



PILAR – CCN CERT

¿Qué es PILAR?

La aplicación CHINCHÓN para análisis de riesgos podría considerarse como la precursora de PILAR.

PILAR es un conjunto de herramientas EAR (Entorno de Análisis de Riesgos) cuya función es el análisis y la gestión de riesgos de un sistema de información siguiendo la metodología Magerit (Metodología de Análisis y Gestión de Riesgos de los sistemas de información) y está desarrollada y financiada principalmente por el CCN. Sufre actualizaciones periódicas y existen diversas variantes (Versión Íntegra, Pilar Basic, μ Pilar – Versión Reducida, RMat – Personalizada). Permite la gestión de riesgos en cinco dimensiones: confidencialidad, integridad, disponibilidad, autenticidad y trazabilidad (accountability).

PILAR está dirigida a todas aquellas organizaciones/organismos que cuentan con infraestructuras de TIC y que tienen la necesidad de gestionar de forma eficiente sus activos, realizando Análisis de Impacto y Continuidad de las Operaciones, tanto de manera cuantitativa como cualitativa.

Es de uso libre para todas las AAPP y de pago para la empresa privada, aunque su coste es bastante reducido para las capacidades que tiene y en comparación con otras herramientas similares del mercado. A partir de 1.500 euros licencia/año. Es autoinstalable, traducida a 8 idiomas, dispone de un módulo específico para el **cumplimiento del ENS**, verificación del RGPD y se integra con otras herramientas del CCN – CERT como INÉS – AR.

Los requisitos son contar con un ordenador personal cuyo SO sea MAC, Linux o Windows y máquina virtual java 2 (lenguaje de programación java), opcionalmente se puede usar un repositorio de tipo base de datos con acceso a SQL.

Los objetivos perseguidos por la herramienta Pilar son realizar el análisis de riesgos según la metodología Magerit e ISO/IEC 27005 para el diseño del plan de mejora de la seguridad. Una vez conocidos los riesgos, se pueden determinar una serie de salvaguardas y estimar el riesgo residual. El tratamiento del riesgo es un proceso continuo y recurrente en el que el sistema de protección se va mejorando regularmente para afrontar nuevos riesgos y aumentar la confianza que el sistema merece para los responsables y los usuarios.

Los resultados que se obtienen con el uso de la herramienta son:

- Impacto potencial y residual.
- Riesgo potencial y residual.
- Mapa de riesgos.
- Plan de mejora de la seguridad.
- Monitorización continua del Estado de Riesgo.

Sus ventajas principales se centran en conocer los Riesgos a fin de poder tratarlos, conocer el grado de cumplimiento de diferentes perfiles de seguridad: ISO 27002, protección de datos de carácter personal (RGPD), ENS, etc., e implementar la metodología Magerit e ISO/IEC 27005.

En definitiva, PILAR interesa a todos aquellos que trabajan con información mecanizada y los sistemas informáticos que la tratan. Si dicha información o los servicios que se prestan gracias a ella son valiosos, PILAR les permitirá saber cuanto de este valor está en juego y les ayudará a protegerla.

Jorge Noguerales.

Miembro del área de trabajo de Ciberseguridad de AES