

# GESTIÓN DE LA CIBERSEGURIDAD BASADA EN EL ANÁLISIS DE RIESGOS DE LAS EMPRESAS

UNA FORMA DE OBTENER LO QUE REALMENTE SE NECESITA  
Y AHORRAR RECURSOS Y DINERO

Sergio Losilla . Digital Hand Made  
Fernando Acero. Consultor Ciberseguridad



### PERFIL DEL FORMADOR Y CONSULTOR EXTERNO DE DIGITAL HAND MADE



**FERNANDO ACERO**  
**EX DIRECTOR CIBERDEFENSA**  
**EJÉRCITO DEL AIRE**

El Coronel en la Reserva D. Fernando Antonio ACERO MARTÍN, es miembro de la 37 Promoción de la Academia General del Aire, con la que obtuvo el Despacho de Teniente de la Escala de Tropas y Servicios en el año 1985. Durante su primer año como Teniente, realiza el Curso de Transmisiones en la Escuela de Transmisiones del Ejército del Aire, sita en Cuatro Vientos. Finalizado el curso es destinado al Ala 14 y, posteriormente, realiza el curso de Electrónica y Transmisión Digital. Al ascender a Capitán pasó destinado al Escuadrón de Vigilancia Aérea de Villatobas (Toledo) y tras realizar el Curso de Transporte Aéreo Militar en Salamanca, al 42 Grupo de Fuerzas Aéreas como profesor, contando con 2600 horas de vuelo.

Al margen de la actividad de vuelo, en todos sus destinos ha tenido cometidos relacionados con el mantenimiento de sistemas, las comunicaciones, electrónica, informática, cifra, guerra electrónica, o con la seguridad en las comunicaciones y de la información.

Tras finalizar el VI Curso de Estado Mayor de las Fuerzas Armadas, fue destinado a la Sección de Recursos de Material de la División de Logística del Estado Mayor del Aire. Ha sido Director de Ciberdefensa del Ejército del Aire. En el ámbito Civil y desde el año 1987, ha publicado numerosos libros, artículos y enciclopedias, sobre temas de seguridad, informática y electrónica, para diversas.

Además, es colaborador asiduo de foros especializados en programación, seguridad informática, derecho informático, privacidad y criptografía

# RIESGOS ABSTRACTOS



# FUNDAMENTOS DE LA CIBERSEGURIDAD



**ANÁLISIS DE RIESGOS**



**GESTIÓN DE RIESGOS**

# DEFINICIONES

**Análisis de Riesgos** metodología que **identifica las amenazas** que acechan a los distintos componentes pertenecientes o relacionados con un Sistema de Información (activos); para **determinar la vulnerabilidad** del sistema ante esas amenazas y para **estimar el impacto** o grado de perjuicio que una seguridad insuficiente puede tener en la organización, obteniendo cierto **conocimiento del riesgo que se corre**.

**Gestión de Riesgos** es una metodología que se basa en los resultados obtenidos en el análisis anterior, que permite **seleccionar e implantar las medidas o “salvaguardas” de seguridad** adecuadas para **conocer, prevenir, impedir, reducir o controlar los riesgos** identificados y así **reducir al mínimo su potencialidad o sus posibles perjuicios**.

# MAPA CONCEPTUAL



# ANÁLISIS DE RIESGOS PERMITE

- 1. Identificar los activos que hay que proteger.**
- 2. Identificar los elementos del sistema que soportan ese valor; es decir, aquellos donde los ataques pueden causar daño a la organización.**
- 3. Establecer medidas de seguridad para protegernos contra los ataques.**
- 4. Estimar indicadores de la posición de riesgo para ayudar a los que tienen que tomar decisiones evitando situaciones overkill (medidas desproporcionadas) o underkill (medidas insuficientes para los riesgos a los que se enfrenta el sistema), es decir mejorando la eficiencia y eficacia de las inversiones en ciberseguridad.**
- 5. Estimar ciertos riesgos a la hora de invertir en una empresa.**

# NOTA PARA LOS INVERSORES

**¿Nos basta con un informe de auditoría independiente, un informe de cuentas y un informe de gestión, para valorar el riesgo de invertir en una empresa, digitalizada o que ha sufrido una transformación digital?**



# LA REALIDAD

ACTUALIDAD

## El 53% de las empresas españolas fueron víctimas de un ataque de ransomware el año pasado

Aina Pou Rodríguez  
25 mayo, 2020

7 Compartido 1,209 Visualizaciones

Nuevos productos Tecnología

## El 60% de las pymes afectadas por un ciberataque cierra en 6 meses

Por INESE 27 noviembre, 2019

692 0

### Tipos de incidentes más comunes (%)

Virus o gusanos informáticos	23
Fraude por correo electrónico	21
Ransomware (back-ups recuperados)	19
Ataque a la cadena de suministro	18
Ataque de denegación de Servicio (DDoS)	18
Dispositivos perdidos y datos confidenciales	18

Ciberseguridad Executive

## Las empresas españolas sufren 436 ciberataques a la semana en los últimos 6 meses

Por B.L. 1 diciembre, 2019

Durante los últimos 6 meses las **empresas españolas han recibido de media 436 ciberataques semanalmente**. Así lo revela el informe "Threat Intelligence 2019" de Check Point. Este estudio apunta también que se observa una tendencia al alza en cuanto al número de ataques a nivel general a las compañías.

### LO MÁS LEÍDO

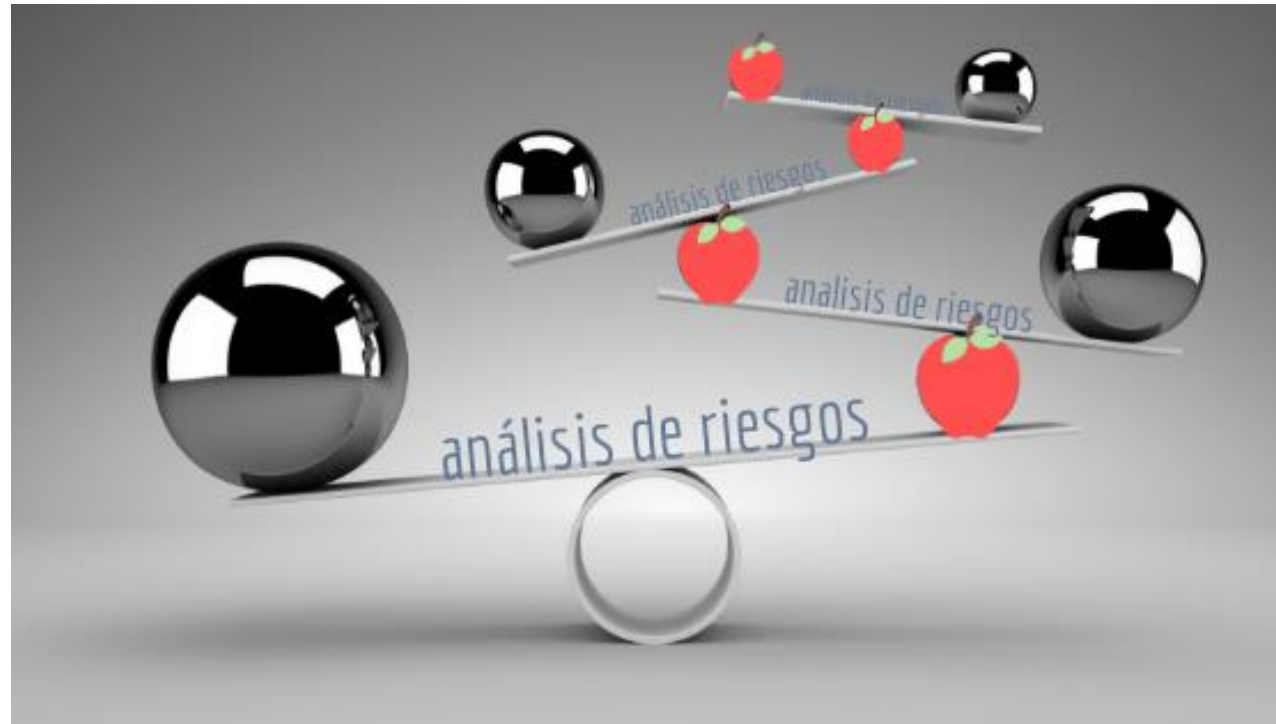


Cinco herramientas gratuitas para descifrar ransomware

**El coste medio para las empresas españolas de un ciberataque supera los 66.800 euros**

# LA ÚNICA SOLUCIÓN

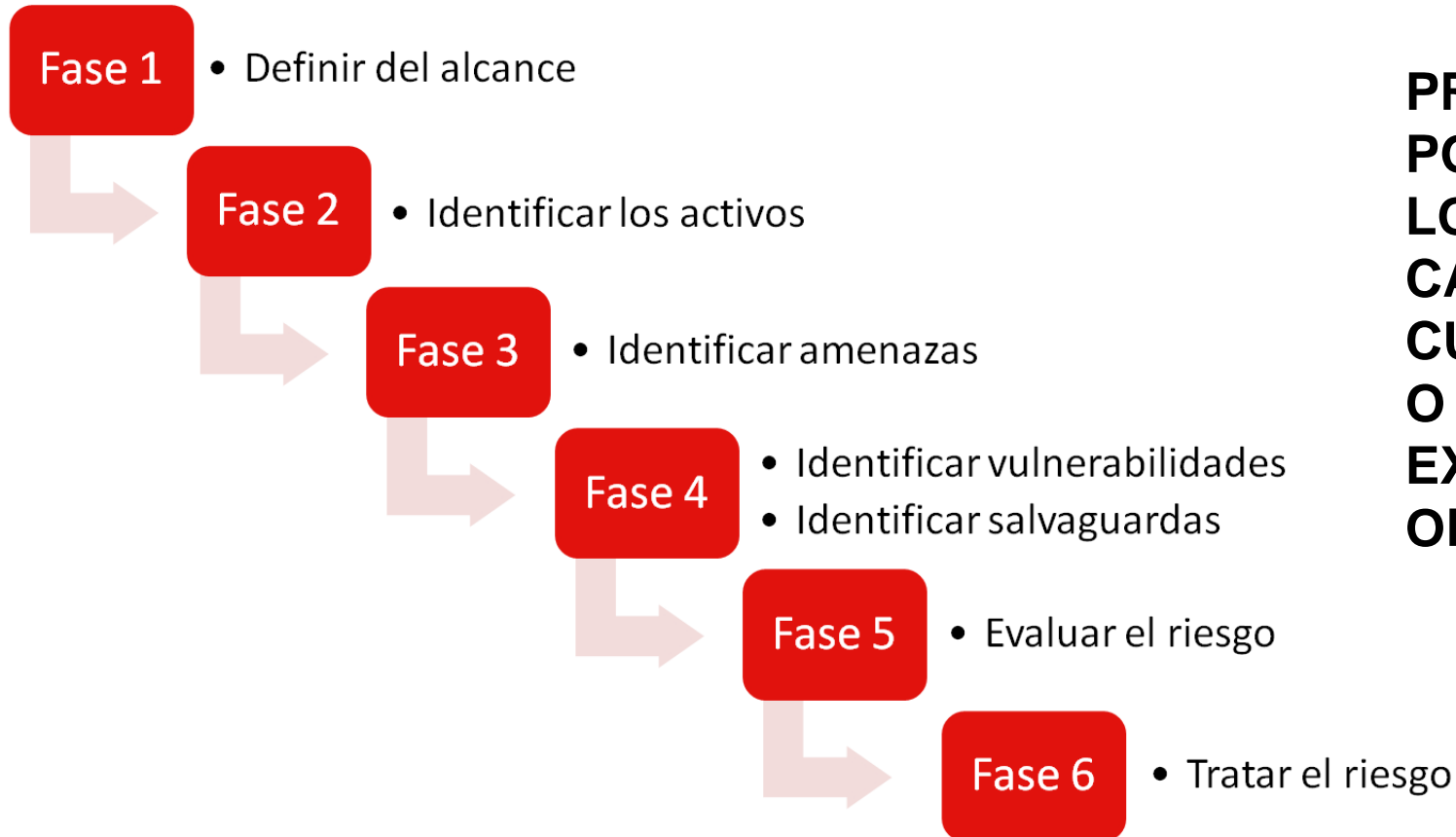
**CON 3.330.000 PYMES, UN 1% SON 33.300 EMPRESAS QUE CIERRAN ANUALMENTE POR CIBERATAQUES**



# CARACTERÍSTICAS DE LOS ACTIVOS

- A. Los activos de **información** suelen estar caracterizados por sus requisitos de **confidencialidad, disponibilidad e integridad.**
- B. Los activos de **servicio** suelen estar caracterizados por su **disponibilidad.**
- C. Tanto los de **información, como los de servicio**, pueden tener requisitos de **autenticidad y trazabilidad.**

# FASES Y CICLO



**PROCESO CÍCLICO E ITERATIVO, POR EJEMPLO, CUANDO CAMBIAN LOS SISTEMAS, CUANDO CAMBIAN LAS AMENAZAS, CUANDO CAMBIA LA TECNOLOGÍA O CAMBIA LA SUPERFICIE DE EXPOSICIÓN DE LA ORGANIZACIÓN.**

# VALORACIÓN DEL IMPACTO

IMPACTO = VALOR X DEGRADACIÓN.

		<i>degradación</i>		
		1%	10%	100%
<i>valor</i>	MA	M	A	MA
	A	B	M	A
	M	MB	B	M
	B	MB	MB	B
	MB	MB	MB	MB

# RESILIENCIA



**Capacidad de un sistema para seguir operando en un ambiente cibernéticamente degradado.**

# CÁLCULO DEL RIESGO

**RIESGO = PROBABILIDAD X IMPACTO.**

<i>riesgo</i>		<i>probabilidad</i>				
		MB	B	M	A	MA
<i>impacto</i>	MA	A	MA	MA	MA	MA
	A	M	A	A	MA	MA
	M	B	M	M	A	A
	B	MB	B	B	M	M
	MB	MB	MB	MB	B	B

# ESCALAS DE IMPACTO, RIESGO Y PROBABILIDAD

escalas		
impacto	probabilidad	riesgo
<b>MA:</b> muy alto	<b>MA:</b> prácticamente seguro	<b>MA:</b> crítico
<b>A:</b> alto	<b>A:</b> probable	<b>A:</b> importante
<b>M:</b> medio	<b>M:</b> posible	<b>M:</b> apreciable
<b>B:</b> bajo	<b>B:</b> poco probable	<b>B:</b> bajo
<b>MB:</b> muy bajo	<b>MB:</b> muy raro	<b>MB:</b> despreciable



# RIESGOS Y TRATAMIENTO

## Analizar los riesgos en varias dimensiones:

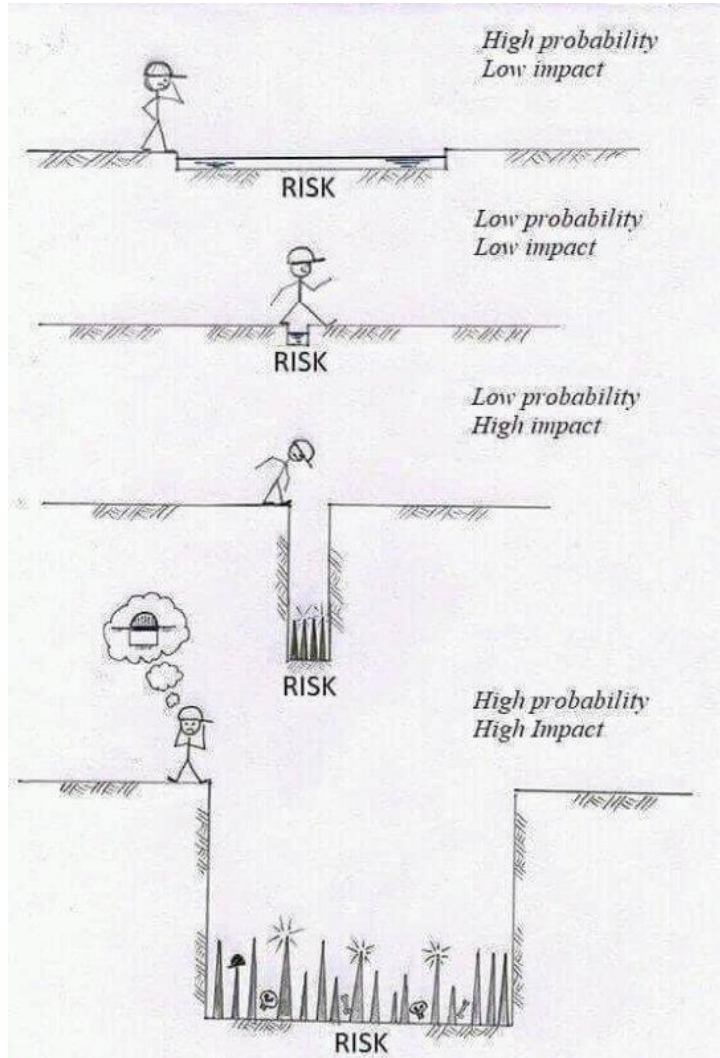
- Confidencialidad.
- Integridad.
- Disponibilidad.
- Autenticidad.
- Trazabilidad.

## Para tratar el riesgo se proponen:

- Salvaguardas (o contramedidas).
- Normas de seguridad.
- Procedimientos de seguridad.



# GESTIÓN DEL RIESGO: SALVAGUARDAS



- 1) **ELIMINAR** (TECNOLOGÍA, COSTE ECONÓMICO, EN RIESGOS MUY ALTO Y ALTO)
- 2) **MITIGAR** (PROCEDIMIENTOS, COSTE HUMANO, EN RIESGOS MEDIOS)
- 3) **ASUMIR** (SIEMPRE RIESGO BAJO O MUY BAJO)
- 4) **TRANSFERIR** (COMO COMPLEMENTO A OTRAS MEDIDAS, EN RIESGOS MEDIOS, ALTOS Y MUY ALTOS)

# EFFECTOS DE LAS SALVAGUARDAS

- incrementar el conocimiento que el atacante necesitaría para alcanzar su objetivo.
- incrementar el desembolso que el atacante tendría que realizar para alcanzar su objetivo.

Conseguir con las salvaguardas unos elevados de conocimientos e inversión, reducen la posibilidad de que el ataque se materialice, llevando los riesgos residuales a un nivel aceptable.

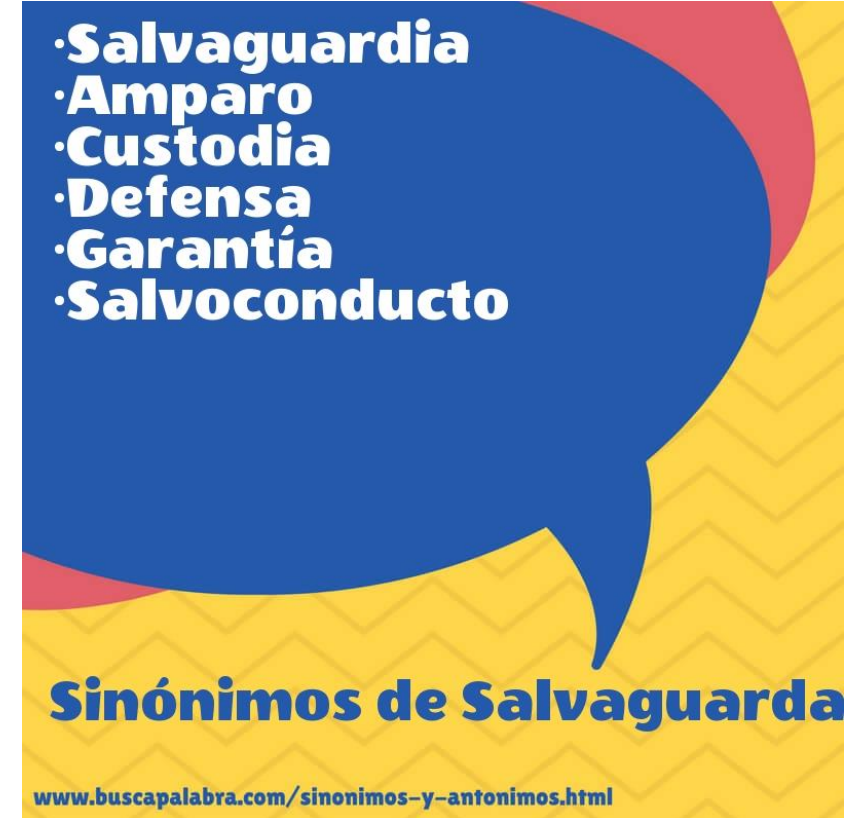


## ASPECTOS DE LAS SALVAGUARDAS:

- (G) Gestión
- (T) Técnico
- (F) Seguridad física
- (P) Seguridad del personal

## TIPO DE PROTECCIÓN DE LA SALVAGUARDA:

- |                                 |                                       |
|---------------------------------|---------------------------------------|
| — PR – prevención               | — AD – administrativa                 |
| — DR – disuasión                | — AW – concienciación                 |
| — EL – eliminación              | — DC – detección                      |
| — IM – minimización del impacto | — MN – monitorización                 |
| — CR – corrección               |                                       |
| — RC – recuperación             | — std – norma                         |
|                                 | — proc – procedimiento                |
|                                 | — cert – certificación o acreditación |



# POLÍTICA SEGINFO MINISDEF

**SEGINFOPER:** Esta norma pretende recoger los requisitos de seguridad relacionados con las personas.

**SEGINFODOC:** Esta norma pretende recoger los requisitos de seguridad relacionados con los documentos.

**SEGINFOSIT:** Esta norma pretende recoger los requisitos de seguridad relacionados con los **Sistemas de Información y Telecomunicaciones**.

**SEGINFOINS:** Esta norma pretende recoger los requisitos de seguridad relacionados con las instalaciones.

**SEGINFOEMP:** Esta norma pretende recoger los requisitos de seguridad relacionados con las empresas (cadena de suministro).

# VER COMPLIANCE VS. CIBERSEGURIDAD



- a) **Determinar los requisitos de cumplimiento normativo: Contractual, legal, estándares industriales, requisitos regulatorios. RGPD.**
- b) **Ciberdelitos y brechas de datos.**
- c) **Licencias y requisitos de propiedad intelectual e industrial: patentes, marcas, derechos, licencias, modelos de utilidad.**
- d) **Controles de importación y exportación.**
- e) **Flujos de información a través de fronteras.**
- f) **Privacidad.**



# METODOLOGÍA MAGERIT

La metodología MAGERIT V. 3 es un método desarrollado por el Consejo Superior de Administración Electrónica, que es un organismo del Ministerio de Hacienda y Administraciones Públicas de España, éste pretende **analizar y gestionar los riesgos presentes en los sistemas de información.**

## a) **Objetivos directos:**

- Concienciar a los responsables de las organizaciones de información de la **existencia de riesgos** y de la necesidad de gestionarlos.
- Ofrecer un **método sistemático para analizar los riesgos** derivados del uso de tecnologías de la información y comunicaciones (TIC).
- Ayudar a descubrir y planificar el tratamiento oportuno para **mantener los riesgos bajo control.**

## b) **Objetivos indirectos:**

- **Preparar a la Organización** para procesos de **evaluación, auditoría, certificación o acreditación.**



# TALLER CIBERSEGURIDAD: ESTRATEGIA, METODOLOGÍA Y RECURSOS

[https://administracionelectronica.gob.es/pae\\_Home/pae\\_Documentacion/pae\\_Metodolog/pae\\_Magerit.html](https://administracionelectronica.gob.es/pae_Home/pae_Documentacion/pae_Metodolog/pae_Magerit.html)

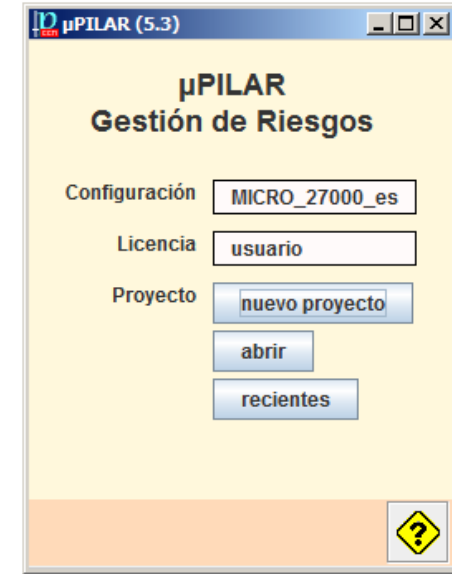
The screenshot shows a web browser window displaying the PAE (Portal de Administración Electrónica) website. The browser's address bar shows the URL: [https://administracionelectronica.gob.es/pae\\_Home/pae\\_Documentacion/pae\\_Metodolog/pae\\_Magerit.html](https://administracionelectronica.gob.es/pae_Home/pae_Documentacion/pae_Metodolog/pae_Magerit.html). The website header includes the PAE logo, navigation links for language (Castellano, Català, Euskara, Galego, Valencià, English), and buttons for 'Escuchar', 'Identificarse', and 'Registrarse'. A search bar is also present. The main navigation menu includes 'Actualidad', 'Estrategias', 'Soluciones - CTT', 'Observatorio - OBSAE', 'Documentación', and 'Organización'. The breadcrumb trail reads: 'Estás en: Inicio > Documentación > Metodologías y Guías > MAGERIT v.3 : Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información'. The main content area features the 'magerit' logo, the title 'MAGERIT v.3 : Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información', and options to 'Opinar', 'Escuchar', 'Imprimir PDF', and 'Compartir'. Below this, there is a 'Documentación' section with a list of related documents: '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'. Three PDF files are listed: 'Libro I : Método (PDF - 1,47 MB)', 'Libro II: Catálogo de Elementos (PDF - 3,37 MB)', and 'Libro III: : Guía de Técnicas (PDF - 1,28 MB)'. On the right side, there is a 'Suscríbete a nuestra newsletter' button and a 'Tu opinión es importante' banner.

# HERRAMIENTA PILAR



La Herramienta PILAR (**Procedimiento Informático y Lógico de Análisis de Riesgos**), desarrollada por e Prof. Mañas, en colaboración con el Centro Criptológico Nacional y el MAP. Dispone de librerías que permiten aplicar Magerit V. 3 y realizar el análisis y la gestión de los riesgos en distintos marcos normativos.

Licencia gratuita para las AAPP.



- Versiones específicas para pymes, para AAPP y simplificadas.
- Adaptada al ESN y a la ISO 27001.
- Base de datos de amenazas.
- Base de datos de salvaguardas.

<https://www.ccn-cert.cni.es/soluciones-seguridad/ear-pilar.html>


Archivo Editar Ver Historial Marcadores Herramientas Ayuda

PAe - MAGERIT v.3 : Metodolog x PILAR x Manejo de la herramienta PILAR x MAGERIT 3.0 - Auditoría de Sis x +

← → ↻ 🏠 🔒 https://www.ccn-cert.cni.es/soluciones-seguridad/ear-pilar.html

Getting Started Remo Conference

Bienvenido Su búsqueda 🔍 Abrir sesión

 DEFENSA FRENTE A LAS CIBERAMENAZAS

CCN-CERT | Gestión de incidentes | Guías | Informes | Formación | Soluciones | ENS | Seguridad al día | Comunicación | Empresas | CiberCOVID19 | Registro

**ÚLTIMA HORA** 09/07/2020 13:49

Resumen del II Encuentro del Esquema Nacional de Seguridad

Inicio > Soluciones > PILAR

**SOLUCIONES**

- AMPARO >
- ANA >
- ATENEA >
- CARMEN >
- CCNDroid >
- CLARA >
- CLAUDIA >
- microCLAUDIA >
- ELISA >
- EMMA >
- GLORIA >

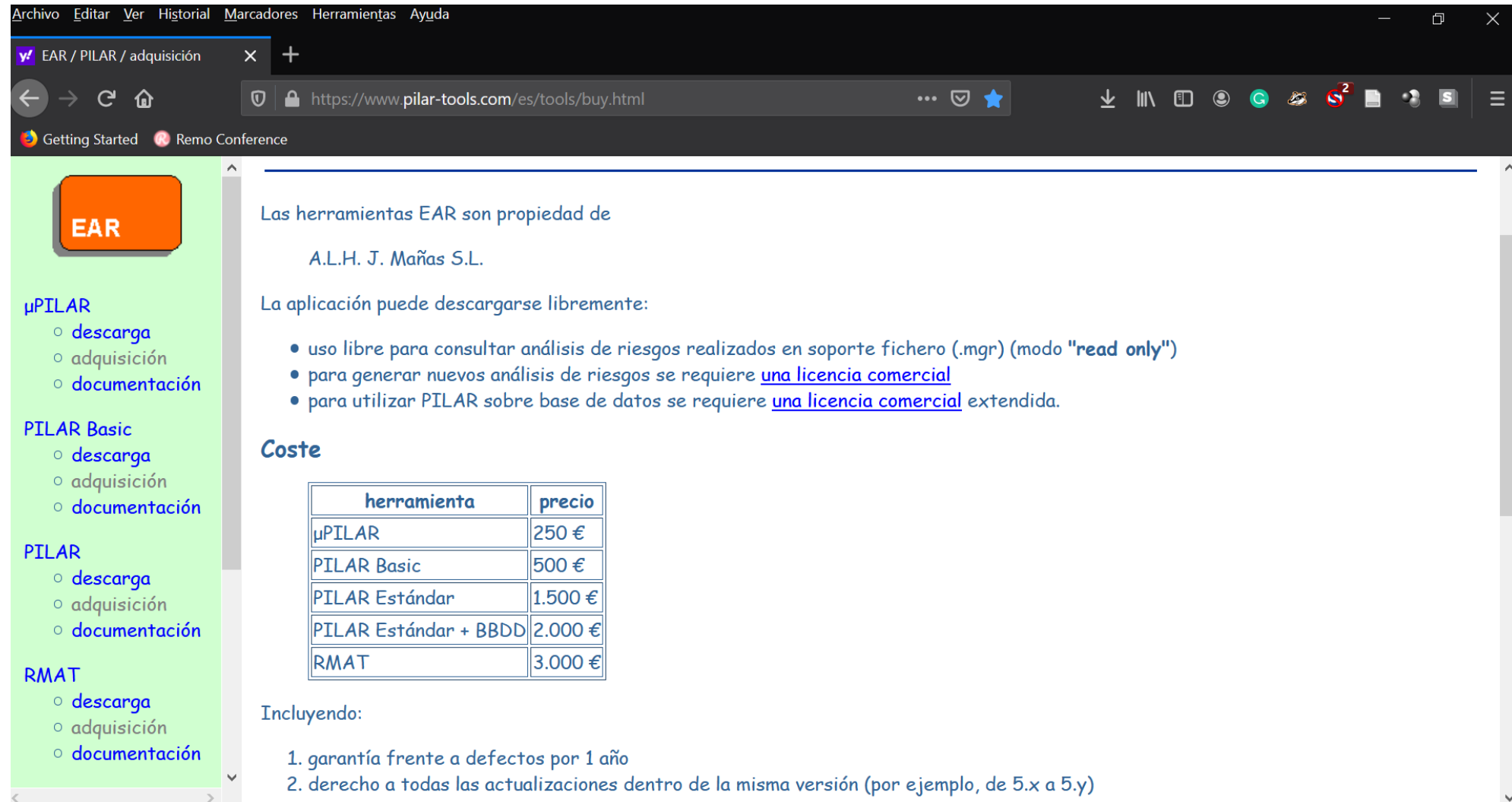
**EAR/PILAR**

Las herramientas EAR (Entorno de Análisis de Riesgos) soportan 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 parcialmente por el CCN. Se actualizan periódicamente y existen diversas variantes:

- **PILAR**: versión íntegra de la herramienta
- **PILAR Basic**: versión sencilla para Pymes y Administración Local
- **µPILAR**: versión de PILAR reducida, destinada a la realización de análisis de riesgos muy rápidos
- **RMAT** (Risk Management Additional Tools) Personalización de herramientas

Volver

# TALLER CIBERSEGURIDAD: ESTRATEGIA, METODOLOGÍA Y RECURSOS



Archivo Editar Ver Historial Marcadores Herramientas Ayuda

EAR / PILAR / adquisición

https://www.pilar-tools.com/es/tools/buy.html

Getting Started Remo Conference

**EAR**

**μPILAR**

- descarga
- adquisición
- documentación

**PILAR Basic**

- descarga
- adquisición
- documentación

**PILAR**

- descarga
- adquisición
- documentación

**RMAT**

- descarga
- adquisición
- documentación

Las herramientas EAR son propiedad de

A.L.H. J. Mañas S.L.

La aplicación puede descargarse libremente:

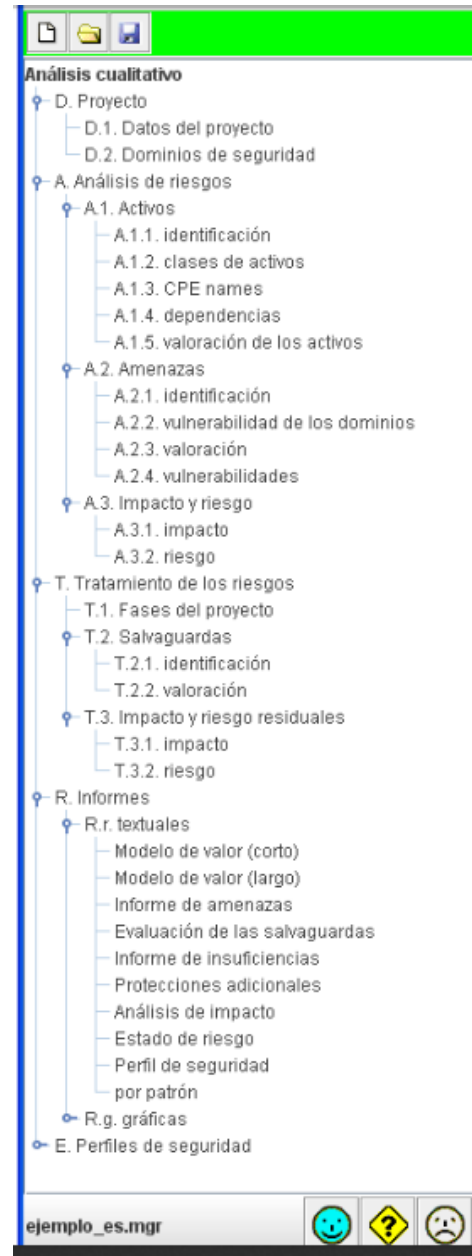
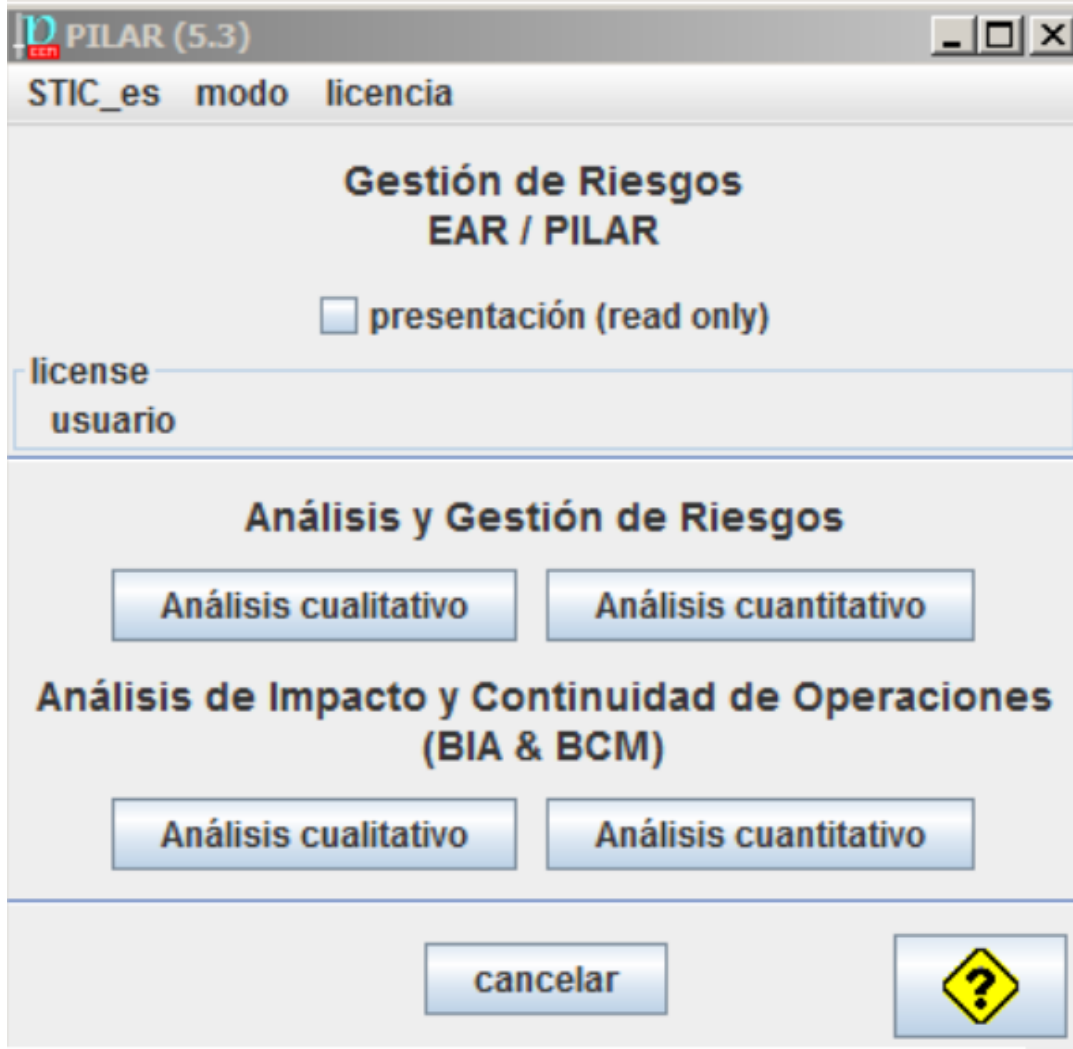
- uso libre para consultar análisis de riesgos realizados en soporte fichero (.mgr) (modo "read only")
- para generar nuevos análisis de riesgos se requiere [una licencia comercial](#)
- para utilizar PILAR sobre base de datos se requiere [una licencia comercial](#) extendida.

**Coste**

herramienta	precio
μPILAR	250 €
PILAR Basic	500 €
PILAR Estándar	1.500 €
PILAR Estándar + BBDD	2.000 €
RMAT	3.000 €

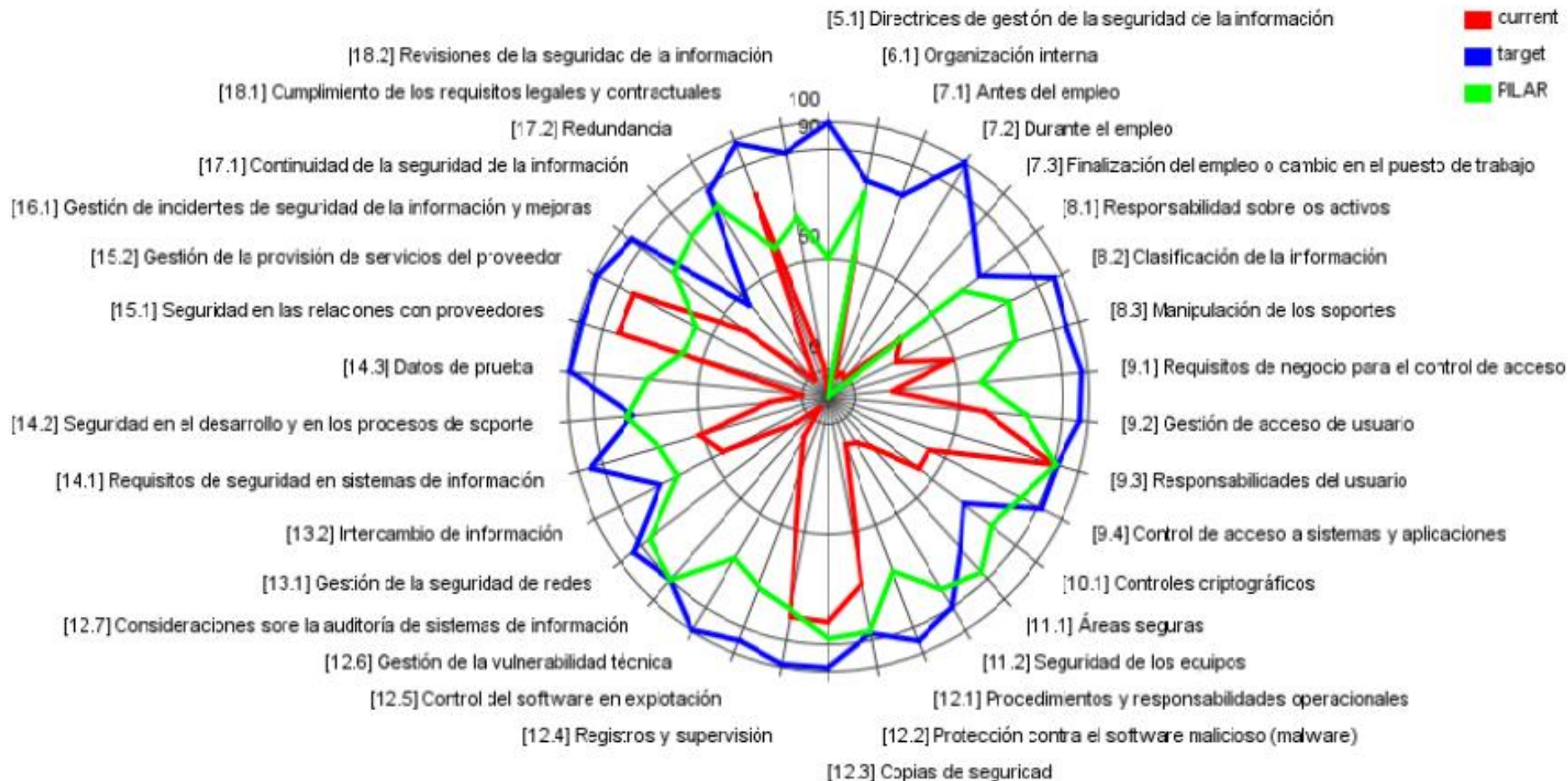
Incluyendo:

1. garantía frente a defectos por 1 año
2. derecho a todas las actualizaciones dentro de la misma versión (por ejemplo, de 5.x a 5.y)



- Proyecto
- Análisis de riesgos
  - Activos
  - Amenazas
  - Impacto y riesgo
- Tratamiento de los riesgos
  - Fases del proyecto
  - Salvaguardas
  - Impacto y riesgo residual
- Informes
  - Textuales
  - Gráficos
- Perfiles de seguridad

# MAPA DE RIESGOS



# TALLER CIBERSEGURIDAD: ESTRATEGIA, METODOLOGÍA Y RECURSOS

Archivo Editar Ver Historial Marcadores Herramientas Ayuda

EAR / PILAR / documentación

https://www.pilar-tools.com/es/tools/pilar/v74/doc.html

Getting Started Remo Conference

**EAR**

- μPILAR
  - descarga
  - adquisición
  - documentación
- PILAR Basic
  - descarga
  - adquisición
  - documentación
- PILAR
  - descarga
  - adquisición
  - documentación
- RMAT
  - descarga
  - adquisición
  - documentación

**EAR / PILAR**  
documentación

---

## Metodología

- [MAGERIT - versión 3](#). Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información.

## Versiones

- [Historia](#)

## Primera vez

- [Primera vez](#) /pdf
- [Visita rápida](#) /video

## Manuales de usuario

- [Gestión de riesgos](#) /pdf
- [Gestión de la continuidad](#) /pdf

## Ayuda (pantallas)



# AUTODIAGNÓSTICO LIGERO DE INCIBE

<https://adl.incibe.es/>

adl.incibe.es



Herramienta de Autodiagnóstico



## Conoce tus riesgos en cinco minutos

Las empresas dependen para su funcionamiento de la información y de la tecnología: ordenadores, teléfonos móviles y tabletas, bases de datos, líneas de comunicaciones...

Pero, ¿has pensado alguna vez en lo que ocurriría si, de repente, perdistes la información de tu negocio o la capacidad de acceder a ella? Seguro que tu empresa está expuesta a amenazas que ni siquiera imaginas.

¿Quieres gestionar la seguridad de tu negocio?

Te proponemos una evaluación inicial del riesgo de seguridad de tu negocio en función de cómo utilizas la tecnología: correo electrónico, página web, tabletas, smartphones, etc.

Reflexiona sobre estas sencillas cuestiones para conocer el estado de ciberseguridad de tu empresa y cuáles son los riesgos que te afectan. Así sabrás por dónde empezar a mejorar.

▶ [Calcula el riesgo de tu negocio](#)

Esta herramienta es un primer paso para mejorar la ciberseguridad de tu negocio. Si necesitas más información consulta el apartado [Protege tu empresa. ¿Qué te interesa?](#)

Permite realizar un análisis de riesgos para pequeñas empresas, mediante una serie de preguntas sencillas.

# RESUMEN:

- A. LA CIBERSEGURIDAD NECESITA UN ENFOQUE METODOLÓGICO RIGUROSO y HOLÍSTICO.
- B. PARA LA TOMA DE DECISIONES Y PARA VALORAR UNA INVERSIÓN EMPRESARIAL, ES IMPRESCINDIBLE REALIZAR UN ANÁLISIS DE RIESGOS.
- C. EL ANÁLISIS DE RIESGOS NOS PERMITIRÁ CONOCER EL RIESGO Y VALORAR NUESTROS ACTIVOS, MARCARÁ LAS PRIORIDADES Y NOS PERMITIRÁ OPTIMIZAR LA INVERSIÓN EN CIBERSEGURIDAD.
- D. EL ANÁLISIS DE RIESGOS TAMBIÉN ES EL PUNTO DE PARTIDA PARA LOS PLANES DE CONTINUIDAD DE NEGOCIO, ANÁLISIS DE IMPACTO DE NEGOCIO (BIA) Y CERTIFICACIONES, POR LO QUE ES CONVENIENTE DISPONER DE ÉL CUANTO ANTES.
- E. HAY VARIAS METODOLOGÍAS Y HERRAMIENTAS, PERO RECOMIENDO MAGERIT V.3 Y LA HERRAMIENTA PILAR, DE LAS QUE HAY MUCHA INFORMACIÓN DISPONIBLE EN INTERNET.
- F. DEBEMOS DARNOS CUENTA DEL **TREMENDO ERROR QUE SUPONE** EL TOMAR DECISIONES DE CIBERSEGURIDAD, ESPECIALMENTE SI SOMOS UN CEO, SIN TENER DELANTE UN ANÁLISIS DE RIESGOS BIEN HECHO.

# PREGUNTAS

