

El ENS y la Metodología de AR.

Hace ya un tiempo que se comenzaron las implantaciones del ENS allá donde hay presupuesto para ello. Personalmente no he participado en ninguna, y bien que lo lamento, pero si estoy en contacto con gente que trabaja en ello, tanto personal de la Administración como consultores.

Una cosa que me llamó la atención desde un principio fue si la propia Administración es usuaria de sus propias metodologías, es decir, si [MAGERIT](#) es un estándar de facto dentro de la Administración.

Desde luego la conclusión es clara: SI.

El primero en contestar afirmativamente a esta pregunta fue alguien del Ministerio de Defensa quien me confirmó que MAGERIT es la metodología de AR utilizada en proyectos OTAN. No solo esto sino que además me confirmaron que la herramienta EAR/PILAR, dispone de una biblioteca específica de amenazas, probabilidades etc diseñada por comités internos de la OTAN. PILAR dispone de una herramienta adicional llamada RMAT (Herramientas Adicionales para la Gestión del Riesgo) que permite definir o modificar catálogos de amenazas y salvaguardias.

Por su trabajo, esta persona me confirma que en reuniones conjuntas con distintos ministerios y relativas a gestión de seguridad, nunca se pone en duda que MAGERIT sea la metodología de AR a utilizar.

Naturalmente la persona que me aporta esta información tiene la suficiente graduación (es militar) y puesto funcional dentro del Ministerio de Defensa.

Hace unos días me contestaron a un correo que envié solicitando datos sobre MAGERIT. Lo hicieron desde la Dirección General para el Impulso de la Administración Electrónica y me comentaron que además de en proyectos OTAN, se utiliza en proyectos desarrollados con el Consejo de Europa.

En este correo se afirma categóricamente que MAGERIT tiene una fuerte implantación en la Administración española y que es muy poco probable el uso de otra metodología. Así mismo me informaron que CRAMM va a dejar de ser soportada por Siemens, que en su momento adquirió Insight Consulting que fue la empresa que la desarrolló. Ya no es utilizada por el Gobierno británico.

¿Qué dice el ENS al respecto?.

“Artículo 13. Análisis y gestión de los riesgos.

1. Cada organización que desarrolle e implante sistemas para el tratamiento de la información y las comunicaciones realizará su propia gestión de riesgos.

*2. Esta gestión se realizará por medio del análisis y tratamiento de los riesgos a los que está expuesto el sistema. **Sin perjuicio de lo dispuesto en el anexo II, se empleará alguna metodología reconocida internacionalmente.***

3. Las medidas adoptadas para mitigar o suprimir los riesgos deberán estar justificadas y, en todo caso, existirá una proporcionalidad entre ellas y los riesgos.”

¿Es MAGERIT una metodología reconocida internacionalmente?.

No existe un “catálogo oficial” de metodologías reconocidas internacionalmente pero tenemos algunos indicadores claros:

- Su uso en proyectos OTAN y de la Comisión Europea.
- La European Network and Information Security Agency (ENISA) así la considera en sus métodos de valoración del riesgo (http://rm-inv.enisa.europa.eu/methods_tools/m_magerit.html)

Más adelante, el propio ENS dice en el ANEXO II:

“4.1 Planificación [op.pl].

4.1.1 Análisis de riesgos [op.pl.1].

Categoría BÁSICA

*Bastará un análisis informal, realizado en **lenguaje natural**. Es decir, una exposición textual que describa los siguientes aspectos:*

- a) Identifique los activos más valiosos del sistema.*
- b) Identifique las amenazas más probables.*
- c) Identifique las salvaguardas que protegen de dichas amenazas.*
- d) Identifique los principales riesgos residuales.*

Categoría MEDIA

*Se deberá realizar un análisis semi-formal, usando **un lenguaje específico, con un catálogo básico de amenazas y una semántica definida**. Es decir, una presentación con tablas que describa los siguientes aspectos:*

- a) Identifique y valore cualitativamente los activos más valiosos del sistema.*
- b) Identifique y cuantifique las amenazas más probables.*
- c) Identifique y valore las salvaguardas que protegen de dichas amenazas.*
- d) Identifique y valore el riesgo residual.*

Categoría ALTA

*Se deberá realizar un análisis formal, usando **un lenguaje específico, con un fundamento matemático reconocido internacionalmente**. El análisis deberá cubrir los siguientes aspectos:*

- a) Identifique y valore cualitativamente los activos más valiosos del sistema.*
- b) Identifique y cuantifique las amenazas posibles.*
- c) Identifique las vulnerabilidades habilitantes de dichas amenazas.*
- d) Identifique y valore las salvaguardas adecuadas.*
- e) Identifique y valore el riesgo residual.”*

¿Qué es un fundamento matemático reconocido internacionalmente?. Siendo purista se podría pensar que existe una forma exacta y “matemática” de hacer un análisis de riesgos, pero nada más lejos de la realidad. El cálculo matemático de un riesgo siempre se basa en valoraciones subjetivas muy variables dependiendo del activo, amenaza, vulnerabilidad, probabilidad, entorno etc.

Cualquier metodología consistente propone fórmulas matemáticas para el cálculo del riesgo, pero eso no significa que dos personas usando la misma metodología lleguen a los mismos valores.

En cualquier caso, MAGERIT si tiene un modelo matemático basado en fórmulas para calcular degradaciones, impactos etc (Ver MAGERIT versión 2 – III Guía de Técnicas).

¿Qué piensan los profesionales?.

Pues como es lógico el abanico de opiniones es muy amplio. Hay quien reprocha a MAGERIT el poco uso que tiene como herramienta de tratamiento del riesgo. Personalmente pienso que es lógico, MAGERIT no es una herramienta de tratamiento, lo es de análisis.

Hay quienes ven en EAR/PILAR (herramienta que implementa MAGERIT) algo tremendamente rígido. Otras opiniones van en sentido contrario. Hay quienes incluso opinan que dado que tiene un sistema de catálogos que se puede cargar en la herramienta, es perfectamente válida para empresas privadas o cualquier otra organización, de hecho se vende a empresas privadas.

Como la mejor manera de hacerse una idea es comprobarlo uno mismo, yo me he instalado PILAR ENS 5.1 y llevo ya unas cuantas horas. No me parece rígido, me parece muy completo y con un excelente sistema de ayuda. Es el consultor quien controla el proceso porque controla la herramienta y no al revés.

Es difícil por no decir imposible, sacar una valoración en foros o puntos de opinión al respecto. Como siempre ocurre, cada uno valora positivamente aquello que conoce y controla.

A tener en cuenta.

El documento CCN-STIC-001 publicado por el Centro Criptológico Nacional con el título SEGURIDAD DE LAS TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES QUE MANEJAN INFORMACIÓN NACIONAL CLASIFICADA EN LA ADMINISTRACIÓN.

Este documento tiene como alcance:

“17. Esta Política es de aplicación a todos los Sistemas que manejen información nacional clasificada¹ en la Administración.

18. Los responsables de Sistemas de la Administración que manejen información no clasificada podrán hacer uso voluntario de este documento.”

En cuanto a MAGERIT dice:

“64. Por ello, el análisis y gestión de riesgos de seguridad estará presente en el proceso de desarrollo del sistema. Esta actividad será realizada coordinadamente por los responsables de diseño y operación utilizando la metodología MAGERIT y sus herramientas de apoyo. El objetivo de esta actividad será asegurara que se cumplen los requisitos mínimos de aplicación a la información nacional clasificada.”

“78. Cada organismo que desarrolle e implante sistemas realizará su gestión de riesgos

¹ *La Administración clasifica la información en 5 niveles: secreto, reservado, confidencial, difusión limitada y sin clasificar*

de acuerdo a unos criterios comunes proporcionados por la Autoridad de Acreditación. Se empleará la metodología MAGERIT y las herramientas que la soporten para realizar este proceso.”

Cuando dice “las herramientas que la soporten” es evidente que se está refiriendo a EAR/PILAR y/o microPILAR.

Conclusión.

Por desgracia la conclusión no deja de ser otra pregunta: ¿Va a permitir la Administración el uso de otras metodologías de AR que no sean MAGERIT?.

De momento no hay ninguna obligatoriedad y por lo tanto se puede usar cualquier metodología que se ciña a los requerimientos. Con el tiempo veremos si se establece MAGERIT con carácter obligatorio.

Rafael González