



IMPUESTOS NACIONALES 🇧🇴

Metodología MAGERIT

MAGERIT

Es una metodología de análisis y gestión de riesgos elaborada por el Consejo Superior de Administración Electrónica de España, que ofrece un método sistemático para analizar los riesgos derivados del uso de tecnologías de la información y comunicaciones para de esta forma implementar las medidas de control más adecuadas que permitan tener los riesgos mitigados. Además de esto, cuenta con todo un documento que reúne técnicas y ejemplos de cómo realizar el análisis de riesgos.

MAGERIT

MAGERIT se basa en analizar el impacto que puede tener para la empresa la violación de la seguridad, buscando identificar las amenazas que pueden llegar a afectar la compañía y las vulnerabilidades que pueden ser utilizadas por estas amenazas, logrando así tener una identificación clara de las medidas preventivas y correctivas más apropiadas.

MAGERIT

Presenta una guía completa y paso a paso de cómo llevar a cabo el análisis de riesgos. Esta metodología está dividida en tres libros.

PRIMER LIBRO

- Hace referencia al Método, donde se describe la estructura que debe tener el modelo de gestión de riesgos. Este libro está de acuerdo a lo que propone ISO para la gestión de riesgos.

SEGUNDO LIBRO

- Es un Catálogo de Elementos, el cual es una especie de inventario que puede utilizar la empresa para enfocar el análisis de riesgo. Es así como contiene una división de los activos de información que deben considerarse, las características que deben tenerse en cuenta para valorar los activos identificados y además un listado con las amenazas y controles que deben tenerse en cuenta.

TERCER LIBRO

- Es una Guía de Técnicas, lo cual lo convierte en un factor diferenciador con respecto a otras metodologías. En esta tercera parte se describen diferentes técnicas frecuentemente utilizadas en el análisis de riesgos. Contiene ejemplos de análisis con tablas, algoritmos, árboles de ataque, análisis de costo beneficio, técnicas gráficas y buenas prácticas para llevar adelante sesiones de trabajo para el análisis de los riesgos.

- Esta metodología es muy útil para aquellas empresas que inicien con la gestión de la seguridad de la información, pues permite enfocar los esfuerzos en los riesgos que pueden resultar más críticos para una empresa, es decir aquellos relacionados con los sistemas de información. Lo interesante es que al estar alineado con los estándares de ISO es que su implementación se convierte en el punto de partida para una certificación o para mejorar los sistemas de gestión.

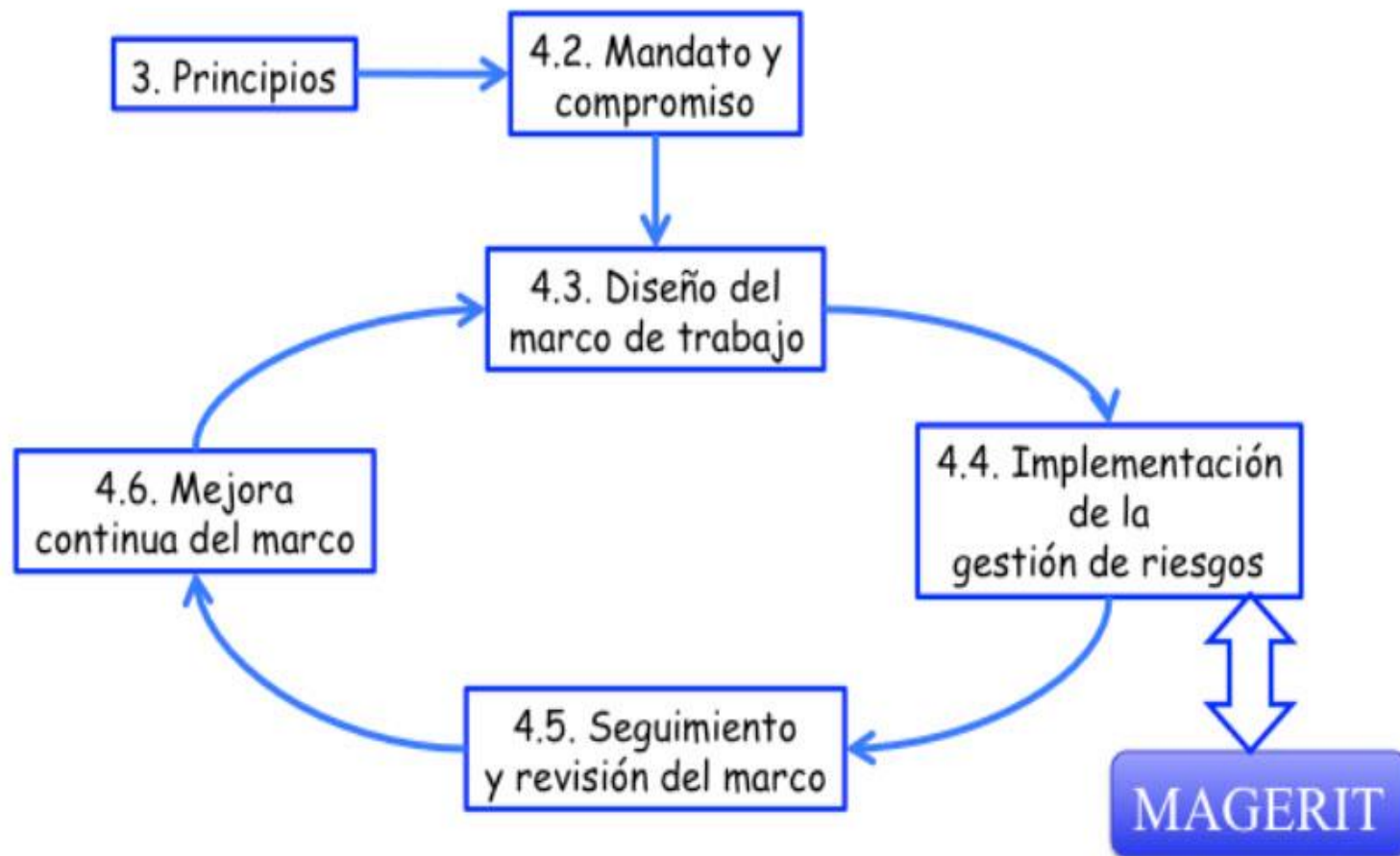


Ilustración 1. ISO 31000 - Marco de trabajo para la gestión de riesgos

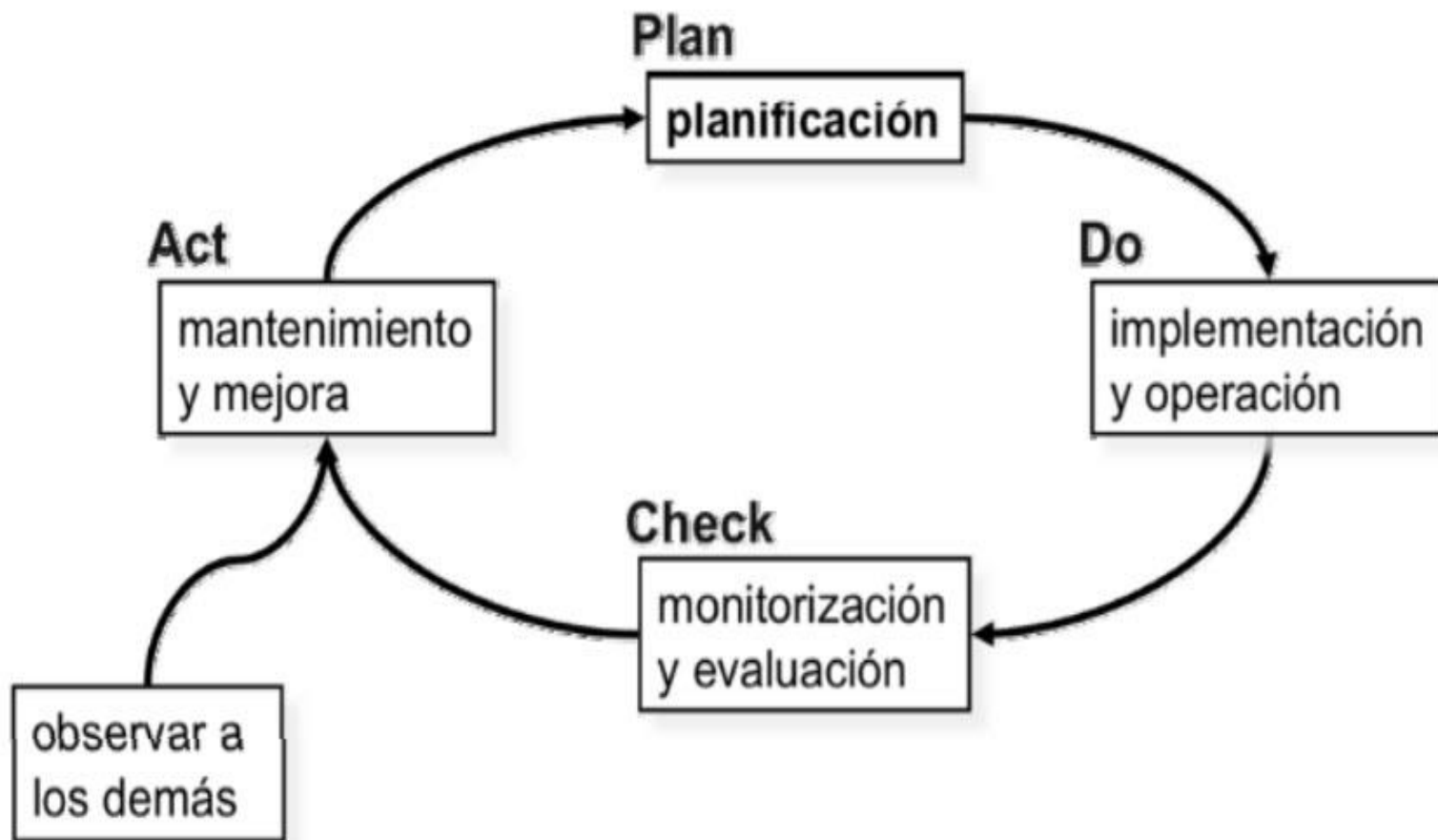


Ilustración 2. Ciclo PDCA

Capítulo 4 - Proceso de Gestión de Riesgos

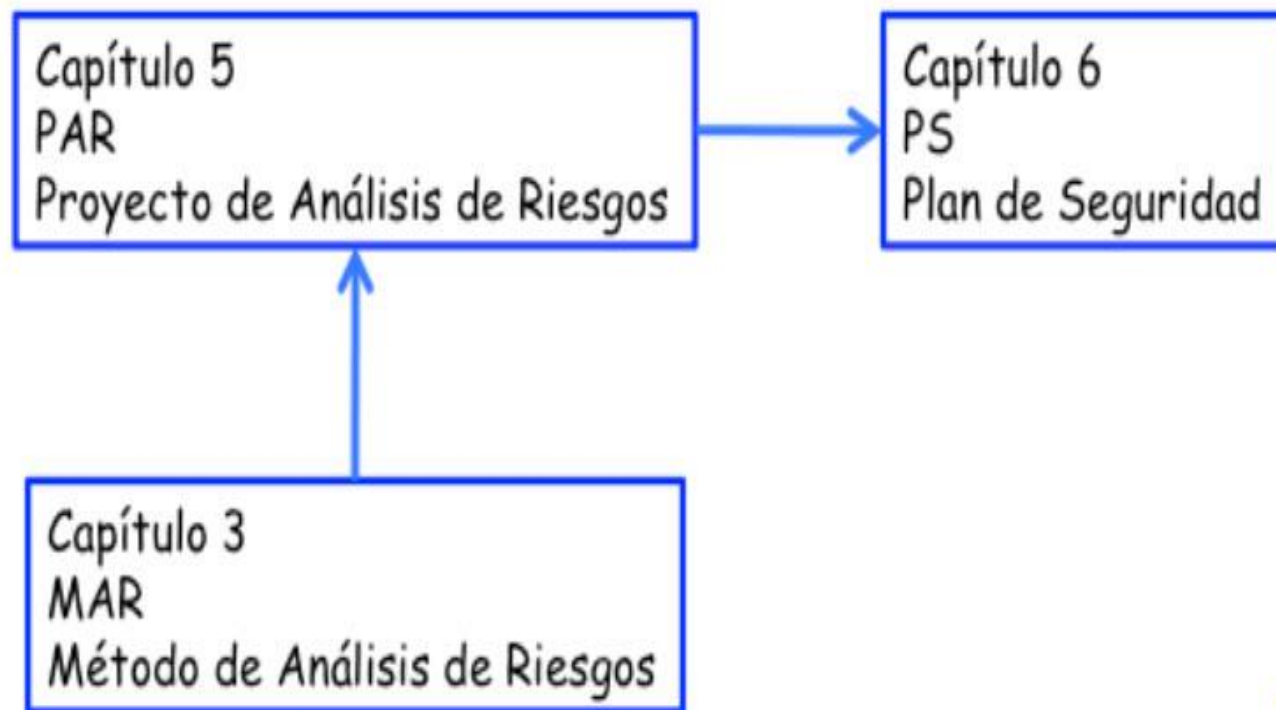


Ilustración 3. Actividades formalizadas

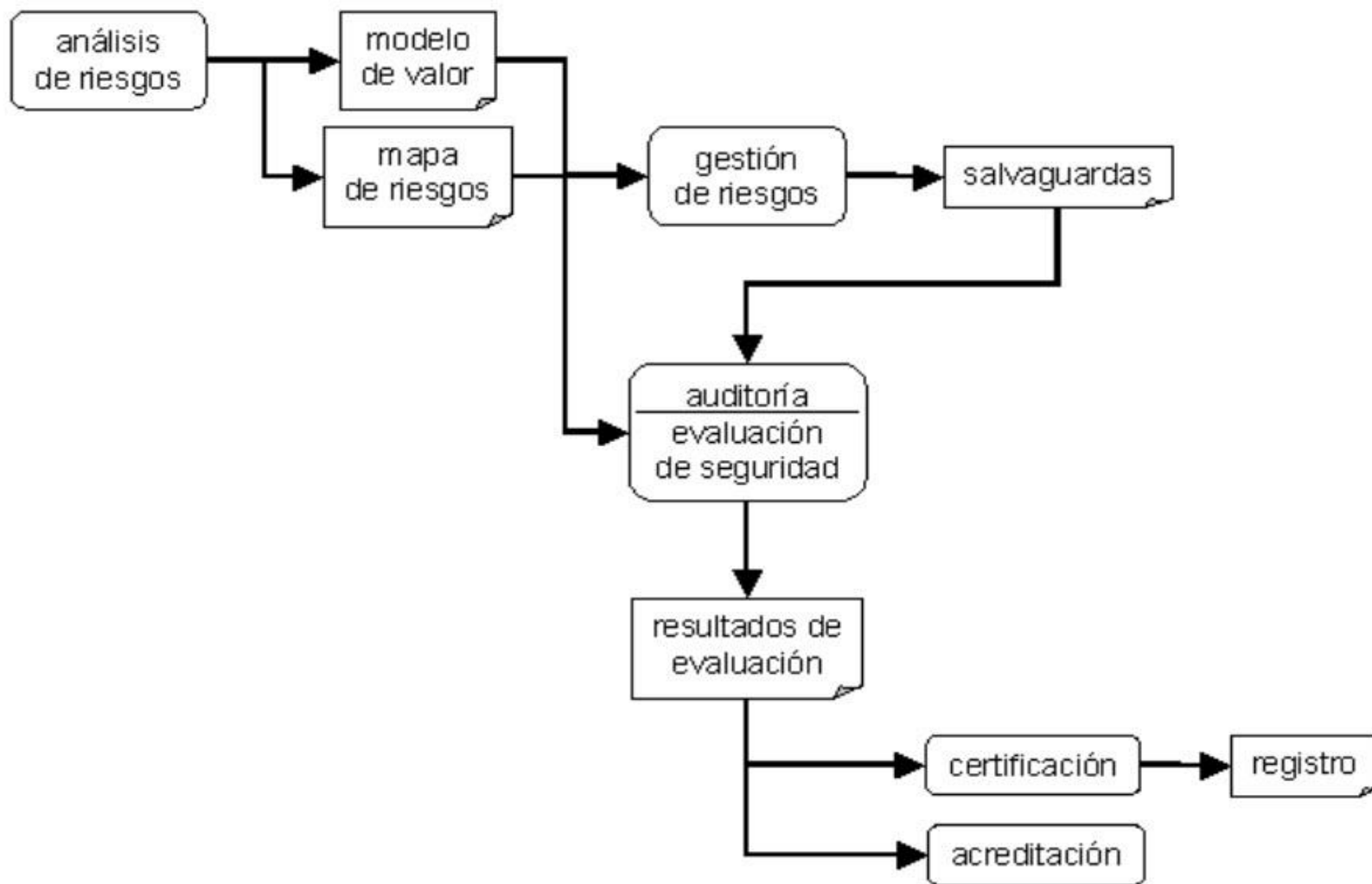


Ilustración 4. Contexto de certificación y acreditación de sistemas de información

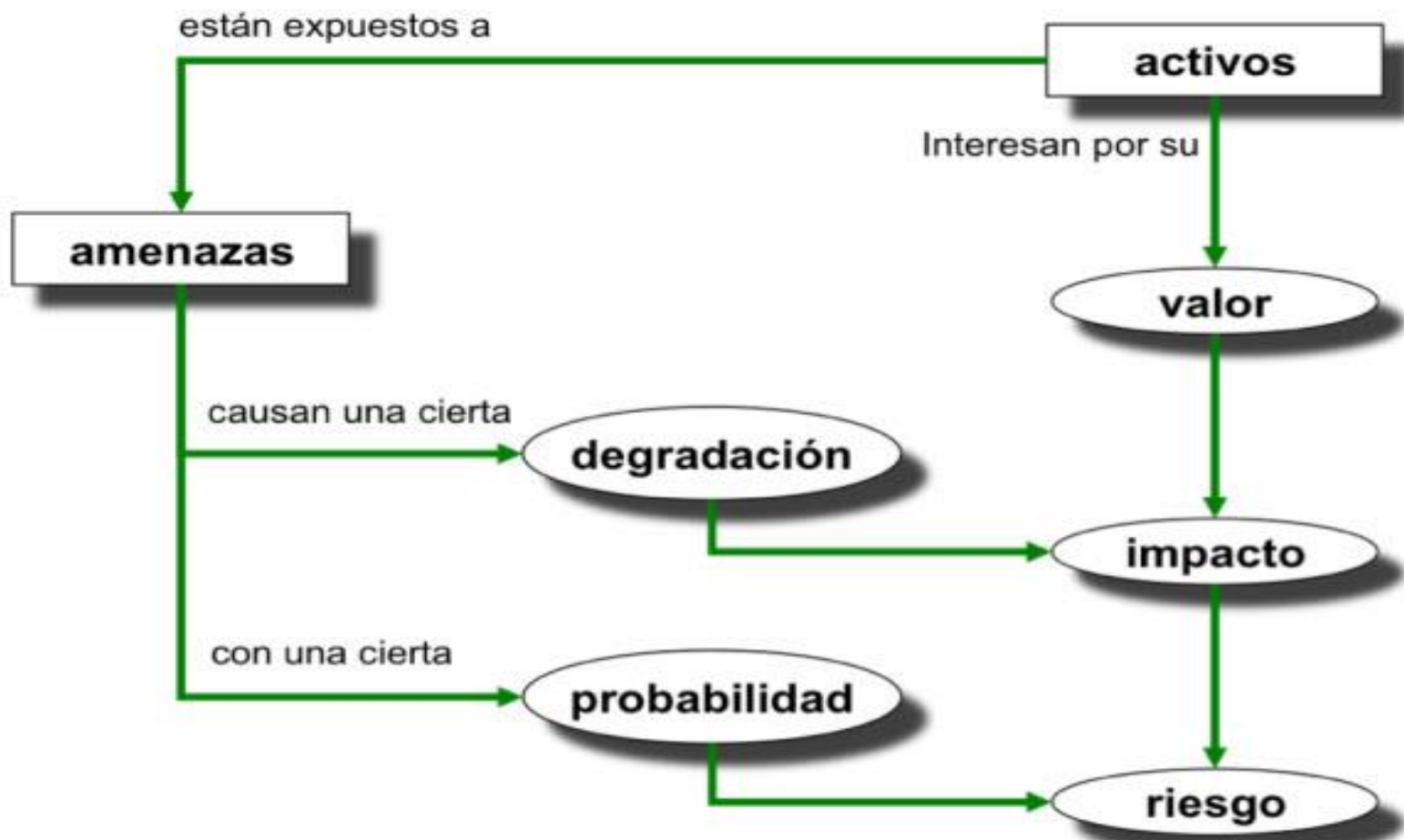


Ilustración 7. Elementos del análisis de riesgos potenciales

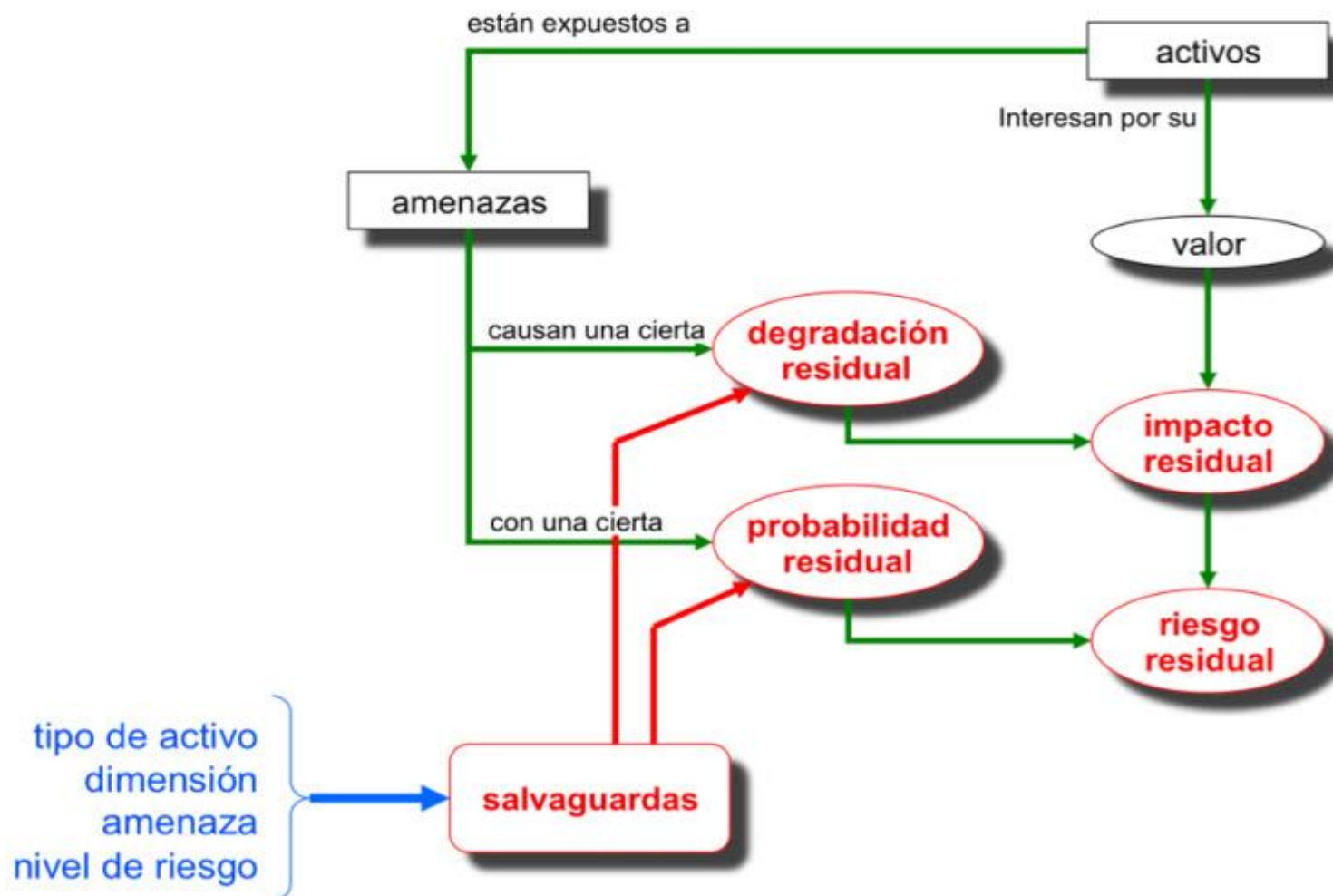


Ilustración 10. Elementos de análisis del riesgo residual

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

MAR: Análisis de riesgos

MAR.1: Caracterización de los activos

MAR.11: Identificación de los activos

Objetivos

- Identificar los activos que componen el sistema, determinando sus características, atributos y clasificación en los tipos determinados

Productos de entrada

- Inventario de datos manejados por el sistema
- Inventario de servicios prestados por el sistema
- Procesos de negocio
- Diagramas de uso
- Diagramas de flujo de datos
- Inventarios de equipamiento lógico
- Inventarios de equipamiento físico
- Locales y sedes de la Organización
- Caracterización funcional de los puestos de trabajo

MAR: Análisis de riesgos

MAR.1: Caracterización de los activos

MAR.11: Identificación de los activos

Productos de salida

- Relación de activos a considerar
- Caracterización de los activos: valor propio y acumulado
- Relaciones entre activos

Técnicas, prácticas y pautas

- Ver “Libro II – Catálogo”.
- Diagramas de flujo de datos
- Diagramas de procesos
- Entrevistas (ver "Guía de Técnicas")
- Reuniones

MAR: Análisis de riesgos

MAR.1: Caracterización de los activos

MAR.12: Dependencias entre activos

Objetivos

- Identificar y valorar las dependencias entre activos, es decir la medida en que un activo de orden superior se puede ver perjudicado por una amenaza materializada sobre un activo de orden inferior

Productos de entrada

- Resultados de la tarea T1.2.1, Identificación
- Procesos de negocio
- Diagramas de flujo de datos
- Diagramas de uso

Productos de salida

- Diagrama de dependencias entre activos

Técnicas, prácticas y pautas

- Diagramas de flujo de datos
- Diagramas de procesos
- Entrevistas (ver "Guía de Técnicas")
- Reuniones
- Valoración Delphi (ver "Guía de Técnicas")

MAR: Análisis de riesgos

MAR.1: Caracterización de los activos

MAR.13: Valoración de los activos

Objetivos

- Identificar en qué dimensión es valioso el activo
- Valorar el coste que para la Organización supondría la destrucción del activo

Productos de entrada

- Resultados de la tarea MAR.11, Identificación de los activos
- Resultados de la tarea MAR.12, Dependencias entre activos

Productos de salida

- **Modelo de valor:** informe de valor de los activos

Técnicas, prácticas y pautas

- Ver "Libro II – Catálogo".
- Entrevistas (ver "Guía de Técnicas")
- Reuniones
- Valoración Delphi (ver "Guía de Técnicas")

MAR: Análisis de riesgos

MAR.2: Caracterización de las amenazas

MAR.21: Identificación de las amenazas

Objetivos

- Identificar las amenazas relevantes sobre cada activo

Productos de entrada

- Resultados de la actividad MAR.1, Caracterización de los activos
- Informes relativos a defectos en los productos. Esto es, informes de vulnerabilidades.

Productos de salida

- Relación de amenazas posibles

Técnicas, prácticas y pautas

- Catálogos de amenazas (ver "Catálogo de Elementos")
- Árboles de ataque (ver "Guía de Técnicas")
- Entrevistas (ver "Guía de Técnicas")
- Reuniones
- Valoración Delphi (ver "Guía de Técnicas")

MAR: Análisis de riesgos

MAR.3: Caracterización de las salvaguardas

MAR.31: Identificación de las salvaguardas pertinentes

Objetivos

- Identificar las salvaguardas convenientes para proteger el sistema

Productos de entrada

- modelo de activos del sistema
- modelo de amenazas del sistema
- indicadores de impacto y riesgo residual
- informes de productos y servicios en el mercado

Productos de salida

- Declaración de aplicabilidad: relación justificada de las salvaguardas necesarias
- Relación de salvaguardas desplegadas

Técnicas, prácticas y pautas

- Catálogos de salvaguardas (ver "Catálogo de Elementos")
- Árboles de ataque (ver "Guía de Técnicas")
- Entrevistas (ver "Guía de Técnicas")
- Reuniones

MAR: Análisis de riesgos

MAR.3: Caracterización de las salvaguardas

MAR.32: Valoración de las salvaguardas

Objetivos

- Determinar la eficacia de las salvaguardas pertinentes

Productos de entrada

- Inventario de salvaguardas derivado de la tarea MAR.31

Productos de salida

- **Evaluación de salvaguardas** : informe de salvaguardas desplegadas, caracterizadas por su grado de efectividad
- **Informe de insuficiencias (o vulnerabilidades)**: relación de salvaguardas que deberían estar pero no están desplegadas o están desplegadas de forma insuficiente

Técnicas, prácticas y pautas

- Entrevistas (ver "Guía de Técnicas")
- Reuniones
- Valoración Delphi (ver "Guía de Técnicas")

MAR: Análisis de riesgos

MAR.4: Estimación del estado de riesgo

MAR.41: Estimación del impacto

Objetivos

- Determinar el impacto potencial al que está sometido el sistema
- Determinar el impacto residual al que está sometido el sistema

Productos de entrada

- Resultados de la actividad MAR.1, Caracterización de los activos
- Resultados de la actividad MAR.2, Caracterización de las amenazas
- Resultados de la actividad MAR.3, Caracterización de las salvaguardas

Productos de salida

- Informe de impacto (potencial) por activo
- Informe de impacto residual por activo

Técnicas, prácticas y pautas

- Análisis mediante tablas (ver "Guía de Técnicas")
- Análisis algorítmico (ver "Guía de Técnicas")

MAR: Análisis de riesgos

MAR.4: Estimación del estado de riesgo

MAR.42: Estimación del riesgo

Objetivos

- Determinar el riesgo potencial al que está sometido el sistema
- Determinar el riesgo residual al que está sometido el sistema

Productos de entrada

- Resultados de la actividad MAR.1, Caracterización de los activos
- Resultados de la actividad MAR.2, Caracterización de las amenazas
- Resultados de la actividad MAR.3, Caracterización de las salvaguardas
- Resultados de la actividad MAR.4, Estimaciones de impacto

MAR: Análisis de riesgos

MAR.4: Estimación del estado de riesgo

MAR.42: Estimación del riesgo

Productos de salida

- Informe de riesgo (potencial) por activo
- Informe de riesgo residual por activo

Técnicas, prácticas y pautas

- Análisis mediante tablas (ver "Guía de Técnicas")
- Análisis algorítmico (ver "Guía de Técnicas")

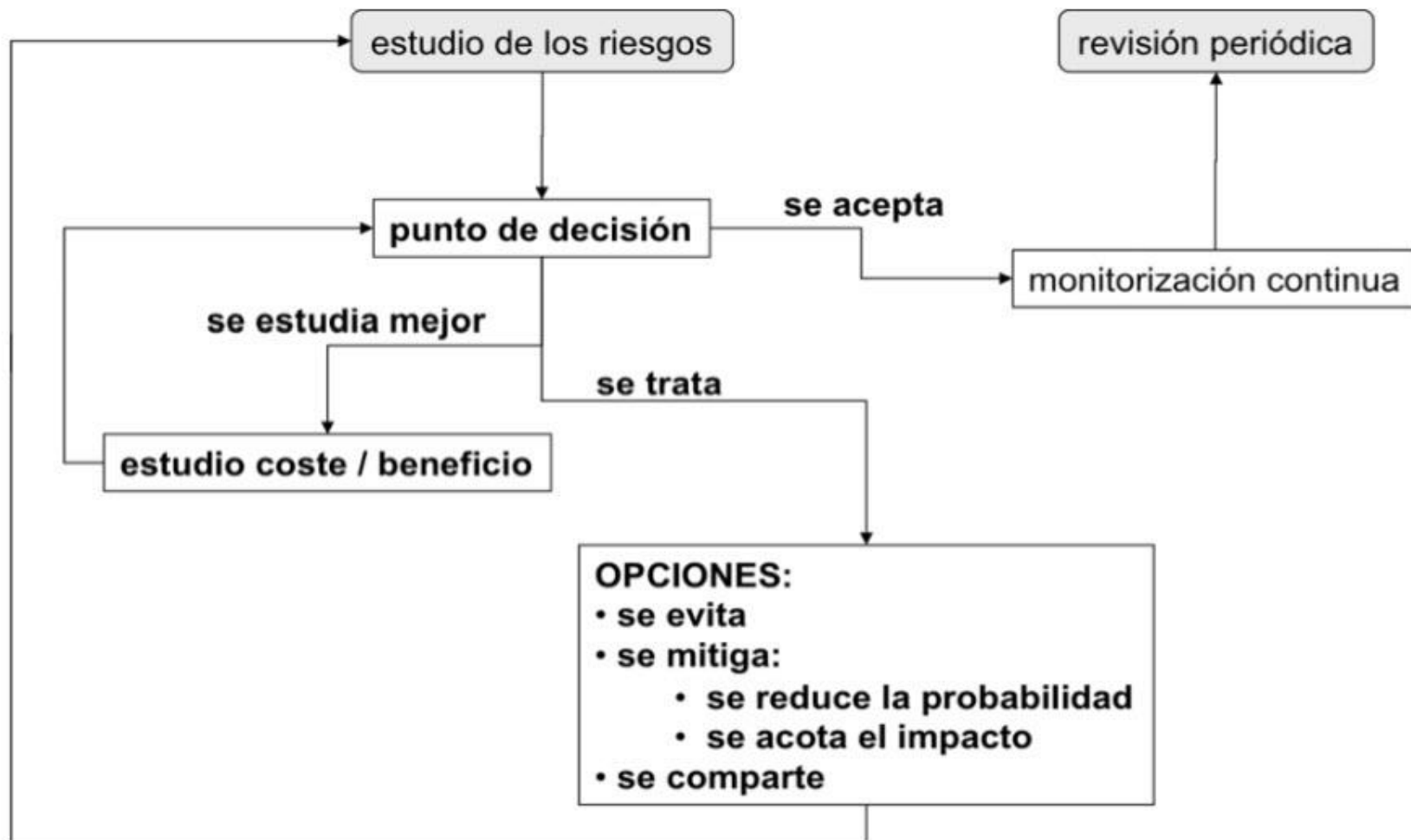


Ilustración 11. Decisiones de tratamiento de los riesgos



IMPUESTOS NACIONALES 🇧🇴

Muchas gracias...