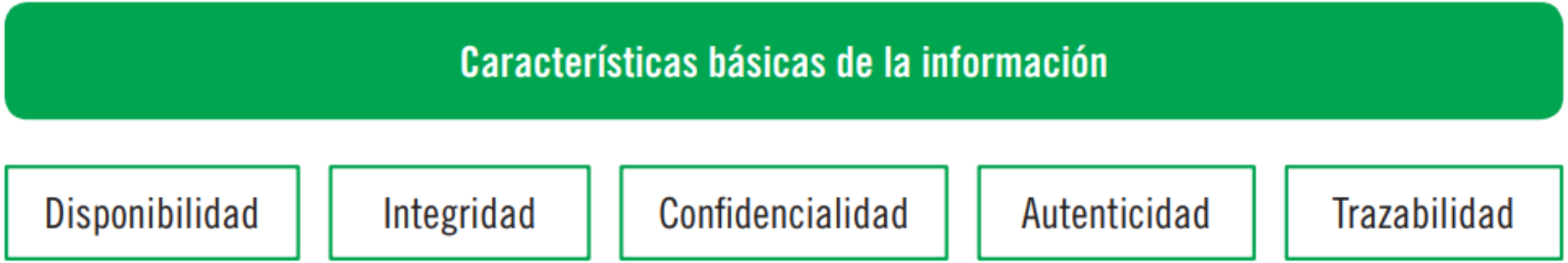
Análisis de riesgos de los sistemas de información

Introducción al análisis de riesgos

Un riesgo es un evento o conjunto de eventos que puede poner en peligro un proyecto de la organización o que puede impedir su éxito

Conceptos básicos de la gestión de riesgos



Aparte de los conceptos referentes a las características de la información, para una correcta comprensión de la gestión de riesgos hay que tener claros los siguientes conceptos:

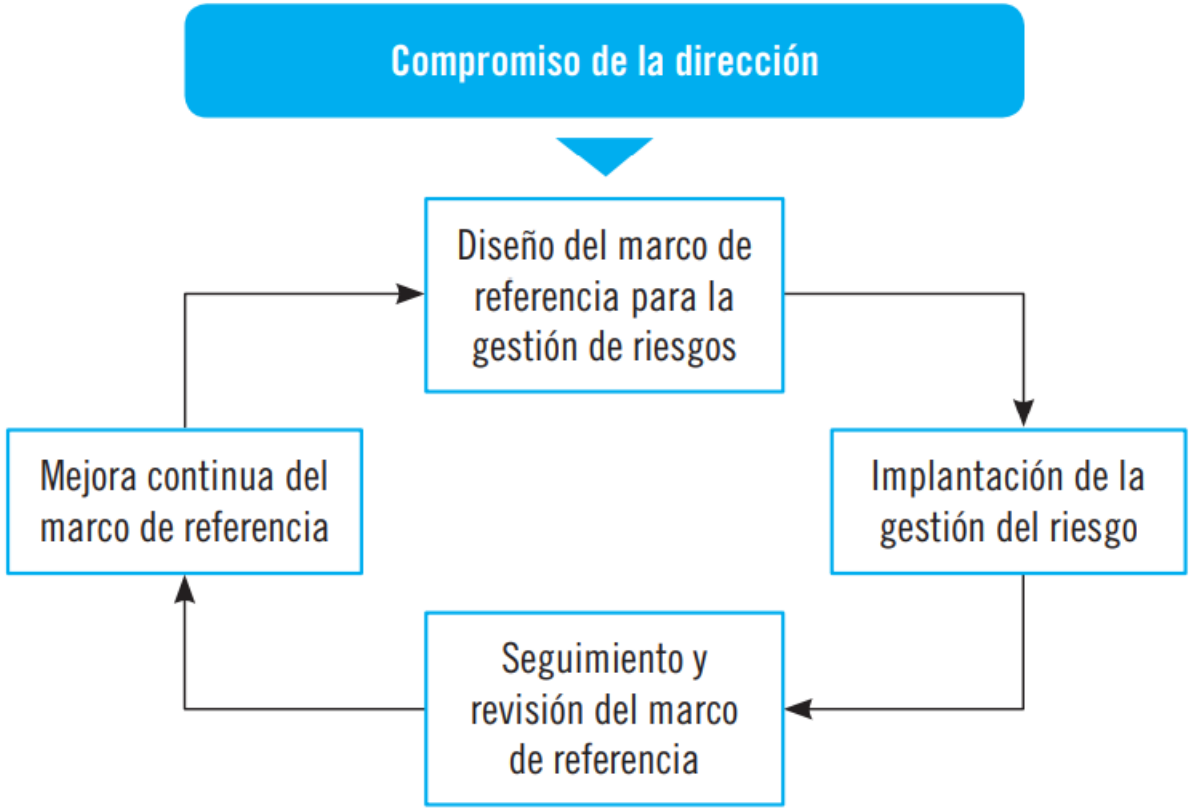
- **Riesgo**: estimación de las probabilidades de que una amenaza se materialice sobre los activos de la organización, causando efectos negativos o pérdidas.
- **Análisis de riesgos**: proceso y metodología utilizados para estimar la magnitud de los riesgos a los que se expone una organización.
- **Tratamiento del riesgo**: procesos realizados para modificar los riesgos de una organización.

Estándar ISO 31000 de gestión y tratamiento de riesgos

Principios de la norma ISO 31000: La gestión de riesgos:
1. Crea valor.
2. Está integrada en los procesos de la organización.
3. Forma parte de la toma de decisiones.
4. Trata explícitamente la incertidumbre.
5. Es sistemática.
6. Está basada en la mejor información disponible.
7. Está hecha a medida.
8. Tiene en cuenta factores humanos y culturales.
9. Es transparente e inclusiva.
10. Es dinámica, iterativa y sensible al cambio.
11. Facilita la mejora continua de la organización.

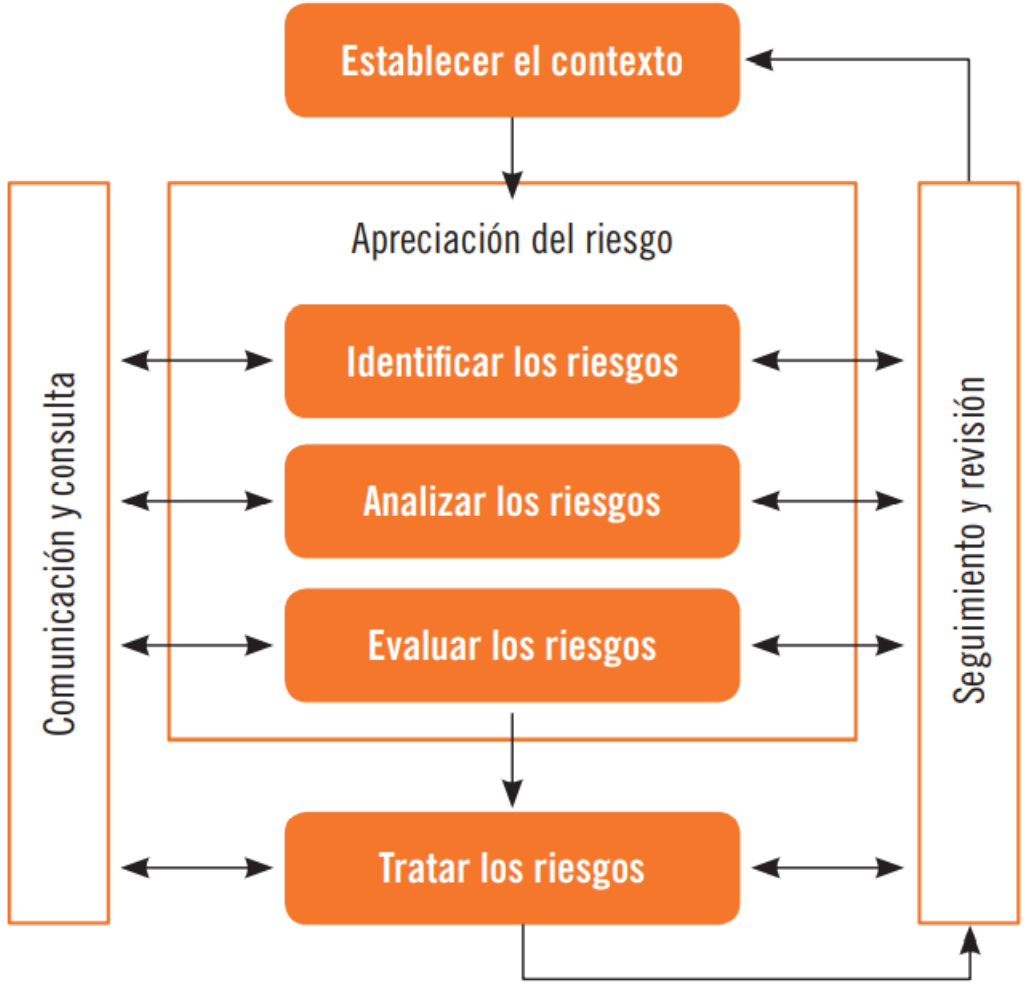
Marco de trabajo para la gestión del riesgo

La norma ISO 31000 también establece un marco de referencia o framework para la gestión de riesgos formado por las siguientes actividades:



Proceso de gestión del riesgo

La norma ISO 31000 establece, después de introducir los principios de gestión del riesgo y el marco de trabajo, un proceso de gestión del riesgo con un conjunto de fases y pasos recomendados para que las organizaciones lo adapten e implanten correctamente, consiguiendo mejoras en la efectividad y precisión ante posibles amenazas.



Principales tipos de vulnerabilidades, fallos de programa, programas maliciosos y su actualización permanente, así como criterios de programación segura

Principales tipos de vulnerabilidades/fallos de programa

Una vulnerabilidad es un fallo de seguridad en un programa o en un sistema de información. No todos los fallos de programas son fallos de seguridad.

Vulnerabilidades de configuración

Son vulnerabilidades generadas por una mala gestión del software por parte del usuario final. No se originan por un fallo del diseño en sí, sino que se originan en el momento en el que el usuario configura el sistema erróneamente.

Validación de entrada

Se trata de una vulnerabilidad que se genera cuando la aplicación no comprueba adecuadamente la entrada de datos que provienen desde el exterior.

Salto de directorio

Es una vulnerabilidad que se aprovecha de la falta de seguridad de los servicios de red para moverse por los directorios de la aplicación hasta llegar a su directorio raíz.

Principales tipos de vulnerabilidades/fallos de programa

Inyección de comandos en el sistema operativo

La inyección de comandos en el sistema operativo consiste en la capacidad que tiene el usuario para ejecutar comandos en el sistema operativo que puedan poner en peligro su integridad

Inyección SQL

Se trata de una vulnerabilidad que se localiza en el nivel de base de datos del programa o aplicación. Se produce cuando el filtrado de las variables utilizadas con código SQL no se realiza correctamente

Error de búfer

Un búfer es un espacio de la memoria de un disco o de un instrumento digital reservada para el almacenamiento de información digital de forma temporal hasta que esta se procese

Principales tipos de vulnerabilidades/fallos de programa

Fallo de autenticación

Vulnerabilidad que se origina cuando el programa no puede autenticar correctamente al usuario que intenta acceder en él.

Error en la gestión de recursos

Este tipo de vulnerabilidad ocurre cuando el fallo de programa permite al usuario no autorizado provocar una gestión deficiente de los recursos del sistema, provocando un consumo excesivo en estos.

Error de diseño

Son vulnerabilidades ocasionadas cuando el programador realiza el diseño de la aplicación con fallos y errores, tanto en el diseño inicial como en su desarrollo posterior.

Programas maliciosos y su actualización permanente

Un programa malicioso o **malware** es un tipo de programa diseñado para que usuarios no autorizados accedan a un sistema de información sin autorización de su propietario y producir efectos indeseados en este.

Dentro de estos programas se engloban una gran variedad de software: virus, troyanos, gusanos, spyware, etc.

Criterios de programación segura

■ Protección de los **desbordamientos de pila** (problemas provocados por el exceso de flujo de datos en la pila de una función) utilizando funciones seguras.

■ Utilizar el **flujo de datos** para un control continuo del trabajo realizado.

■ Realización de **pruebas y testeos** de programas en ejecución para analizar sus fallos y errores.

■ Creación de **parches, actualizaciones** de programas que arreglan los fallos detectados en las aplicaciones.

■ Utilización de **técnicas criptográficas y de cifrado** para evitar que el software sea modificado por usuarios no autorizados.

Particularidades de los distintos tipos de código malicioso

- Destrucción o modificación de información.
- Robo de información y de claves de acceso.
- Propagación a otros equipos de una misma red o a través de Internet.
- Introducir publicidad de forma masiva.
- Comprometer la integridad de aplicaciones y sistemas operativos.

Tipos de códigos maliciosos

- Virus.
- Cookies.
- Troyanos.
- Keyloggers.
- Spyware.
- Gusanos o worms.

Principales elementos del análisis de riesgos y sus modelos de relaciones

Activo

Un activo es un recurso del sistema de información, necesario para garantizar el correcto funcionamiento de los procesos de la organización.

Amenaza

Una amenaza es cualquier evento que puede afectar al activo de un sistema de información, provocando un incidente de seguridad y produciendo efectos adversos (materiales o inmateriales) o pérdidas de información.

Tipos de amenazas

Grupo	Definición
Criminalidad	Acciones causadas por humanos que incumplen requerimientos legales. Son ejemplos el sabotaje, el robo, el espionaje, el fraude, etc.
Sucesos de origen físico	Eventos de origen natural y/o técnico, además de eventos causados por humanos de forma indirecta. Por ejemplo: inundaciones, sobrecargas eléctricas, fallos de corriente, incendios, etc.
Negligencia y decisiones institucionales	Acciones realizadas por personas con poder e influencia sobre el sistema de información. Por ejemplo: gestión deficiente de contraseñas y permisos de usuario, falta de protocolo y normas de actuación, falta de formación, falta de capacitación, etc.

Principales elementos del análisis de riesgos y sus modelos de relaciones

Vulnerabilidad

Una vulnerabilidad consiste en alguna característica o capacidad de un activo del sistema de información que lo hace susceptible a amenazas. También se define como la capacidad de actuación o reacción de un sistema de información ante la aparición de amenazas, además de la capacidad de recuperación de los daños ocasionados.

Riesgo

Como se ha mencionado anteriormente, un riesgo es la posibilidad de que una amenaza se materialice causando efectos negativos o positivos

Control atenuante

Se consideran atenuantes aquellos activos y medidas que consiguen reducir las posibilidades de amenazas y, por tanto, el nivel de riesgo del sistema de información de la organización.

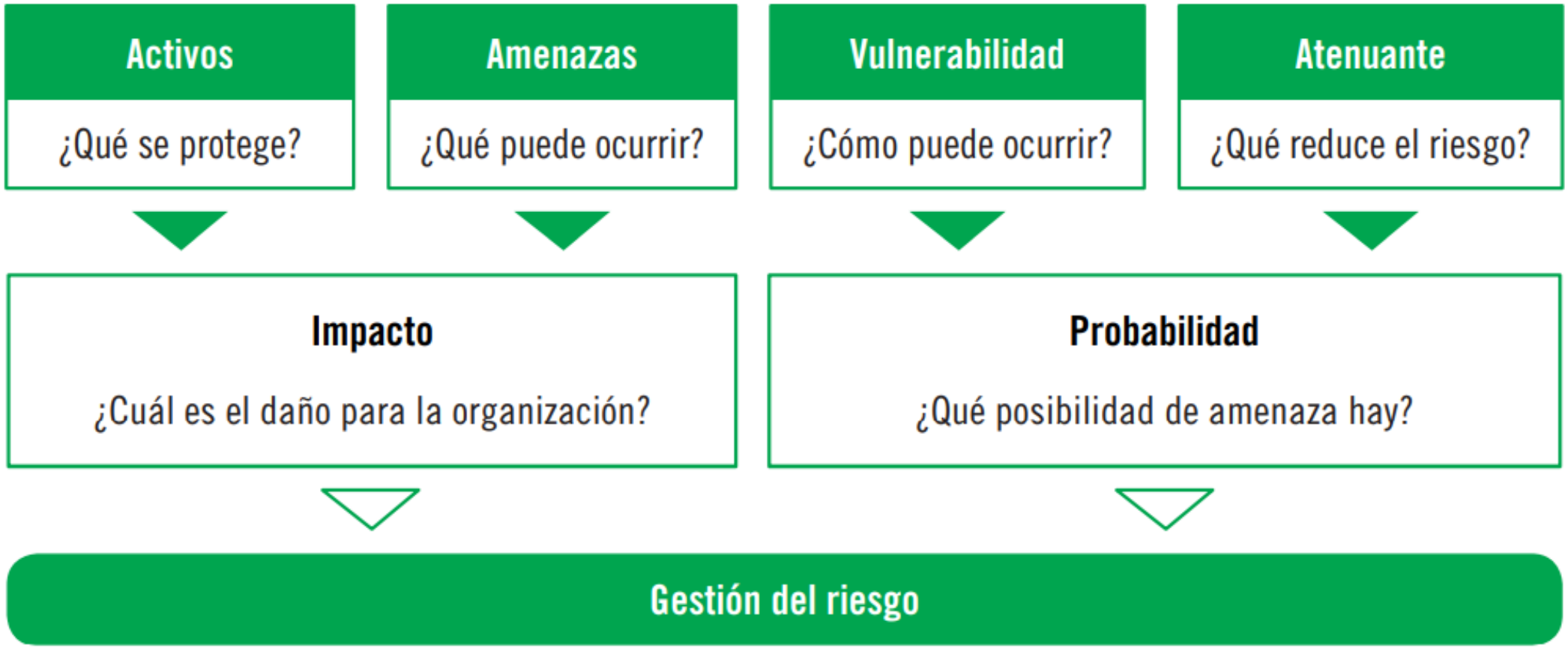
Impacto

El impacto es la magnitud del daño que provoca un ataque exitoso en el que se han perjudicado la confidencialidad, la disponibilidad, la integridad y la autenticidad de la información del sistema.

Probabilidad

La probabilidad se define como la estimación de posibilidades de que se materialice el riesgo o, lo que es lo mismo, que se produzca una amenaza real.

Modelos de relaciones de conceptos de gestión de riesgos



Metodologías cualitativas y cuantitativas de análisis de riesgos

Tipos de controles de seguridad	
Control	**Descripción**
Disuasorio	Su finalidad principal es reducir la probabilidad de recibir un ataque.
Preventivo	Su finalidad es proteger al sistema de información de sus vulnerabilidades, intentando impedir el acceso de los atacantes o reduciendo el impacto de los daños causados.
Correctivo	Tienen como finalidad principal reducir el impacto de una amenaza.
Detectivo	Se encargan de detectar e impedir posibles ataques.

Metodología cuantitativa de análisis de riesgos

El enfoque cuantitativo del análisis de riesgos tiene en cuenta **dos elementos**:

1. La probabilidad de ocurrencia de un evento
2. El impacto que puede provocar en caso de que suceda

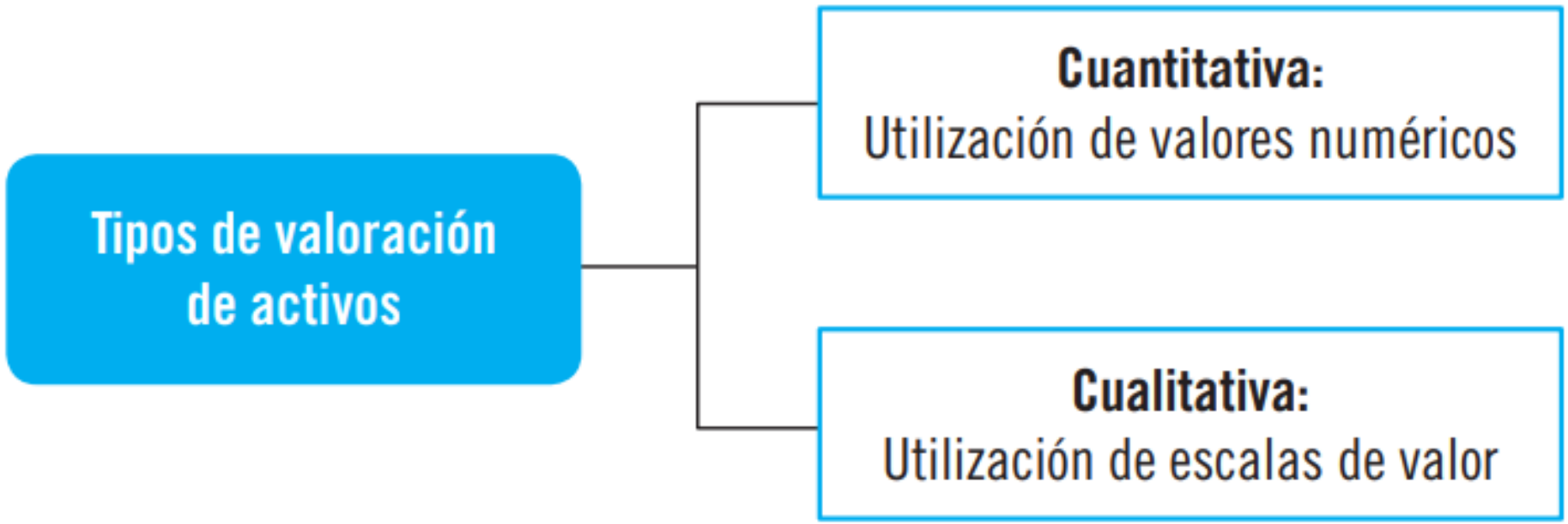
Metodología cualitativa de análisis de riesgos

Al revés que la metodología cuantitativa, la metodología cualitativa se basa en el raciocinio humano para calcular las pérdidas potenciales estimadas sin necesidad de utilizar métodos probabilísticos. Es la metodología utilizada con más frecuencia para el análisis de riesgos.

Identificación de los activos involucrados en el análisis de riesgos y su valoración

Fases del proceso de análisis y gestión de riesgos
1. Identificación de los activos.
2. Valoración de los activos.
3. Identificación de las amenazas.
4. Determinación del impacto de una amenaza.
5. Determinación del riesgo.
6. Establecimiento de salvaguardas (atenuantes).
7. Revisión del impacto y determinación del impacto residual.
8. Revisión del riesgo y determinación del riesgo residual.

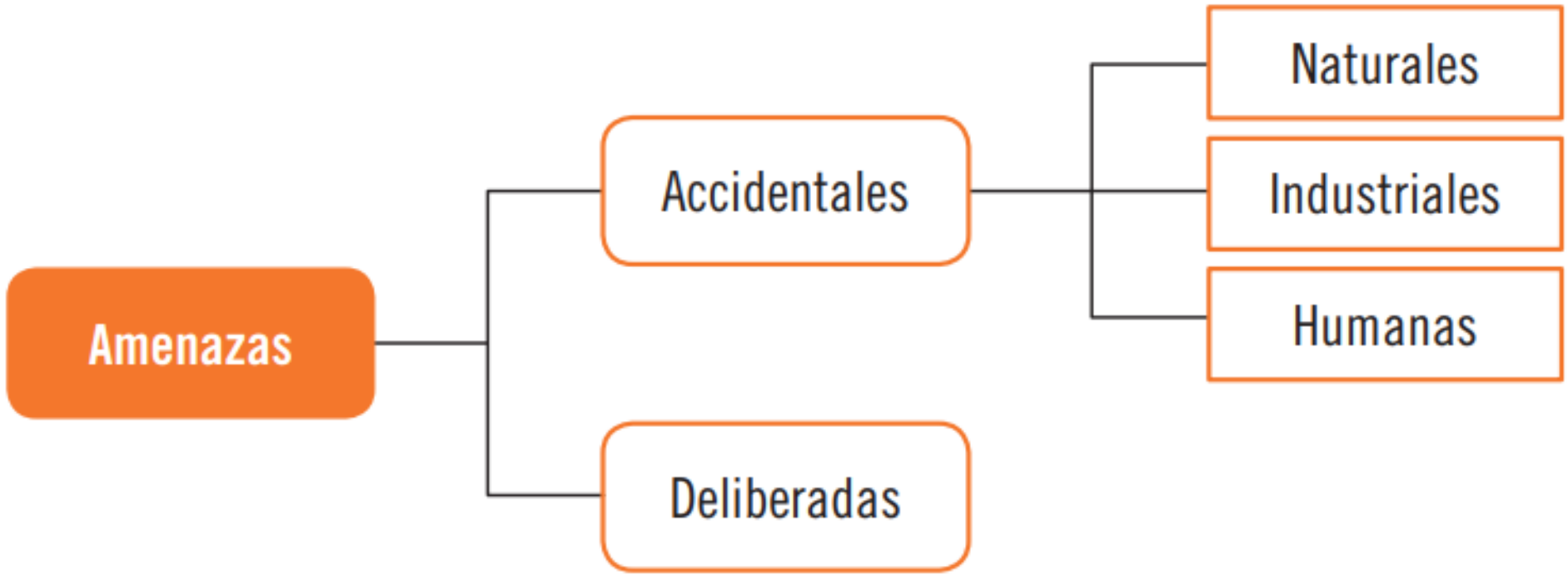
Tipos de valoraciones de activos



Las dimensiones de valoración de los activos

DIMENSIONES DE VALORACIÓN DE LOS ACTIVOS	
Dimensión	**Descripción**
Disponibilidad	¿Cuál sería la importancia del activo si este no estuviera disponible?
Integridad	¿Qué importancia tendría que el activo sufriera modificaciones descontroladas?
Confidencialidad	¿Cuál sería la importancia del conocimiento del activo por usuarios no autorizados?
Autenticidad	¿Cuál sería la importancia del acceso al activo por parte de personas no autorizadas?
Trazabilidad	¿Cuál sería la importancia de la falta de constancia de la utilización del activo?

Identificación de las amenazas que pueden afectar a los activos identificados previamente



Identificación de las amenazas

Los **principales activos** son los siguientes:

- Tipo de activo (dispositivo de almacenamiento, red de comunicación, etc.).
- Las dimensiones del activo que hacen que tenga un valor considerable.
- La experiencia de la organización en relación a anteriores incidencias ocurridas con el activo.
- Los defectos del activo notificados por su fabricante de origen.

Una vez descritas las características del activo, habrá que registrar información detallada de la amenaza:

- Efectos de la amenaza debidamente explicados.
- Entrevistas realizadas que han aportado información para la detección de la amenaza.
- Historial de amenazas relevantes, tanto de la organización como de otras organizaciones.

Ejemplos de amenazas frecuentes

■ **Suplantación**: esta amenaza se produce cuando un usuario no autorizado suplanta la identidad de otro usuario haciéndose pasar por este.

■ **Alteración**: modificación y alteración de la información o de algún dato concreto del sistema de información.

■ **Repudio**: negación de la producción de un hecho. Es frecuente que un empleado realice alguna acción perjudicial para la organización y que, posteriormente, lo niegue.

■ **Divulgación de información**: comunicación de información confidencial o de valor a terceros que no deberían conocerla.

■ **Denegación del servicio**: incapacidad de acceder a un servicio determinado del sistema de información. Suele producirse por saturación de datos de entrada.

■ **Elevación de privilegios**: utilización de privilegios de mayor nivel por usuarios no autorizados para ello.

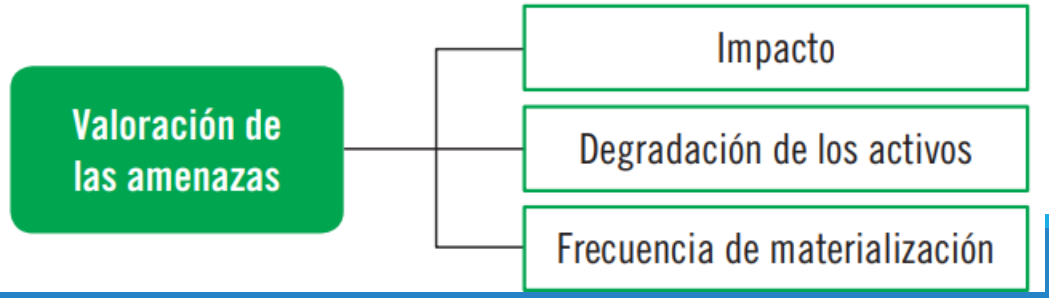
Ejemplos de amenazas frecuentes

Amenaza	Ejemplo
Suplantación	Envío de correos electrónicos con la identidad de otro usuario.
Alteración	Modificación no autorizada de los datos de un archivo.
Repudio	Empleado que elimina datos importantes del sistema y que, posteriormente, niega este hecho.
Divulgación de información	Envío por error de correos electrónicos con datos confidenciales de los clientes de la organización.
Denegación del servicio	Ataque de denegación del servicio mediante el envío excesivo de datos al sistema de información, provocando su saturación y evitando el acceso de otros usuarios.
Elevación de privilegios	Obtención y utilización de los privilegios y permisos del administrador sin autorización.

Valoración de las amenazas

Su valoración se calculará tomando como referencia los siguientes elementos:

- Daños producidos en los activos de la organización.
- Capacidad de reproducción y expansión de la amenaza a otros activos del sistema.
- Capacidad de explotación de la amenaza.
- Usuarios que se pueden ver afectados en caso de producirse la amenaza.
- Capacidad de detección y descubrimiento de la amenaza cuando esta se produzca.



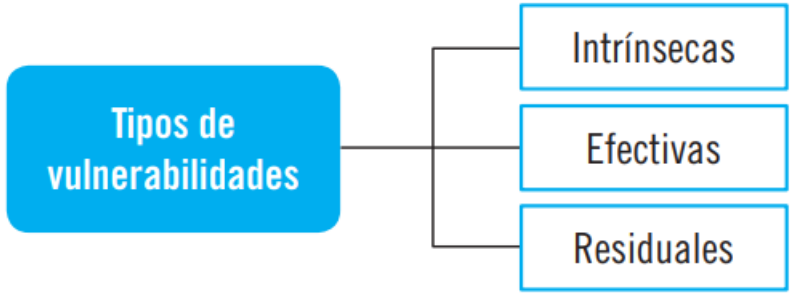
Análisis e identificación de las vulnerabilidades existentes en los sistemas de información que permitirían la materialización de amenazas, incluyendo análisis local, análisis remoto de caja blanca y de caja negra

Se consideran tres tipos de vulnerabilidades:

■ **Vulnerabilidad intrínseca**: vulnerabilidad que proviene directa y exclusivamente del activo y de la amenaza.

■ **Vulnerabilidad efectiva**: que se ha generado a raíz de una salvaguarda ya existente en el sistema de información.

■ **Vulnerabilidad residual**: generada por la aplicación de salvaguardas implantadas siguiendo el resultado del proceso de análisis y gestión de riesgos.



Algunos ejemplos de vulnerabilidades

- Vulnerabilidades de seguridad física:
  - Accesos de personal no autorizado al recinto.
  - Desastres naturales (rayos, inundaciones, etc.).
  - Incendios.
- Vulnerabilidades en las conexiones de red:
  - Fallos en el cortafuegos o firewall.
  - Intrusiones y accesos no autorizados a través de la red.
- Vulnerabilidades en la infraestructura de red:
  - Fallos y vulnerabilidades presentes en dispositivos de red como routers, hubs, switches, etc.
- Vulnerabilidades en el correo electrónico.
- Vulnerabilidades en las aplicaciones de gran valor y en sistemas operativos

Escalas que valorarán la frecuencia de ocurrencia y su probabilidad

Valor de la vulnerabilidad	Frecuencia	Probabilidad
Muy frecuente	Varias veces al día.	Entre el 75 y el 100 %.
Bastante frecuente	Una vez al día.	Entre el 50 y el 75 %.
Frecuente	Una vez en semana.	Entre el 25 y el 50 %.
Poco frecuente	Una vez al mes.	25 % o menos.

Análisis local para la detección de vulnerabilidades

El análisis local de vulnerabilidades en un sistema de información se realiza mediante la ejecución de pruebas de software.

- **Pruebas estáticas**: pruebas que no requieren la ejecución del código de la aplicación para poder realizarse.

- **Pruebas dinámicas**: al contrario que las estáticas, las dinámicas necesitan que se esté ejecutando la aplicación en el momento de la realización de la prueba. Su principal ventaja es su mayor precisión en el momento de evaluar el comportamiento de la aplicación analizada.

Análisis remoto de caja blanca

El análisis remoto de caja blanca se realiza con la ejecución de pruebas que examinan la estructura interna de la aplicación y de los componentes del sistema.

Análisis de caja blanca	
Ventajas	**Desventajas**
Las pruebas son muy minuciosas y los resultados obtenidos más precisos.	Requiere muchos y costosos recursos.
Las recomendaciones obtenidas de los resultados de estas pruebas también son más precisas y eficaces.	No hay simulación de intrusión para verificar su efectividad.
Detecta tanto las vulnerabilidades más inmediatas como las más profundas (de configuración y de diseño de la aplicación).	

Análisis de caja negra

Los análisis de caja negra consisten en una serie de pruebas que evalúan exclusivamente las entradas y salidas del sistema de información.

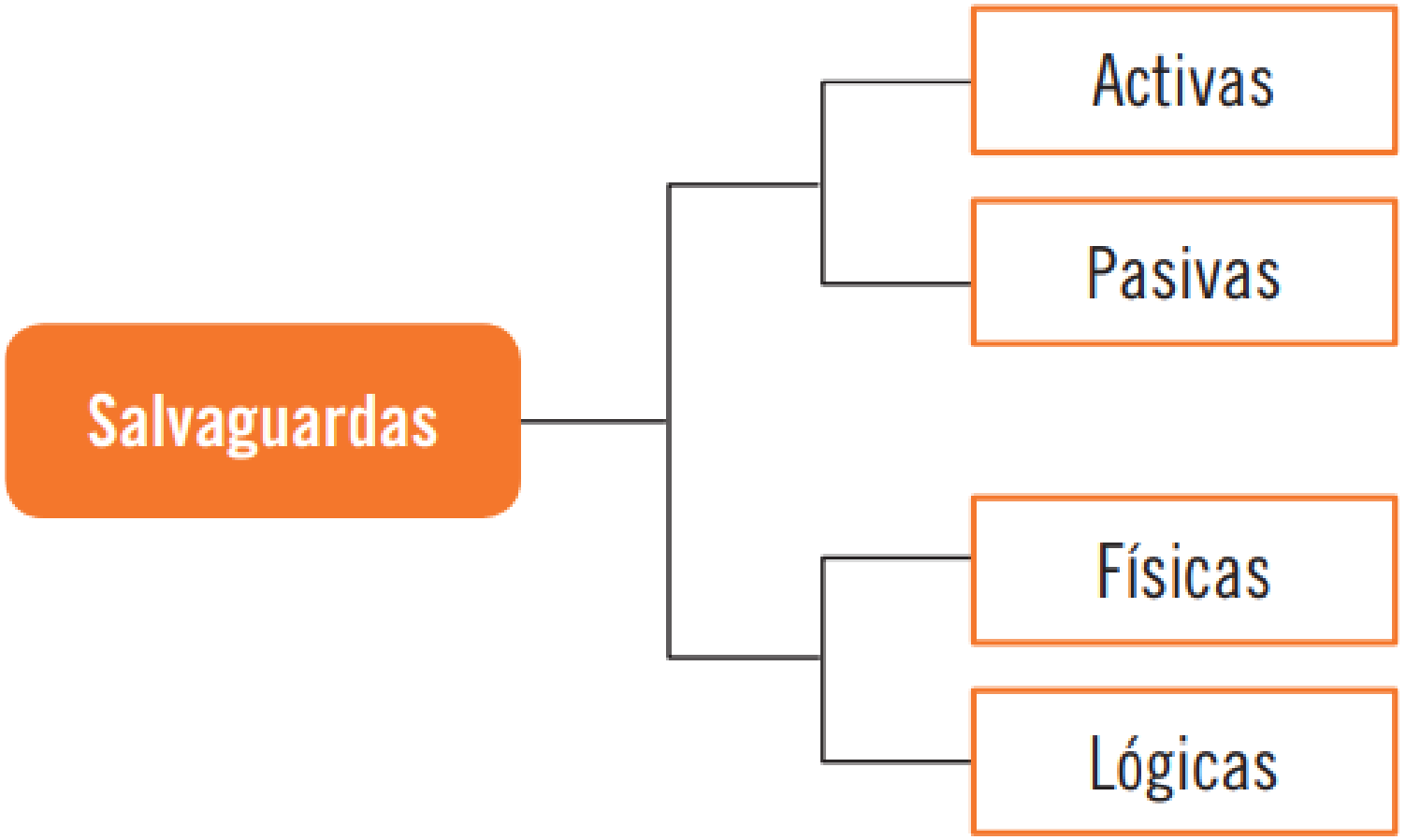
Análisis de caja negra	
Ventajas	**Desventajas**
Facilita información que permite realizar estimaciones reales de las amenazas.	Recopilar toda la información pública necesaria puede ser un trabajo bastante laborioso.
Obtiene la información a través del análisis de información pública (interna y externa).	Las vulnerabilidades más profundas y ocultas pueden ser pasadas por alto en el análisis.
Los recursos de la organización utilizados para este tipo de pruebas son bastante reducidos.	Las recomendaciones formuladas a partir de los resultados de esta prueba son de carácter general.

Optimización del proceso de auditoría y contraste de vulnerabilidades e informe de auditoría

El informe de auditoría

El informe de auditoría es un documento formalizado que contiene los objetivos de la auditoría, las metodologías utilizadas, los resultados obtenidos y las conclusiones y recomendaciones aportadas por los auditores.

Identificación de las medidas de salvaguarda existentes en el momento de la realización del análisis de riesgos y su efecto sobre las vulnerabilidades y amenazas



Estimación del impacto potencial

Teniendo en cuenta el par activo-amenaza, pueden establecerse una serie de escenarios de impacto teniendo en cuenta la degradación del activo provocada por la amenaza y la valoración de dicho activo. Se categoriza el valor de los activos en:

- Muy alto.
- Alto.
- Medio.
- Bajo.
- Muy bajo.

Por otro lado, se categoriza su degradación provocada por la amenaza en:

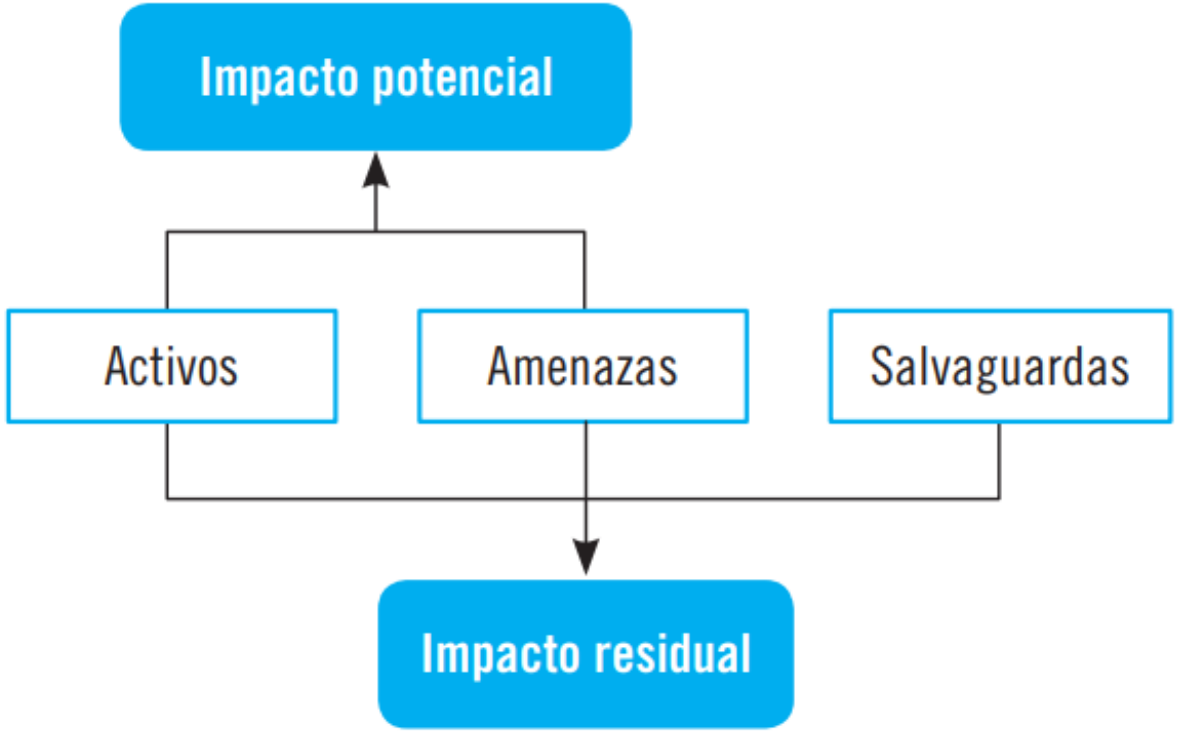
- Degradación inferior al 1 % de su valor.
- Degradación entre el 1 y el 10% de su valor.
- Degradación de más del 10 % de su valor.

Estimación del impacto potencial

	IMPACTO	Degradación del activo		
		Inferior al 1 %	1-10 %	Superior al 10 %
Valor del activo	Muy alto	MEDIO	ALTO	MUY ALTO
	Alto	BAJO	MEDIO	ALTO
	Medio	MUY BAJO	BAJO	MEDIO
	Bajo	MUY BAJO	MUY BAJO	BAJO
	Muy bajo	MUY BAJO	MUY BAJO	MUY BAJO

Estimación del impacto residual

El impacto residual, al contrario que el impacto potencial, tiene en cuenta la actuación de las salvaguardas sobre el riesgo del sistema de información.



Determinación de la probabilidad e impacto de materialización de los escenarios

Probabilidad de materialización de los escenarios de riesgo

Esta probabilidad viene clasificada en cinco categorías distintas:

PROBABILIDAD	ESCALA	DESCRIPCIÓN	CALIFICACIÓN
Raro	0-20 %	Eventualidad casi nula	1
Improbable	20-40 %	Solo ocurre en ocasiones excepcionales	2
Probable	40-60 %	Puede ocurrir o no ocurrir	3
Altamente probable	60-80 %	Puede ocurrir bastantes veces	4
Casi certeza	80-100 %	Casi siempre ocurre	5

Impacto de materialización de los escenarios de riesgo

Impacto	DESCRIPCIÓN	CALIFICACIÓN
Muy bajo	Impacto insignificante.	1
Bajo	Efectos mínimos para la organización.	2
Medio	Efectos considerables sobre los activos.	3
Alto	Efectos muy considerables para la organización en general.	4
Muy alto	Efectos irreparables o difícilmente reparables para la organización.	5

Establecimiento del nivel de riesgo para los distintos pares de activo y amenaza

Cuando ya se han categorizado **los pares activo/amenaza** y establecidos los **distintos niveles de impacto y probabilidad de una amenaza**, el siguiente paso es la **estimación del riesgo**.

Los datos de entrada que se deberán utilizar para la estimación del riesgo serán los siguientes:

- Identificación y valoración de los activos.
- Identificación y valoración de las amenazas.
- Identificación y valoración de las salvaguardas.
- Impacto estimado con los pares activo/amenaza identificados.

Nivel de riesgo de los escenarios de los pares activo/amenaza

- Nivel de riesgo despreciable.
- Nivel de riesgo bajo.
- Nivel de riesgo moderado.
- Nivel de riesgo importante.
- Nivel de riesgo crítico.

La ubicación de cada riesgo en una u otra categoría se calculará con el producto de las calificaciones de su impacto y de su probabilidad:

RIESGO = IMPACTO x PROBABILIDAD

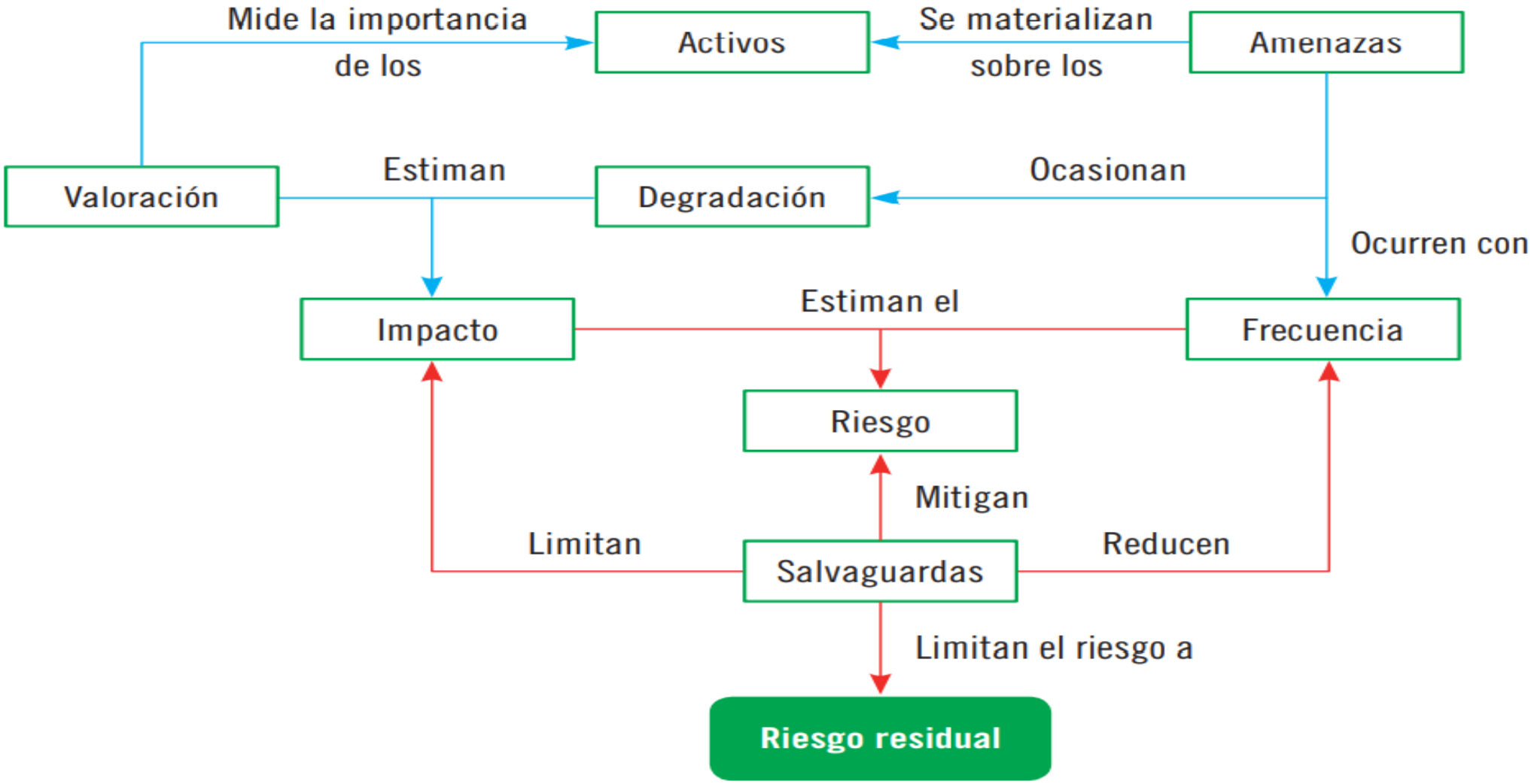
Nivel de riesgo de los escenarios de los pares activo/amenaza

De este modo, los niveles de riesgo para cada par activo/amenaza (impacto/ probabilidad) se ven reflejados en la tabla siguiente:

Nivel de riesgo		Probabilidad				
		Raro	Improbable	Probable	Altamente probable	Casi certeza
Impacto	Muy bajo	D	D	D	B	B
	Bajo	D	B	B	M	M
	Medio	B	M	M	I	I
	Muy alto	M	I	I	C	C
	Alto	I	C	C	C	C

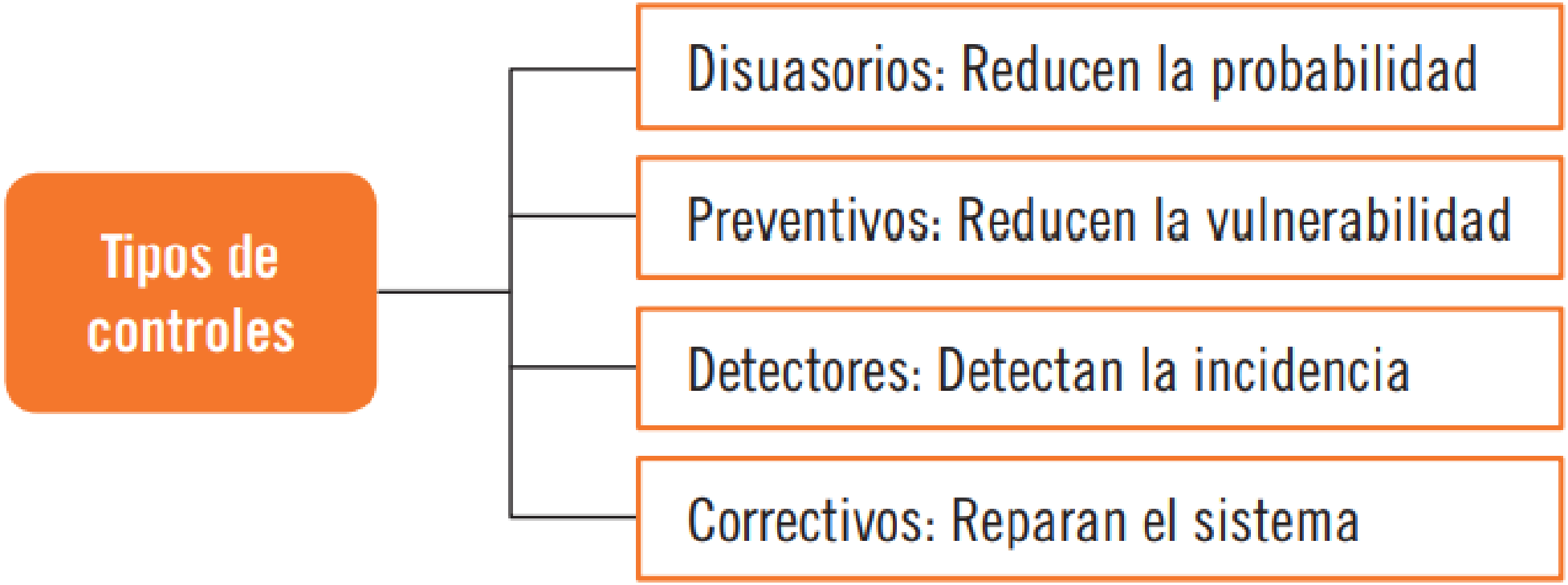
- D - Verde claro: Nivel de riesgo despreciable.
- B - Verde oscuro: Nivel de riesgo bajo.
- M - Amarillo: Nivel de riesgo moderado.
- I - Naranja: Nivel de riesgo importante.
- C - Rojo: Nivel de riesgo crítico

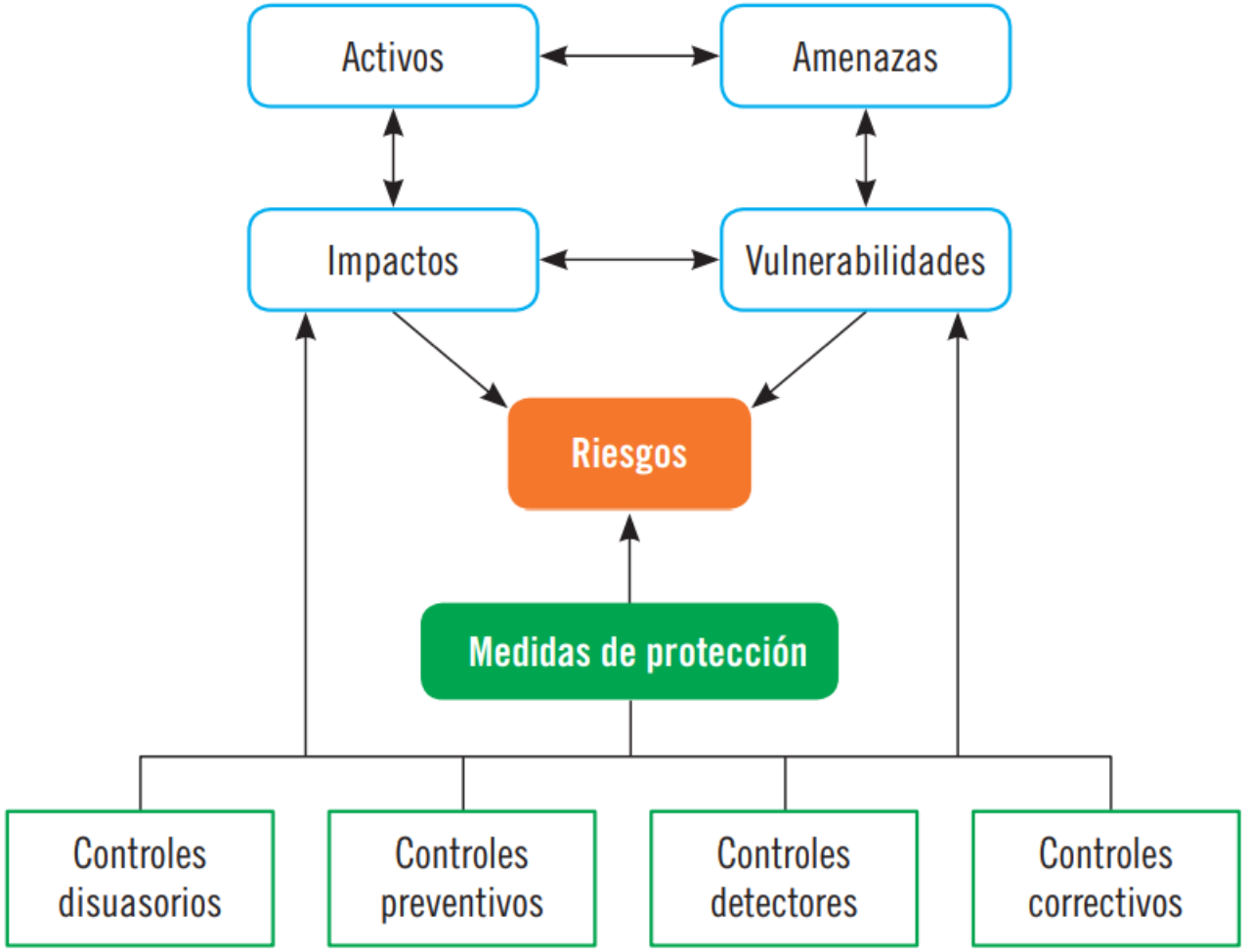
Visión general de la gestión de riesgos



Relación de las distintas alternativas de gestión de riesgos

La política de gestión de riesgos de la organización decidirá qué tipo de control se va a implantar en su sistema de información, distinguiendo entre:




Activos
Amenazas
Impactos
Vulnerabilidades
Riesgos
Medidas de protección
Controles disuasorios
Controles preventivos
Controles detectores
Controles correctivos

Guía para la elaboración del plan de gestión de riesgos

Recomendaciones básicas para la elaboración del plan

1. Conocer y entender el funcionamiento de la administración de riesgos

La organización debe tener claros y bien definidos los conceptos que forman parte de la gestión de riesgos: riesgo, amenaza, vulnerabilidad, activo, salvaguarda, etc.

2. Definir las acciones del plan de gestión de riesgos

Deben establecerse acciones como los activos que se quieren evaluar, las posibles amenazas que se pueden materializar, qué metodología se va a utilizar, cuáles serán los umbrales de riesgo aceptables, etc.

3. Conseguir el apoyo de la dirección y de profesionales externos

En casos en los que la reducción o eliminación del riesgo conlleva un coste elevado, se recomienda recurrir a profesionales externos que permitan la gestión del riesgo con menores costes y delegación de responsabilidades.

Recomendaciones básicas para la elaboración del plan

4. Identificar las consecuencias de cada riesgo

Teniendo en cuenta que cada riesgo conlleva consecuencias con perjuicios distintos, deben poder identificarse y valorar para conocer qué riesgos es necesario priorizar y atajar con más inmediatez.

5. Eliminar las amenazas irrelevantes

Deberán descartarse aquellas amenazas cuyo impacto y probabilidad de ocurrencia sean mínimos para concentrar los recursos y esfuerzos en amenazas que puedan afectar a activos de alto valor, con la elaboración de un plan de contingencia.

6. Inventariar los activos susceptibles de riesgo

Para tener controlados los riesgos, se recomienda tener un inventario de todos los activos de valor susceptibles de sufrir alguna amenaza. El inventario deberá actualizarse con cierta periodicidad.

7. Asignar probabilidades

Para cada activo, deberán asignarse las probabilidades de materialización de cada activo y la frecuencia con la que se pueden producir.

Recomendaciones básicas para la elaboración del plan

8. Asignar el impacto

Una vez asignadas las probabilidades, hay que asignar el grado de degradación que sufriría cada activo en caso de producirse la amenaza

9. Determinar el riesgo para cada activo

Con las probabilidades y los impactos estimados para cada activo, deberá calcularse una combinación de ambos factores para estimar el riesgo potencial de cada activo.

10. Clasificar los riesgos

Con los riesgos calculados para cada activo, deberá elaborase una lista con todos ellos siguiendo un orden de prioridad de actuación: a mayor riesgo, mayor prioridad de actuación y viceversa.

11. Calcular el riesgo total

Se calculará el riesgo total del sistema de información de la organización haciendo un promedio aritmético de todos los riesgos calculados de cada activo.

Recomendaciones básicas para la elaboración del plan

12. Diseñar estrategias de reducción de riesgos

Para reducir el riesgo global de la organización, deberán tomarse decisiones de actuación sobre qué tipos de controles se pueden implantar y qué efectos pueden tener sobre los riesgos de la organización.

13. Desarrollar planes de contingencia

Para los riesgos más importantes (que afectan a activos más valiosos y ocurren con más frecuencia) deberá diseñarse un plan de contingencia que permita reducirlos en el menor tiempo posible y restituir la situación previa, evitando que los daños ocasionados se expandan.

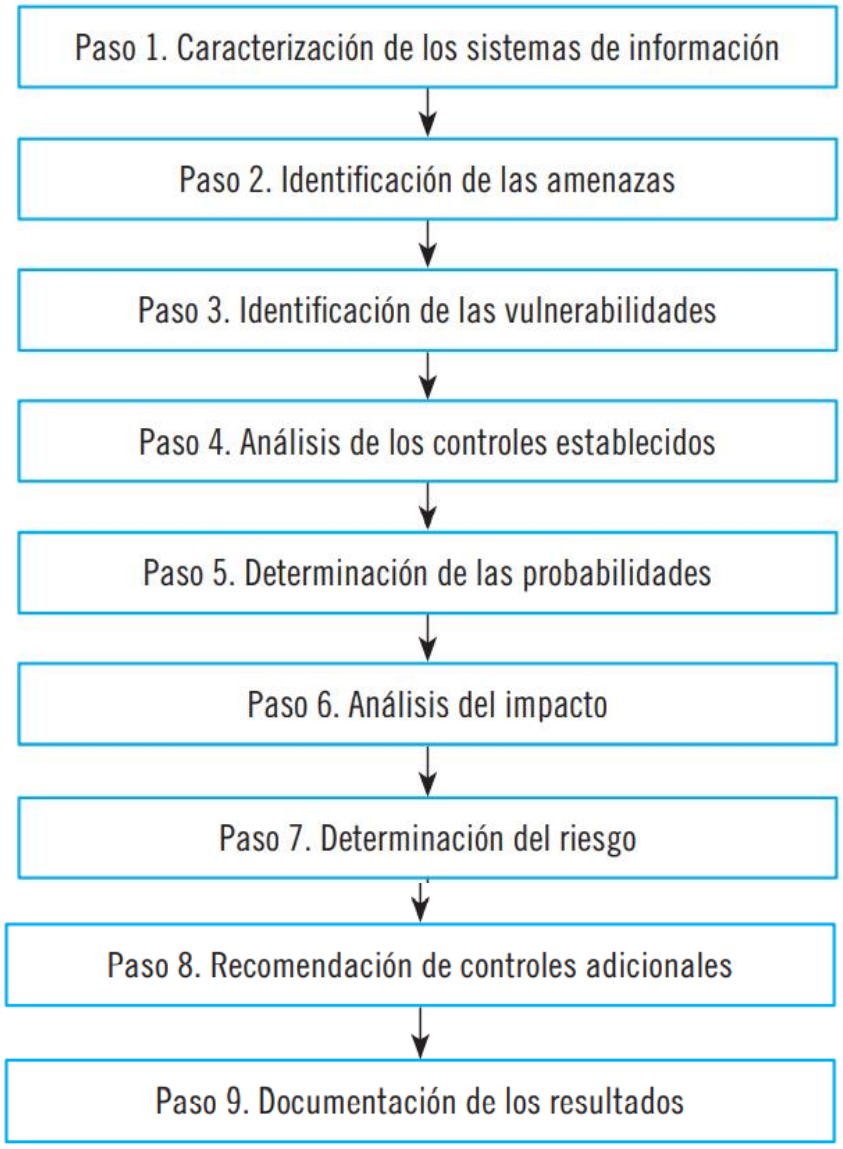
14. Analizar la efectividad de las estrategias implantadas

Una vez puesta en marcha la gestión de riesgos y las salvaguardas y controles previstos, deberá analizarse de nuevo el riesgo para cada activo y el riesgo global de la organización. Si los riesgos no se han reducido o la reducción ha sido mínima, significará que las medidas implantadas no son eficaces y será necesaria una nueva evaluación para detectar en qué fallan y cómo pueden solucionarse.

Exposición de la metodología NIST SP 800-30

EL INSTITUTO NACIONAL DE NORMAS Y TECNOLOGÍA (NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY O NIST) LLEVA EDITANDO DESDE LOS AÑOS NOVENTA UNA SERIE DE PUBLICACIONES REFERIDAS A LA SEGURIDAD DE LA INFORMACIÓN.

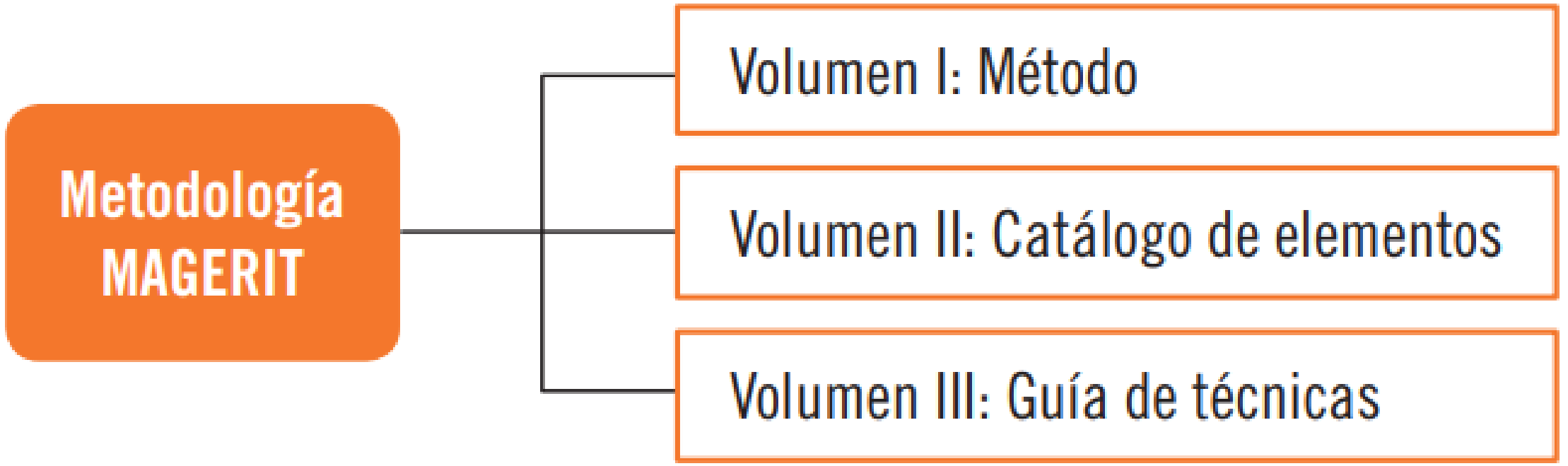
Fases del análisis y gestión de riesgos según la metodología NIST SP800-30



Exposición de la metodología Magerit versión 2

LA METODOLOGÍA DE ANÁLISIS Y GESTIÓN DE RIESGOS DE LOS SISTEMAS DE INFORMACIÓN DE LAS ADMINISTRACIONES PÚBLICAS O METODOLOGÍA MAGERIT FUE DISEÑADA POR EL CSAE (CONSEJO SUPERIOR DE ADMINISTRACIÓN ELECTRÓNICA) Y ES DE CARÁCTER PÚBLICO

Estructura de las guías Magerit



Metodología Magerit

Capítulo I: Introducción

Se trata de un capítulo introductorio, en el que se describen los organismos que elaboraron y promulgaron esta metodología. También se destaca la importancia de la gestión de riesgos para las organización.

Capítulo II: Visión de conjunto

Se describen los conceptos referentes a la gestión de riesgos de un modo introductorio para ofrecer una visión global de la importancia de la materia.

Capítulo III: Método de análisis de riesgos

Aquí ya se describe con profundidad la metodología para identificar y valorar los activos, amenazas, vulnerabilidades y salvaguardas, además de ofrecer una guía para estimar adecuadamente el impacto y el riesgo (tanto residuales como potenciales) de los sistemas de información.

Metodología Magerit

Capítulo IV: Proceso de gestión de riesgos

El capítulo IV de Magerit incluye todas las actividades que se realizan en el proceso de gestión de riesgos.

Capítulo V: Proyectos de análisis de riesgos

Este capítulo está centrado en los proyectos que se efectúan cuando las organizaciones desarrollan su primer análisis de riesgos y en sus posteriores revisiones y actualizaciones

Capítulo VI: Plan de seguridad

En el capítulo VI se hace referencia a las actividades necesarias para desarrollar un plan de seguridad por parte de las organizaciones.

Metodología Magerit

Capítulo VII: Desarrollo de sistemas de información

Este capítulo se enfoca específicamente en los sistemas de información y aplica las tareas y conceptos de gestión de riesgos descritos hasta el momento a las particularidades de las tecnologías de la información y comunicación para una mayor eficacia y reducción de los riesgos de estos sistemas.

Capítulo VIII: Consejos prácticos

Se incluyen consejos y recomendaciones prácticas para una mayor comprensión e implantación de las técnicas y metodologías descritas a lo largo de toda la guía.

Metodología Magerit

Epígrafes:

Son seis epígrafes en los que se incluyen:

- Un **glosario** con los términos principales de la gestión de riesgos tanto en español como en inglés.
- Las **referencias de la bibliografía** utilizada para la elaboración de la guía.
- El **marco legal** de la seguridad de los sistemas de información.
- El **marco de evaluación y certificación** de los sistemas de gestión de la seguridad de la información.
- La **herramienta Pilar**: herramienta para la gestión de riesgos que utilizan las Administraciones Públicas en España.
- La **evolución de la metodología** Magerit en sus versiones v1 y v2 respecto a la última versión.