

Metodología de análisis y gestión de riesgos: MAGERIT

SEGURIDAD EN REDES TELEMÁTICAS

F. Expósito
Curso 2002/2003

Índice

- | Introducción
- | MAGERIT
- | Objetivos
- | Usos
- | Estructura
- | Guías
- | Herramientas oficiales
- | Conclusiones
- | Bibliografía

Introducción

┆ ¿Qué es el Análisis y Gestión de Riesgos?

Es el ‘corazón’ de toda actuación organizada en materia de seguridad y de la gestión global de seguridad. Influye en las Fases y actividades de tipo estratégico y condiciona la profundidad de las fases y actividades de tipo logístico.

┆ El Análisis de Riesgos implica:

- ┆ Determinar **qué** se necesita proteger.
- ┆ **De qué** hay que protegerlo.
- ┆ **Cómo** hacerlo.

MAGERIT

I ¿Qué es MAGERIT?

La Metodología de Análisis y GEstión de RIegos de las AdminisTraciones públicas, MAGERIT, es un método formal para investigar los riegos que soportan los Sistemas de Información, y para recomendar las medidas apropiadas que deberían adoptarse para controlar estos riesgos.

I ¿Quién lo ha elaborado?

MAGERIT ha sido elaborada por un equipo interdisciplinar del Comité Técnico de Seguridad de los Sistemas de Información y Tratamiento Automatizado de Datos Personales, SSITAD, del Consejo Superior de Informática.

Objetivos

▮ **Principal:**

- ▮ *Estudiar los riesgos que soporta un sistema de información y el entorno asociado a él.*

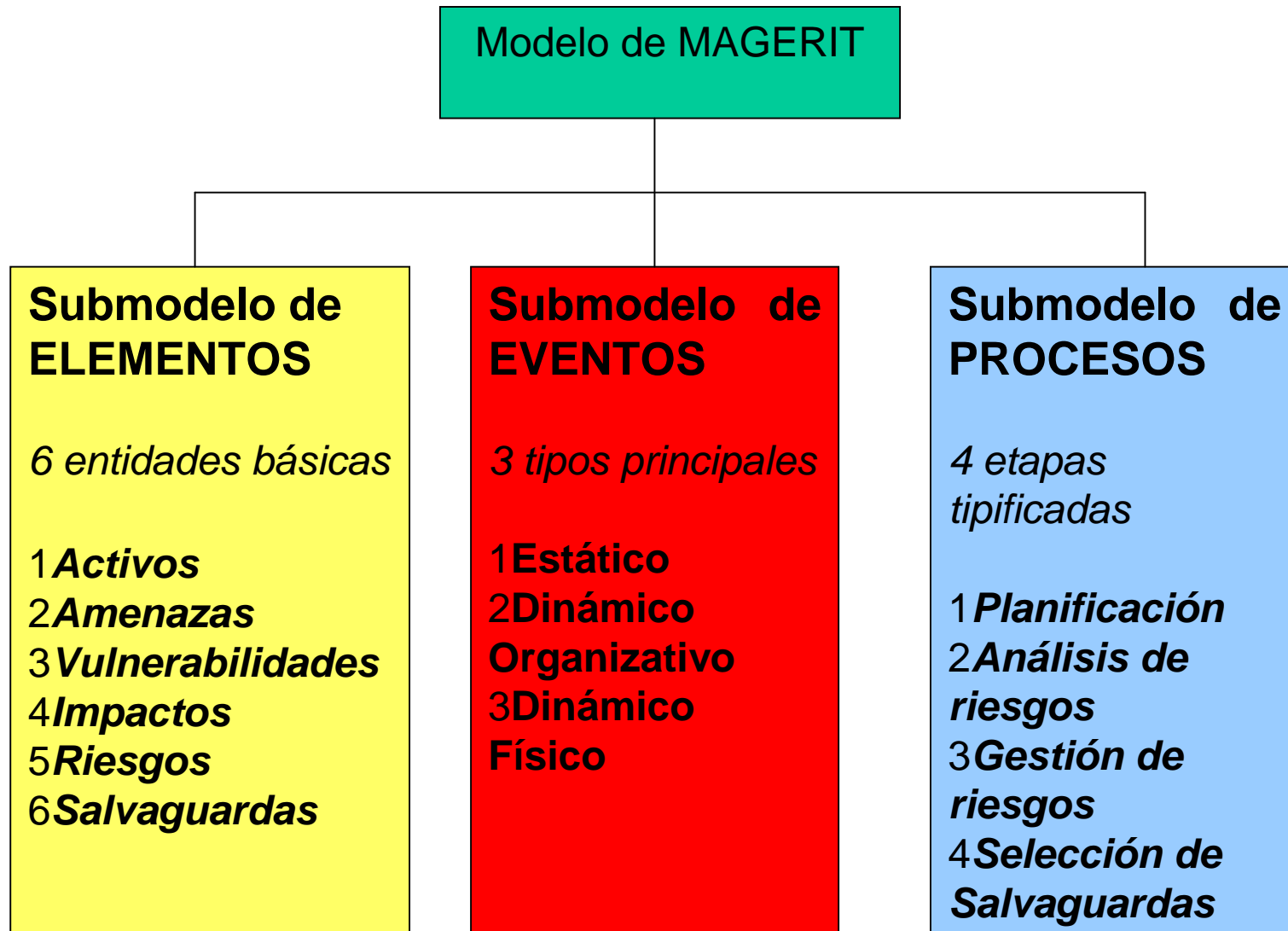
▮ **A largo plazo:**

- ▮ *Se prepara su articulación con los mecanismos de evaluación, homologación y certificación de seguridad de sistemas de información de organismos internacionales.*

Usos

- | Aportar racionalidad en el conocimiento del estado de seguridad de los Sistemas de Información y en la introducción de medidas de seguridad.
- | Tratar de que no haya elementos del Sistema de Información que queden fuera del análisis.
- | Incrustar mecanismos de seguridad en el corazón mismo de los Sistemas de Información:
 - | para paliar las insuficiencias de los sistemas.
 - | para asegurar el desarrollo de los Sistemas.

Estructura



Estructura: Submodelo de ELEMENTOS (I)

I Submodelo de ELEMENTOS:

I Se basa en 6 entidades:

I **Activos:**

Recursos del sistema de información o relacionados con éste, necesarios para que la organización funcione correctamente y alcance los objetivos propuestos por su dirección.

5 tipos:

1. Entorno
2. Sistema de Información
3. La información
4. Funcionalidades de la organización
5. Otros activos

Estructura: Submodelo de ELEMENTOS (II)

I Amenazas:

Los eventos que pueden desencadenar un incidente en la organización, produciendo daños materiales o pérdidas inmateriales en sus activos.

I Vulnerabilidad:

Ocurrencia real de materialización de una Amenaza sobre un Activo.

I 2 aspectos:

- Estático → función
- Dinámico → mecanismo

I 2 acepciones:

- Intrínseca; 2 tipos:
- Efectiva

Estructura: Submodelo de ELEMENTOS (III)

I **Impacto:**

Daño producido a la organización por un posible incidente.

La diferencia en las estimaciones de los estados de seguridad obtenidas antes y después del evento.

3 tipos:

- I Cuantitativo
- I Cualitativo con pérdidas orgánicas
- I Cualitativo con pérdidas funcionales

Estructura: Submodelo de ELEMENTOS (IV)

| **Riesgo**

Posibilidad de que se produzca un impacto dado en la organización.

| **'Función o Servicio' de salvaguarda, 'Mecanismo' de salvaguarda**

| **'Función o Servicio' de salvaguarda**

Reducción del riesgo.

| **'Mecanismo' de salvaguarda**

Dispositivo, físico o lógico, capaz de reducir el riesgo.

| **2 tipos:**

- Preventivas
- Curativas

Estructura: Submodelo de EVENTOS (I)

| Símil: ‘Ciudad amurallada’

- | Activos están dentro.
- | Amenazas = enemigo exterior.
- | Salvaguardas = murallas
- | Brechas = vulnerabilidades
- | *El ataque de las amenazas aprovecha las brechas y causa impactos en los Activos. El refuerzo de salvaguardas repara los Impactos y reduce las brechas-vulnerabilidades.*

Estructura: Submodelo de EVENTOS (II)

- | *Este submodelo está cada vez más superado debido a los nuevos tipos de amenaza*
- | Nuevo símil: '**Ciudades abiertas**' casi 'sin fronteras' más que 'Ciudades amuralladas' cerradas
 - | Requieren salvaguardas dinámicas y flexibles.
 - | En cada 'urbanización' de Activos hay que 'incrustar' salvaguardas dinámicas
 - | Las salvaguardas crecen con la urbanización, la 'patrullan' y cambian de aspecto para burlar a agresores cada vez más inteligentes.

Estructura: Submodelo de EVENTOS (III)

- | 3 vistas:
 - | Vista estática
 - | Vista dinámica de tipo organizativo
 - | Vista dinámica de tipo físico
- | 2 subescenarios:
 - | **Ataque:** *análisis de los riesgos; parte de la materialización de la amenaza o agresión a uno o varios Tipos de Activos de la Organización.*
 - | **Defensa:** *gestión de los riesgos; muestra como se pueden articular frente a cada ataque, las salvaguardas apropiadas.*

Estructura: Submodelo de PROCESOS (I)

I 4 etapas:

I **Planificación del Proyecto de Riesgos**

Consideraciones iniciales para arrancar el proyecto de análisis y gestión de riesgos.

- *Estudia la oportunidad de realizarlo*
- *Se definen objetivos que ha de cumplir y su ámbito.*
- *Planifica medios materiales y humanos para su realización, inicializando el lanzamiento del proyecto.*

I **Análisis de riesgos**

Se identifican y valoran las diversas entidades, para obtener una evaluación del riesgo y una estimación del umbral de riesgo deseable.

Estructura: Submodelo de PROCESOS (II)

I **Gestión de riesgos**

- I Se identifican funciones y servicios de salvaguarda reductoras del riesgo.
- I Se seleccionan los que son aceptables en función de las salvaguardas existentes y las restricciones, tras simular diversas combinaciones.

I **Selección de salvaguardas**

- I Se prepara el plan de implantación de los mecanismos de salvaguarda y los procedimientos de seguimiento de la implantación.
- I Se recopilan los documentos del AGR, para obtener los documentos finales del proyecto y realizar las presentaciones de resultados a diversos niveles.

Guías (I)

I **Guía de Aproximación**

Conceptos básicos de seguridad de los sistemas de información.

I **Guía de Procedimientos**

- I Representa el núcleo del método.
- I Se completa con la Guía de Técnicas. Ambas constituyen un conjunto autosuficiente. Basta su contenido para comprender la terminología y para realizar el Análisis y Gestión de Riesgos de cualquier sistema de información
- I Orientada a cómo tratar los riesgos detectados.
- I Tiene en cuenta el avance científico, normativo y normalizador en materia de seguridad de los sistemas de información.

Guías (II)

I **Guía de Técnicas**

Proporciona las claves para comprender y seleccionar las técnicas más adecuadas para los procedimientos de análisis y gestión de riesgos de seguridad de sistemas de información.

I **Guía para Responsables del Dominio protegible**

- I Dirigida a los Directivos cuyas Organizaciones utilicen sistemas de información.
- I La corresponsabilidad en materia de seguridad entre directivos, usuarios y técnicos tiene en MAGERIT un marco preciso.

Guías (III)

I **Guía para Desarrolladores de Aplicaciones**

- I Orientada a contemplar los mecanismos de seguridad apropiados durante el desarrollo de una aplicación.
- I Diseñada para ser utilizada como documento de referencia por los desarrolladores de aplicaciones.

I **Arquitectura de la información y especificaciones de la interfaz para el intercambio de datos**

Permite que un técnico informático estructure la información que ha de intercambiar en todo producto informatizado semejante o relacionado con la herramienta MAGERIT.

I **Referencia de Normas legales y técnicas**

Referencia a la documentación normativa en materia de seguridad a fecha 31.12.96

Herramientas oficiales

I **Herramienta 1** (*Introductoria*)

Apoyo para la identificación de riesgos menores a los que bastará aplicar globalmente medidas básicas de seguridad 'práctica' y de riesgos mayores a cada uno de los cuales será necesario aplicar un nuevo Análisis y Gestión de Riesgos más detallado.

I **Herramienta 2** (*Avanzada*)

Permite realizar un Análisis y Gestión de riesgos detallado y afrontar así proyectos de complejidad media o alta en materia de seguridad.

Conclusiones

- | *MAGERIT estudia los peligros a los que se encuentra expuesto un sistema de información y el entorno que le rodea de una forma escalonada.*
- | *Da cobertura a cualquier tipo de posible sistema de información, independientemente de su complicación o importancia.*
- | *Se adapta a la complejidad de los sistemas, ya que permite ser aplicado en mayor o menor profundidad.*
- | *Una iniciativa a tener en cuenta por 2 razones:*
 - | *Es fruto del trabajo de una organismo de gran reputación como es el Ministerio de Administraciones Públicas*
 - | *Es una metodología de carácter público y su utilización no requiere autorización previa.*

Bibliografía

- [1] **Ministerio de Administraciones Públicas.** *Metodología de Análisis y Gestión de Riesgos MAGERIT* Coeditado por el Ministerio de Administraciones Públicas y el Boletín Oficial del Estado. ISBN 84-340-0960-9. Incluye un CD con la Herramienta 1 Introductoria.
- [2] **Sánchez - Ignoto** *La seguridad informática* 1991
- [3] **Lamere** *La Seguridad Informática. Metodología* 1985
- ! **URLs:**
- [4] *Web del Ministerio de Administraciones Públicas. Consejo Superior de Informática:*
www.map.es/csi/csi.htm
- [5] *Las Siete Guías Metodológicas:*
www.map.es/csi/herramientas/GuiasMagerit.exe
- [6] *Herramienta MAGERIT:*
www.map.es/csi/herramientas/HerramientaMagerit.exe
- [7] *Foro MAGERIT:*
<http://foro.map.es/>
- [8] *Herramienta chinchon versión 1.3 :*
<http://jungla.dit.upm.es/~pepe/chinchon/README.htm>

Fin

¡Gracias!

F. Expósito Gutiérrez