XII Jornadas STIC CCN-CERT

Ciberseguridad,
hacia una respuesta y disuasión efectivas

Enfoque unificado para el análisis de riesgos multinorma (ENS y RGPD) en las administraciones locales

centro criptológico nacional

- Elisa García Martín
- Ingeniería e Integración Avanzadas (Ingenia), S.A
- egmartin@ingenia.es

Índice

1. Introducción. El análisis de riesgos como requisito regulatorio.
2. ¿Cómo hacer el análisis de riesgos? Metodologías, herramientas y guías.
3. Un enfoque práctico del análisis de riesgos en la administración local.
4. Conclusiones.

Índice

Introducción. El análisis de riesgos como requisito regulatorio

¿Por qué un análisis de riesgos de seguridad de la información?

RIESGO: Estimación del **grado de exposición** a que una amenaza se materialice, causando un impacto en la organización.

ANÁLISIS Y GESTIÓN DE RIESGOS: **Proceso sistemático** para **estimar** la magnitud de los riesgos a que está expuesta la organización e identificar los mecanismos para **mitigarlos**.

PROTECCIÓN DE LA INFORMACÍÓN ORIENTADA A RIESGOS REALES: No sobreproteger, ni *infra*proteger

Introducción. El análisis de riesgos como requisito regulatorio

¿Qué normativa en Administración Pública exige un análisis de riesgos?

Esquema Nacional de Seguridad (ENS)	Reglamento General de Protección de Datos (RGPD) y Ley Orgánica (LOPD + GDD)
• **Artículo 6.** Gestión de la seguridad basada en riesgos • **Artículo 13.** Análisis y gestión de riesgos • **Medida de seguridad op.pl.1.** Análisis de riesgos	• **RGPD. Artículo 32**. Seguridad del tratamiento • **LOPD+gdd. Artículo 28**. Obligaciones generales del responsable y encargado del tratamiento
Disposición adicional primera LOPD + gdd. Medidas de seguridad en el ámbito del sector público	

Introducción. El análisis de riesgos como requisito regulatorio

¿Qué normativa en Administración Pública exige un análisis de riesgos?

Índice

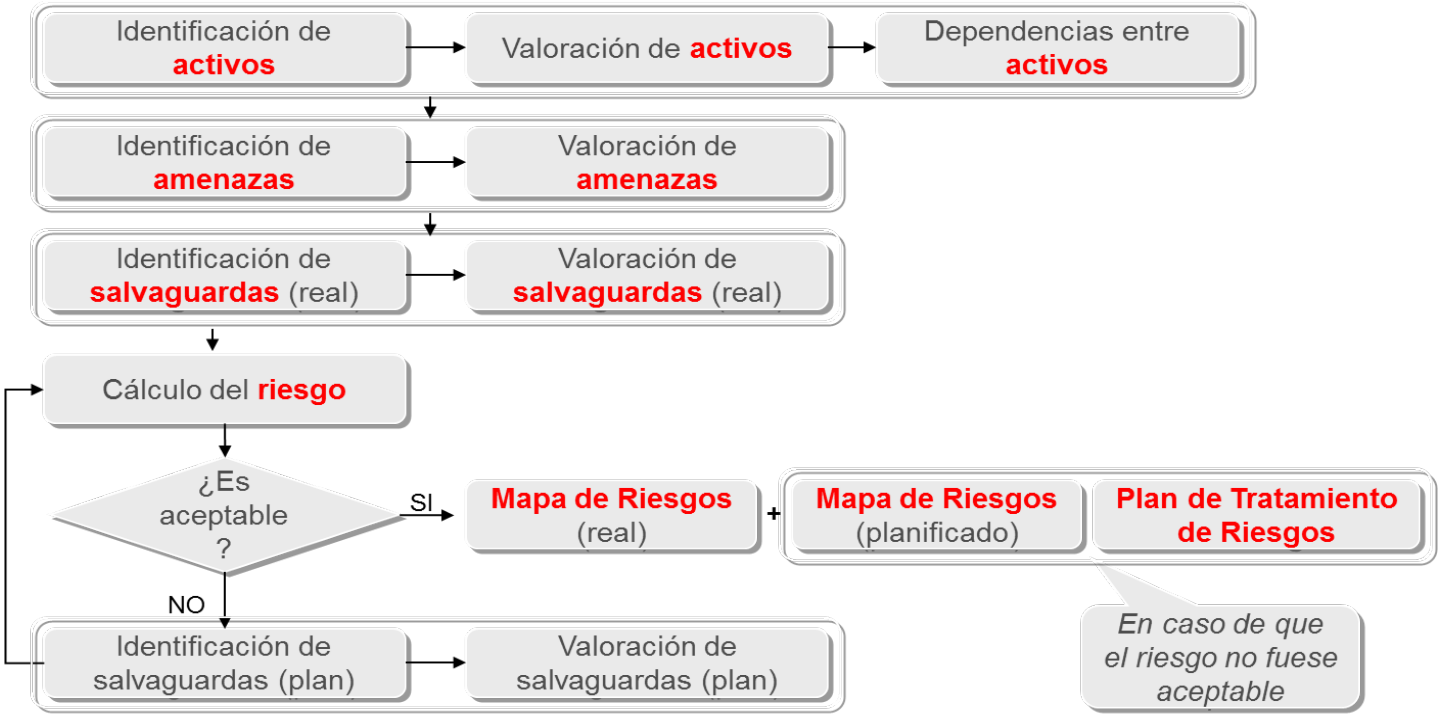
1. Introducción. El análisis de riesgos como requisito regulatorio.

2. **¿Cómo hacer el análisis de riesgos? Metodologías, herramientas y guías.**

3. Un enfoque práctico del análisis de riesgos en la administración local.

4. Conclusiones

Cómo hacer el análisis de riesgos. Metodologías, herramientas y guías



Cómo hacer el análisis de riesgos. Metodologías, herramientas y guías

magerit

Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información

</pilar>
Herramientas de análisis y gestión de riesgos.

Programa Informático Lógico para el Análisis de Riesgos (desarrollada y financiada parcialmente por el CCN.)

- ✓ La **metodología MAGERIT** garantiza el cumplimiento de la medida de seguridad op.pl.1 hasta categoría ALTA.
- ✓ Las **herramientas PILAR (PILAR, PILAR BASIC y µPILAR)** soportan el análisis y la gestión de riesgos de un sistema de información siguiendo la metodología MAGERIT.
- ✓ Ya existen **guías** sobre análisis de riesgos, MAGERIT y uso de las herramientas PILAR.

Cómo hacer el análisis de riesgos. Metodologías, herramientas y guías

Metodología y herramienta	magerit	pilar
Catálogo de Activos	Sistemas de información asociados a los servicios e información afectados por ENS y tratamientos de datos personales. Valorados en las dimensiones DICAT y, además, DP.	
Catálogo de amenazas	Además de las asociadas a desastres naturales/Industriales y errores Humanos intencionados/Inintencionados, se incluye el catálogo de amenazas para los derechos y libertades de las personas físicas (PR).	
Catálogo de salvaguardas	Controles del Anexo II del ENS. Medidas jurídicas del RGPD.	
Riesgos	Riesgos para los distintos activos, amenazas y dimensiones de seguridad (DICAT) y privacidad (DP).	

Índice

1. Introducción. El análisis de riesgos como requisito regulatorio.

2. ¿Cómo hacer el análisis de riesgos? Metodologías, herramientas y guías.

3. **Un enfoque práctico del análisis de riesgos en la administración local.**

4. Conclusiones.

Un enfoque práctico del análisis de riesgos en la administración local

Un modelo práctico del análisis de riesgos (ENS y RGPD) basado en las similitudes entre entidades locales: una Guía

Catálogos de servicios afectados por el **ENS** en entidades locales

Tratamientos de datos personales afectados por **RGPD y LOPD** en entidades locales

Plataformas tecnológicas propios de entidades locales

Guía de Análisis de Análisis y Gestión de Riesgos con μPILAR en la Administración Local promovida por CCN y AEPD

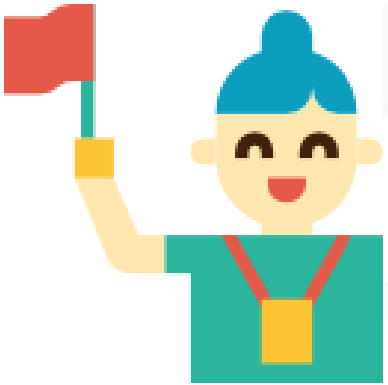
CCN Centro Criptológico Nacional

aepd agencia española protección datos

Un enfoque práctico del análisis de riesgos en la administración local

Una **visita guiada** por el modelo práctico con PILAR

EAR/PILAR



</pilar>

Herramientas de análisis y gestión de riesgos.

ccn-cert

Índice

1. Introducción. El análisis de riesgos como requisito regulatorio.

2. ¿Cómo hacer el análisis de riesgos? Metodologías, herramientas y guías.

3. Un enfoque práctico del análisis de riesgos en la administración local.

4. **Conclusiones.**

Conclusiones

- Una **Guía** de Análisis de Análisis y Gestión de Riesgos con PILAR en la Administración Local promovida por CCN y AEPD.
- Un **facilitador** para mejorar la seguridad y el cumplimiento (ENS, RGPD)

XII Jornadas STIC CCN-CERT

Ciberseguridad, hacia una respuesta y disuasión efectivas

- **E-Mails**
  - info@ccn-cert.cni.es
  - ccn@cni.es
  - organismo.certificacion@cni.es
- **Websites**
  - www.ccn.cni.es
  - www.ccn-cert.cni.es
  - oc.ccn.cni.es
- **Síguenos en**

centro criptológico nacional