MAGERIT versión 3

Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información

MAGERIT v3 proporciona un método **sistemático** para analizar los riesgos derivados del uso de las Tecnologías de la Información y Comunicaciones (**TIC**) y planificar las acciones necesarias para mantener esos riesgos bajo control.

Resumen de MAGERIT Versión 3 (Octubre 2012)

La metodología MAGERIT v3 se organiza en tres documentos principales para guiar a las organizaciones en el proceso de gestión de la seguridad de la información.

Libro I: Método - El Proceso de Gestión de Riesgos

Este libro constituye el núcleo de la metodología y describe el **Modelo de Gestión de Riesgos**, que se enfoca en el ciclo de vida de la seguridad de la información. La versión 3 se actualiza para mejorar su alineación con la normativa **ISO/IEC 27001**.

El proceso central se basa en los siguientes pasos secuenciales:

1. Planificación

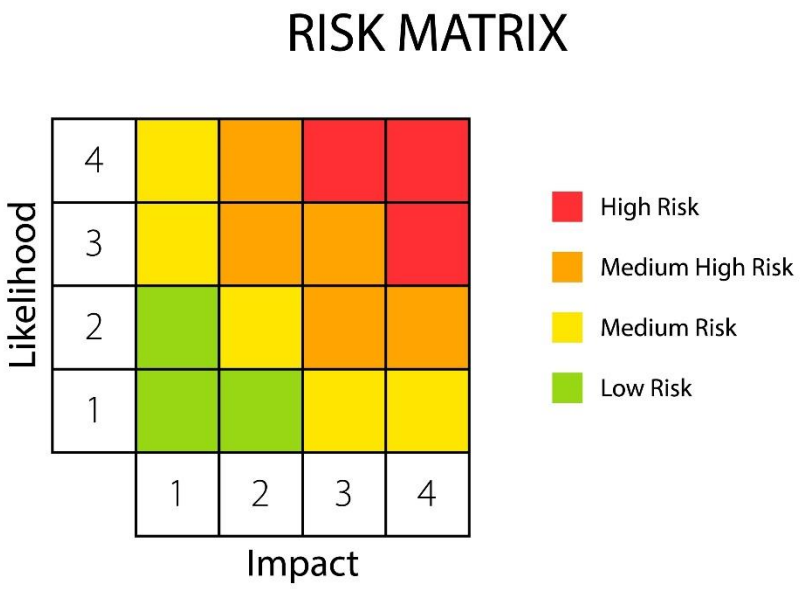
- **Definición del Alcance:** Se establece qué partes del Sistema de Información (SI) se van a analizar.
- **Identificación de Activos:** Se identifican los activos **esenciales** (la información y los servicios, valorados según su **Confidencialidad, Integridad, Disponibilidad, Autenticidad y Trazabilidad**) y los activos de **soporte** (hardware, software, personal, instalaciones, etc.) necesarios para materializar los esenciales.
- **Valoración de Activos:** Se asigna un valor a cada dimensión de seguridad (C, I, D, A, T) para los activos esenciales, lo que permite cuantificar el daño potencial.

2. Análisis de Riesgos

- **Identificación de Amenazas:** Se identifican los eventos que podrían causar daño a los activos (por ejemplo, incendios, fallos eléctricos, errores humanos, *malware*).

- **Valoración de Impactos (Daño):** Se calcula el impacto (*I*) sobre el negocio si una amenaza se materializa sobre un activo (daño en términos de valor, reputación, legal, etc.).
- **Estimación de la Probabilidad:** Se estima la frecuencia o la probabilidad (*P*) de que una amenaza se materialice.
- Estimación del Riesgo: Se calcula el Riesgo Potencial (o Riesgo Inherente) como la combinación del impacto y la probabilidad:

  Riesgo Potencial = Impacto X Probabilidad



3. Gestión de Riesgos (Tratamiento)

- **Identificación de Salvaguardas:** Se identifican y seleccionan las medidas de seguridad (controles) que se van a aplicar o que ya están en uso para reducir el riesgo.
- **Cálculo del Riesgo Residual:** Las salvaguardas reducen el impacto o la probabilidad de las amenazas. El **Riesgo Residual** es el riesgo que queda tras la aplicación de las salvaguardas.
- **Tratamiento del Riesgo:** La organización debe decidir cómo gestionar el riesgo residual:
  - **Reducir:** Aplicar o mejorar las salvaguardas.
  - **Transferir:** Ceder el riesgo a un tercero (ej. seguros).
  - **Evitar:** Cambiar el proceso para eliminar el riesgo.

    - **Aceptar:** Asumir el riesgo, si está por debajo del umbral de riesgo aceptable.

4. Monitorización y Revisión

El proceso de gestión de riesgos es un ciclo continuo. Se debe **monitorizar** la efectividad de las salvaguardas y **revisar** periódicamente el análisis de riesgos para adaptarse a los cambios del entorno, la tecnología y las amenazas emergentes.

Libro II: Catálogo de Elementos

Este libro actúa como una **referencia** y una **fuente de conocimiento** para estandarizar los elementos clave utilizados en el análisis.

- **Catálogo de Activos:** Detalla los tipos de activos esenciales (información, servicios) y de soporte (personal, hardware, software, red, etc.).
- **Catálogo de Amenazas:** Proporciona una lista exhaustiva de las amenazas comunes, categorizadas por su origen (naturales, industriales, accidentales, intencionadas, por fallos) y por su tipo (físicas, lógicas, ambientales). Por ejemplo: desastres, fallos de *hardware*/software, ataques de denegación de servicio, errores de operación.
- **Catálogo de Salvaguardas:** Enumera y clasifica las medidas de seguridad que se pueden aplicar para proteger los activos y tratar los riesgos. Incluye salvaguardas de tipo:
    - Organizativo (políticas, procedimientos).
    - Físico (controles de acceso, seguridad perimetral).
    - Lógico (cifrado, *firewalls*, autenticación).

Libro III: Guía de Técnicas

Este documento complementario describe una variedad de **técnicas** prácticas que se pueden utilizar para llevar a cabo el análisis y la gestión de riesgos descritos en el Libro I.

- **Técnicas de Análisis:** Métodos para la **identificación y valoración de activos** (ej. entrevistas, cuestionarios), la **determinación de amenazas y vulnerabilidades** (ej. análisis de incidentes, listas de comprobación) y la **estimación de impactos y probabilidades.**
- **Técnicas de Tratamiento:** Estrategias y métodos para la **selección, especificación e implantación de salvaguardas**

(ej. análisis coste-beneficio, especificación de requisitos).
- **Técnicas de Seguimiento:** Métodos para **monitorizar** la efectividad del sistema de gestión de seguridad de la información y la conformidad con los requisitos establecidos.

Objetivos y Uso de MAGERIT v3

El principal objetivo de MAGERIT v3 es:

1. **Ofrecer un método** para analizar los riesgos de los SI de forma sistemática y reproducible.
2. **Ayudar a tomar decisiones informadas** sobre la seguridad, priorizando las inversiones en protección para los activos más valiosos y los riesgos más altos.
3. **Facilitar el cumplimiento** del Esquema Nacional de Seguridad (**ENS**) en España, ya que el análisis de riesgos con MAGERIT es la forma recomendada para cumplir con el requisito de gestión de riesgos del ENS.

La metodología está diseñada para ser utilizada tanto en el sector público como en el privado, siendo una **herramienta clave** para la planificación y la justificación de las inversiones en seguridad.