



Incidentes de Ciberseguridad

Tarea 2

ESTHER CARRILLO GÁLVEZ

Índice

Apartado 1: Priorización y jerarquía de activos: A partir de la lista de activos de la introducción, se deben priorizar y jerarquizar.....	3
Apartado 2: Valoración de los dominios de seguridad.	10
Apartado 3: Determinación de las amenazas y sus salvaguardas dispuestas.	12
Apartado 4: Estimación del riesgo que tendría que considerar la empresa para su estudio y toma de decisiones.....	15
Apartado 5: Taxonomía de incidentes.	18
Bibliografía.....	19

Apartado 1: Priorización y jerarquía de activos: A partir de la lista de activos de la introducción, se deben priorizar y jerarquizar

Activo	Dirección IP	Función empresa	Esencial	Justificación
ERP	192.168.1.25	Soporte Gestor Empresarial	Servicio	Un fallo podría paralizar las finanzas de la producción.
SCADA	192.168.1.23	Supervisión / Control / Firewall / Inventario		Podría suponer la paralización de la fábrica y poner en riesgo la integridad y disponibilidad de los datos.
B.D. ECO/FIN	192.168.1.25	Base de datos ECO/FIN	Información	Contiene datos financieros muy sensibles que podrían suponer un riesgo económico importante para la empresa en caso de filtración/modificación.
Router	192.168.1.1	Conexión a internet	Red	Punto de conexión a internet frontera de seguridad.
MES	192.168.1.24	Servidor Gestor Factoría		Su fallo interrumpe directamente la

				producción. Sirve como puente de ataque entre la red TI y la OT.
Switch	192.168.1.11	Three-Legged Switch		Un fallo provocaría en la segmentación de la red supone un riesgo para la comunicación interna.
PLC	192.168.1.22	Controlador lógico		Puede suponer un fallo en la línea de producción.
Puestos trabajo	192.168.1.50-99	Puestos de trabajo	Equipamiento informático	Muy crítico porque es la entrada para el malware
SOC	192.168.1.101	IDS/SIEM/NAS/VAUTL		Un fallo no supone la paralización de la producción.
Big Data IA	192.168.1.50-99	Sistemas Big Data, IA		Un fallo no supone un gran riesgo en la producción diaria.
Portal Web	192.168.1.102	Portales web		Un fallo afecta a la comunicación, pero no a la producción.
Maquetas, Prot. y Lanzaderas	192.168.1.102	Maquetas, prototipos, lanzaderas		Su fallo no afecta a los sistemas en producción.

Relación y dependencias entre los activos

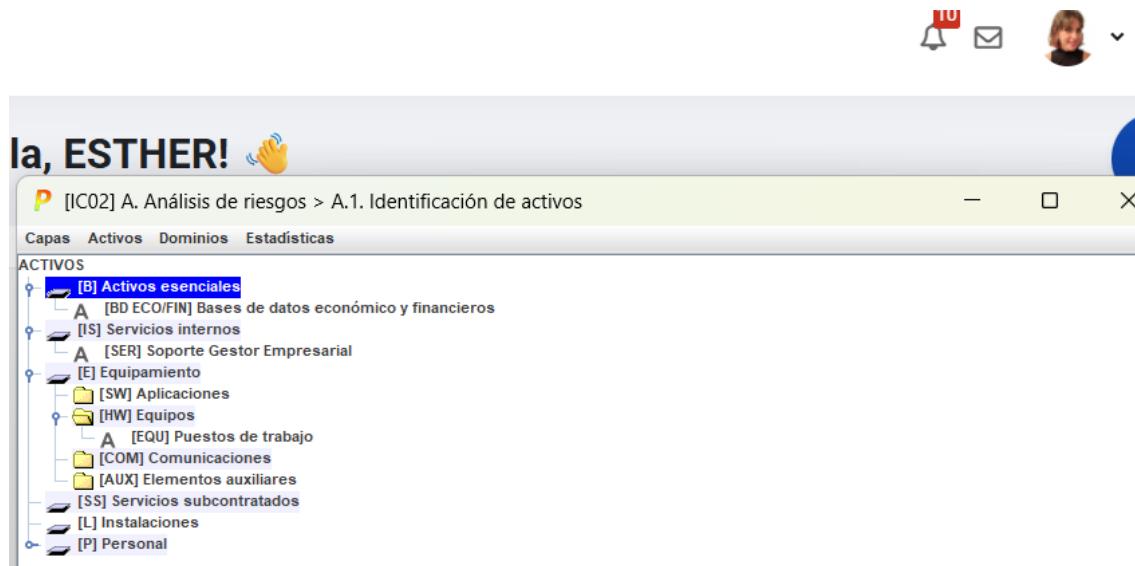
Activo	Dependencias	Justificación
ERP	BD ECO/FIN, BD Inventario, MES, Switch, Router	Centraliza los datos recogidos del MES, de la BD y depende de la comunicación entre redes del switch y el router.
SCADA	MES, Switch, Router, PLC	Gestiona los procesos industriales, combinando los datos recibidos del MES y PLC. Y depende del router y switch para la conectividad entre redes.
BD ECO/FIN	SOC, ERP, Switch, Router	Los datos recogidos deben ponerse en común en el ERP para poder ser gestionados. Deben ser monitorizados por el SOC.
BD Inventario	SCADA, ERP, MES	Almacena y supervisa el stock actual. El ERP administra los datos, el SCADA los supervisa y el MES lo desarrolla.
Router	Switch	El switch proporciona la conectividad de todas las subredes.
MES	ERP, SCADA, PLC, Switch	Sin el ERP y el SCADA los datos de producción, no podrían ser gestionados ni controlados. Todos dependen del PLC para generar la información a tiempo real de la producción.
Switch	Router, servidores	La conectividad y conexión de los activos dependen de los dispositivos conectados.

PLC	SCADA, Switch, MES	Automatizan los procesos industriales gracias a los datos y órdenes de SCADA y MES.
Puestos de trabajo	ERP, Big Data, Switch, SOC, SCADA, MES, Router, Switch	La plantilla depende de los sistemas y de la conectividad para realizar las tareas pertinentes a la gestión de la empresa.
SOC	Router, Switch, servidores	Se basan en los logs y tráfico de la red para monitorizar y supervisar la red.
Big Data, IA	Todas las BD, MES, SCADA	Analiza datos provenientes de otros sistemas internos.
Portal web	Router, Switch, Labo_Server	Requiere del servidor Labo_Server para su alojamiento y del router para la conexión a internet.

Se creará un nuevo proyecto desde la ventana principal y se introducen los datos pertinentes al proyecto.



Se seleccionan los cuatro activos indicados en la tabla para su previo uso en la herramienta PILAR (Proceso Informático de Localización y Análisis de Riesgos)



☰

¡Hola, ESTHER! 🤝

P [IC02] A. Análisis de riesgos > A.1. Identificación de activos > activo

código BD ECO/FIN	CLASES DE ACTIVOS
nombre Bases de datos económico y financieros	<ul style="list-style-type: none"> ↳ <input checked="" type="checkbox"/> [essential] Información y servicios esenciales <ul style="list-style-type: none"> ↳ <input checked="" type="checkbox"/> [info] información <ul style="list-style-type: none"> <input type="checkbox"/> [biz] datos de interés para el negocio <input type="checkbox"/> [com] datos de interés comercial <input type="checkbox"/> [adm] datos de la administración pública <input checked="" type="checkbox"/> [vr] datos vitales (registros de la organización) <input type="checkbox"/> [per] datos personales <input checked="" type="checkbox"/> [classified] información clasificada ↳ <input type="checkbox"/> [service] servicio <input type="checkbox"/> [bp] proceso de negocio <input type="checkbox"/> [ppd] tratamiento de datos personales ↳ <input type="checkbox"/> [arch] Arquitectura del sistema ↳ <input type="checkbox"/> [qualifier] Características ↳ <input type="checkbox"/> [D] Datos / Información ↳ <input type="checkbox"/> [keys] Claves criptográficas ↳ <input type="checkbox"/> [S] Servicios ↳ <input type="checkbox"/> [SW] Aplicaciones (software) ↳ <input type="checkbox"/> [HW] Equipamiento informático (hardware) ↳ <input type="checkbox"/> [COM] Redes de comunicaciones ↳ <input type="checkbox"/> [Media] Soportes de información ↳ <input type="checkbox"/> [AUX] Equipamiento auxiliar ↳ <input type="checkbox"/> [L] Instalaciones ↳ <input type="checkbox"/> [P] Personal ↳ <input type="checkbox"/> [other] Otras clases
dominio [INF] Información	
datos	

☰

¡Hola, ESTHER! 🤝

P [IC02] A. Análisis de riesgos > A.1. Identificación de activos > activo

código SER	CLASES DE ACTIVOS
nombre Soporte Gestor Empresarial	<ul style="list-style-type: none"> ↳ <input checked="" type="checkbox"/> [essential] Información y servicios esenciales <ul style="list-style-type: none"> ↳ <input type="checkbox"/> [info] información ↳ <input checked="" type="checkbox"/> [service] servicio <ul style="list-style-type: none"> <input checked="" type="checkbox"/> [operations] operaciones <ul style="list-style-type: none"> <input type="checkbox"/> [logistics] de logística <input type="checkbox"/> [intelligence] de inteligencia <input type="checkbox"/> [personnel] relativos al personal <input type="checkbox"/> [financial] financieros <input type="checkbox"/> [administrative] administrativos <input type="checkbox"/> [programme] programas <input type="checkbox"/> [project] proyecto <input type="checkbox"/> [bp] proceso de negocio <input type="checkbox"/> [ppd] tratamiento de datos personales ↳ <input type="checkbox"/> [arch] Arquitectura del sistema ↳ <input type="checkbox"/> [qualifier] Características ↳ <input type="checkbox"/> [D] Datos / Información ↳ <input type="checkbox"/> [keys] Claves criptográficas ↳ <input checked="" type="checkbox"/> [S] Servicios ↳ <input type="checkbox"/> [SW] Aplicaciones (software) ↳ <input type="checkbox"/> [HW] Equipamiento informático (hardware) ↳ <input type="checkbox"/> [COM] Redes de comunicaciones ↳ <input type="checkbox"/> [Media] Soportes de información ↳ <input type="checkbox"/> [AUX] Equipamiento auxiliar ↳ <input type="checkbox"/> [L] Instalaciones ↳ <input type="checkbox"/> [P] Personal ↳ <input type="checkbox"/> [other] Otras clases
dominio [SER] Servicios	
datos	

Hola, ESTHER!

P [IC02] A. Análisis de riesgos > A.1. Identificación de activos > activo

código
EQU

nombre
Puestos de trabajo

dominio
[EQU] Equipamientos Informáticos

datos

CLASES DE ACTIVOS

- ↳ [essential] Información y servicios esenciales
- ↳ [info] información
- ↳ [service] servicio
 - [operations] operaciones
 - [logistics] de logística
 - [intelligence] de inteligencia
 - [personnel] relativos al personal
 - [financial] financieros
 - [administrative] administrativos
 - [programme] programas
 - [project] proyecto
 - [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)
 - [host] grandes equipos (host)
 - [mid] equipos medios
 - [pc] informática personal
 - [mobile] informática móvil
 - [hand-held] dispositivos de mano
 - [pda] agendas electrónicas
 - [vhost] equipos virtuales (máquinas virtuales)
 - [cluster] cluster
 - [backup] equipamiento de respaldo

Hola, ESTHER!

P [IC02] A. Análisis de riesgos > A.1. Identificación de activos > activo

código
RED

nombre
Acceso principal Internet

dominio
[RED] Acceso principal Internet

datos

CLASES DE ACTIVOS

- ↳ [essential] Información y servicios esenciales
- ↳ [info] información
- ↳ [service] servicio
 - [operations] operaciones
 - [logistics] de logística
 - [intelligence] de inteligencia
 - [personnel] relativos al personal
 - [financial] financieros
 - [administrative] administrativos
 - [programme] programas
 - [project] proyecto
 - [bp] proceso de negocio
 - [ppd] tratamiento de datos personales
- ↳ [arch] Arquitectura del sistema
 - [sap] punto de [acceso al] servicio
- ↳ [ip] sistema de protección de frontera lógica
 - [0] no hay nada
 - [pkt] filtro de paquetes (nivel 3)
 - [firewall] cortafuegos (control de sesión)
 - [proxy] monitorización de la aplicación (nivel 7)
 - [r2p] 1 cortafuegos (2 puertas) + agente proxy
 - [r3p] 1 cortafuegos (3 puertas) + agente proxy
 - [dmz] 2 cortafuegos + dmz + agente proxy
 - [gtwy] pasarela (cambio de protocolo)
 - [ine] INE (cifrado de la información en tránsito)
 - [diode] diodo (dispositivo unidireccional)
 - [gap] air gap (air wall)
 - [pps] sistema de protección física del perímetro
 - [tempest] protección contra emanaciones electromagnéticas

Apartado 2: Valoración de los dominios de seguridad.

En este apartado se determina el nivel de importancia que tienen los activos esenciales en sus diferentes dominios de seguridad definidos. Además, se indican un par de factores atenuantes por cada dominio.

A continuación, se hará una valoración del nivel de seguridad que debe tener cada uno de los activos esenciales creados.

activo / dominio de seguridad	[D]	[I]	[C]	[A]	[T]	[DP]
[IC02] IC02-Clasificación de Riesgos y Potenciales Incidentes						
↳ [essential] Información y servicios esenciales	[10]	[10]	[10]	[10]	[9]	
↳ [BD ECO/FIN] Bases de datos económico y financieros	[10]	[10]	[10]	[9]	[9]	
↳ [SER] Soporte Gestor Empresarial	[10]	[8]	[8]	[10]	[9]	
↳ [P] Puestos de trabajo	[8]	[9]	[8]	[7]	[7]	
↳ [RED] Acceso principal Internet	[10]	[9]	[10]	[9]	[9]	
↳ Dominios de seguridad						
↳ [base] Base						
↳ [SER] Servicios	[10]	[8]	[8]	[10]	[9]	
↳ [SER] Soporte Gestor Empresarial	[10]	[8]	[8]	[10]	[9]	
↳ [RED] Acceso principal Internet	[10]	[9]	[10]	[9]	[9]	
↳ [EQU] Equipamientos Informáticos	[8]	[9]	[8]	[7]	[7]	
↳ [INF] Información	[10]	[10]	[10]	[9]	[9]	

Se identifican los factores agravantes y atenuantes de cada uno de los dominios de seguridad de la empresa.

Dominio Servicios [SER]

criterios
Domini... ↳ [base] Base ↳ [SER] Servicios ↳ [111.d] (30%) conectado a Internet ↳ [105.a] (10%) se permite el acceso a Internet ↳ [104.e] (10%) con conflictos de interés ↳ [106.d] (10%) objetivo muy atractivo ↳ [103.b] (10%) muy interesado ↳ [102.g] (5%) con ánimo de causar daño ↳ [102.a] (5%) económica (beneficios en dinero) ↳ [101.g] (10%) personal interno ↳ [101.b] (5%) competidor comercial ↳ [101.a] () público en general

Dominio Acceso principal Internet [RED]

The screenshot shows a user interface for the RED domain. At the top, there's a header with a yellow 'P' icon, the text '[IC02] A. Análisis de riesgos > A.3. Factores agravantes | atenuantes', and a 'criterio' button. Below the header is a tree view of risk factors under the 'Acceso principal Internet' category. The categories and their sub-items are:

- [101.a] () público en general
- [111.b] () conectado a un conjunto reducido y controlado de redes
 - [105.a] (10%) se permite el acceso a Internet
 - [104.d] (10%) con problemas de conciencia
 - [106.d] (10%) objetivo muy atractivo
 - [103.b] (10%) muy interesado
 - [102.h] (5%) con ánimo de provocar pérdidas
 - [101.h] (10%) bandas criminales
 - [101.b] (5%) competidor comercial
 - [101.a] () público en general

Dominio Equipamientos Informáticos [EQU]

The screenshot shows a user interface for the EQU domain. At the top, there's a header with a yellow 'P' icon, the text '[IC02] A. Análisis de riesgos > A.3. Factores agravantes | atenuantes', and a 'criterio' button. Below the header is a tree view of risk factors under the 'Equipamientos Informáticos' category. The categories and their sub-items are:

- Domínicos de seguridad
 - [base] Base
 - [SER] Servicios
 - [RED] Acceso principal Internet
 - [EQU] Equipamientos Informáticos
 - [111.d] (30%) conectado a Internet
 - [105.a] (10%) se permite el acceso a Internet
 - [104.d] (10%) con problemas de conciencia
 - [106.d] (10%) objetivo muy atractivo
 - [103.b] (10%) muy interesado
 - [102.h] (5%) con ánimo de provocar pérdidas
 - [102.b] (5%) beneficios comerciales
 - [101.h] (10%) bandas criminales
 - [101.g] (10%) personal interno
 - [101.b] (5%) competidor comercial
 - [101.a] () público en general
 - [INF] Información

Dominio Información [INF]

The screenshot shows a user interface for the INF domain. At the top, there's a header with a yellow 'P' icon, the text '[IC02] A. Análisis de riesgos > A.3. Factores agravantes | atenuantes', and a 'criterio' button. Below the header is a tree view of risk factors under the 'Información' category. The categories and their sub-items are:

- Domínicos de seguridad
 - [base] Base
 - [SER] Servicios
 - [RED] Acceso principal Internet
 - [EQU] Equipamientos Informáticos
 - [INF] Información
 - [106.d] (10%) objetivo muy atractivo
 - [103.b] (10%) muy interesado
 - [102.f] (5%) con ánimo destructivo
 - [102.b] (5%) beneficios comerciales
 - [101.h] (10%) bandas criminales
 - [101.b] (5%) competidor comercial
 - [101.a] () público en general

Apartado 3: Determinación de las amenazas y sus salvaguardias dispuestas.

Amenazas localizadas en cada uno de los activos:

[BD ECO/FIN] Bases de datos económicos y financieros y [SER] Soporte Gestor Empresarial

The screenshot shows a software interface for threat analysis. At the top, there's a navigation bar with links: Página Principal, Área personal, Mis cursos, Mis cursos (dropdown), Recursos, and Enlaces. On the far right, there are icons for notifications (14), a bell, and an envelope.

The main area has two panels. The left panel is titled "ASSETS" and contains a tree view of assets:

- [B] Activos esenciales
 - [BD ECO/FIN] Bases de datos económico y financieros
 - [A.13] Repudio (negación de actuaciones)
- [IS] Servicios internos
 - [SER] Soporte Gestor Empresarial
 - [A.13] Repudio (negación de actuaciones)
- [E] Equipamiento
- [SS] Servicios subcontratados
- [L] Instalaciones
- [P] Personal

The right panel is titled "THREATS" and contains a tree view of threats:

- [N] Desastres naturales
- [I] De origen industrial
- [E] Errores y fallos no intencionados
- [A] Ataques deliberados
- [PR] Riesgos sobre la privacidad

[EQU] Puestos de Trabajo

The screenshot shows a software interface for threat analysis. At the top, there's a navigation bar with links: Página Principal, Área personal, Mis cursos, Mis cursos (dropdown), Recursos (dropdown), and Enlaces (dropdown). On the far right, there are icons for notifications (14), a bell, and email.

The main window title is "[IC02] A. Analysis > A.4. Threats". The left pane is titled "ASSETS" and contains a hierarchical tree view:

- [B] Activos esenciales
- [IS] Servicios internos
- [E] Equipoamiento
 - [SW] Aplicaciones
 - [HW] Equipos
 - [EQU] Puestos de trabajo
 - [N.1] Fuego
 - [N.2] Daños por agua
 - [N.3] Desastres naturales
 - [I.1] Fuego
 - [I.2] Daños por agua
 - [I.3] Desastres industriales
 - [I.3] Contaminación medioambiental
 - [I.4] Contaminación electromagnética
 - [I.5.2] Avería de origen físico
 - [I.6] Corte del suministro eléctrico
 - [I.7] Condiciones inadecuadas de temperatura o humedad
 - [I.11] Emanaciones electromagnéticas (TEMPEST)
 - [E.23] Errores de mantenimiento / actualización de equipos (hardware)
 - [E.24] Caída del sistema por agotamiento de recursos
 - [E.25] Pérdida de equipos
 - [A.7] Uso no previsto
 - [A.11] Acceso no autorizado
 - [A.13] Repudio (negación de actuaciones)
 - [A.23] Manipulación del hardware
 - [A.24] Denegación de servicio
 - [A.25] Robo de equipos
 - [A.26] Ataque destructivo
 - [COM] Comunicaciones
 - [AUX] Elementos auxiliares
 - [SS] Servicios subcontratados
 - [I] Instalaciones
 - [P] Personal

The right pane is titled "THREATS" and lists the following categories:

 - [N] Desastres naturales
 - [I] De origen industrial
 - [E] Errores y fallos no intencionados
 - [A] Ataques deliberados
 - [PR] Riesgos sobre la privacidad

At the bottom right, there are "Close" and "help" buttons.

[RED] Acceso principal Internet

The screenshot shows the cidead software interface with the following details:

- Header:** Página Principal, Área personal, Mis cursos, Mis cursos ▾, Recursos ▾, Enlaces ▾, 14 notifications, and user profile.
- Left Panel (Assets):**
 - ASSETS**
 - [B] Activos esenciales
 - [IS] Servicios internos
 - [E] Equipo
 - [SW] Aplicaciones
 - [HW] Equipos
 - [COM] Comunicaciones
 - [RED] Acceso principal Internet
 - [E.8] Fallo de servicios de comunicaciones
 - [E.2] Errores del administrador del sistema / de la seguridad
 - [E.9] Errores de [re]-encaminamiento
 - [E.10] Errores de secuencia
 - [E.15] Alteración de la información
 - [E.19] Fugas de información
 - [E.24] Caida del sistema por agotamiento de recursos
 - [A.5] Suplantación de la identidad
 - [A.7] Uso no previsto
 - [A.9] [Re]-encaminamiento de mensajes
 - [A.10] Alteración de secuencia
 - [A.11] Acceso no autorizado
 - [A.12] Análisis de tráfico
 - [A.13] Repudio (negación de actuaciones)
 - [A.14] Intercepción de información (escucha)
 - [A.15] Modificación de la información
 - [A.18] Destrucción de la información
 - [A.24] Denegación de servicio
 - [A.51] Inyección de código malicioso (a través de una frontera lógica)
 - [A.52] Extracción de información (a través de una frontera lógica)
 - [A.53] Acceso no autorizado (a través de una frontera lógica)
 - [AUX] Elementos auxiliares
 - [SS] Servicios subcontratados
 - [L] Instalaciones
 - [P] Personal - Central Panel (Threats):**
 - threats**
 - [] +
 - THREATS**
 - [N] Desastres naturales
 - [I] De origen industrial
 - [E] Errores y fallos no intencionados
 - [A] Ataques deliberados
 - [PR] Riesgos sobre la privacidad- Right Panel (Assets):**
 - assets**
 - [] +

Salvaguardas asociadas a cada activo.

Dominio Servicios [SER]

P [I]C02] A.5. Medidas > A.5.1. Salvaguardas									
Editar Expandir Ver Exportar Importar Estadísticas									
[SER] Servicios									
aspe...	tdp	reco...	nivel	salvaguarda	dud...	aplica	com...	curr...	surg...
				SALVAGUARDAS					L2-L3
<input type="checkbox"/>	G	EL		○ [IA] Identificación y autenticación					n.a.
<input type="checkbox"/>	T	EL		○ [AC] Control de acceso lógico					n.a.
<input type="checkbox"/>	G	PR		○ [D] Protección de la Información					n.a.
<input type="checkbox"/>	G	EL		○ [K] Protección de claves criptográficas [SC-12]					n.a.
<input type="checkbox"/>	G	PR	2	○ [S] Protección de los Servicios					L2
<input type="checkbox"/>	G	PR		○ [SW] Protección de las Aplicaciones Informáticas (SW)					n.a.
<input type="checkbox"/>	G	PR		○ [HW] Protección de los Equipos Informáticos (HW)					n.a.
<input type="checkbox"/>	G	PR		○ [COM] Protección de las Comunicaciones					n.a.
<input type="checkbox"/>	G	PR		○ [M] Protección de los Soportes de Información					n.a.
<input type="checkbox"/>	G	PR		○ [AUX] Elementos Auxiliares					n.a.
<input type="checkbox"/>	F	EL		○ [PPE] Protección física de los equipos					n.a.
<input type="checkbox"/>	F	PR		○ [L] Protección de las instalaciones					n.a.
<input type="checkbox"/>	P	PR		○ [P] Gestión del Personal					n.a.
<input type="checkbox"/>	G	CR	5	○ [M] Gestión de incidentes					L2-L3
<input type="checkbox"/>	T	PR		○ [Tools] Herramientas de seguridad					n.a.
<input type="checkbox"/>	G	CR		○ [V] Gestión de vulnerabilidades					n.a.
<input type="checkbox"/>	T	MN	4	○ [A] Registro y auditoría					L2-L3
<input type="checkbox"/>	G	RC		○ [BC] Continuidad del negocio					n.a.
<input type="checkbox"/>	G	AD	4	○ [G] Organización					L2-L3
<input type="checkbox"/>	G	AD		○ [E] Relaciones Externas					n.a.
<input type="checkbox"/>	G	AD	2	○ [NEW] Adquisición / desarrollo					L2
<input type="checkbox"/>	G	PR		○ [PDS] Servicios potencialmente peligrosos					n.a.
<input type="checkbox"/>	G	PR		○ [IP] Sistema de protección de frontera lógica					n.a.
<input type="checkbox"/>	F	EL		○ [PPS] Protección del perímetro físico					n.a.
<input type="checkbox"/>	G	EL		○ [TEMPEST] Protección de emanaciones (TEMPEST) [PE-19]					n.a.

Dominio Equipamientos Informáticos [EQU]

P [IC02] A.5. Medidas > A.5.1. Salvaguardas

Editar Expandir Ver Exportar Importar Estadísticas

EQU] Equipamientos Informáticos				salvaguarda	dud...	aplica	com...	curr...	largo	PILAR
aspe...	tdp	reco...	nivel							
			SALVAGUARDAS							L2-L3
	G	EL		• [IA] Identificación y autenticación						n.a.
	T	EL		• [AC] Control de acceso lógico						n.a.
	G	PR		• [D] Protección de la Información						n.a.
	G	EL		• [K] Protección de claves criptográficas [SC-12]						n.a.
	G	PR		• [S] Protección de los Servicios						n.a.
	G	PR	5	• [SW] Protección de las Aplicaciones Informáticas (SW)						n.a.
	G	PR		• [HW] Protección de los Equipos Informáticos (HW)						L2-L3
	G	PR		• [COM] Protección de las Comunicaciones						n.a.
	G	PR		• [M] Protección de los Soportes de Información						n.a.
	G	PR	4	• [AUX] Elementos Auxiliares						L2-L3
	F	EL	5	• [PPE] Protección física de los equipos						L3
	F	PR		• [IL] Protección de las Instalaciones						n.a.
	P	PR		• [P] Gestión del Personal						n.a.
	G	CR	5	• [IM] Gestión de incidentes						L2-L3
	T	PR	4	• [tools] Herramientas de seguridad						L2-L3
	G	CR		• [V] Gestión de vulnerabilidades						n.a.
	T	MN	4	• [A] Registro y auditoría						L2-L3
	G	RC	3	• [BC] Continuidad del negocio						L2-L3
	G	AD	4	• [G] Organización						L2-L3
	G	AD	3	• [E] Relaciones Externas						L2-L3
	G	AD	4	• [NEW] Adquisición / desarrollo						L2-L3
	G	PR		• [PDS] Servicios potencialmente peligrosos						n.a.
	G	PR		• [IP] Sistema de protección de frontera lógica						n.a.
	F	EL		• [PPS] Protección del perímetro físico						n.a.
	G	EL	1 (o)	• [TEMPEST] Protección de emanaciones (TEMPEST) [PE-19]						L2

Dominio Acceso principal Internet [RED]

P [IC02] A.5. Medidas > A.5.1. Salvaguardas

Editar Expandir Ver Exportar Importar Estadísticas

[RED] Acceso principal Internet				salvaguarda	dud...	aplica	com...	curr...	largo	PILAR
aspe...	tdp	reco...	nivel							
			SALVAGUARDAS							L2-L5
	G	EL		• [IA] Identificación y autenticación						n.a.
	T	EL	7	• [AC] Control de acceso lógico						L2-L4
	G	PR		• [D] Protección de la Información						n.a.
	G	EL		• [K] Protección de claves criptográficas [SC-12]						n.a.
	G	PR		• [S] Protección de los Servicios						n.a.
	G	PR		• [SW] Protección de las Aplicaciones Informáticas (SW)						n.a.
	G	PR		• [HW] Protección de los Equipos Informáticos (HW)						n.a.
	G	PR	9	• [COM] Protección de las Comunicaciones						L2-L5
	G	PR		• [AUX] Elementos Auxiliares						n.a.
	F	EL		• [PPE] Protección física de los equipos						n.a.
	F	PR		• [IL] Protección de las Instalaciones						n.a.
	P	PR		• [P] Gestión del Personal						n.a.
	G	CR	5	• [IM] Gestión de incidentes						L2-L3
	T	PR	7	• [tools] Herramientas de seguridad						L2-L4
	G	CR		• [V] Gestión de vulnerabilidades						n.a.
	T	MN	4	• [A] Registro y auditoría						L2-L3
	G	RC	3	• [BC] Continuidad del negocio						L2-L3
	G	AD	4	• [G] Organización						L2-L3
	G	AD	5	• [E] Relaciones Externas						L2-L3
	G	AD	5	• [NEW] Adquisición / desarrollo						L2-L3
	G	PR		• [PDS] Servicios potencialmente peligrosos						n.a.
	G	PR	7	• [IP] Sistema de protección de frontera lógica						L2-L4
	F	EL		• [PPS] Protección del perímetro físico						n.a.
	G	EL		• [TEMPEST] Protección de emanaciones (TEMPEST) [PE-19]						n.a.

Dominio Información [INF]

The screenshot shows a table titled "[INF] Información" under the "Salvaguardas" section. The table has columns for aspe..., tdp, reco..., nivel, salvaguarda, dud..., aplica, com..., curr..., target, and PILAR. The "target" column contains values such as L2-L3, n.a., and L2-L3. The "PILAR" column contains values such as L2-L3, n.a., and L2-L3.

aspe...	tdp	reco...	nivel	salvaguarda	dud...	aplica	com...	curr...	target	PILAR
				SALVAGUARDAS						L2-L3
	G	EL		• I [IA] Identificación y autenticación						n.a.
	T	EL		• I [AC] Control de acceso lógico						n.a.
	G	PR		• I [D] Protección de la Información						n.a.
	G	EL		• I [K] Protección de claves criptográficas [SC-12]						n.a.
	G	PR		• I [S] Protección de los Servicios						n.a.
	G	PR		• I [SW] Protección de las Aplicaciones Informáticas (SW)						n.a.
	G	PR		• I [HW] Protección de los Equipos Informáticos (HW)						n.a.
	G	PR		• I [COM] Protección de las Comunicaciones						n.a.
	G	PR		• I [M] Protección de los Soportes de Información						n.a.
	G	PR		• I [AUX] Elementos Auxiliares						n.a.
	F	EL		• I [PPE] Protección física de los equipos						n.a.
	F	PR		• I [L] Protección de las Instalaciones						n.a.
	P	PR		• I [P] Gestión del Personal						n.a.
	G	CR	5	• I [IM] Gestión de incidentes						L2-L3
	T	PR		• I [tools] Herramientas de seguridad						n.a.
	G	CR		• I [V] Gestión de vulnerabilidades						n.a.
	T	MN	4	• I [A] Registro y auditoría						L2-L3
	G	RC		• I [BC] Continuidad del negocio						n.a.
	G	AD	4	• I [G] Organización						L2-L3
	G	AD		• I [E] Relaciones Externas						n.a.
	G	AD	2	• I [NEW] Adquisición / desarrollo						L2
	G	PR		• I [PDS] Servicios potencialmente peligrosos						n.a.
	G	PR		• I [IP] Sistema de protección de frontera lógica						n.a.
	F	EL		• I [PPS] Protección del perímetro físico						n.a.
	G	EL		• I [TEMPEST] Protección de emanaciones (TEMPEST) [PE-19]						n.a.

Apartado 4: Estimación del riesgo que tendría que considerar la empresa para su estudio y toma de decisiones.

Se obtiene la información de los riesgos a los que está sometida la empresa y la herramienta PILAR marca los riesgos con un valor y un color.

The screenshot shows a table titled "A.6. Riesgo" under the "Riesgo" section. The table has columns for activo, [D], [I], [C], [A], [T], and [DP]. The "activos" row contains items such as BD ECO/FIN, Soporte Gestor Empresarial, Puestos de trabajo, and Acceso principal Internet. The "PILAR" column contains values such as (5,9), (5,9), (4,8), and (5,9).

activo	[D]	[I]	[C]	[A]	[T]	[DP]
ACTIVOS	(7,4)	(6,1)	(6,5)	(6,5)	(5,9)	
I [BD ECO/FIN] Bases de datos económico y financieros					(5,9)	
S [SER] Soporte Gestor Empresarial					(5,9)	
S [EQUI] Puestos de trabajo	(6,3)	(4,9)	(5,5)		(4,8)	
S [RED] Acceso principal Internet	(7,4)	(6,1)	(6,5)	(6,5)	(5,9)	

Página Principal Área personal Mis cursos Más ▾ Modo

15

[ICO2] A. Análisis de riesgos > A.6. Riesgo

Exportar

	potencial	current	target	PILAR	[D]	[I]	[C]	[A]	[T]	[DP]
ACTIVOS										
I [BD ECO/FIN] Bases de datos económico y financieros					(7,4)	(5,5)	(6,5)	(6,5)	(5,9)	
S [SER] Soporte Gestor Empresarial									(5,9)	
S [EQU] Puestos de trabajo					(6,3)	(4,9)	(5,5)		(4,8)	
S [RED] Acceso principal Internet					(7,4)	(5,5)	(6,5)	(6,5)	(5,9)	

Página Principal Área personal Mis cursos Más ▾ Modo

15

[ICO2] A. Análisis de riesgos > A.6. Riesgo

Exportar

	potencial	current	target	PILAR	[D]	[I]	[C]	[A]	[T]	[DP]
ACTIVOS										
I [BD ECO/FIN] Bases de datos económico y financieros					(7,4)	(5,5)	(6,5)	(6,5)	(5,9)	
S [SER] Soporte Gestor Empresarial									(5,9)	
S [EQU] Puestos de trabajo					(6,3)	(4,9)	(5,5)		(4,8)	
S [RED] Acceso principal Internet					(7,4)	(5,5)	(6,5)	(6,5)	(5,9)	

Página Principal Área personal Mis cursos Más ▾ Modo

15

[ICO2] A. Análisis de riesgos > A.6. Riesgo

Exportar

	potencial	current	target	PILAR	[D]	[I]	[C]	[A]	[T]	[DP]
ACTIVOS										
I [BD ECO/FIN] Bases de datos económico y financieros					(6,1)	(5,5)	(5,9)	(3,3)	(3,0)	
S [SER] Soporte Gestor Empresarial									(3,0)	
S [EQU] Puestos de trabajo					(3,3)	(1,8)	(2,5)		(1,8)	
S [RED] Acceso principal Internet					(6,1)	(5,5)	(5,9)	(3,3)	(2,9)	

Página Principal Área personal Mis cursos Más ▾ Modo

15

[ICO2] A. Análisis de riesgos > A.6. Riesgo

Exportar

	[D]	[I]	[C]	[A]	[T]	[DP]	potencial	current	target	PILAR
ACTIVOS										
I [BD ECO/FIN] Bases de datos económico y financieros							(7,4)	(7,4)	(7,4)	(6,1)
S [SER] Soporte Gestor Empresarial										
S [EQU] Puestos de trabajo							(6,3)	(6,3)	(6,3)	(3,3)
S [RED] Acceso principal Internet							(7,4)	(7,4)	(7,4)	(6,1)

P [IC02] A. Análisis de riesgos > A.6. Riesgo

Exportar

	activo	potencial	current	target	PILAR
<input type="checkbox"/>	ACTIVOS	{6,1}	{5,5}	{5,5}	{5,5}
<input type="checkbox"/>	I [BD ECO/FIN] Bases de datos económico y financieros				
<input type="checkbox"/>	S [SER] Soporte Gestor Empresarial				
<input type="checkbox"/>	S [EQU] Puestos de trabajo	(4,9)	(4,9)	(4,9)	(1,8)
<input type="checkbox"/>	S [RED] Acceso principal Internet	(6,1)	(5,5)	(5,5)	(5,5)

P [IC02] A. Análisis de riesgos > A.6. Riesgo

Exportar

	activo	potencial	current	target	PILAR
<input type="checkbox"/>	ACTIVOS	{6,5}	{6,5}	{6,5}	{5,9}
<input type="checkbox"/>	I [BD ECO/FIN] Bases de datos económico y financieros				
<input type="checkbox"/>	S [SER] Soporte Gestor Empresarial				
<input type="checkbox"/>	S [EQU] Puestos de trabajo	(5,5)	(5,5)	(5,5)	(2,5)
<input type="checkbox"/>	S [RED] Acceso principal Internet	(6,5)	(6,5)	(6,5)	(5,9)

P [IC02] A. Análisis de riesgos > A.6. Riesgo

Exportar

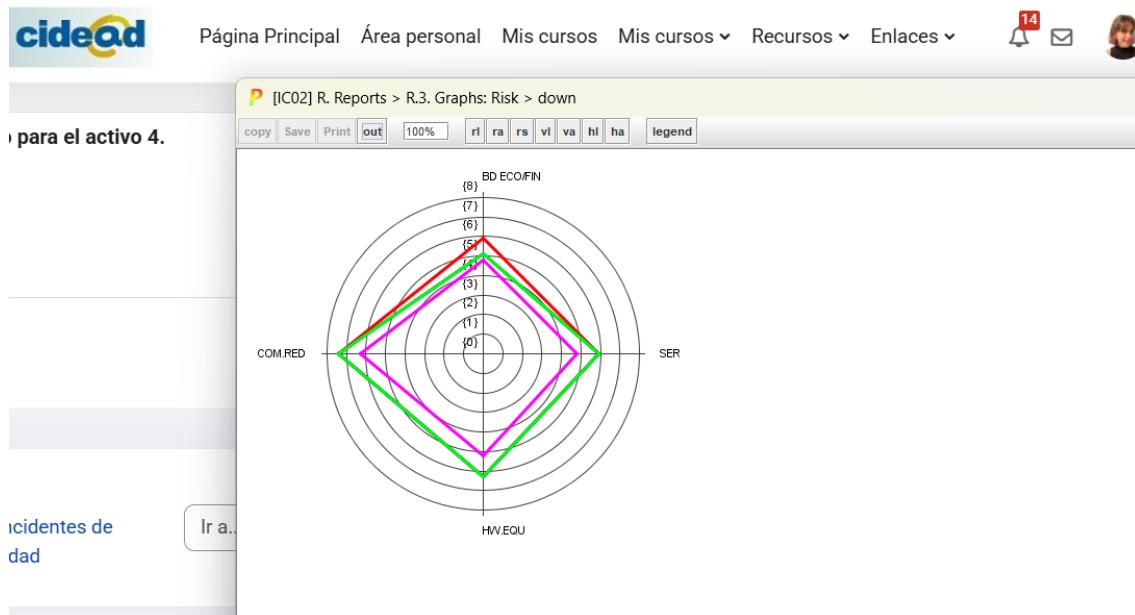
	activo	potencial	current	target	PILAR
<input type="checkbox"/>	ACTIVOS	{6,5}	{6,5}	{6,5}	{3,3}
<input type="checkbox"/>	I [BD ECO/FIN] Bases de datos económico y financieros				
<input type="checkbox"/>	S [SER] Soporte Gestor Empresarial				
<input type="checkbox"/>	S [EQU] Puestos de trabajo				
<input type="checkbox"/>	S [RED] Acceso principal Internet	(6,5)	(6,5)	(6,5)	(3,3)

P [IC02] A. Análisis de riesgos > A.6. Riesgo

Exportar

	activo	potencial	current	target	PILAR
<input type="checkbox"/>	ACTIVOS	{5,9}	{5,9}	{5,9}	{3,0}
<input type="checkbox"/>	I [BD ECO/FIN] Bases de datos económico y financieros	(5,9)	(5,9)	(5,9)	(2,9)
<input type="checkbox"/>	S [SER] Soporte Gestor Empresarial	(5,9)	(5,9)	(5,9)	(3,0)
<input type="checkbox"/>	S [EQU] Puestos de trabajo	(4,8)	(4,8)	(4,8)	(1,8)
<input type="checkbox"/>	S [RED] Acceso principal Internet	(5,9)	(5,9)	(5,9)	(2,9)

Se genera un informe con gráficas de riesgo para los cuatro activos de la empresa.



Apartado 5: Taxonomía de incidentes.

Para cada uno de los cuatro activos seleccionados, se determina un tipo de incidente que podría producirse en relación a sus riesgos.

Activo	Incidente	Grupo al que pertenece	Justificación
B.D. ECO/FIN	Uso indebido de datos por empleado con privilegios	Abuso	Un empleado con privilegios extrae datos financieros de la BD para un fin comercial.
ERP	Manipulación/modificación de las órdenes de producción	Fraude	Un atacante modifica una orden de compra con fines personales y sabotear a la empresa.
Router	Acceso no autorizado	Intrusión	El atacante accede al router mediante una vulnerabilidad explotada.
Puestos de trabajo	Pérdida portátil	Daños	El portátil perdido supone una puerta de entrada a cualquiera y más si no dispone de clave de acceso.

Bibliografía

Centro Criptológico Nacional (CCN-CERT). (s.f.). *Documentos*. Recuperado de <https://pilar.ccn-cert.cni.es/docman/documentos>

Dirección General de Modernización Administrativa, Procedimientos e Impulso de la Administración Electrónica. (2012). *Magerit versión 3.0: Metodología de análisis y gestión de riesgos de los Sistemas de Información. Libro I: Método*. Ministerio de Hacienda y Administraciones Públicas. Recuperado de <https://pilar.ccn-cert.cni.es/docman/documentos/1-magerit-v3-libro-i-metodo/file>

PILAR-Tools. (2025). *PILAR Basic - Manual de Usuario*. Recuperado de https://www.pilar-tools.com/doc/manual_basic_es_2025.pdf