

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

Magerit¹ 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

Castellano | Català | Euskara | Galego | Valencià | English Escuchar

PAE portal administración electrónica

Actualidad | Estrategias | Soluciones - CTT | Observatorio - OBSAE | Documentación

Estás en: [Portal de la Administración Electrónica](#) > [Portada de Documentación](#) > [Portada de Metodologías y Guías](#) > [Portada de Gestión de Riesgos de los Sistemas de Información](#)

Documentación

Legislación nacional ▾

Legislación autonómica ▾

Legislación Unión Europea ▾

Metodologías y Guías ▴

Portada de Metodologías y Guías



MAGERIT v.3 : Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información

 Valorar
  Opinar
  Escuchar
  Imprimir PDF
  Compartir

Documentación

▶ **MAGERIT versión 3 (versión español): Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información.** - Edita: © Ministerio de Hacienda y Administraciones Públicas, octubre 2012.- NIPO: 630-12-171-8

 [Libro I: Método \(PDF-1,47 MB\)](#)

 [Libro II: Catálogo de Elementos \(PDF-3,37 MB\)](#)

 [Libro III: Guía de Técnicas \(PDF-1,28 MB\)](#)

▶ **MAGERIT V.3 (English version): Methodology for Information Systems Risk Analysis and Management.** - Edita: © Ministerio de Hacienda y Administraciones Públicas, julio 2014.- NIPO: 630-14-162-0

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

3. Herramienta PILAR

PILAR² 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.

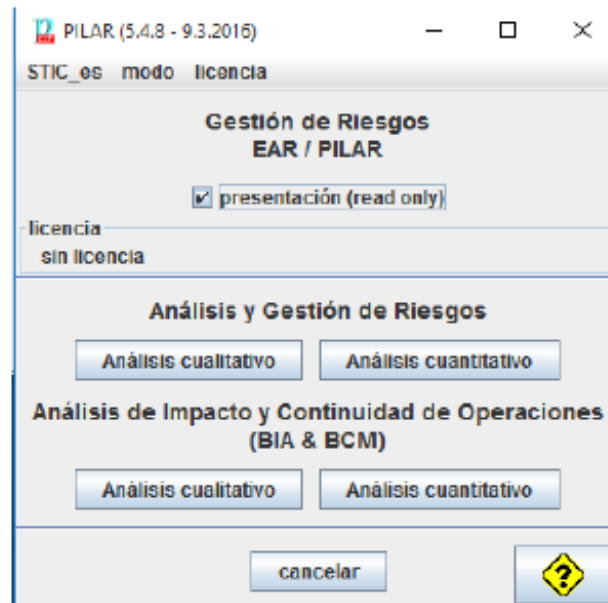


Figura 2. Pantalla Principal Pilar

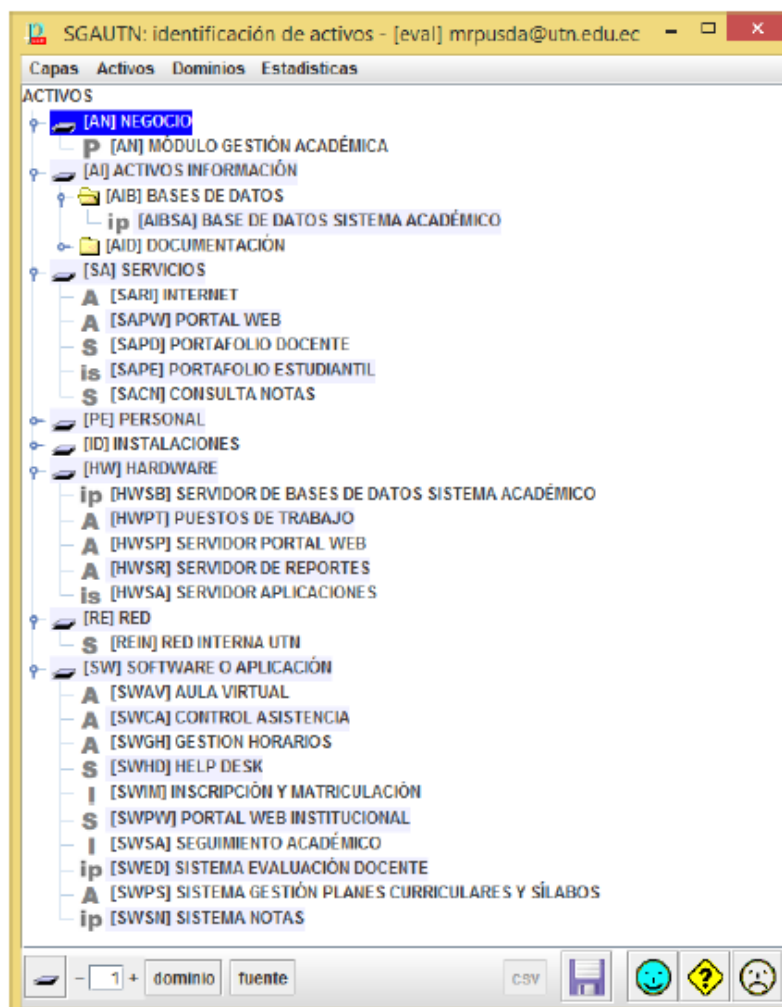


Figura 3. Pantalla Pilar con la identificación de activos

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.

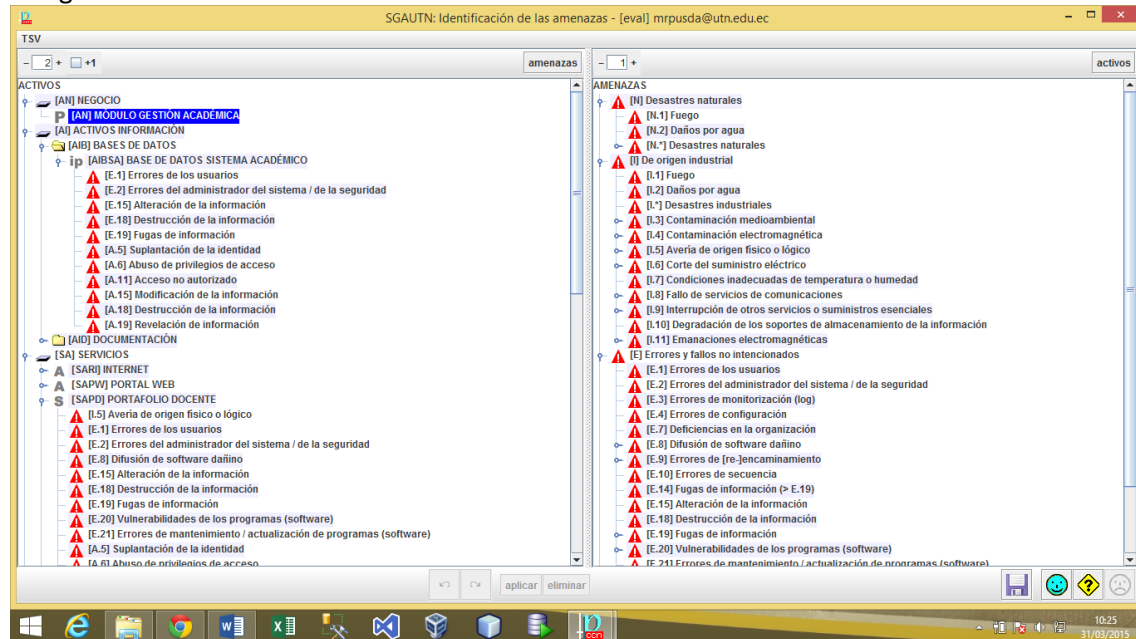


Figura 4. Pantalla Pilar con Amenazas módulo Gestión Académica

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

The screenshot shows the PILAR tool interface with the title 'SGAUTN: Valoración de las amenazas - [eval] mrpusda@utn.edu.ec'. It displays a table with columns for 'activo', 'frecuencia', '[D]', '[I]', '[C]', '[A]', and '[T]'. The table lists various assets and their corresponding recommended valuation percentages. The assets are categorized into '[AN] NEGOCIO', '[AN] MÓDULO GESTIÓN ACADÉMICA', '[AI] ACTIVOS INFORMACIÓN', '[AI] BASES DE DATOS', '[AI] DOCUMENTACIÓN', '[SA] SERVICIOS', and '[SA] INTERNET'. The valuation percentages are shown in green cells, indicating a high level of risk or importance for most assets.

activo	frecuencia	[D]	[I]	[C]	[A]	[T]
[AN] NEGOCIO						
[AN] MÓDULO GESTIÓN ACADÉMICA		0	100%	100%	100%	100%
[AI] ACTIVOS INFORMACIÓN						
[AI] BASES DE DATOS						
[AI] [AIBSA] BASE DE DATOS SISTEMA ACADÉMICO		0	100%	100%	100%	
[AI] [AID] DOCUMENTACIÓN						
[AI] [AIDAS] CONTRATOS ADQUISICIONES HERRAMIENTAS DE DESARROLLO						
[AI] [AIDCD] CONTRATOS PERSONAL DESARROLLO						
[AI] [AIDEO] ESTATUTO ORGÁNICO Y REGLAMENTOS UTN		0	100%	10%	100%	
[AI] [AIDES] ESTUDIOS ANÁLISIS Y DISEÑO SISTEMAS INFORMACIÓN						
[AI] [AIDLE] LEY ORGÁNICA DE EDUCACIÓN SUPERIOR						
[AI] [AIDMF] MANUAL DE FUNCIONES UTN						
[AI] [AIDMUJ] MANUALES USUARIO/TÉCNICO SISTEMA ACADÉMICO		0	100%	100%	100%	
[AI] [AIDPD] PLAN DESARROLLO INFORMÁTICO						
[AI] [AIDCC] POLÍTICAS DE USO DE CONTROLES CRIPTOGRÁFICOS		100%	10%	100%	100%	
[AI] [AIDPP] POLÍTICAS DE PRUEBAS Y CAMBIOS SISTEMA ACADÉMICO		50%	100%	100%	100%	
[AI] [AIDSR] POLÍTICAS SEGURIDAD INFORMACIÓN Y REDES		50%	10%	100%	100%	
[AI] [AIDSA] POLÍTICAS DE GESTIÓN Y ACCESO A SISTEMAS Y APLICACIONES						
[AI] [AIDRE] REGISTRO ERRORES SISTEMA ACADÉMICO		5%	100%	100%	100%	
[AI] [AIDRD] REGLAMENTO SISTEMA GESTIÓN DOCUMENTAL		0	100%	100%	100%	
[SA] SERVICIOS						
[SA] [SARQ] INTERNET		50%	50%	50%	100%	100%
[SA] [SAPW] PORTAL WEB		100%	100%	100%	100%	100%
[SA] [SAPD] PORTAFOLIO DOCENTE		100%	100%	100%	100%	100%
[SA] [SAPJ] PORTAFOLIO ESTUDIANTE		100%	100%	100%	100%	100%
[SA] [SACN] CONSULTA NOTAS		100%	100%	100%	100%	100%
[PE] PERSONAL						
[PE] [PEJD] DIRECTOR DEPARTAMENTO INFORMÁTICA		10%	50%	50%		
[PE] [PEAS] ANALISTAS DE SISTEMAS		20%	100%	100%		
[PE] [PEPJ] DIRECTOR PROYECTOS INFORMÁTICOS		50%	100%	100%		
[PE] [PEDS] DESARROLLADORES DE SOFTWARE		20%	100%	100%		
[PE] [PEBD] ADMINISTRADOR BASE DE DATOS		50%	100%	100%		
[PE] [PEJF] ESTADÍSTICAS FINALES		10%	100%	100%		

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 Pusedá Chulde, y José Guillermo Jácome León. Editorial Ibarra-Ecuador.