Herramienta PILAR

En el Portal de la Administración Electrónica está disponible la información sobre la metodología MAGERIT: Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información

http://administracionelectronica.gob.es/pae_Home/pae_Documentacion/pae_Metodolog/pae_Magerit.html

Es recomendable consultar los aspectos básicos de MAGERIT 3.0. Podéis además descargar el **Libro I: Método**, para utilizarlo como material de consulta.

PILAR es una herramienta que implementa la metodología MAGERIT de análisis y gestión de riesgos, desarrollada por el Centro Criptológico Nacional (CCN) y de amplia utilización en la administración pública española.

Se puede descargar del Portal del CCN-CERT en:

https://www.ccn-cert.cni.es/herramientas-de-ciberseguridad/ear-pilar.html

Antes de empezar a usar la herramienta PILAR, es recomendable también leer la descripción del ejemplo **Análisis de Riesgos en la AEMET** de aplicación de Magerit con esta herramienta (aunque sea de la versión 2 puede servir como guía): http://administracionelectronica.gob.es/pae_Home/dms/pae_Home/documentos/Documentacion/Metodologias-y-guias/Mageritv3/MAGERIT_-_Analisis_de_riesgos_en_la_AEMET.pdf

Manual de PILAR (Versión 6.2)

https://www.ccn-cert.cni.es/pdf/guias/series-ccn-stic/400-guias-generales/2133-ccn-stic-470-h1-manual-de-la-herramienta-de-analisis-de-riesgos-pilar-6-2/file.html

Realización de la práctica

Arrancad la **herramienta PILAR**, seleccionando el modo **Presentación**, y ejecutad el programa con la configuración de ***Análisis y Gestión de Riesgos, en modo cualitativo***. Abrid el fichero de ejemplo (**ejemplo_es.mgr**).

1.- Comprobad los campos que aparecen en la descripción del **Proyecto.**

Indicad las dimensiones de seguridad contempladas en el proyecto. Poned algunos ejemplos de los criterios considerados para la Valoración de los activos.

2.- Análisis de Riesgos: explorad los apartados: **activos**, **dependencias entre activos**, **amenazas**.

Anotad algunos (al menos 5) ejemplos de cada apartado. Localizad a qué activos afectan los errores de usuario y a qué activos afecta el fuego. Buscad ejemplos de amenazas que afecten a los datos de los usuarios, y amenazas que afecten al procesado de datos. Identificad alguna de las amenazas con mayor impacto.

3.- Explorad las **salvaguardas**.

Poned algún ejemplo de salvaguardas de los siguientes tipos: para la protección de las comunicaciones, para la identificación y autenticación, para la protección del perímetro físico, para la protección de la información, y para la gestión de claves criptográficas.

4.- Abrid la ventana de **Impacto y Riesgo**-> Valores acumulados (Impacto).

Poned algún ejemplo de impacto potencial más elevado, y de menos relevante, indicando a qué activo y dimensión afectan. Explicad la diferencia entre las fases "Potencial", "Actual", y "Objetivo".

5.- En el apartado **Perfiles de seguridad**: observad los aspectos cubiertos en los informes de seguridad según las normas ISO/IEC 27002 (Buenas prácticas, versión 2013) y según el Reglamento LOPD.

Anotad algunos ejemplos del grado de cumplimiento de cada una de las normas.