

CONSEJO SUPERIOR DE INFORMÁTICA Y PARA EL IMPULSO DE LA ADMINISTRACIÓN ELECTRÓNICA - MINISTERIO DE ADMINISTRACIONES PÚBLICAS

MAGERIT. Versión 1.0

Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información de las Administraciones Públicas.

<http://www.csi.map.es/csi/pg5m20.htm>

MAGERIT. Versión 1.0 es una metodología de análisis y gestión de riesgos de los sistemas informáticos de Las Administraciones públicas. El objetivo general de esta norma es garantizar la seguridad los sistemas de información, identificando problemas y definiendo protocolos que los eviten.

El análisis de los riesgos generados por el uso de sistemas informáticos determina las políticas de seguridad en los sistemas de Información mediante:

- Planificación de la seguridad
- Implantación de salvaguardias (Implicación de todos los recursos humanos e informáticos en los sistemas de seguridad)
- Seguimiento de los sistemas de seguridad (Reacción a los eventos, registros de incidencias y recuperación de estados de seguridad)

Estructura de MAGERIT:

Se desarrolla en tres submodelos:

- a) Elementos(Proporciona los componentes del sistema (Activos, Amenazas, Vulnerabilidades ,Impacto, Riesgo, Salvaguardas)
- b) Eventos: *Relaciona los elementos entre si y con el tiempo*
- c) Procesos: Describe el proyecto de seguridad a construir en 4 etapas (Planificación, Análisis de riesgos, Gestión de Riesgos, Selección de Salvaguardias)

Interfaces

Para construir proyectos específicos de seguridad MAGERIT cuenta con interfaces de enlace con METRICA VERSIÓN 2.1. Estas herramientas permiten analizar la seguridad del sistema antes de su desarrollo, incorporar las defensas necesarias y controlar su efectividad a lo largo de todo su ciclo vital.

Guías:

Magerit cuenta con las siguientes guías

- Aproximación
- Procedimientos
- Técnicas
- Responsables del dominio protegible
- Desarrolladores de aplicaciones
- Arquitectura de la información y especificaciones de la interfaz de intercambio de datos.
- Referencias de Normas Legales y Técnicas(31 de diciembre de 1996)

Comentario

Los conceptos que se emplean para definir los distintos aspectos de MAGERIT son confusos para un no iniciado en temas informáticos.

“El modelo normativo de MAGERIT se apoya en tres submodelos: El Submodelo de Elementos proporciona los “componentes” que el Submodelo de Eventos va a relacionar entre sí y con el tiempo, mientras que el Submodelo de Procesos será la descripción funcional (“el esquema explicativo”) del proyecto de seguridad a construir”

La norma está anticuada tanto en las referencias legales que proporciona como en su articulación con los mecanismos de evaluación, homologación y certificación de seguridad de sistemas informáticos(ITSEC) desarrollados a escala europea. Está en proyecto el desarrollo de una nueva versión 2.0

Para los archiveros tiene utilidad en tanto se puede aplicar este método de análisis y evaluación de riesgos a la seguridad y conservación, tanto de nuestros sistemas informáticos como de los propios fondos de Archivo y de los sistemas de descripción y control tradicionales. Basta con examinar los ejemplos en la red de ficheros incluidos dentro del Sistema MAGERIT 1.0 (Incendio, Inundación, Fallo del equipo físico, Avería

de la climatización, Corte suministro eléctrico, Errores, Sustracción física, Sustracción lógica, Indisponibilidad personal etc...). Su aplicación probablemente sencilla requiere sin embargo la asistencia de un especialista en informática aunque el archivero es esencial para definir los riesgos materiales asociados al sistema.