

MAGERIT v3: Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información

Introducción

El presente documento de investigación tiene como objetivo proporcionar una visión completa y estructurada de la metodología **MAGERIT (Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información)** en su versión 3.0. Esta metodología, desarrollada por el Consejo Superior de Administración Electrónica (CSAE) del Gobierno de España, se ha consolidado como un marco de referencia esencial para la gestión de la seguridad de la información, especialmente en el ámbito de las Administraciones Públicas y en empresas con Sistemas de Información (SI) críticos.

1. Definición de MAGERIT

MAGERIT es un **método formal y sistemático** diseñado para investigar los riesgos a los que están expuestos los Sistemas de Información y para recomendar las medidas de seguridad (salvaguardas) más adecuadas para gestionarlos.

Su propósito fundamental es ayudar a las organizaciones a tomar decisiones informadas sobre la seguridad de sus SI, alineando la gestión de riesgos con los objetivos de negocio. La metodología se enmarca dentro del **Esquema Nacional de Seguridad (ENS)** en España, siendo un pilar para el cumplimiento de sus requisitos.

2. Objetivos de MAGERIT

Los objetivos de MAGERIT se dividen en directos e indirectos, todos orientados a establecer una cultura de gestión de riesgos en la organización.

Objetivos Principales

Tipo de Objetivo	Descripción
Concienciación	Concienciar a los responsables de la organización sobre la existencia de riesgos en sus SI y la necesidad urgente de gestionarlos de forma proactiva.
Sistemático	Ofrecer un método sistemático y repetible para analizar los riesgos derivados del uso de las Tecnologías de la Información y Comunicaciones (TIC).
Tratamiento	Ayudar a descubrir y planificar el tratamiento oportuno de los riesgos, asegurando que estos se mantengan bajo un nivel de control aceptable.
Preparación	Preparar a la organización para procesos de evaluación, auditoría, certificación o acreditación, como el cumplimiento del Esquema Nacional de Seguridad (ENS).

Empresas y Sectores de Aplicación

MAGERIT es de **aplicación obligatoria** para todas las **Administraciones Públicas españolas** en cumplimiento del ENS (Real Decreto 311/2022).

Su adopción se extiende a sectores donde la continuidad del negocio y la protección de datos son vitales, tales como:

- **Infraestructuras Críticas:** Empresas de energía, transporte, telecomunicaciones y servicios esenciales cuya interrupción podría tener un impacto grave en la sociedad.
- **Sector Financiero y Seguros:** Organizaciones que gestionan grandes volúmenes de datos personales y transacciones económicas, donde la integridad y la confidencialidad son primordiales.
- **Sector Sanitario:** Hospitales y clínicas que manejan historiales médicos y datos de salud altamente sensibles.

3. Fases del Análisis de Riesgos

El proceso de análisis de riesgos propuesto por MAGERIT (Libro I - Método) se desarrolla en una secuencia lógica de pasos que van desde la identificación de los elementos hasta la

estimación del riesgo residual.

Fase	Tarea Principal	Descripción
Paso 1	Determinación y Valoración de Activos	Se identifican todos los activos del SI (información, hardware, software, servicios, personal, etc.) y se les asigna un valor en función de las dimensiones de seguridad: Confidencialidad, Integridad, Disponibilidad, Autenticidad y Trazabilidad.
Paso 2	Identificación de Amenazas	Se determinan las amenazas a las que están expuestos los activos (ej. fallos técnicos, desastres naturales, ataques intencionados). Se valora la degradación que causarían y su probabilidad de ocurrencia.
Paso 3	Identificación de Salvaguardas	Se identifican las medidas de protección (salvaguardas) existentes o a implementar. Se evalúa su eficacia para reducir la probabilidad de las amenazas o mitigar el daño.
Paso 4	Estimación del Impacto Residual	Se calcula el daño potencial sobre un activo si una amenaza se materializa, una vez aplicadas las salvaguardas. Se pasa de un Impacto Potencial a un Impacto Residual.
Paso 5	Estimación del Riesgo Residual	Se calcula el riesgo final, que es el impacto residual ponderado por la probabilidad residual de la amenaza. El objetivo es que este Riesgo Residual sea aceptable para la organización.

4. Aplicación Práctica: Mejora de la Seguridad Informática

Protección de la Base de Datos de Clientes

Consideremos una empresa de comercio electrónico cuyo activo más crítico es la Base de Datos de Clientes.

Fase de MAGERIT	Ejemplo de Activo/Riesgo	Aplicación Práctica para la Mejora de la Seguridad
Paso 1: Activos	Activo: Base de Datos de Clientes (BDC).	Valoración: Confidencialidad y Disponibilidad Alta . La pérdida de cualquiera de estas dimensiones tendría un impacto catastrófico (multas RGPD, cese de operaciones).
Paso 2: Amenazas	Amenaza: Fallo del servidor de la BDC por sobrecalentamiento.	Riesgo Potencial: Pérdida de disponibilidad del servicio durante 48 horas.
Paso 3: Salvaguardas	Salvaguarda Implementada: Sistema de refrigeración redundante y monitorización de temperatura.	Acción: Se instala un sistema de climatización de respaldo en el centro de datos y se configura una alerta automática.
Paso 4: Impacto Residual	Impacto Potencial: Pérdida total de servicio (48h).	Impacto Residual: Interrupción de servicio de 1 hora (tiempo de conmutación al sistema de respaldo).
Paso 5: Riesgo Residual	Riesgo Potencial: Alto.	Riesgo Residual: Bajo. La inversión en la salvaguarda ha reducido el riesgo a un nivel aceptable, mejorando la seguridad informática.

Referencias

- CCN-CERT. *MAGERIT – versión 3.0 Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información*. Disponible en: <https://www.ccn-cert.cni.es/es/documentos->

[publicos/1789-magerit-libro-i-metodo/file?format=html](#)

2. Piranirisk. *MAGERIT: gestión de riesgos de Seguridad de la Información*. Disponible en: <https://www.piranirisk.com/es/blog/metodologia-magerit-gestion-riesgos-sistemas-de-informacion>
3. Gobierno de España. *Esquema Nacional de Seguridad (ENS)*. Disponible en: <https://administracionelectronica.gob.es/ctt/ens>
4. Jaymon Security. *Análisis de riesgos de una empresa - Práctica Magerit 3*. Disponible en: <https://jaymonsecurity.es/analisis-riesgos-empresa/>