Centro de
Investigación en
Computación

MAGERIT

Resumen

Background

Course

Ciberseguridad

Instructor

Acosta Bermejo Raúl

Lecture notes

2025-A
Febrero del 2025
Última actualizacioón

Instituto
Politécnico
Nacional

Table of contents (outline)

Tabla de contenido

1. Introducción
2. Descripción del Estándar
3. Catálogos
4. Técnicas
5. Varios temas

Introducción

Definiciones

Introducción

Definiciones

MAGERIT

Metodología de **A**nálisis y **GE**stión de **R**iesgos de los Sistemas de **I**nformación.

- Fue creado por el CSAE (**C**onsejo **S**uperior de **A**dministración **E**lectrónica).
- Da cumplimiento a las directrices de la OCDE (principio 6) y al Esquema Nacional de Seguridad de España.
- Versiones:
  - 1ª. 1997.
  - 2ª. 2006, intervalo de 9 años.
  - 3ª. 2012, intervalo de 6 años.
- Sigue la terminología de la normativa ISO 31000 y da cuumplimiento a la "Implementación de la Gestión de los Riesgos" de esta.
- Referencias
  - https://administracionelectronica.gob.es/pae_Home/pae_Documentacion/pae_Metodolog/pae_Magerit.html

Introducción

Definiciones

Documentos

- Está formado por:
  - Libro I: Método. 127 páginas.
  - Libro II: Catálogo de elementos. 75 páginas.
  - Libro III: Guía de Técnicas. 42 páginas.
- .

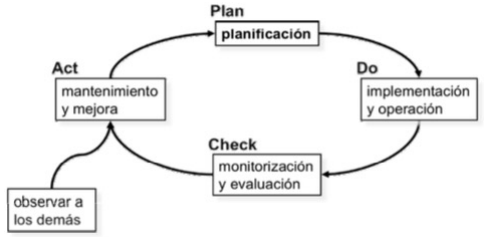


Ilustración 2. Ciclo PDCA

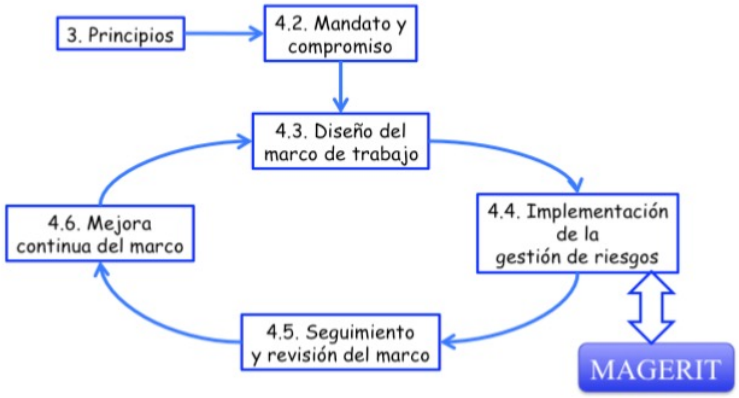


Ilustración 1. ISO 31000 - Marco de trabajo para la gestión de riesgos

Descripción del Estándar

Resumen

Descripción

Del estándar

MAGERIT

Define 3 elementos:

i. El proceso de gestión de riesgos.

ii. El método de análisis de riesgos.

Considera los siguientes elementos:

1. **Activos**. Son los elementos del sistema de información que soportan la misión de la Organización.
2. **Amenazas**. Son cosas que les pueden pasar a los activos causando un perjuicio a la Organización
3. **Salvaguardas**/Contramedidas. Son medidas de protección desplegadas para que aquellas amenazas no causen [tanto] daño.

Con estos elementos se puede estimar:

1. **Impacto**. Lo que podría pasar.
2. **Riesgo**. Lo que probablemente pase.

Descripción

Del estándar

Proceso

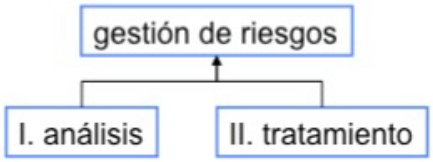


Ilustración 5. Gestión de riesgos

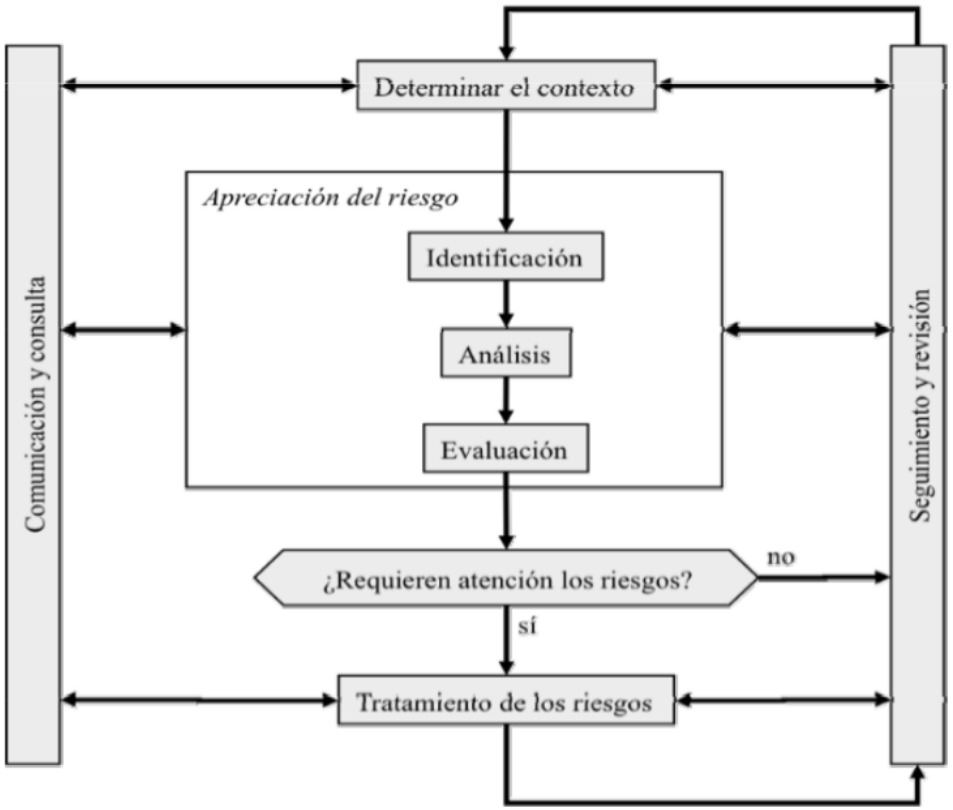


Ilustración 6. Proceso de gestión de riesgos (fuente: ISO 31000)

Descripción

Del estándar

MAR – Método de Análisis de Riesgos
MAR.1 – Caracterización de los activos
MAR.11 – Identificación de los activos
MAR.12 – Dependencias entre activos
MAR.13 – Valoración de los activos
MAR.2 – Caracterización de las amenazas
MAR.21 – Identificación de las amenazas
MAR.22 – Valoración de las amenazas
MAR.3 – Caracterización de las salvaguardas
MAR.31 – Identificación de las salvaguardas pertinentes
MAR.32 – Valoración de las salvaguardas
MAR.4 – Estimación del estado de riesgo
MAR.41 – Estimación del impacto
MAR.42 – Estimación del riesgo

Método

Pasos

1. Activos
   i. identifica Información y Servicios.
   ii. Otros temas son: dependencias, valoración, dimensiones.
2. Amenazas
   i. Identificación, valoración, impacto, riesgo
3. Salvaguardas
4. Impacto residual
5. Riesgo residual

Descripción

Del estándar

Zonas

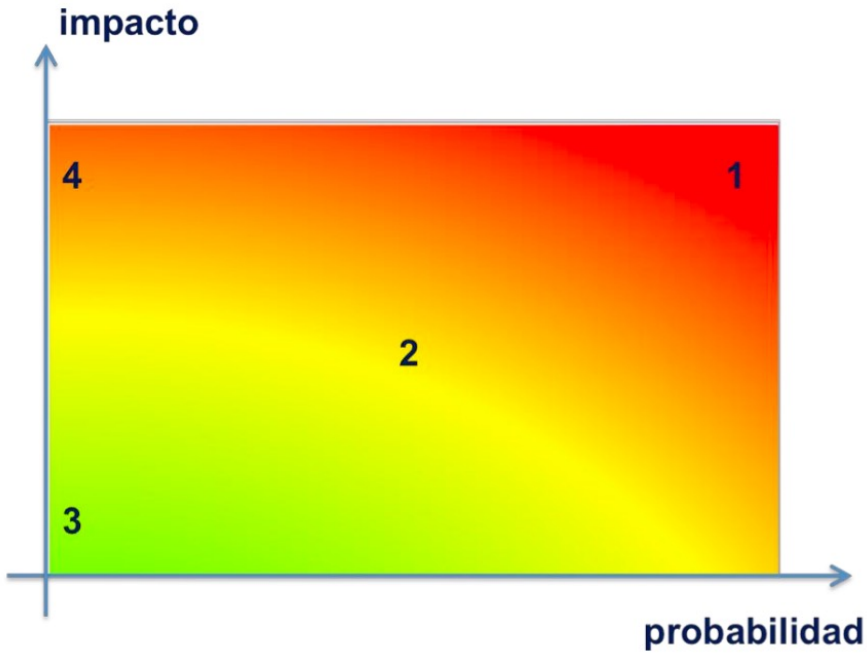


Ilustración 9. El riesgo en función del impacto y la probabilidad

Descripción

Del estándar

MA	muy alta	casi seguro	fácil
A	alta	muy alto	medio
M	media	posible	difícil
B	baja	poco probable	muy difícil
MB	muy baja	muy raro	extremadamente difícil

Tabla 1. Degradación del valor

Rangos

Impacto vs Probabilidad

MA	100	muy frecuente	a diario
A	10	frecuente	mensualmente
M	1	normal	una vez al año
B	1/10	poco frecuente	cada varios años
MB	1/100	muy poco frecuente	siglos

Tabla 2. Probabilidad de ocurrencia

Descripción

Del estándar

factor	nivel	significado
0%	**L0**	inexistente
	L1	inicial / ad hoc
	L2	reproducible, pero intuitivo
	L3	proceso definido
	L4	gestionado y medible
100%	**L5**	optimizado

Tabla 4. Eficacia y madurez de las salvaguardas

Salvaguardas

10 tipos

efecto	tipo
preventivas: reducen la probabilidad	[PR] preventivas [DR] disuasorias [EL] eliminatorias
acotan la degradación	[IM] minimizadoras [CR] correctivas [RC] recuperativas
consolidan el efecto de las demás	[MN] de monitorización [DC] de detección [AW] de concienciación [AD] administrativas

Tabla 3. Tipos de salvaguardas

Descripción

Del estándar

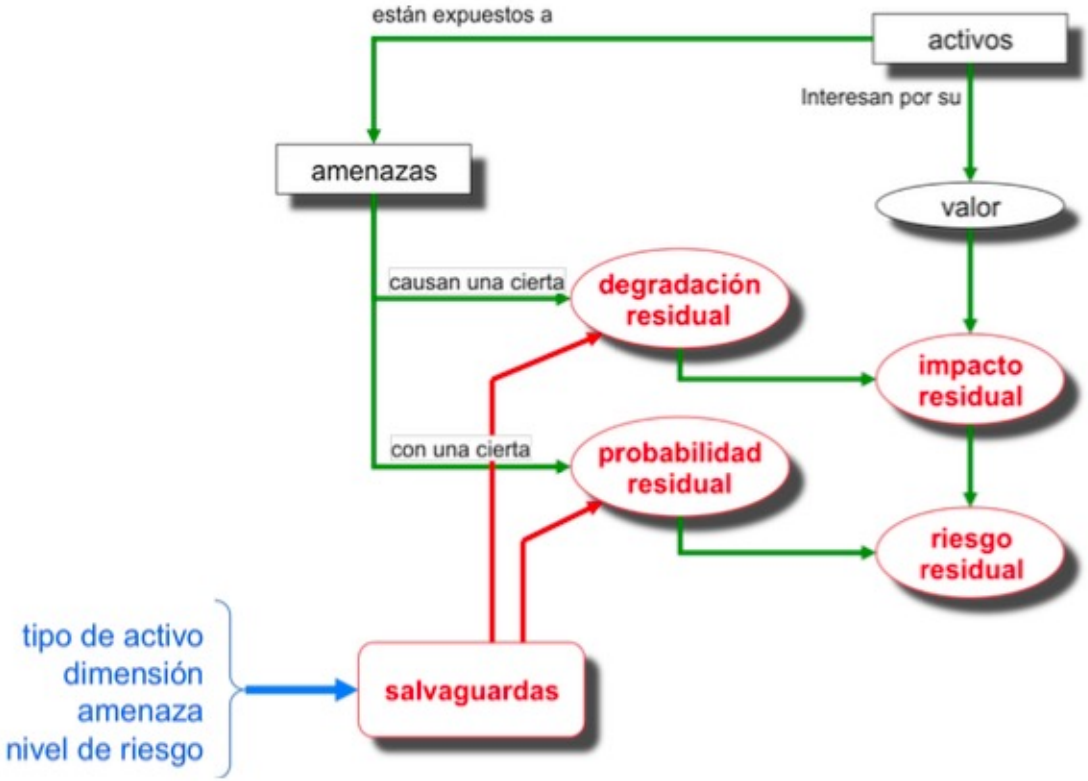


Ilustración 10. Elementos de análisis del riesgo residual

Catálogos del Estándar

Resumen

Catálogos

Del estándar

Amenazas

Lista y descripción

1. Desastres naturales.
   i. Fuego, Daños por agua, etc.
   ii. Total 3 tipos
2. De origen industrial.
   i. Fuego, Daños por agua.
   ii. Total 10 tipos
3. Errores y fallos no intencionados
   i. Difusión de software dañino.
   ii. Escapes de información.
   iii. Total 28 tipos
4. Ataques intencionados
   i. Manipulación de bitácoras.
   ii. Total 24 tipos

Catálogos

Del estándar

12 fichas

Apéndice 2. Fichas

Las siguientes secciones proporciona fichas para la captura de datos en un proyecto de análisis y gestión de riesgos.

Reproduzca las fichas siguientes, una por activo, del tipo que corresponda.

A2.1. [info] Activos esenciales: información

[info] Información	
código:	**nombre:**
descripción:	
propietario:	
responsable:	
tipo (marque todos los adjetivos que procedan) Ver Sección 2.1.	

Valoración de la información, típicamente en las siguientes dimensiones de seguridad:

- [I] integridad
- [C] confidencialidad
- [A] autenticidad de los datos
- [T] trazabilidad de los datos, quién ha modificado qué

Valoración		
dimensión	***valor***	***justificación***
[I]		
[C]		
[A]		
[T]		

Las dependencias normalmente identifican servicios y personas que manejan esta información:

Dependencias de activos inferiores (hijos)	
activo:	**grado:**

Catálogos

Del estándar

Plan

Programa$_1$, Programa$_2$, …, Programa$_N$

A4.6. Plan de seguridad

Conjunto de programas de seguridad que permiten materializar las decisiones de gestión de riesgos.

1. Marco de referencia
   - Política de seguridad de la organización
   - Relación de normas y procedimientos
2. Responsables y responsabilidades (a nivel de organización)
3. Programas de seguridad

   Por cada programa identificado:
   - objetivo genérico
   - prioridad o urgencia
   - ubicación temporal: ¿cuándo se llevará a cabo?
   - salvaguardas involucradas
   - unidad responsable de su ejecución
   - estimación de costes financieros
   - estimación de recursos
   - estimación de impacto para la organización

Cuando llega el momento para ser acometido, cada programa de seguridad debe detallar:

- Su objetivo genérico.
- Las salvaguardas concretas a implantar o mejorar, detallando sus objetivos de calidad, eficacia y eficiencia

Técnicas del Estándar

Resumen

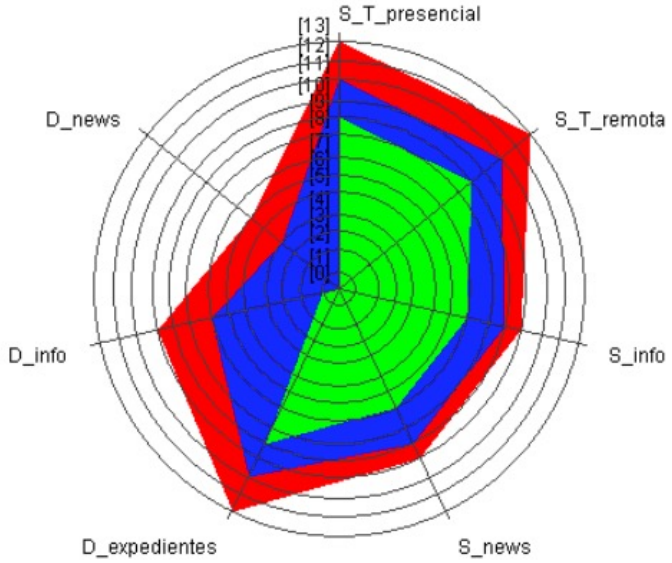
Técnicas

Del estándar

Propuestas

Utilizar

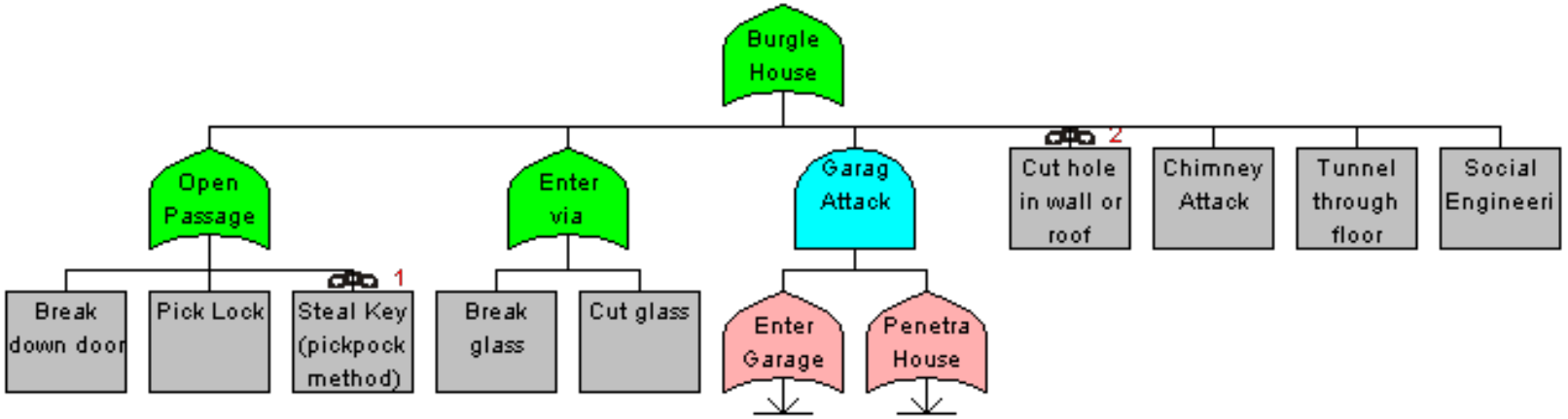
1. Tablas
2. Análisis algorítmico
3. Árboles de ataque
4. Gráficas
5. Técnica Delphi



Técnicas

Del estándar

Árboles de Ataque



Varios temas

A revisar personalmente

Resumen

Varios temas

Ejemplos

Framework
Evaluación de Riesgos

https://wikis.ec.europa.eu/pages/viewpage.action?pageId=50108960

MITIGATE

Ref. Ares(2018)1203121 - 05/03/2018

EUROPEAN COMMISSION

MITIGATE

Multidimensional, IntegraTed, rIsk assessment framework and dynamic, collaborative risk manaGement tools for critical information infrAstrucTrurEs

www.mitigateproject.eu

Grant Agreement No.653212
Topic: H2020-DS-2014-01
"Risk Management and Assurance Models"
Innovation Action

Deliverable D7.4

Repositories of Empirical Knowledge

Contractual Date of Delivery:	M30 / February 2018
Editor:	David Incertis, Rafael Company (VPF), Spyros Papstergiou, Eleni-Maria Kalogeraki (UPRC)
Work-package:	7
Distribution / Type:	PU
Version:	1.0
File:	D7.4_Repositories of Empirical Knowledge_final

The end

Contacto

Raúl Acosta Bermejo

http:www.cic.ipn.mx
http://www.ciseg.cic.ipn.mx/

racostab@ipn.mx
racosta@cic.ipn.mx

57-29-60-00
Ext. 56652