiéndose la aplicación en la vía de ataque

Consejos prácticos: Para descubrir y modelar las dependencias entre activo

mal	***bien***
• servicio → aplicación • aplicación → equipo	• servicio → aplicación • servicio → equipo

Dependencias de los servicios

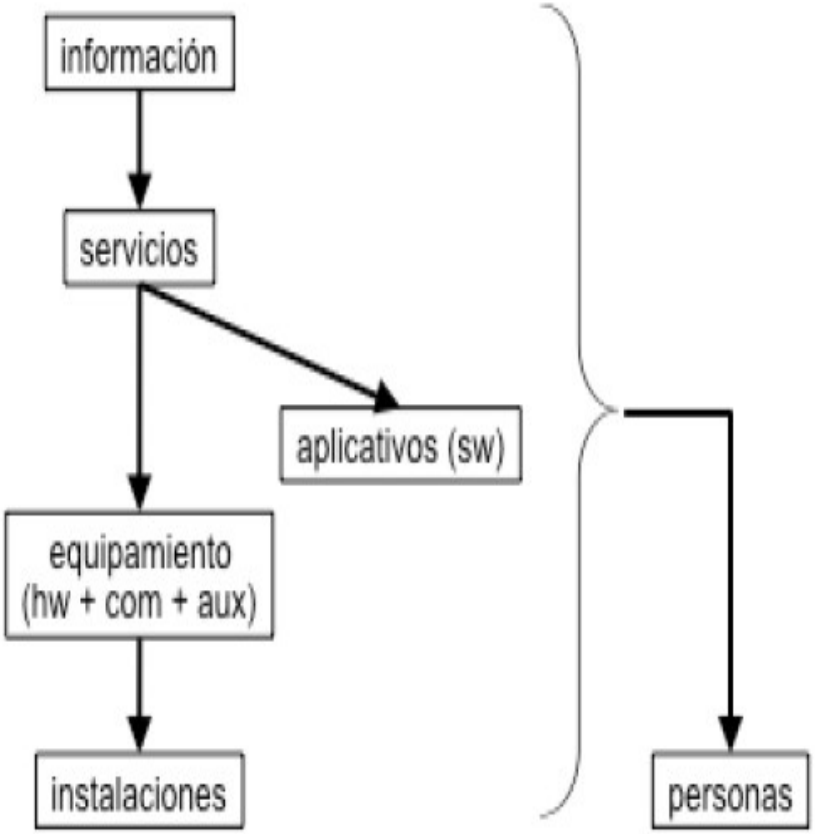
La información que maneja un sistema o bien se pone por encima de los servicios, o bien se agrupa

. información → servicios → equipamiento (incluyendo datos, aplicaciones, equipos, …)

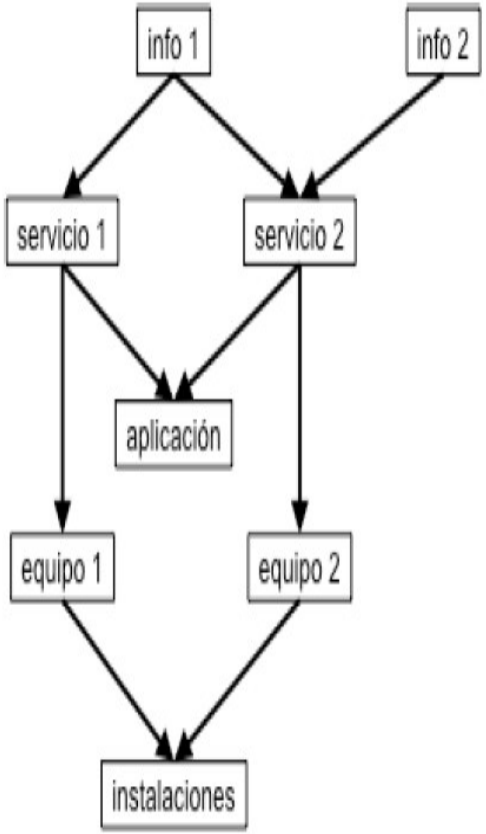
.{ información + servicios } → equipamiento (incluyendo datos, aplicaciones, equipos, …)

No es correcto decir que una aplicación dependa del equipo donde se ejecuta. El razonamiento de quien tal afirma es que "la aplicación no funcionaría sin equipo", lo que es correcto; pero no es lo que interesa reflejar. Si tanto la aplicación como el equipo son son necesarios para prestar un servicio, se debe decir explícitamente, sin buscar caminos retorcidos.

Consejos prácticos: Para descubrir y modelar las dependencias entre activo



Jerarquía de dependencias



Dependencias entre activos para la prestación de unos servicios

Consejos prácticos: Para valorar activos

- Utilizar las tablas de valoración como las del capítulo 4 del "Catálogo de Elementos".
- A menudo no existe el responsable único y singular de un activo y/o servicio, sino que varias personas dentro de la Organización tienen opinión cualificada al respecto. Hay que oírlas todas. Y llegar a un consenso. Si el consenso no es obvio, puede requerir
  - un careo: junte a los que opinan e intente que lleguen a una opinión común
  - un Delphi: mande cuestionarios a los que opinan e intente que converjan a una opinión común
- Datos de carácter personal
  - Los datos de carácter personal están tipificados por leyes y reglamentos, requiriendo de la Organización que adopte una serie de medidas de protección independientes del valor del activo.

Consejos prácticos: Para identificar amenazas

- La tarea aparece como imposible: para cada activo, en cada dimensión, identificar amenazas.
- Se puede partir de la **experiencia pasada**, propia o de organizaciones similares. Lo que ha ocurrido puede repetirse y, en cualquier caso, sería impresentable no tenerlo en cuenta.
- Complementariamente, un **catálogo de amenazas** como el incluido en el "Catálogo de Elementos" ayuda a localizar lo que conviene considerar en función del tipo de activo y de las dimensiones en las que tiene un valor propio o acumulado.
- A menudo se recurre a idear **escenarios de ataque** que no son sino dramatizaciones de cómo un atacante se enfrentaría a nuestros sistemas.
  - Esta técnica es la que a veces se denomina "**árboles de ataque**".
  - **Póngase en la piel del atacante** e imagine qué haría con sus conocimientos y su capacidad económica.
  - Puede que tenga que **plantearse diferentes** situaciones dependiendo del perfil técnico del atacante o de sus recursos técnicos y humanos.
  - Estas dramatizaciones son interesantes para poder calcular impactos y riesgos; pero además serán muy útiles a la hora de convencer a la alta dirección y a los usuarios de por qué una amenaza no es teórica sino muy real. Es más, cuando evalúe las salvaguardas puede ser conveniente revisar estos escenarios de ataque.
- Es habitual que **las herramientas de soporte al análisis de riesgos** aporten perfiles típicos para apoyar en esta tarea.

Consejos prácticos: Para valorar amenazas

- Hay muchos motivos que agudizan el peligro de una amenaza:
  - que no requiera grandes conocimientos técnicos por parte del atacante
  - que no requiera gran inversión en equipo por parte del atacante
  - que haya un enorme beneficio económico en juego (que el atacante puede enriquecerse)
  - que haya un enorme beneficio en juego (que el atacante pueda salir fuertemente beneficiado, en su estima, en su conocimiento por todo el mundo, ...); por lo que más quiera, evite los retos y jamás alardee de que su sistema de información es invulnerable: no lo es y no tiene gracia que se lo demuestren
  - que haya un mal ambiente de trabajo, semilla de empleados descontentos que se vengan a través de los sistemas, simplemente para causar daño
  - que haya una mala relación con los usuarios externos, que se vengan a través de nuestros sistemas
- Partiendo de un valor estándar, hay que ir aumentando o disminuyendo sus calificaciones de frecuencia y degradación hasta reflejar lo más posible el caso concreto

Consejos prácticos: Para seleccionar salvaguardas

- Probablemente la única forma es tirar de catálogo. Use un (sistema) experto que le ayude a ver qué solución es adecuada para cada combinación de:
  - tipo de activo
  - amenaza a la que está expuesto
  - dimensión de valor que es motivo de preocupación
  - nivel de riesgo
- A menudo encontrará muchas soluciones para un problema, con diferentes calidades.
- En estos casos debe elegir una solución proporcionada a los niveles de impacto y riesgo calculados.
- Muchas salvaguardas son de bajo coste, bastando configurar adecuadamente los sistemas u organizar normativa para que el personal haga las cosas de forma adecuada.
- Pero algunas contra medidas son realmente costosas (en su adquisición, en su despliegue, en su mantenimiento periódico, en la formación del personal a su cargo, ...).
  - En estos casos conviene ponderar si el coste de la salvaguarda no supera el riesgo potencial; es decir, tomar siempre decisiones de gasto que supongan un ahorro neto.
- A la hora de desplegar salvaguardas hay que considerar su facilidad de uso.

Consejos prácticos

- Aproximaciones sucesivas
  - El análisis de riesgos puede ser muy laborioso, requiriendo tiempo y esfuerzo.
  - Además, hay que introducir muchos elementos que no son objetivos, sino estimaciones del analista, lo que implica que haya que explicar y consensuar lo que significa cada cosa para no estar expuestos a impactos o riesgos que se ignoran o se infravaloran, ni convertir la paranoia en un dispendio de recursos injustificados.
  - Si hay que ser prácticos y efectivos, conviene realizar aproximaciones sucesivas.
  - Se empieza por un análisis somero, de alto nivel, identificando rápidamente lo más crítico:
    - activos de gran valor
    - vulnerabilidades manifiestas o, simplemente, recomendaciones de libro de texto porque no hay nada más prudente que aprender en cabeza ajena, aprovechando la experiencia de los demás.
  - Este análisis de riesgos es imperfecto, evidentemente; pero cabe confiar en que lleve en la dirección correcta.

Consejos prácticos

- Protección básica
  - Existen numerosas fuentes, entre las que cabe destacar:
    - normas internacionales, por ejemplo [ISO 27002]
    - normas sectoriales
    - normas corporativas, especialmente frecuentes en pequeñas delegaciones de grandes organizaciones
  - Las ventajas de protegerse por catálogo son:
    - es muy rápido
    - cuesta menos esfuerzo que ponerse a analizar y decidir
    - se logra un nivel homogéneo con otras organizaciones parecidas
  - Los inconvenientes de protegerse por catálogo son:
    - el sistema puede protegerse frente a amenazas que no padece, lo que supone un gasto injustificado
    - el sistema puede estar inadecuadamente protegido frente a amenazas reales

Consejos prácticos

- Protección básica
  - En base a la tipificación de los activos
    - Si usted tiene datos de carácter personal calificados de nivel alto, tiene que cifrarlos.
    - Si usted tiene datos clasificados como confidenciales, tiene que etiquetarlos y cifrarlos.
    - Aparte de cumplir con la legislación y normativa específica, habrá llevado a cabo una especie de "vacunación preventiva" de activos que seguro que son importantes.
    - Si usted tiene una red local conectada al exterior, tiene que poner un cortafuegos en el punto de conexión.

Consejos prácticos

- Protección básica
  - En base al valor de los activos
    - Si usted tiene todos los datos operacionales en soporte informático, tiene que hacer copias de seguridad.
    - Si usted tiene equipos informáticos, manténgalos al día con las actualizaciones del fabricante.
    - Lo que vale hay que cuidarlo, por si le pasara algo, sin entrar en muchas precisiones de qué les puede pasar exactamente.

Consejos prácticos

- Protección básica
  - En base a las amenazas
    - Si se trata de un sistema de la llamada administración electrónica (tramitación administrativa no presencial) o si los sistemas se usan para comerciar electrónicamente (compras y ventas no presenciales), **registre cuidadosamente quién hace qué en cada momento** pues se enfrentará a incidencias con los usuarios, teniendo que determinar quién tiene razón y quien paga los perjuicios. También habrá quien quiera usar sus servicios sin tener derecho a ello (fraude).
    - Lo que se puede necesitar, es necesario, y parte de las responsabilidades del responsable de seguridad es disponer de la información correcta cuando haga falta.

Consejos prácticos

- Protección básica
  - En base a la exposición
    - Si usted tiene una red de equipos antiguos y se conecta a Internet, debe instalar un cortafuegos.
    - Si tiene usted una aplicación en producción, debe mantenerla al día aplicando mejoras y corrigiendo los defectos anunciados por el fabricante.

Índice

Bibliografía

- Metodología de análisis y gestión de riesgos de los sistemas de información (MAGERIT versión 3)

  https://www.ccn-cert.cni.es/publico/herramientas/pilar5/magerit/
- Curso de Análisis y Gestión de Riesgos de los Sistemas de Información (público). CCN-CERT.

  https://www.ccn-cert.cni.es/elearning/course/view.php?id=12
- Análisis y gestión de riesgos. Ayuda.

https://www.ccn-cert.cni.es/publico/herramientas/Pilar-5.4.1/web/doc/std/cia/index.html

- EAR / herramientas. Entorno de análisis de riesgos

http://www.ar-tools.com/es/index.html