Auditoría informática basada en el Análisis de Riesgos

Trabajo sesión seminario 09 de mayo ACG
Curso 2022-2023

1. Auditoría informática basada en el Análisis de Riesgos

La auditoría informática basada en riesgos es una técnica que permite enfocar los recursos de auditoría hacia los puntos de mayor importancia dentro de las organizaciones [1]. Los planes de auditoría tradicionales tienden a centrarse en los controles que ya tiene implementados y si funcionan correctamente o no. Las auditorías basadas en riesgos comienzan examinando los riesgos inherentes a los que se enfrenta la empresa (identificados por la gerencia y la junta directiva) y luego buscan corregir y reformular sus controles de acuerdo con los riesgos más urgentes y con mayor potencial de pérdida.

Esta técnica está más en consonancia con un enfoque de gestión de riesgos empresariales, ya que examina la organización como un todo en lugar de por departamento, como en una metodología de auditoría tradicional.

2. Metodología Magerit

Magerit[1] es el acrónimo de Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información, creado por el Consejo Superior de Administración Electrónica. El uso de esta metodología es de carácter público, pertenece al Ministerio de Administraciones Públicas español.

Magerit mide la vulnerabilidad por la frecuencia histórica cuantitativa de la materialización de la amenaza sobre el activo, cuando es factible (fiabilidad de un componente hardware, número de fallos de software); o bien por la potencialidad cualitativa de dicha materialización, cuya primera aproximación lleva a emplear una escala vista en las amenazas potenciales (consideradas ahora reales, o sea agresiones).

Esta metodología está dirigida a los medios electrónicos, informáticos y telemáticos, lo cual ha dado lugar al origen de ciertos riesgos que se deben de evitar con medidas preventivas para lograr tener confianza en utilizarlos. No es posible una aplicación racional de medidas de seguridad sin antes analizar los riesgos para, así implantar las medidas proporcionadas a los riesgos, al estado de la tecnología y a los costes (tanto de la ausencia de seguridad como de las salvaguardas).

La figura 1 muestra una captura de pantalla de la página web de la Administración Electrónica española desde donde se puede descargar la última versión de Magerit.

[1] https://administracionelectronica.gob.es/pae_Home/pae_Documentacion/pae_Metodolog/pae_Magerit.html

Figura 1. Web de la administración electrónica con la última versión de Magerit para descarga

3. Herramienta PILAR

PILAR[2] es el acrónimo de Procedimiento Informático-Lógico para el Análisis de Riesgos. Es una herramienta que implementa la metodología MAGERIT, desarrollada por el Centro Criptológico Nacional y de amplia utilización en la administración pública española. Utilizando esta herramienta se puede hacer todas las actividades que se realizan en el Análisis y Gestión de Riesgos:

- Determinación de Activos: Identificación, dependencias y valoración.
- Determinación de Amenazas
- Estimación de Impactos
- Determinación de los criterios de aceptación del riesgo
- Determinación de las medidas de seguridad necesarias o Salvaguardas.

Este software permite hacer un análisis de riesgos sobre las dimensiones de valoración como son: confidencialidad, integridad, disponibilidad, autenticidad y trazabilidad. Además, ayuda con el cálculo del impacto y el riesgo, acumulado, repercutido, potencial y residual. La figura 2 muestra una captura de la pantalla principal de PILAR.

Las salvaguardas se califican por fases, permitiendo la incorporación a un mismo modelo de diferentes situaciones temporales. Típicamente se puede incorporar el resultado de los diferentes proyectos de seguridad a lo largo de la ejecución del plan de seguridad,

[2] https://pilar.ccn-cert.cni.es/

monitorizando la mejora del sistema. PILAR puede hacer análisis cuantitativo y cualitativo. Los resultados se presentan en diversos formatos como gráficas y tablas.

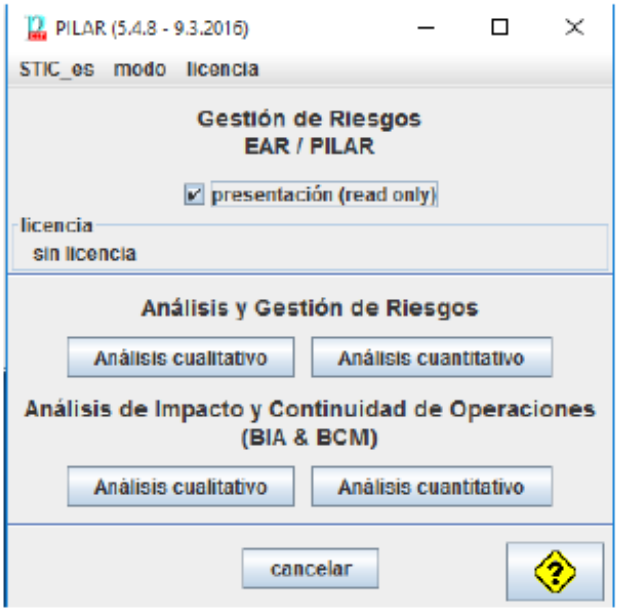

Figura 2. Pantalla Principal Pilar

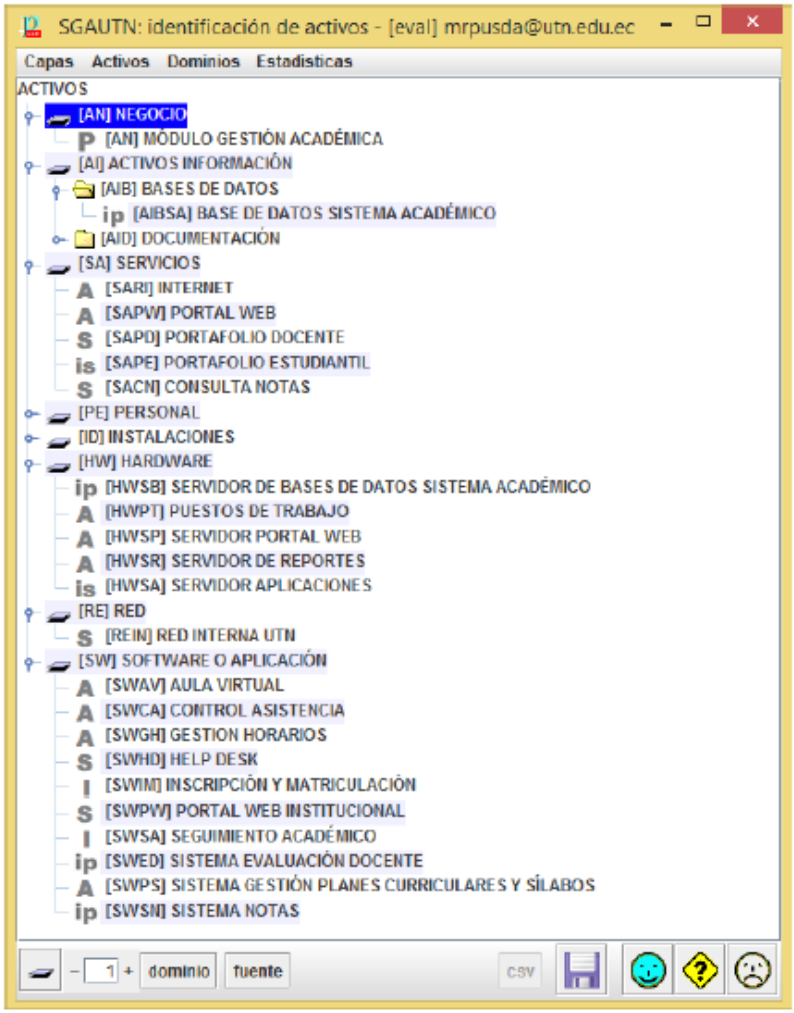

Figura 3. Pantalla Pilar con la identificación de activos

4. Caso práctico

En [2] se presenta un caso práctico de auditoría informática basada en riesgos utilizando la herramienta PILAR. El caso práctico considera la infraestructura tecnológica del departamento de informática de la UTN, Universidad Técnica del Norte, relacionados con el Módulo de Gestión Académica del Sistema Integrado Universitario.

La figura 3 muestra una captura de pantalla de PILAR con el listado de activos clasificados por su función.

La figura 4 muestra las recomendaciones de Pilar asociadas a cada uno de los Activos.

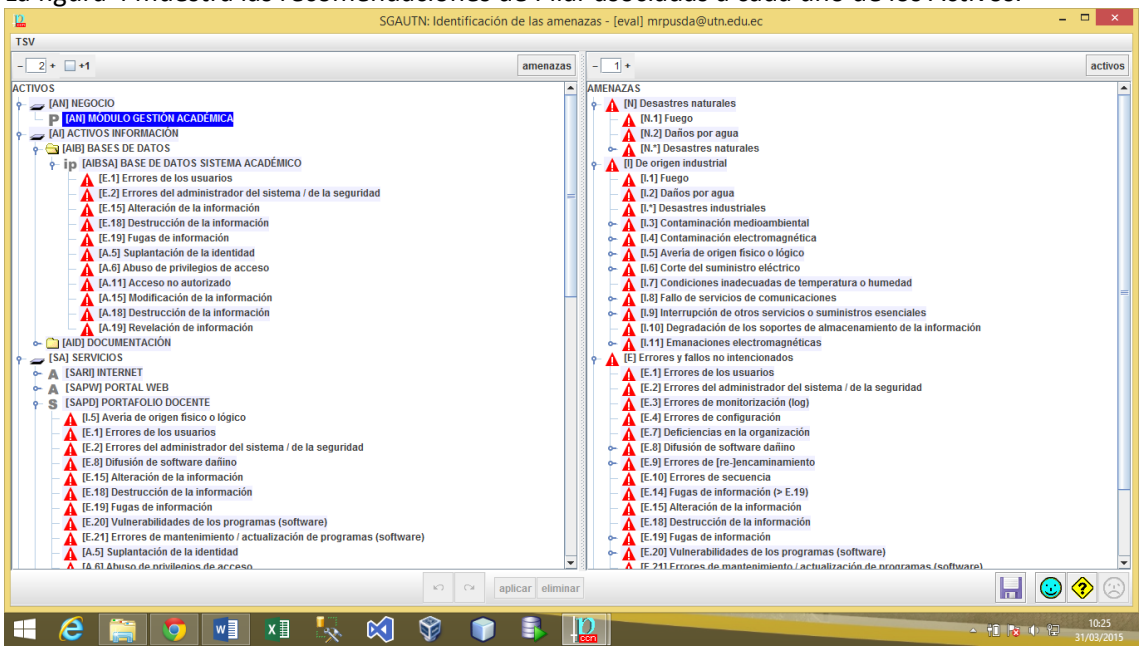

Figura 4. Pantalla Pilar con Amenazas módulo Gestión Académica

La figura 5 detalla los porcentajes de valoración recomendados por Pilar para los Activos.

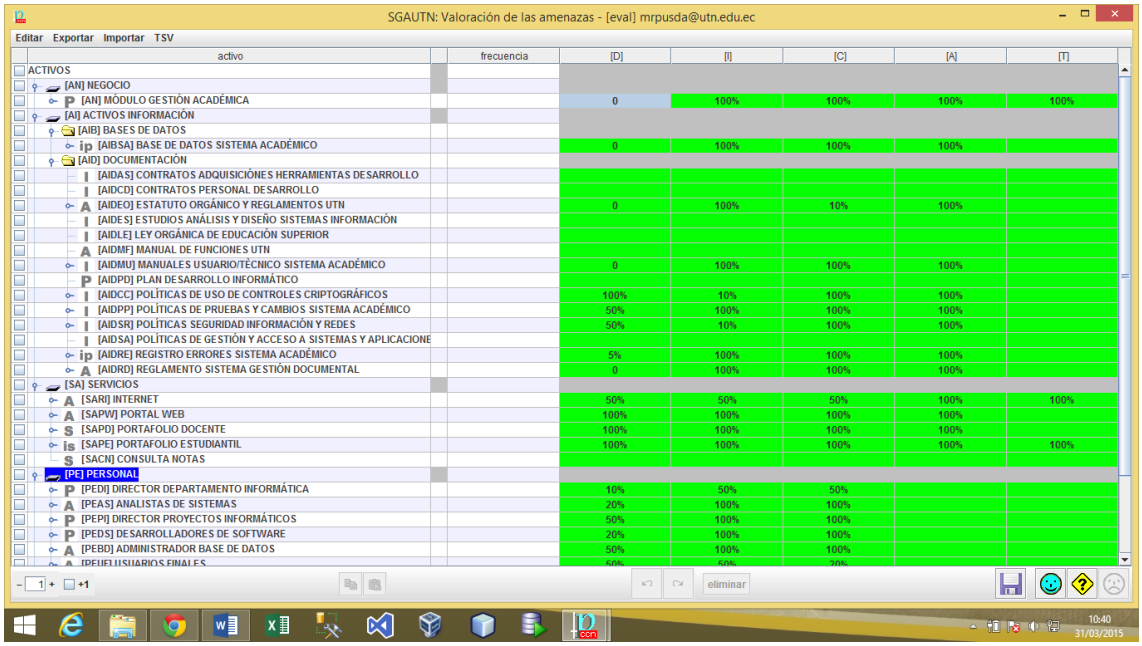

Figura 5. Pantalla Pilar con Valoración Amenazas Módulo Gestión Académica.

5. Reflexión

Reflexiona acerca de cuál crees que es el papel del auditor informático en una auditoría informática basada en riesgos, ¿cuál debe ser su función?.

Fuentes

[1] Auditoria informática basado en el análisis de riesgos de la empresa TecniSeguros S.A. Julio Cesar Calderón Carrasco y David Adolfo Ocaña Aldaz

[2] Fundamentos de auditoría informática basada en riesgos. Daisy Elizabeth Imbaquingo Esparza, Marco Remigio Pusdá Chulde, y José Guillermo Jácome León. Editorial Ibarra-Ecuador.