



---

# TUTORIAL DE PILAR BASIC

---

GESTIÓN Y ANÁLISIS DE RIESGOS



CURSO 22-23

CIDEAD

REALIZADO POR: JOSÉ ANTONIO SANTOS GÓMEZ

## Contenido

Introducción.....	2
Descarga e instalación de PILAR.....	2
Creación de un nuevo proyecto.....	3
Apertura de un proyecto.....	4
Guardado de un proyecto .....	4
Dominios de seguridad.....	5
Fases del proyecto.....	6
Tratamiento de los riesgos.....	6
Análisis de riesgos.....	6
Identificación de activos.....	6
Valoración de los dominios.....	8
Factores agravantes y atenuantes.....	10
Amenazas.....	10
Salvaguardas. (Medidas técnicas y organizativas: Seguridad de la información).....	11
Datos personales.....	13
Riesgos.....	13
Informes.....	14

## Introducción.

PILAR es un software para el análisis y la gestión de riesgos de un sistema de información siguiendo la metodología Magerit.

Los pasos para la implementación de esta metodología (MAGERIT) son los siguientes:

1. Identificación de Activos. Son los activos que posee la Organización clasificados de acuerdo a su función.
2. Valoración de Activos. Es la valoración asignada al activo de acuerdo a la criticidad y teniendo en cuenta las cinco dimensiones de seguridad.
3. Identificación de Amenazas. Son eventos que degradarían el valor de los activos.
4. Frecuencia. Se refiere a los eventos que suceden en un tiempo determinado.
5. Degradación. Es cuán perjudicado resultaría el activo al materializarse las amenazas.
6. Impacto. Es un indicador de qué puede suceder cuando ocurren las amenazas.
7. Cálculo del Riesgo. Es la probabilidad de materialización de amenazas sobre el activo.
8. Identificación y valoración de Salvaguardas. Son las medidas precisas a tomar para reducir el riesgo.
9. Cálculo del Riesgo Residual. Es el riesgo remanente después de aplicar las salvaguardas.

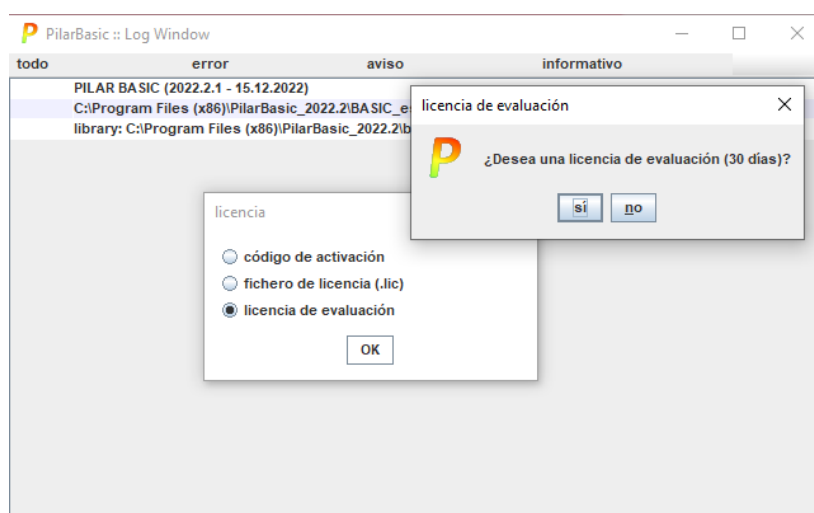
## Descarga e instalación de PILAR.

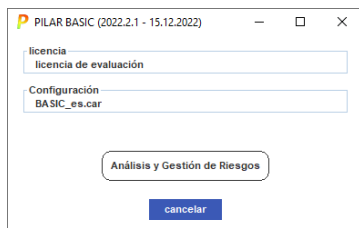
El software se puede descargar desde su página web:

<https://pilar.ccn-cert.cni.es/index.php/pilar/pilar-basic>

Este software está disponible para Windows, Linux y MAC. Es un software con licencia propietaria, que es gratuita para el sector público.

Tras su descarga e instalación nos solicita el código de licencia, en el que podemos seleccionar el de evaluación (30 días).





En la ventana que aparece no se debe cambiar ningún valor, simplemente pulsamos el botón para “Análisis y Gestión de Riesgos”.

Esta ventana aparecerá cada vez que se abra el programa.

## Creación de un nuevo proyecto.

Entonces nos aparecerá la ventana principal, en el que crearemos un nuevo proyecto, mediante la ruta Proyecto → Nuevo. Nos saldrá una ventana emergente en el que se introducen los datos identificativos del proyecto.

código	nombre	valor
org	Organización	ElectroCar
desc	Descripción	Creación de piezas electrónicas de repuestos de coches.
author	Autor	JASG
version	Versión	1.0
date	Fecha	22.12.2022
owner	Responsable del Sistema	NSNC
ciso	Responsable de la Seguridad...	PJSR

At the bottom, there are buttons: descripción, arriba, abajo, nueva, eliminar, estándar, limpiar, and three icons (happy face, question mark, sad face).

Los datos pedidos como el propietario (owner) o el responsable de seguridad (ciso) serían los nombres de tales personas en la empresa. En el caso de la clasificación del proyecto, existen diferentes grados de confidencialidad de este.

Una vez rellenos los datos se pulsa sobre la “cara feliz” y se guardan los datos. Al guardar aparece una nueva ventana con el tratamiento de los riesgos que queremos analizar. En principio se pueden dejar las opciones por defecto.

**biblioteca:** [std] Biblioteca INFOSEC (12.12.2022) (std\_20222.pl5)

**PILAR - Salvaguardas propias**

☒ visible ☒ aplicar ☒ blank => ignorar

**NIST SP800-53 - Security and Privacy Controls for Information Systems and Organizations**

☐ visible ☐ aplicar ☐ salvaguardas no evaluadas

**[77002:2022] Controles de Seguridad de la Información [D, I, C, A, T, V]**

☒ visible ☒ propagar ☒ aplicar

**[77002:2013] Código de prácticas para los controles de seguridad de la información [D, I, C, A, T, V]**

☒ visible ☒ propagar

**[GDPR:2016] Reglamento relativo al tratamiento de datos personales [DP]**

☒ visible ☒ propagar ☒ aplicar

**[SPC] Controles simples de privacidad [DP]**

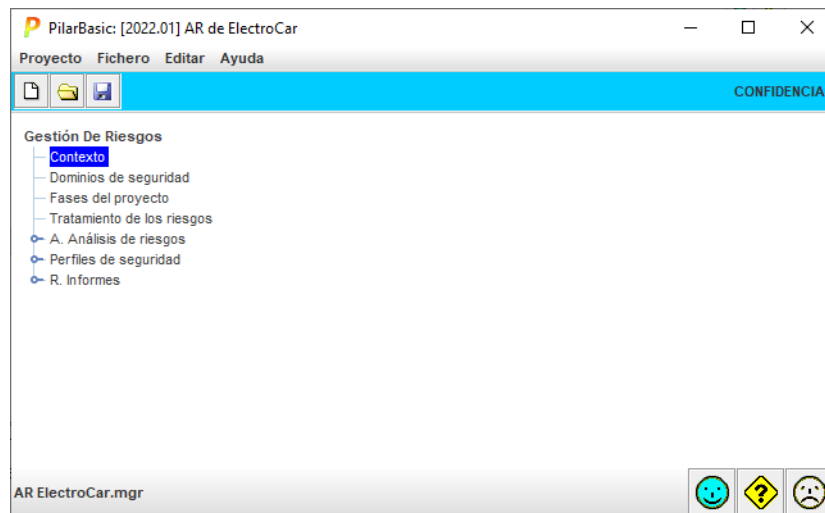
☒ visible ☒ propagar ☒ aplicar

At the bottom, there are two icons (happy face, question mark).

## Apertura de un proyecto.

Para abrir un proyecto creado con antelación se debe seguir la ruta Proyecto → Recientes (Si se ha abierto hace poco) o también mediante la ruta Fichero → Abrir.

A continuación, aparecería la ventana principal de este software, en el que se deben realizar cada una de las opciones disponibles de forma secuencial para conseguir realizar un completo análisis de riesgos.

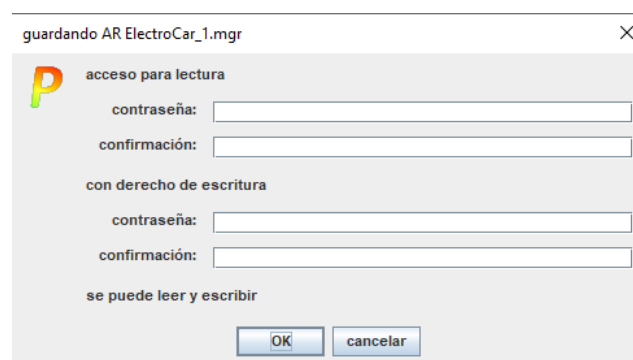


La primera opción “Contexto” nos lleva a rellenar los datos del proyecto que hemos definido anteriormente.

## Guardado de un proyecto

Para guardar el proyecto podemos seguir la ruta Proyecto → Guardar. Entonces nos solicitará el nombre del proyecto y donde guardarlo, se debe seleccionar un directorio con los permisos adecuados.

La primera vez que se guarda o en cada ocasión que se decide “Guardar como” se mostrará una ventana para establecer contraseñas de acceso de lectura y escritura a este proyecto. Si se dejan en blanco cualquier usuario podría acceder y modificar los datos.



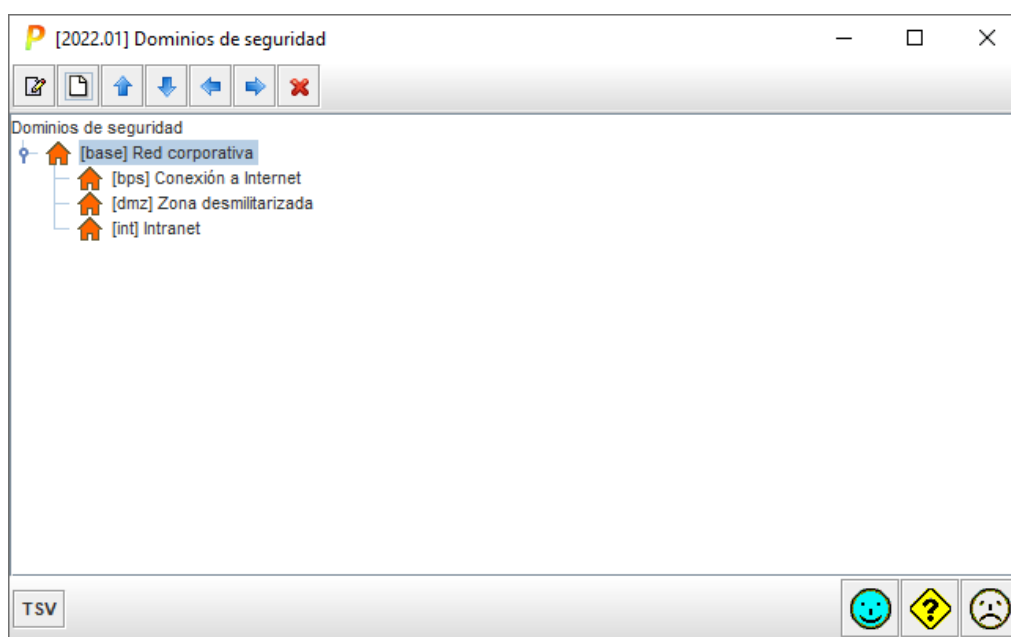
Nota: La creación, apertura y guardado también se pueden llevar a cabo mediante los tres iconos de la barra que está bajo el menú.

## Dominios de seguridad

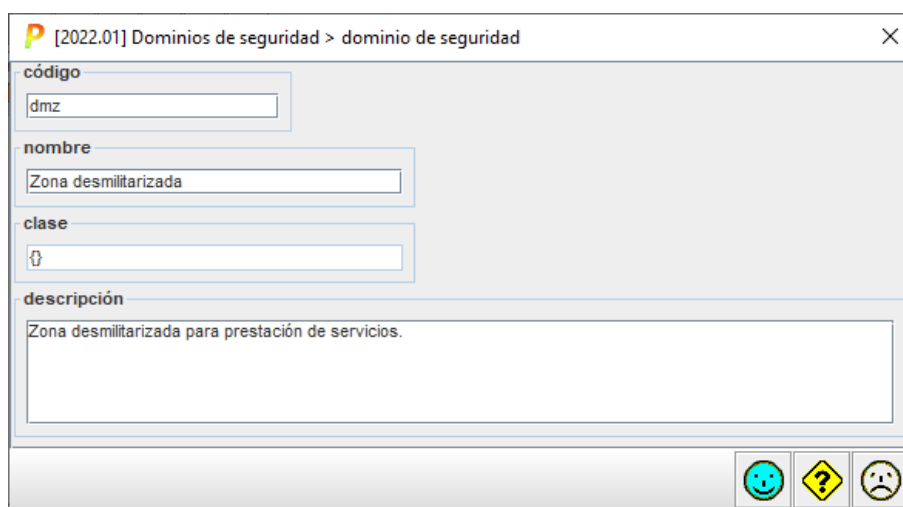
Un dominio permite agrupar los diferentes activos desde el punto de vista de su protección.

Por ejemplo: una empresa puede tener un dominio principal como su red corporativa, que según su topología puede ser una única red, una estructura Three-Legged o una dual-homed, entre otras más complejas. Según la estructura tendrá una o varias zonas de seguridad con sus propios dominios.

En este ejemplo se muestra una empresa con tres dominios una conexión a Internet, una zona desmilitarizada y una Intranet.



Para la creación de los dominios de seguridad se deben usar los iconos superiores. Su pulsamos en el segundo icono se crea un nuevo dominio dentro del que esté seleccionado en la ventana de contenido. Entonces nos aparecerá una ventana para rellenar los datos como la siguiente:

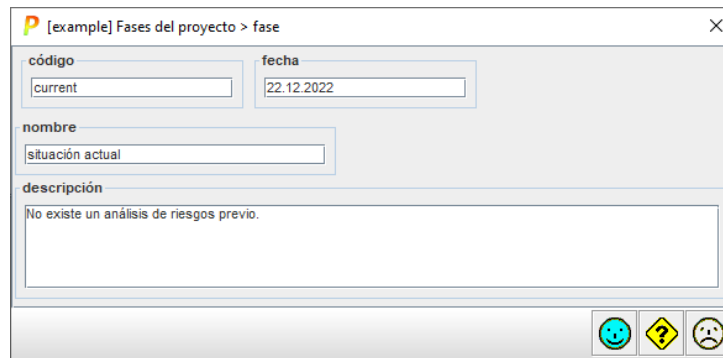


## Fases del proyecto

La opción de fases del proyecto, permite incluir hitos o puntos clave en este proceso de gestión y análisis de riesgos. Por defecto tiene dos elementos:

- Situación actual: sería la situación de partida de este proyecto.
- Situación objetivo: situación a la que se pretende llegar al final del proceso.

Un ejemplo podría ser:



[example] Fases del proyecto > fase

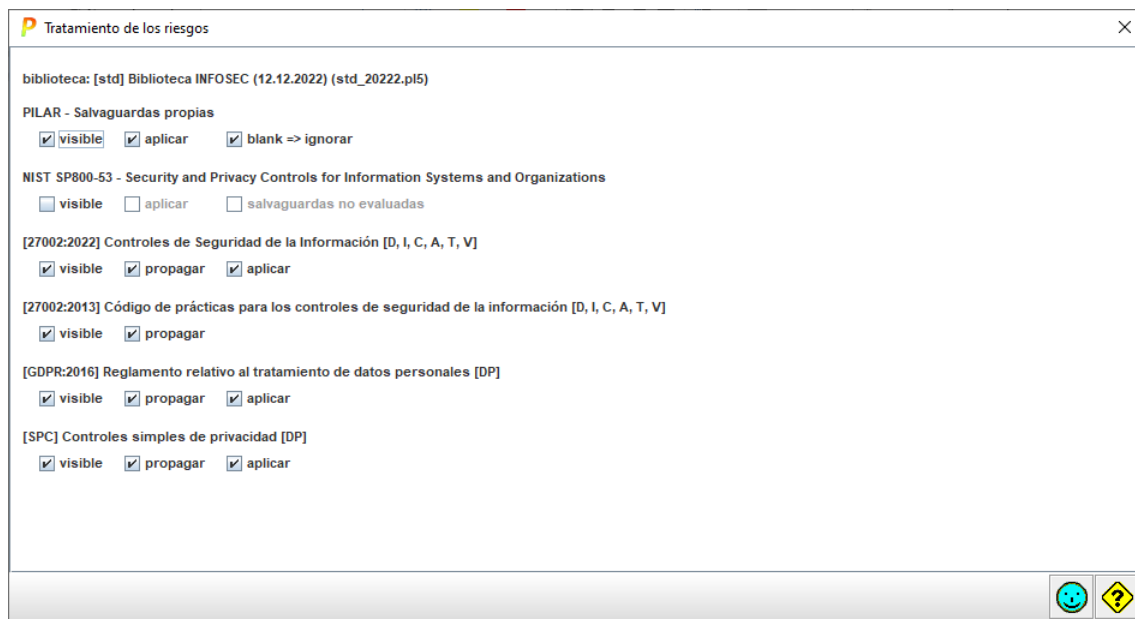
código: current      fecha: 22.12.2022

nombre: situación actual

descripción: No existe un análisis de riesgos previo.

## Tratamiento de los riesgos.

Permite cambiar los controles a aplicar sobre los riesgos de los activos.



Tratamiento de los riesgos

biblioteca: [std] Biblioteca INFOSEC (12.12.2022) (std\_20222.pl5)

PILAR - Salvaguardas propias

☒ visible ☒ aplicar ☒ blank => ignorar

NIST SP800-53 - Security and Privacy Controls for Information Systems and Organizations

☐ visible ☐ aplicar ☐ salvaguardas no evaluadas

[27002:2022] Controles de Seguridad de la Información [D, I, C, A, T, V]

☒ visible ☒ propagar ☒ aplicar

[27002:2013] Código de prácticas para los controles de seguridad de la información [D, I, C, A, T, V]

☒ visible ☒ propagar

[GDPR:2016] Reglamento relativo al tratamiento de datos personales [DP]

☒ visible ☒ propagar ☒ aplicar

[SPC] Controles simples de privacidad [DP]

☒ visible ☒ propagar ☒ aplicar

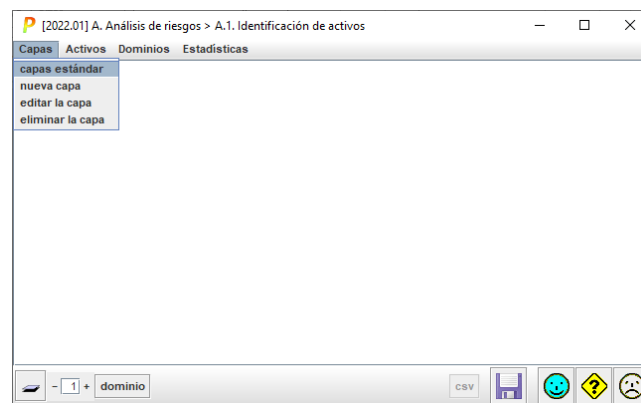
## Análisis de riesgos.

El análisis de riesgos se compone de los pasos citados al comienzo de este tutorial. Veamos estos pasos secuencialmente.

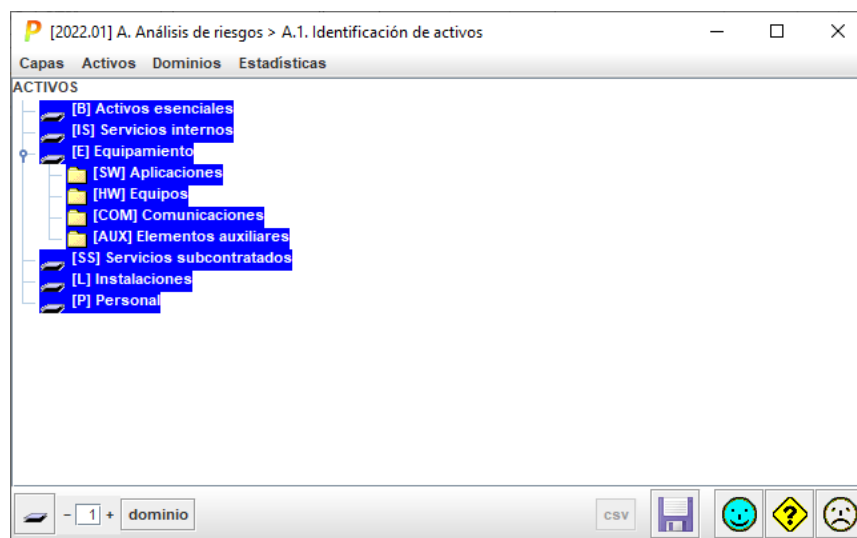
### Identificación de activos.

En este paso se deben recoger los activos de la empresa. Al abrir la pantalla por primera vez aparece la palabra “ACTIVOS” solamente sin ningún elemento. Los activos se deben registrar en una estructura jerárquica en forma de árbol que se compone de capas, podríamos crear estas capas manualmente para tener solo y exclusivamente las que queramos o podemos generar una estructura estándar.

Para la creación de la estructura estándar deberíamos seguir la ruta Capas → Capas estándar.



Tras esta selección podremos ver las capas más usuales:



Todos los activos de las empresas, en la mayoría de casos, podrían registrarse en algunas de esas capas. Si quieres realizar tus propias capas o eliminar alguna se puede usar el menú capas.

La tercera opción del menú nos permite acceder directamente a los dominios que ya han sido creados en pasos anteriores. Aparece aquí de nuevo, ya que los activos pertenecen a una capa y a un dominio de seguridad.

Una vez creadas las capas necesarias y los dominios, llega el momento de crear los activos.

Estos activos deben incorporarse en la capa correcta.

Ejemplo: un activo esencial de información podría ser los datos de los prototipos de las piezas que se construyen en la factoría.

Para registrar un nuevo activo se debe seguir la ruta Activos → Nuevo Activo → Nuevo Activo. Se mostrará la siguiente ventana para su definición:



[2022.01] A. Análisis de riesgos > A.1. Identificación de activos > activo

código

nombre

dominio

datos

CLASES DE ACTIVOS

- ☒ [essential] Activos esenciales
  - ☒ [info] información
    - ☒ [biz] datos de interés para el negocio
    - ☐ [com] datos de interés comercial
    - ☐ [adm] datos de la administración pública
    - ☐ [vr] datos vitales (registros de la organización)
    - ☐ [per] datos personales
    - ☒ [classified] información clasificada
  - ☐ [service] servicio
  - ☐ [bp] proceso de negocio
  - ☐ [ppd] tratamiento de datos personales
- ☐ [arch] Arquitectura del sistema
- ☐ [qualifier] Características
- ☐ [D] Datos / Información
- ☐ [keys] Claves criptográficas
- ☐ [S] Servicios
- ☐ [SW] Aplicaciones (software)
- ☐ [HW] Equipamiento informático (hardware)
- ☐ [COM] Redes de comunicaciones

descripción RGPD

Se debe indicar su código, nombre, dominio y la clasificación en la capa correcta. Se puede profundizar para afinar al mínimo detalle la capa o simplemente marcar sobre un elemento padre, como en el caso de “información clasificada” de la imagen anterior.

Se debe repetir este mismo proceso para cada uno de los activos a analizar.

La última opción del menú, llamada Estadísticas, te permite obtener una tabla con los activos definidos ya sean clasificados por capas o por dominios.

por capas

capa	[essential]	[arch]	[qualifier]	[D]	[keys]	[S]	[SW]	[HW]	[COM]	[Media]	[AUX]	[L]	[PI]	[other]	total
B	1	0	0	0	0	0	0	0	0	0	0	0	0	0	1
IS	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
E	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
SS	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
L	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
P	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
TOTAL	1	0	0	0	0	0	0	0	0	0	0	0	0	0	1

OK

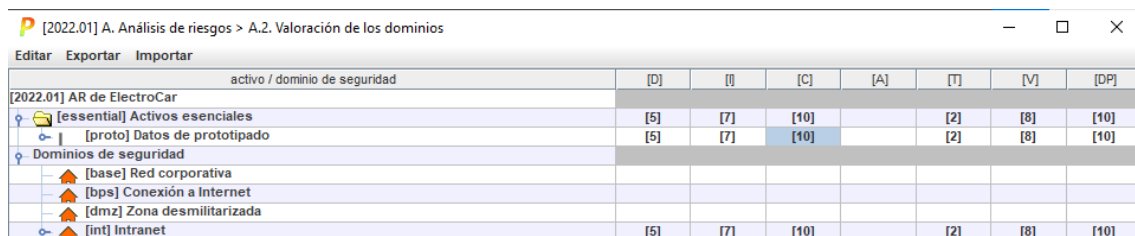
### Valoración de los dominios.

El siguiente paso bajo el epígrafe “Valoración de los dominios” consiste en la valoración del nivel de seguridad que debe tener cada uno de los **activos esenciales creados**, es decir, qué importancia tiene ese activo con respecto a su Disponibilidad [D], Integridad [I], Confidencialidad [C], Autenticidad [A] y Trazabilidad [T]. Se puede establecer un valor entre 0 (mínima importancia) 10 (máxima importancia) a cada uno de esos aspectos (DICAT). Si no se especifica un valor en una dimensión se entenderá que su importancia es mínima. Por ejemplo: una información de prototipos de desarrollo tendrá un valor muy elevado de Confidencialidad.

También existen otros dos parámetros: Valor [V] y Datos de Prototipado [DP].

En el caso de los activos de servicio se deben especificar sus requisitos de disponibilidad. Un ejemplo podría ser el servicio de conexión a Internet.

En el software nos aparecerá una venta con nuestros activos clasificados en la parte superior por sus capas y en la parte inferior por los dominios de seguridad.

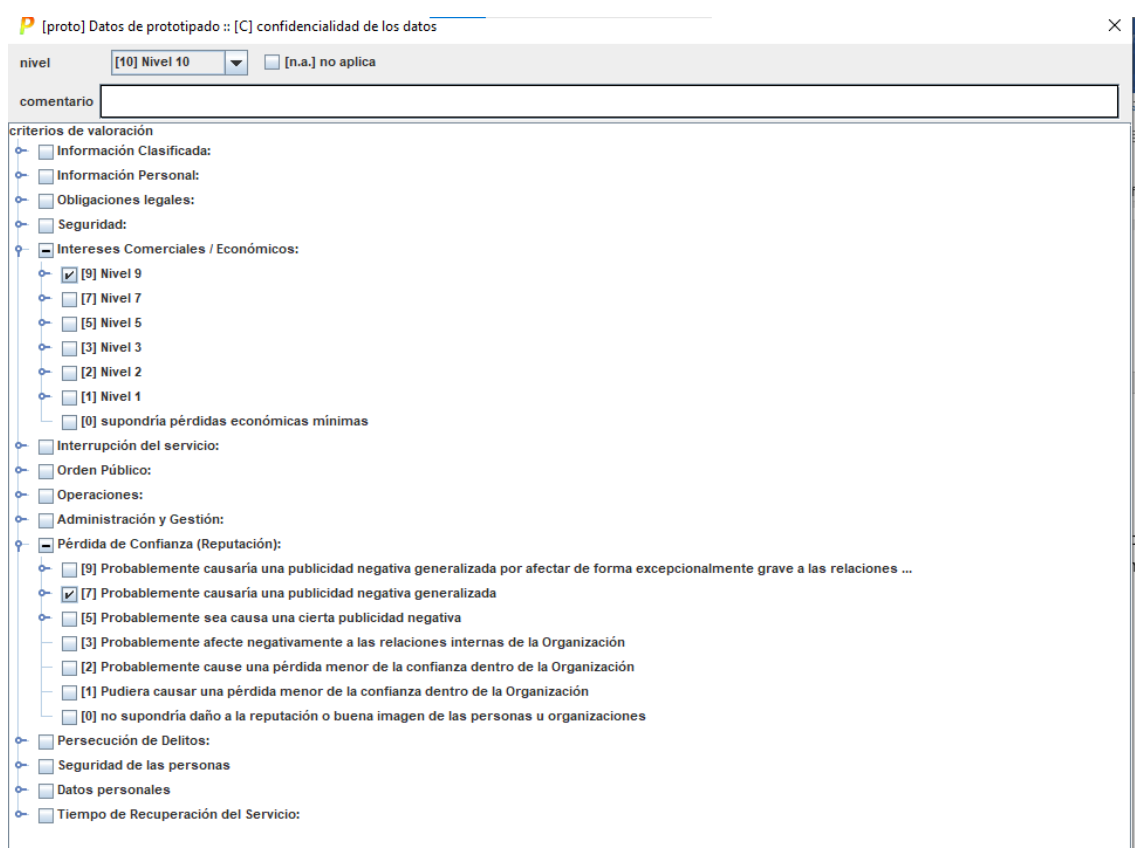


[2022.01] A. Análisis de riesgos > A.2. Valoración de los dominios

Editar Exportar Importar

activo / dominio de seguridad	[D]	[I]	[C]	[A]	[T]	[V]	[DP]
[2022.01] AR de ElectroCar							
[-essential] Activos esenciales	[5]	[7]	[10]		[2]	[8]	[10]
[-proto] Datos de prototipado	[5]	[7]	[10]		[2]	[8]	[10]
Dominios de seguridad							
[-base] Red corporativa							
[-bps] Conexión a Internet							
[-dmz] Zona desmilitarizada							
[-int] Intranet	[5]	[7]	[10]		[2]	[8]	[10]

Si realizamos doble clic en alguna de las casillas que cruzan datos de un activo con su dimensión (D,I,C,A,T,V,DP), como en la casilla que se ve marcada en la imagen anterior de color azul celeste, se mostrará una ventana donde se puede indicar su nivel de importancia con respecto a la dimensión seleccionada.



[proto] Datos de prototipado :: [C] confidencialidad de los datos

nivel: [10] Nivel 10 ☐ [n.a.] no aplica

comentario:

critérios de valoración

- ☐ Información Clasificada:
- ☐ Información Personal:
- ☐ Obligaciones legales:
- ☐ Seguridad:
- ☒ Intereses Comerciales / Económicos:
  - ☒ [9] Nivel 9
  - ☐ [7] Nivel 7
  - ☐ [5] Nivel 5
  - ☐ [3] Nivel 3
  - ☐ [2] Nivel 2
  - ☐ [1] Nivel 1
  - ☐ [0] supondría pérdidas económicas mínimas
- ☐ Interrupción del servicio:
- ☐ Orden Público:
- ☐ Operaciones:
- ☐ Administración y Gestión:
- ☒ Pérdida de Confianza (Reputación):
  - ☐ [9] Probablemente causaría una publicidad negativa generalizada por afectar de forma excepcionalmente grave a las relaciones ...
  - ☒ [7] Probablemente causaría una publicidad negativa generalizada
  - ☐ [5] Probablemente sea causa una cierta publicidad negativa
  - ☐ [3] Probablemente afecte negativamente a las relaciones internas de la Organización
  - ☐ [2] Probablemente cause una pérdida menor de la confianza dentro de la Organización
  - ☐ [1] Pudiera causar una pérdida menor de la confianza dentro de la Organización
  - ☐ [0] no supondría daño a la reputación o buena imagen de las personas u organizaciones
- ☐ Persecución de Delitos:
- ☐ Seguridad de las personas
- ☐ Datos personales
- ☐ Tiempo de Recuperación del Servicio:

En la ventana anterior se puede seleccionar simplemente el nivel de importancia que aparece en la parte superior, pero si se quiere se puede “justificar” desplegando las opciones inferiores y marcando el nivel de importancia en estos aspectos. Los niveles inferiores no afectan si se marca el nivel superior, pero en caso de que el nivel superior no se marque y se marquen las opciones inferiores se realizará un cálculo (automático) para determinar el nivel de importancia, que normalmente se corresponde con el valor superior que se marque.

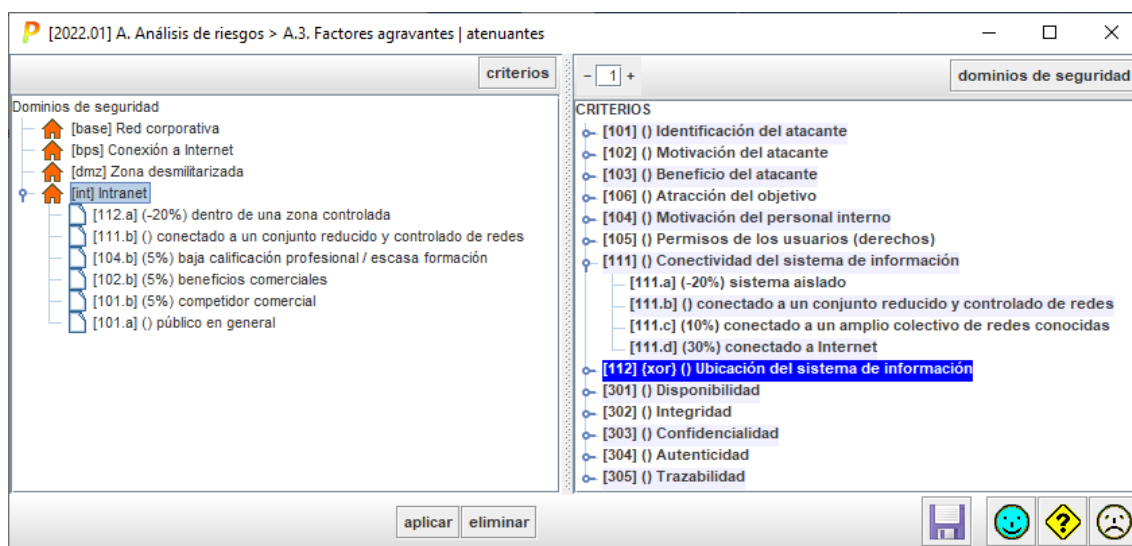
Al finalizar de valorar todos los activos ya se podría pasar al siguiente paso, en caso contrario se mostrará un aviso de que quedan activos por valorar.

## Factores agravantes y atenuantes.

En este paso se pueden identificar diversos factores que pueden variar la seguridad de los diferentes dominios de seguridad de la empresa y, por ende, los activos que se encuentran en esos dominios de seguridad.

En el software, en la ventana que aparece se muestran a la izquierda los dominios y a la derecha una lista con todos los posibles agravantes y atenuantes. Se debe hacer una revisión de este listado para cada uno de los dominios para concretar todos estos factores.

Ejemplo: en la siguiente imagen se muestra que en el dominio “Intranet” se han incorporado una serie de factores agravantes (los de porcentaje positivo) y otros atenuantes (los de porcentaje negativo).

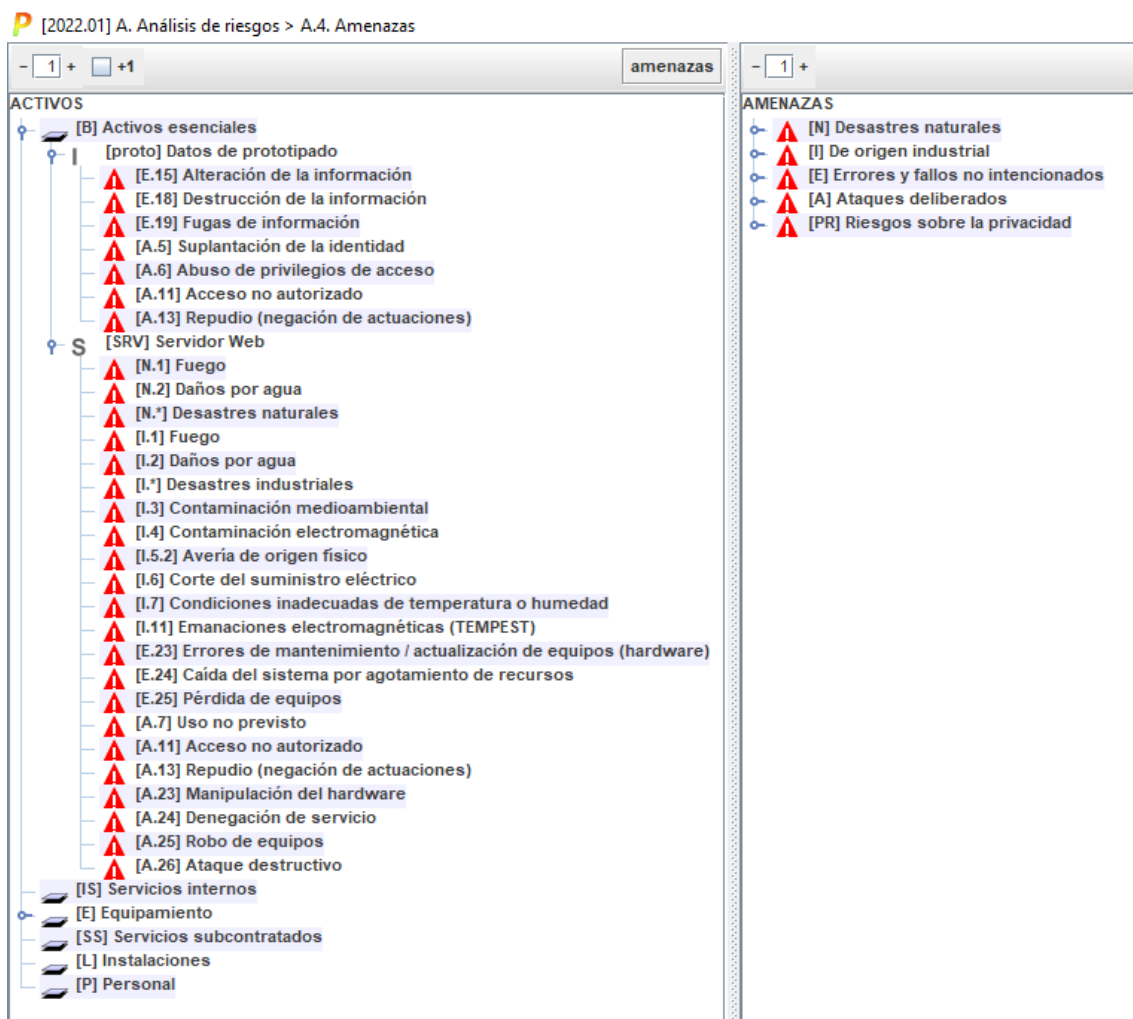


Una vez seleccionados todos estos factores se guardan los datos y se puede proceder al siguiente paso.

## Amenazas.

De forma predeterminada, este software es capaz de aplicar una serie de amenazas predefinidas y típicas sobre los activos creados. Estas amenazas no se pueden editar directamente, habría que localizar el fichero con nombre “tsv\_last.xlsx” en el directorio de su biblioteca (bib\_es) que se encuentra en Archivos de Programa x86 (en Windows), aunque no es recomendable editar el fichero.

En este caso se muestra una serie de amenazas sobre dos activos creados, un activo esencial de “datos de prototipos” y otro activo esencial de tipo hardware que sería el servidor web.



En la zona izquierda se observan los activos con sus amenazas asociadas, mientras que en la parte derecha la lista de posibles amenazas por categorías.

**Salvaguardas.** (Medidas técnicas y organizativas: Seguridad de la información).

En este paso, PILAR nos ofrece un amplio catálogo de salvaguardas o medidas de seguridad para paliar o eliminar las amenazas existentes. Estas amenazas se encuentran clasificadas, de modo que las opciones hijas son un refinamiento de las superiores. El marcar una u otra depende del grado de exactitud que nos marquemos en nuestro análisis.

Las salvaguardas serán aplicadas a los diferentes dominios de seguridad que se hayan creado. Estas salvaguardas variarán de unos dominios a otros, ya que dependen de las amenazas a las que están expuestos los activos presentes en esos dominios.

Cada una de las salvaguardas tiene asociado un valor que va de 0 a 10 en el que el 0 sería un nivel muy bajo de recomendación de aplicación y el 10 implica una total recomendación de aplicación.

En este caso vamos a ver las salvaguardas que se proponen para el ejemplo que estamos realizando en este tutorial. A continuación, procederemos a explicar cada una de las columnas de información:

[0022.01] A. Análisis de riesgos > A.5. Medidas técnicas y organizativas: Seguridad de la información									
Editar Exportar Ver Importar Estadísticas									
id	aspecto	tdp	recomendación	nivel	salvaguarda	dudas	base	comentario	current
1	G	EL	3	3	SALVAGUARDAS				
2	G	STO	3	3	[A1] Identificación y autenticación				
3	G	PROC	3	3	[A1.1] Se dispone de normativa de identificación y autenticación [A1.1]				
4	G	EL	3	3	[A1.2] Se dispone de procedimientos para las tareas de identificación y autenticación [A1.1]				
5	G	EL	3	3	[A1.3] Identificación de los usuarios				
6	G	EL	3	3	[A1.4] Gestión de la identificación y autenticación de usuario				
7	G	EL	4	3	[A1.5] Cuentas especiales (administración)				
8	G	PR	7	3	[A1.6] El mecanismo de autenticación se inhabilita cuando se ve comprometido o hay sospecha de ello				
9	T	EL	3	3	[A1.7] Canal seguro de autenticación [A1.1]				
10	G	EL	3	3	[A1.8] [cert] Nivel de garantía de la autenticación				
11	G	EL	3	3	[A1.9] Elemento - Algo que eres				
12	G	EL	3	3	[A1.10] Mecanismo de autenticación [NIST SP 800-63]				
13	T	EL	7	3	[A2] Control de acceso lógico				
14	T	PR	3	3	[A2.1] modo evaluación				
15	T	EL	3	3	[A2.2] modo evaluación				
16	T	PR	7	3	[A2.3] modo evaluación				
17	T	IM	4	3	[A2.4] [ST] modo evaluación [A2.4]				
18	T	EL	3	3	[A2.5] modo evaluación [A2.4]				
19	T	PR	3	3	[A2.6] modo evaluación				
20	G	PR	3	3	[A2.7] modo evaluación				
21	G	EL	3	3	[A2.8] modo evaluación				
22	G	PR	3	3	[A2.9] modo evaluación				
23	G	PR	3	3	[A2.10] modo evaluación				
24	G	PR	3	3	[A2.11] modo evaluación				
25	G	PR	3	3	[A2.12] modo evaluación				
26	G	PR	3	3	[A2.13] modo evaluación				
27	G	PR	3	3	[A2.14] modo evaluación				
28	G	PR	3	3	[A2.15] modo evaluación				
29	G	PR	3	3	[A2.16] modo evaluación				
30	G	PR	3	3	[A2.17] modo evaluación				
31	G	PR	3	3	[A2.18] modo evaluación				
32	G	PR	3	3	[A2.19] modo evaluación				
33	G	PR	3	3	[A2.20] modo evaluación				
34	G	PR	3	3	[A2.21] modo evaluación				
35	G	PR	3	3	[A2.22] modo evaluación				
36	G	PR	3	3	[A2.23] modo evaluación				
37	G	PR	3	3	[A2.24] modo evaluación				
38	G	PR	3	3	[A2.25] modo evaluación				
39	G	PR	3	3	[A2.26] modo evaluación				
40	G	PR	3	3	[A2.27] modo evaluación				
41	G	PR	3	3	[A2.28] modo evaluación				
42	G	PR	3	3	[A2.29] modo evaluación				
43	G	PR	3	3	[A2.30] modo evaluación				
44	G	PR	3	3	[A2.31] modo evaluación				
45	G	PR	3	3	[A2.32] modo evaluación				
46	G	PR	3	3	[A2.33] modo evaluación				
47	G	PR	3	3	[A2.34] modo evaluación				
48	G	PR	3	3	[A2.35] modo evaluación				
49	G	PR	3	3	[A2.36] modo evaluación				
50	G	PR	3	3	[A2.37] modo evaluación				
51	G	PR	3	3	[A2.38] modo evaluación				
52	G	PR	3	3	[A2.39] modo evaluación				
53	G	PR	3	3	[A2.40] modo evaluación				
54	G	PR	3	3	[A2.41] modo evaluación				
55	G	PR	3	3	[A2.42] modo evaluación				
56	G	PR	3	3	[A2.43] modo evaluación				
57	G	PR	3	3	[A2.44] modo evaluación				
58	G	PR	3	3	[A2.45] modo evaluación				
59	G	PR	3	3	[A2.46] modo evaluación				
60	G	PR	3	3	[A2.47] modo evaluación				
61	G	PR	3	3	[A2.48] modo evaluación				
62	G	PR	3	3	[A2.49] modo evaluación				
63	G	PR	3	3	[A2.50] modo evaluación				
64	G	PR	3	3	[A2.51] modo evaluación				
65	G	PR	3	3	[A2.52] modo evaluación				
66	G	PR	3	3	[A2.53] modo evaluación				
67	G	PR	3	3	[A2.54] modo evaluación				
68	G	PR	3	3	[A2.55] modo evaluación				
69	G	PR	3	3	[A2.56] modo evaluación				
70	G	PR	3	3	[A2.57] modo evaluación				
71	G	PR	3	3	[A2.58] modo evaluación				
72	G	PR	3	3	[A2.59] modo evaluación				
73	G	PR	3	3	[A2.60] modo evaluación				
74	G	PR	3	3	[A2.61] modo evaluación				
75	G	PR	3	3	[A2.62] modo evaluación				
76	G	PR	3	3	[A2.63] modo evaluación				
77	G	PR	3	3	[A2.64] modo evaluación				
78	G	PR	3	3	[A2.65] modo evaluación				
79	G	PR	3	3	[A2.66] modo evaluación				
80	G	PR	3	3	[A2.67] modo evaluación				
81	G	PR	3	3	[A2.68] modo evaluación				
82	G	PR	3	3	[A2.69] modo evaluación				
83	G	PR	3	3	[A2.70] modo evaluación				
84	G	PR	3	3	[A2.71] modo evaluación				
85	G	PR	3	3	[A2.72] modo evaluación				
86	G	PR	3	3	[A2.73] modo evaluación				
87	G	PR	3	3	[A2.74] modo evaluación				
88	G	PR	3	3	[A2.75] modo evaluación				
89	G	PR	3	3	[A2.76] modo evaluación				
90	G	PR	3	3	[A2.77] modo evaluación				
91	G	PR	3	3	[A2.78] modo evaluación				
92	G	PR	3	3	[A2.79] modo evaluación				
93	G	PR	3	3	[A2.80] modo evaluación				
94	G	PR	3	3	[A2.81] modo evaluación				
95	G	PR	3	3	[A2.82] modo evaluación				
96	G	PR	3	3	[A2.83] modo evaluación				
97	G	PR	3	3	[A2.84] modo evaluación				
98	G	PR	3	3	[A2.85] modo evaluación				
99	G	PR	3	3	[A2.86] modo evaluación				
100	G	PR	3	3	[A2.87] modo evaluación				

En la parte superior, bajo el menú de opciones se puede observar que está seleccionado el dominio de “intranet”. En la ventana de contenido hay una serie de columnas, las cuales son:

- Aspecto: hace referencia al campo en el que se aplica, como puede ser:
  - Gestión (G).
  - Técnico (T).
  - Seguridad física (F).
  - Personal (P).
- TDP: Tipo de protección que proporciona la salvaguarda:
  - Prevención (PR).
  - Disuasión (DR).
  - Eliminación (EL).
  - Minimización del impacto (IM).
  - Corrección (CR).
  - Administrativa (AD).
  - Concienciación (AW).
  - Detección (DC).
  - Monitorización (MN).
  - Norma (std).
  - Procedimiento (proc).
  - Recuperación (RC).
  - Certificación o acreditación (cert).
- Salvaguardas: tienen asociadas un peso en función de su importancia, que va de 0 a 3. Algunas se implementan de forma exclusiva y van identificadas porque comienzan por {xor}. Se debe seleccionar la que se quiere usar y sus valores aparecerán entre [].
- Dudas: indica que no se tiene clara la actuación.
- Base: puede tomar el valor n.a. (no asignable) el cual se indica a todas las salvaguardas que no procedan o no tengan un valor de recomendación asignado. El resto se marca con “...” pero para ello se debe pulsar en la celda con el botón derecho y seleccionar “recomendación”.
- Comentario: Se pueden incluir diferentes comentarios a las salvaguardas asociados a las diferentes fases del proyecto, para esclarecer las actuaciones a llevar a cabo.
- Current: marca el nivel actual en el que se encuentra actualmente implementada esa salvaguarda, en todas las salvaguardas no tienen cabida todos los niveles de valores. Los posibles valores son:

- L0 → Inexistente.
- L1 → Inicial /ad hoc.
- L2 → Reproducible, pero intuitivo.
- L3 → Proceso definido.
- L4 → Gestionado y medible.
- L5 → Optimizado.
- Target: marca el nivel que se pretende conseguir tras la aplicación de las acciones para implementar la salvaguarda.
- PILAR: esta columna marca el rango de niveles recomendables que se deberían alcanzar.

IMPORTANTE: En la versión de evaluación no se muestran las salvaguardas de segundo o más nivel (muestra “modo evaluación”), solo las de nivel superior. La única que se muestra al completo es la salvaguarda de “Identificación y autenticación”.

salvaguarda	dudas	base	comentario	current	target	PILAR
SALVAGUARDAS						
✓ [A] Identificación y autenticación				L0-L1	L0-L3	L2-L4
✓ [A.1] Se dispone de normativa de identificación y autenticación [A-1]		---		L0-L1	L0-L3	L2-L4
✓ [A.2] Se dispone de procedimientos para las tareas de identificación y autenticación [A-1]				L0	L1	L2
✓ [A.3] Identificación de los usuarios				L1	L1	L2
✓ [A.4] Gestión de la identificación y autenticación de usuario				L1	L3	L3
✓ [A.5] Cuentas especiales (administración)				L1	L2	L2-L3
✓ [A.6] El mecanismo de autenticación se inhabilita cuando se ve comprometido o hay sospecha de ello				L1	L2	L2-L3
✓ [A.7] Canal seguro de autenticación [SC-11]				L0	L0	L4
✓ [A.8] [xor] Nivel de garantía de la autenticación				L0	L0	L4
✓ [A.9] Biometría - Algo que eres				n.a.	n.a.	n.a.
✓ [A.10] Mecanismo de autenticación (NIST SP 800-63)		n.a.		L0	L1	L3
✓ [AC] Control de acceso lógico		---		L1	L2	L2-L4
✓ [AC.1] modo evaluación				L1	L2	L2-L3
✓ [AC.2] modo evaluación				L1	L2	L2-L3
✓ [AC.3] modo evaluación				L1	L2	L4
✓ [H.5T] modo evaluación [AC-5]		---		L1	L2	L2-L3
✓ [AC.5] modo evaluación [AC-17]				L1	L2	L2-L3
✓ [AC.6] modo evaluación				L1	L2	L3
✓ [D] Protección de la información		---		L0	L0	L2-L3
✓ [D.1] Protección de claves criptográficas [SC-12]		n.a.		n.a.	n.a.	n.a.

Tras definir todos los valores en cada uno de los ámbitos, ya tendríamos definidas las actuaciones a llevar a cabo para reducir las amenazas.

## Datos personales.

En el manejo de datos personales se debe indicar siempre su naturaleza, tratamiento y finalidad. En la declaración de activos, si alguno está relacionado con el tratamiento de estos datos se debe indicar para aplicar la normativa vigente en cuanto a protección de datos. Esta normativa está definida en España por la LODPGDD que se basa en la norma europea RGPD.

En este tutorial no se incluye el uso de esta sección.

## Riesgos.

Por último, se debe obtener información de los riesgos a los que está sometido la empresa, que riesgo residual quedará tras aplicar las salvaguardas marcadas y si este es un riesgo asumible por la empresa.

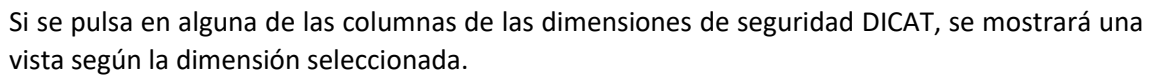
PILAR marca los riesgos con un valor y una gama de colores.



El software muestra los riesgos en cuatro pestañas:

- Potencial: Riesgos potenciales que puede alcanzar la empresa si no se toman medidas.
- Current: Nivel de riesgo actual.

- En cada una de estas pestañas se muestran los riesgos de la lista de activos creada. Estos activos pueden ser expandidos y se pueden observar las amenazas que les afectan con el grado de riesgo que aplican.



La versión de evaluación solo permite visualizar las gráficas de riesgo desde el propio programa.

Ejemplo:

