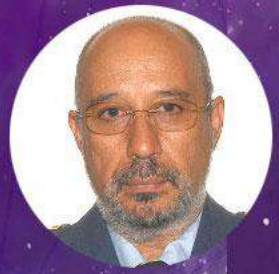
GESTIÓN DE LA CIBERSEGURIDAD BASADA EN EL ANÁLISIS DE RIESGOS DE LAS EMPRESAS

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

Sergio Losilla . Digital Hand Made
Fernando Acero. Consultor Ciberseguridad



DIGITAL HAND MADE

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.

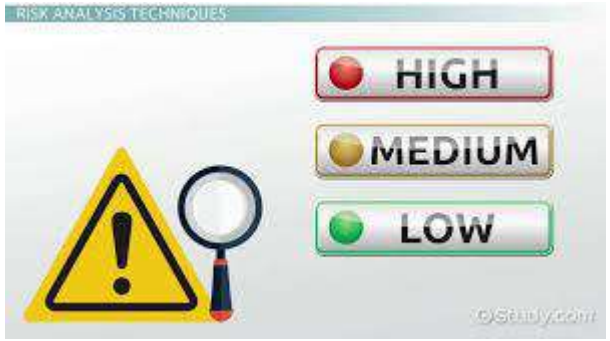
Tras finalizar el VI Curso de Estado Mayor de las Fuerzas Armadas, fue destinado a la Sección de Recursos de Material de la División de Logística del Estado Mayor del Aire. Ha sido Director de Ciberdefensa del Ejército del Aire.
En el ámbito Civil y desde el año 1987, ha publicado numerosos libros, artículos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

DIGITAL HAND MADE

RIESGOS ABSTRACTOS

FUNDAMENTOS DE LA CIBERSEGURIDAD



ANÁLISIS DE RIESGOS

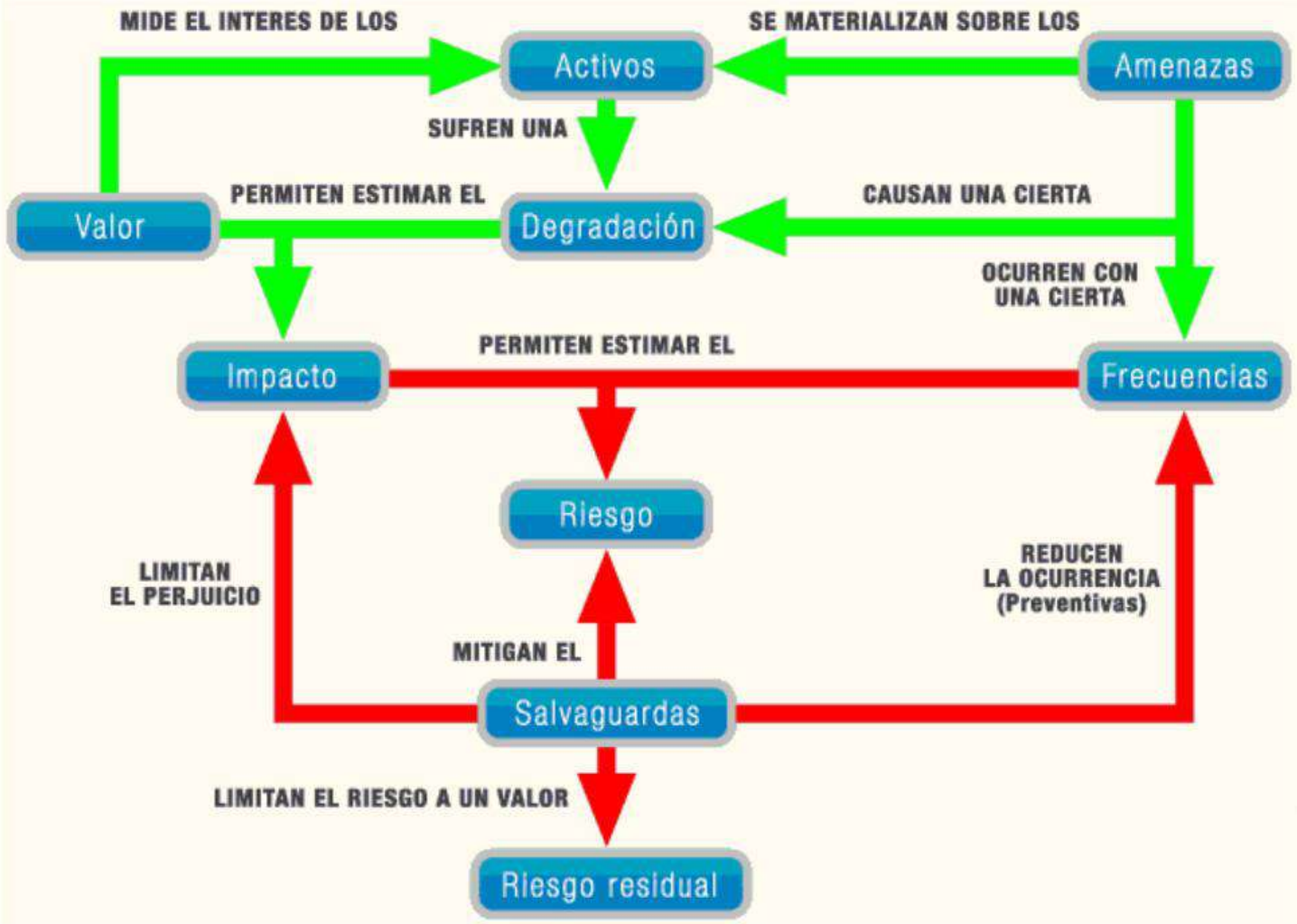
GESTIÓN DE RIESGOS

DEFINICIONES

Análisis de Riegos 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

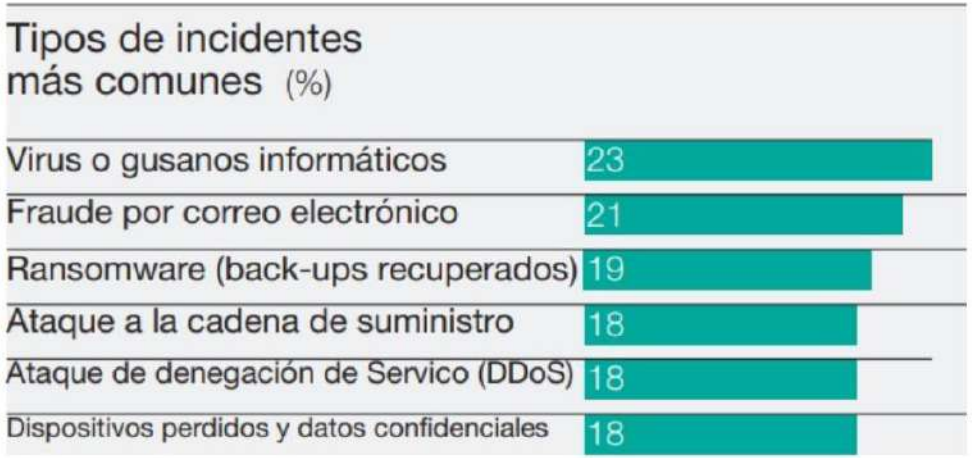
¿Nos basta con un informe de auditoría independiente, un informe de cuentas y un informe de gestión, para valorar el riesgo de invertir en una empresa, digitalizada o que ha sufrido una transformación digital?

LA REALIDAD

Nuevos productos | Tecnología

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

Por **INESE** 27 noviembre, 2019 692 0

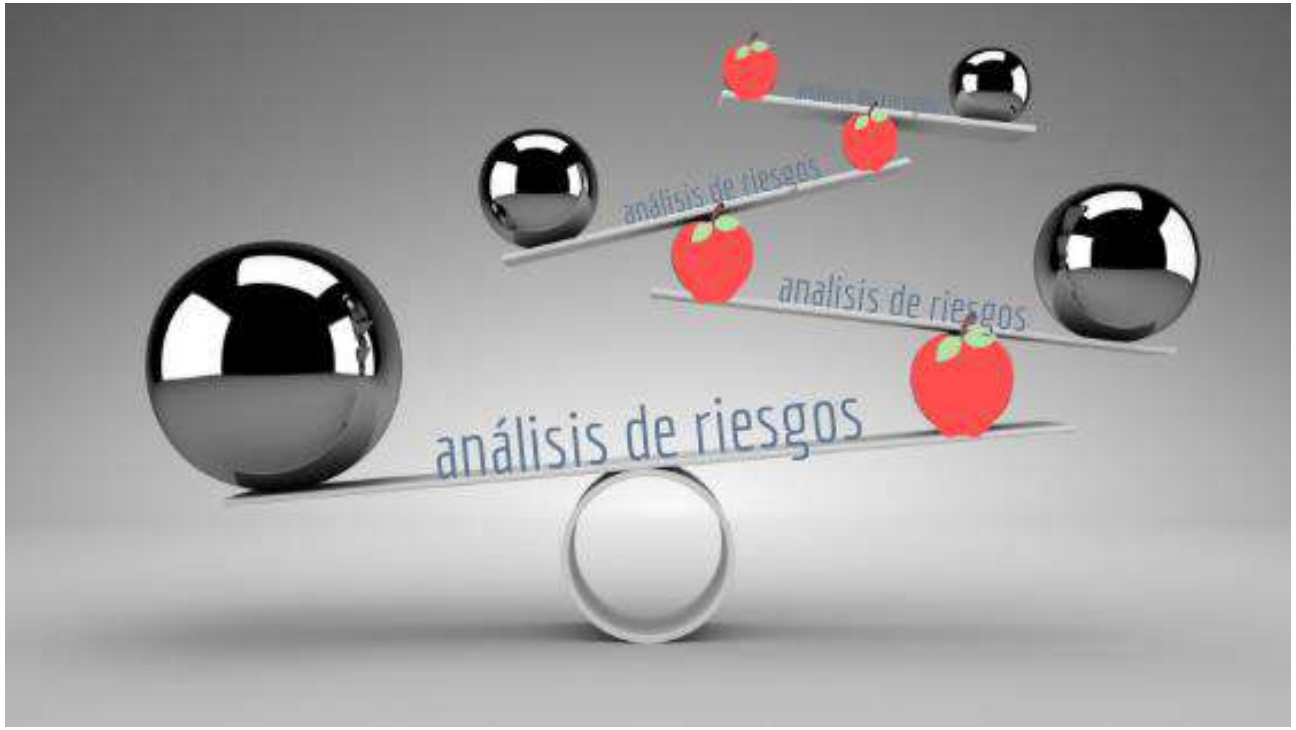


El coste medio para las empresas españolas de un ciberataque supera los 66.800 euros

DIGITAL HAND MADE

LA ÚNICA SOLUCIÓN

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



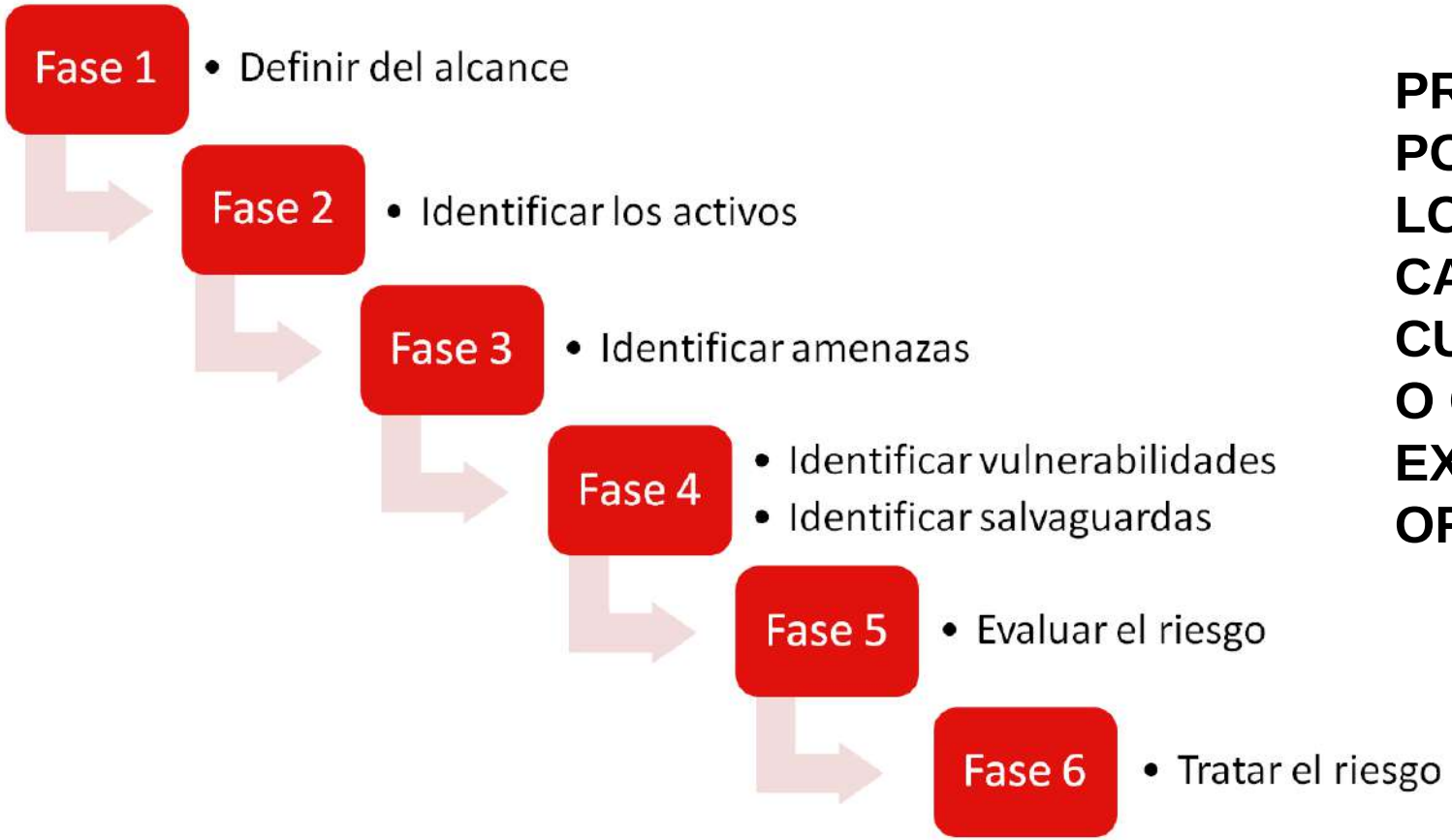
CARACTERÍSTICAS DE LOS ACTIVOS

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.

impacto		*degradación*		
		1%	10%	100%
valor	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.

riesgo		*probabilidad*				
		MB	B	M	A	MA
impacto	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
MA: muy alto	**MA**: prácticamente seguro	**MA**: crítico
A: alto	**A**: probable	**A**: importante
M: medio	**M**: posible	**M**: apreciable
B: bajo	**B**: poco probable	**B**: bajo
MB: muy bajo	**MB**: muy raro	**MB**: despreciable

RIESGOS Y TRATAMIENTO

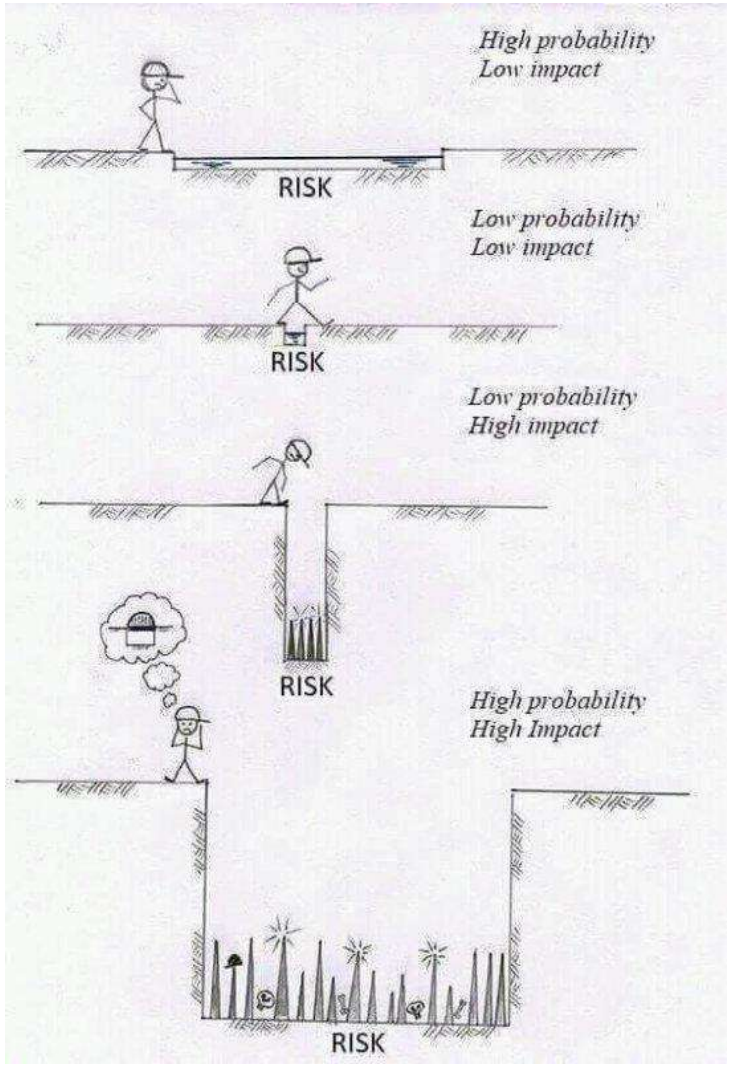
Analizar los riesgos en varias dimensiones:

- 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)

DIGITAL HAND MADE

EFECTOS DE LAS SALVAGUARDAS

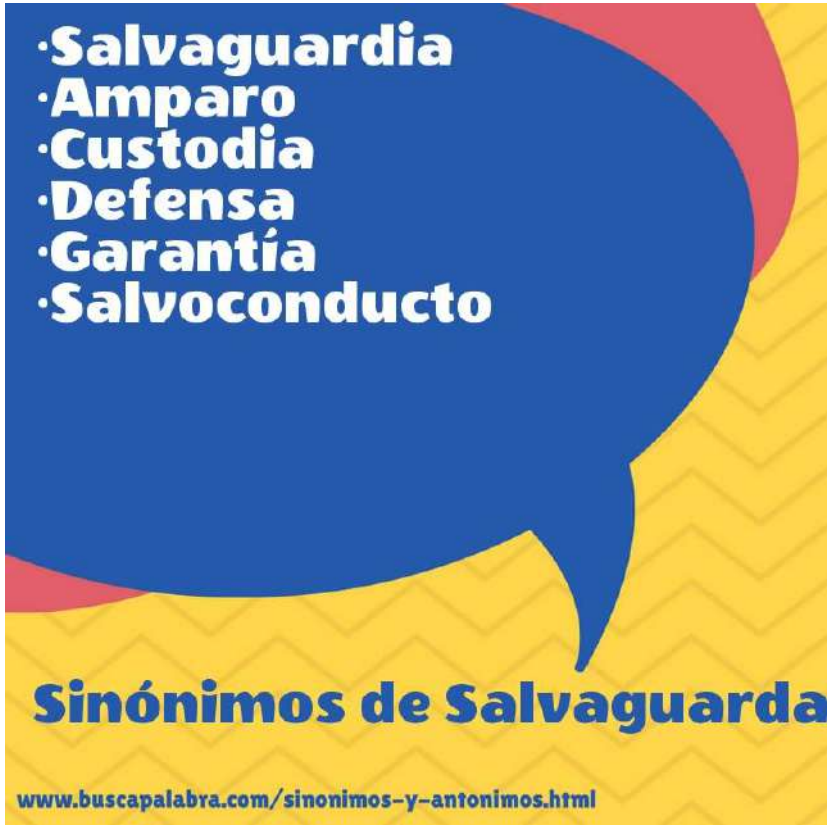
- **incrementar el conocimiento** que el atacante necesitaría para alcanzar su objetivo.

- **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
- DR – disuasión
- EL – eliminación
- IM – minimización del impacto
- CR – corrección
- RC – recuperación

- AD – administrativa
- AW – concienciación
- DC – detección
- MN – monitorización

- 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 os **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) **Cibercrimen 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.**

DIGITAL HAND MADE


magerit
METHODOLOGY FOR INFORMATION SYSTEMS
RISK ANALYSIS AND MANAGEMENT

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.

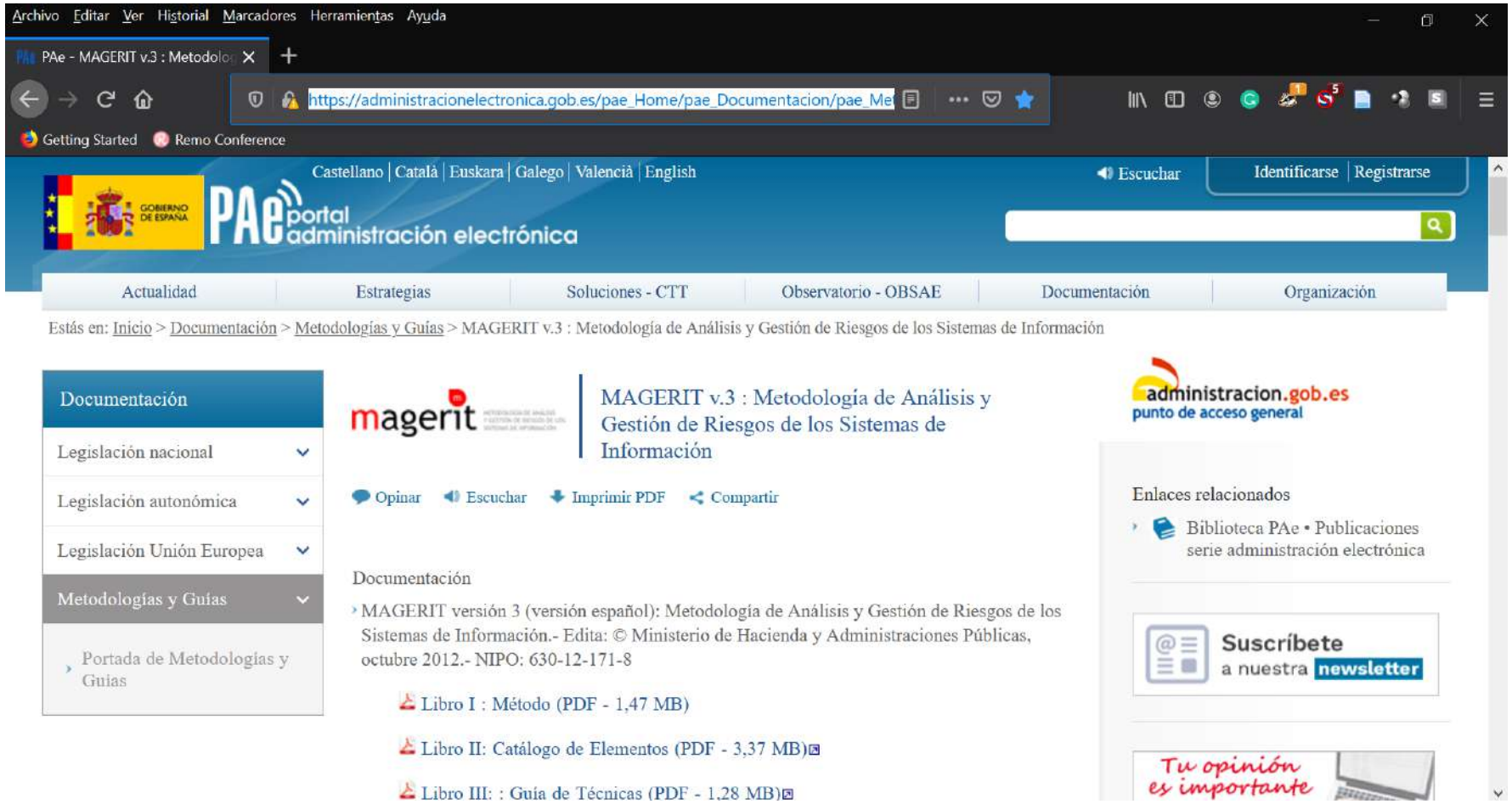
a) Objetivos directos:

- 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.

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

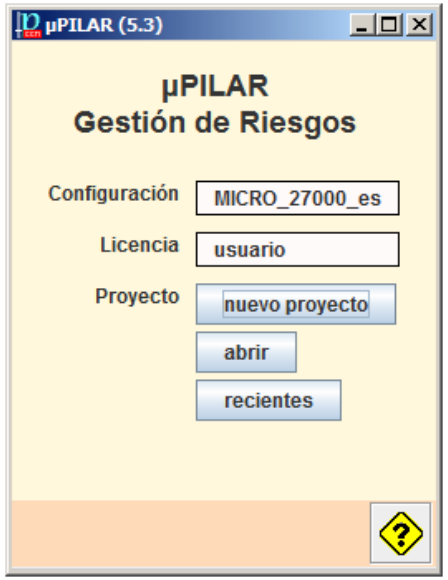


DIGITAL HAND MADE

HERRAMIENTA PILAR

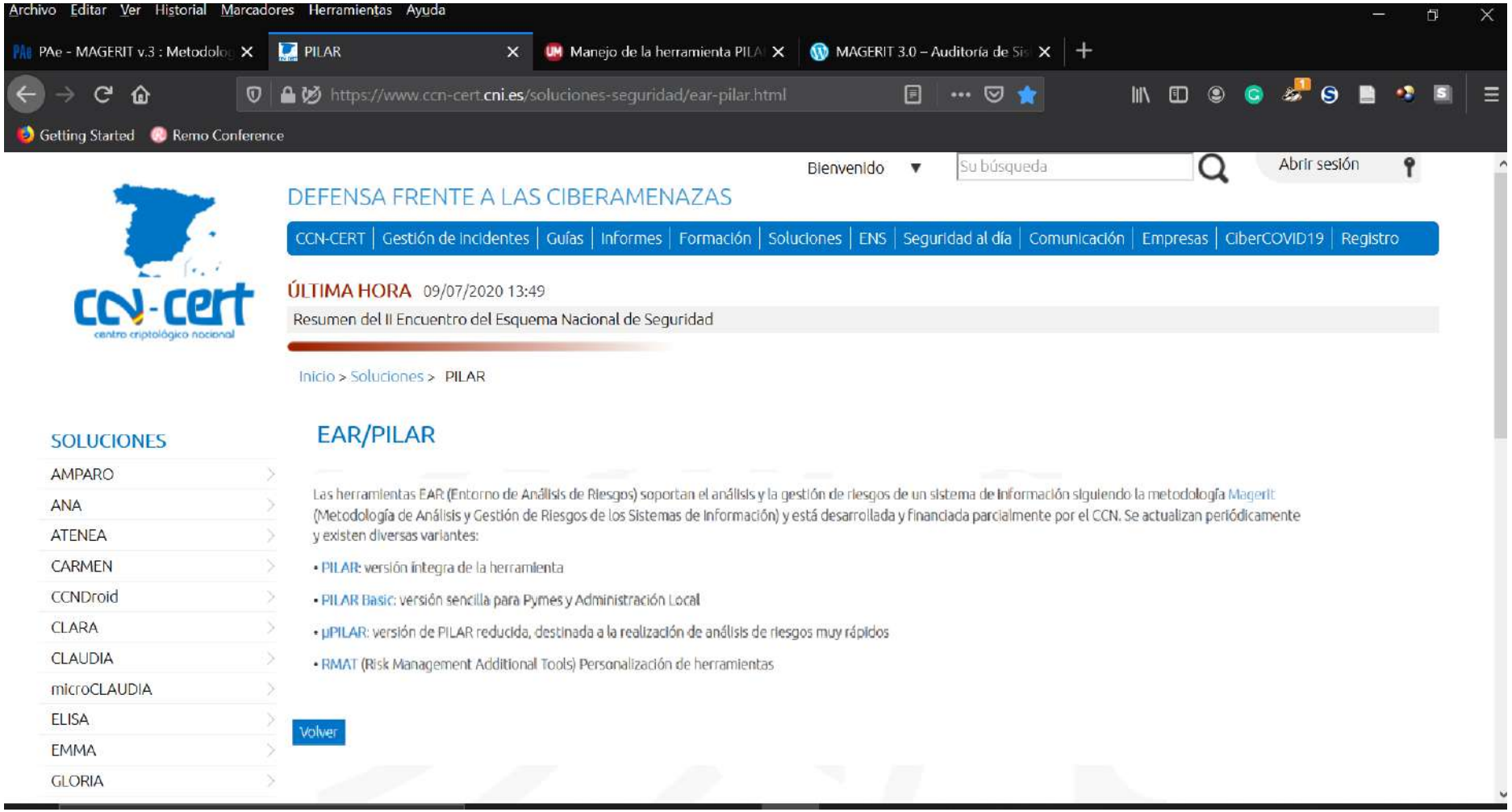
La Herramienta PILAR (**Procedimiento Informático y Lógico de Análisis de Riesgos**), desarrollada por e Prof. Mañas, en colaboración con el Centro Criptológico Nacional y el MAP. Dispone de librerías que permiten aplicar Magerit V. 3 y realizar el análisis y la gestión de los riesgos en distintos marcos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

Licencia gratuita para las AAPP.

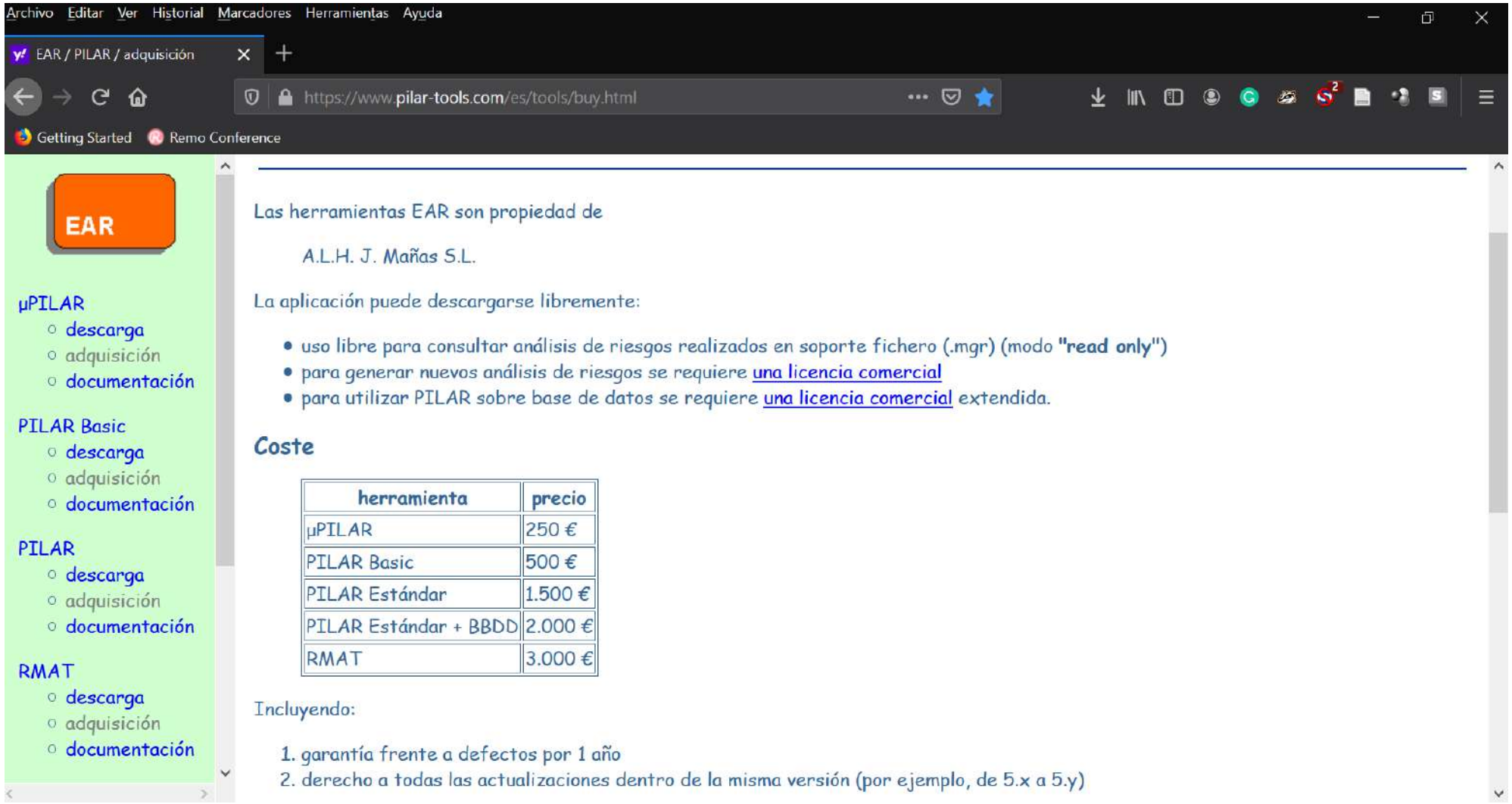


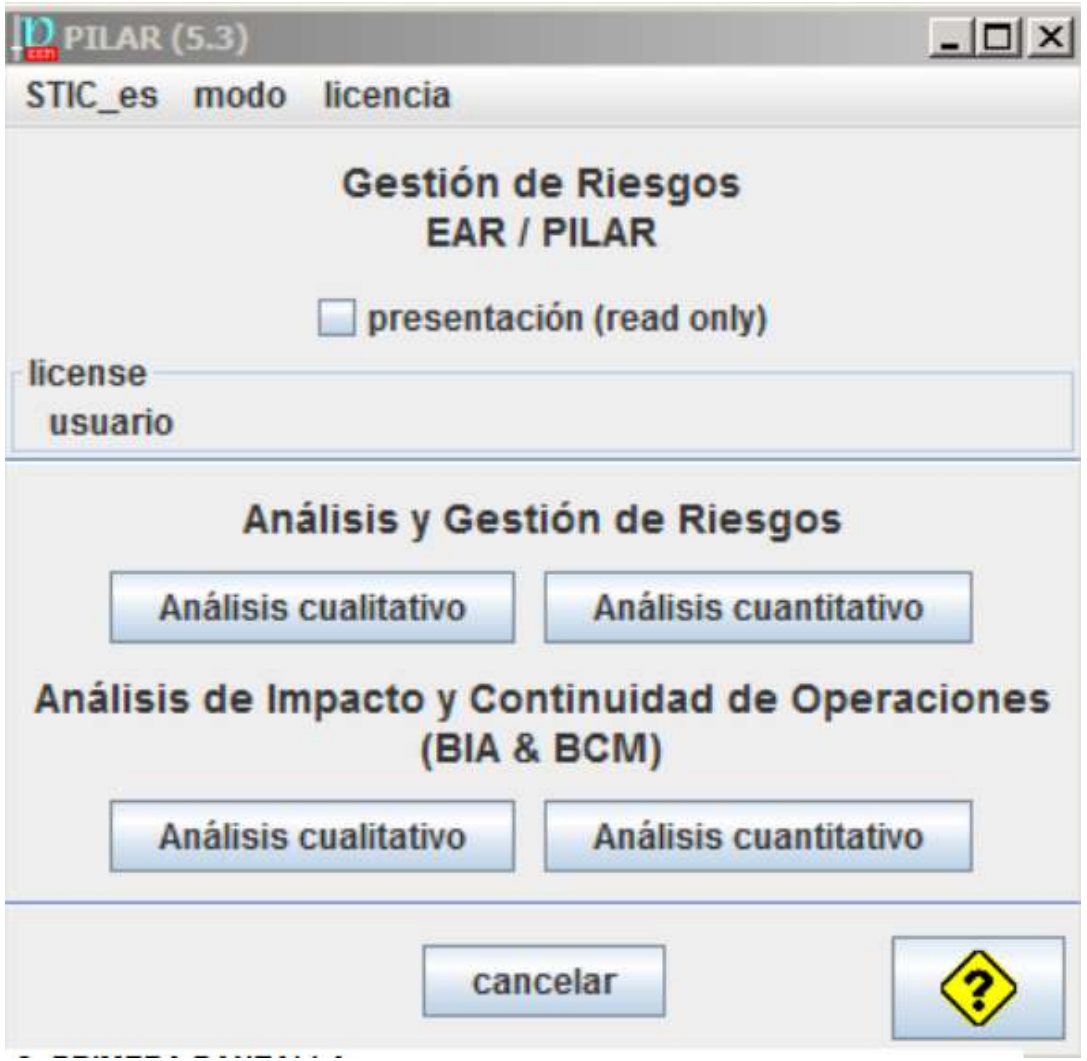
- Versiones específicas para pymes, para AAPP y simplificadas.
- Adaptada al ESN y a la ISO 27001.
- Base de datos de amenazas.
- Base de datos de salvaguardas.

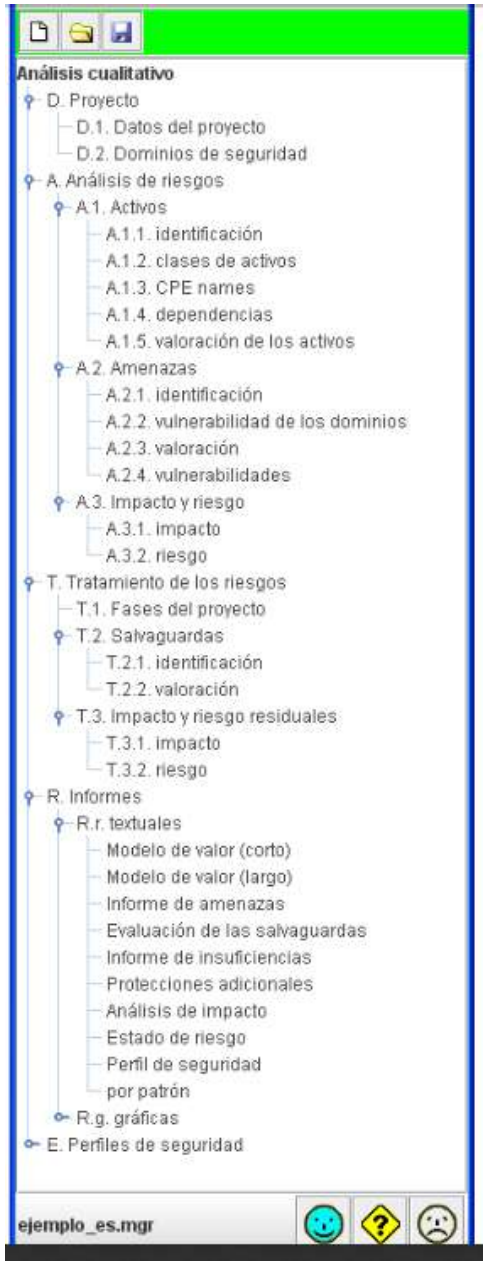
https://www.ccn-cert.cni.es/soluciones-seguridad/ear-pilar.html



DIGITAL HAND MADE

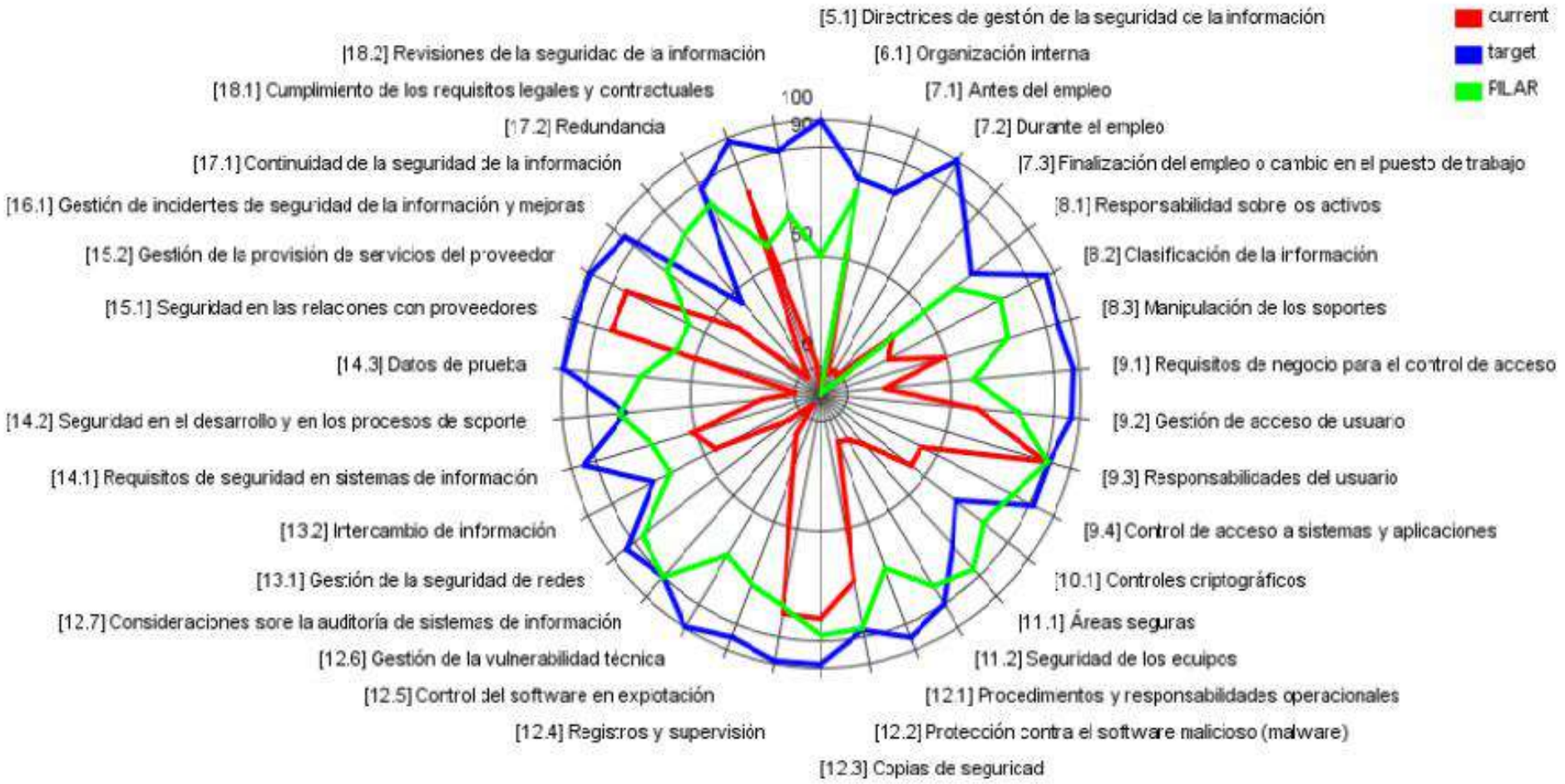

Archivo Editar Ver Historial Marcadores Herramientas Ayuda
EAR / PILAR / adquisición
https://www.pilar-tools.com/es/tools/buy.html
Getting Started
Remo Conference
EAR
μPILAR
descarga
adquisición
documentación
PILAR Basic
descarga
adquisición
documentación
PILAR
descarga
adquisición
documentación
RMAT
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)

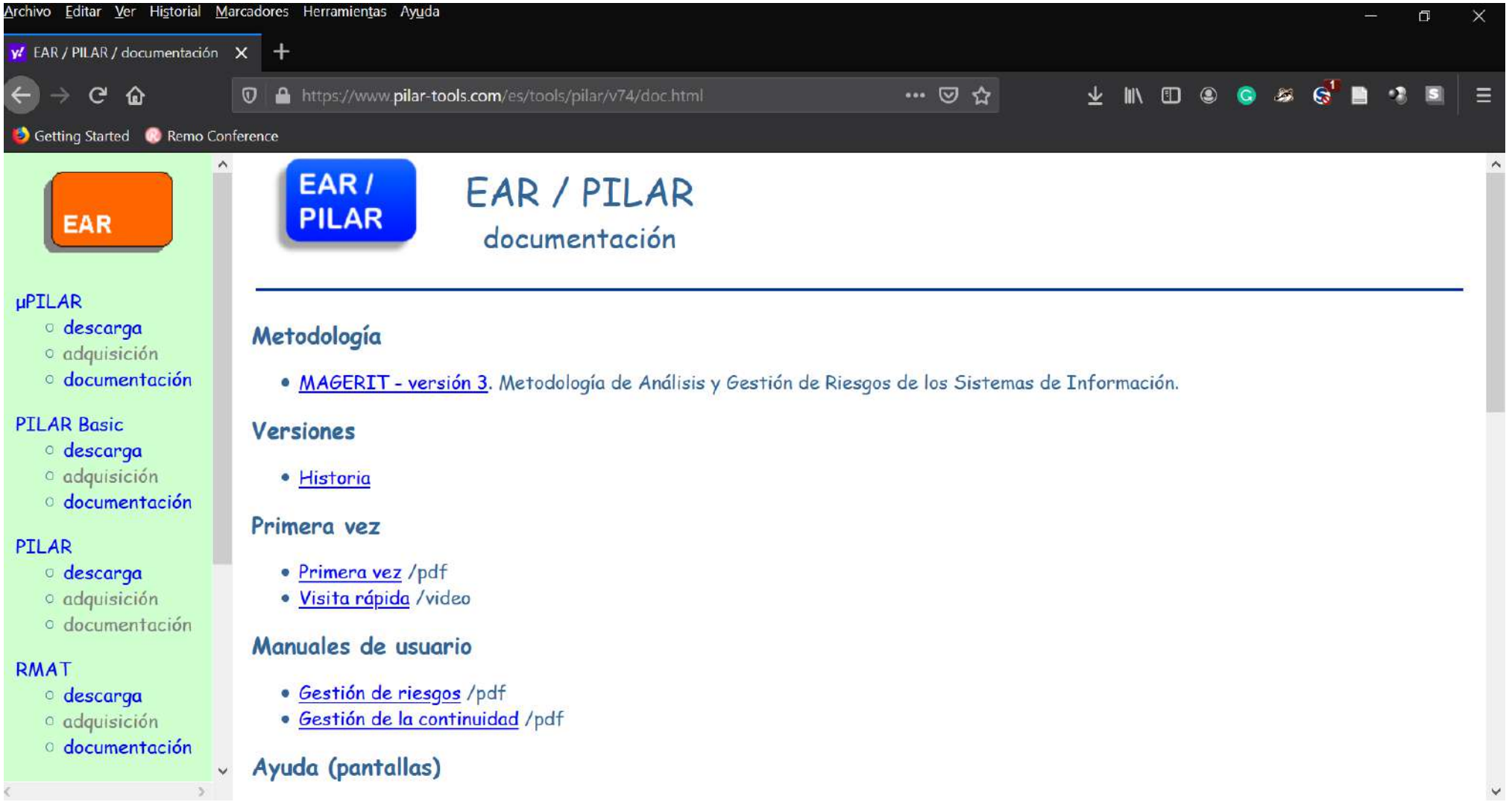




a) Proyecto
b) Análisis de riesgos
    1) Activos
    2) Amenazas
    3) Impacto y riesgo
c) Tratamiento de los riesgos
    1) Fases del proyecto
    2) Salvaguardas
    3) Impacto y riesgo residual
d) Informes
    1) Textuales
    2) Gráficos
e) Perfiles de seguridad

MAPA DE RIESGOS




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
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/

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

DIGITAL HAND MADE

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.

DIGITAL HAND MADE

PREGUNTAS