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

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

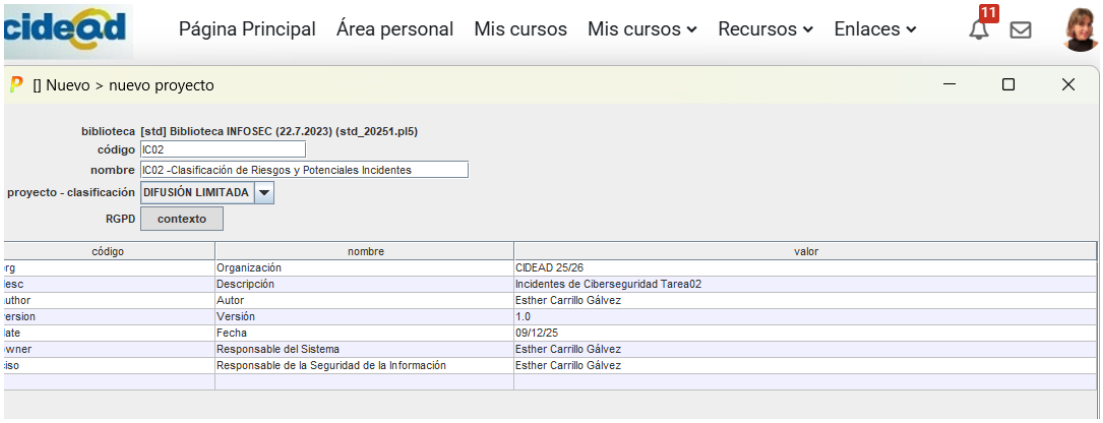
				producción. Sirve como puente de ataque entre la red TI y la OT.
Switch	192.168.1.11	Three-Legged Switch		Un fallo provocaría en la segmentación de la red supone un riesgo para la comunicación interna.
PLC	192.168.1.22	Controlador lógico		Puede suponer un fallo en la línea de producción.
Puestos trabajo	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/VAULT		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

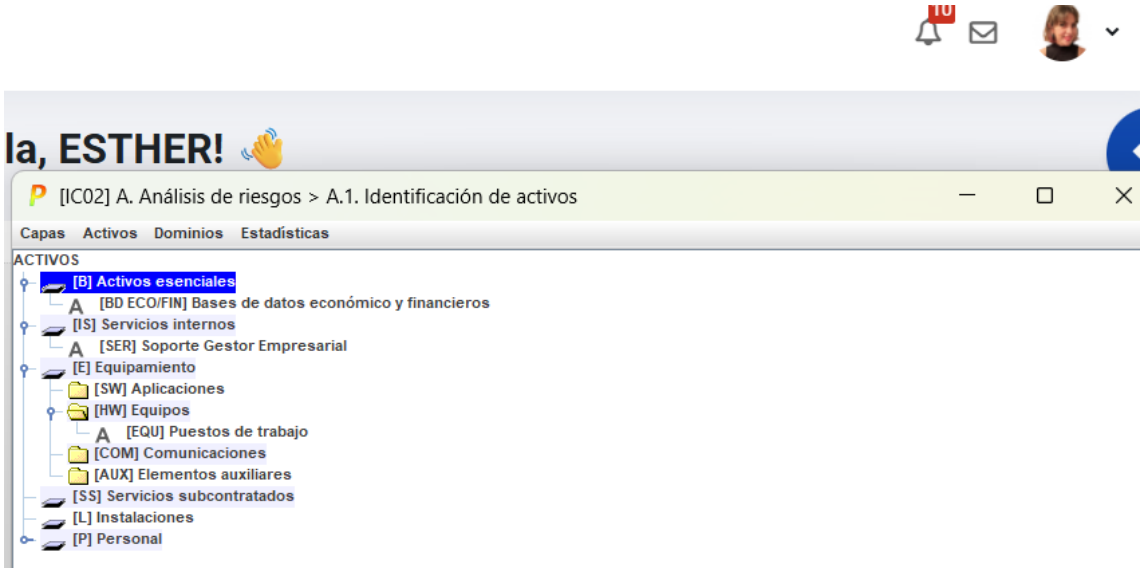
Activo	Dependencias	Justificación
ERP	BD ECO/FIN, BD Inventario, MES, Switch, Router	Centraliza los datos recogidos del MES, de la BD y depende de la comunicación entre redes del switch y el router.
SCADA	MES, Switch, Router, PLC	Gestiona los procesos industriales, combinando los datos recibidos del 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.

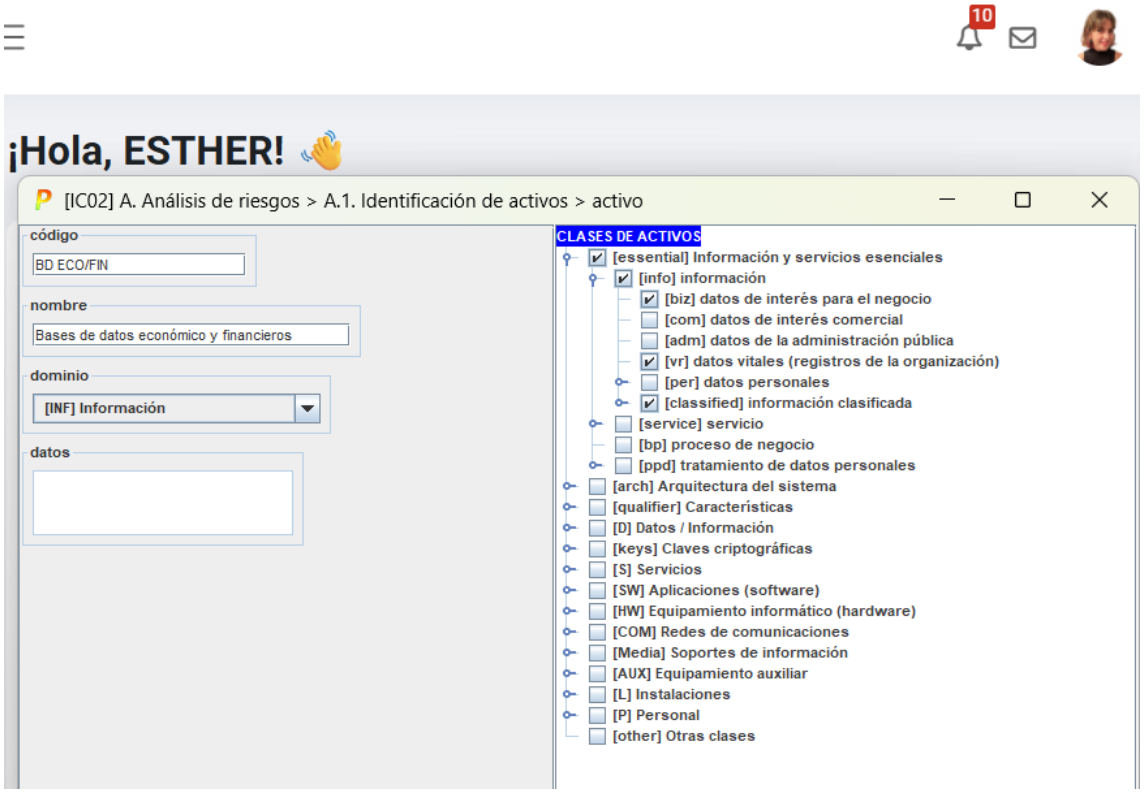
PLC	SCADA, Switch, MES	Automatizan los procesos industriales gracias a los datos y órdenes de SCADA y MES.
Puestos de trabajo	ERP, Big Data, Switch, SOC, SCADA, MES, Router, Switch	La plantilla depende de los sistemas y de la conectividad para realizar las tareas pertinentes a la gestión de la empresa.
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.

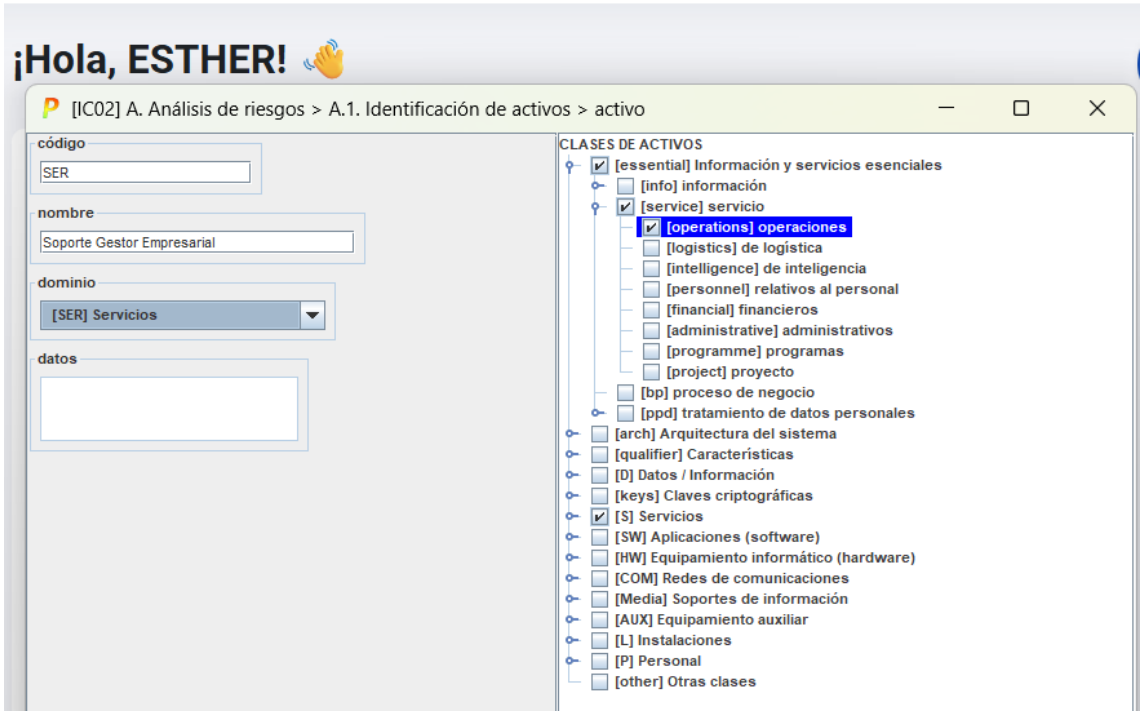
Se creará un nuevo proyecto desde la ventana principal y se introducen los datos pertinentes al proyecto.

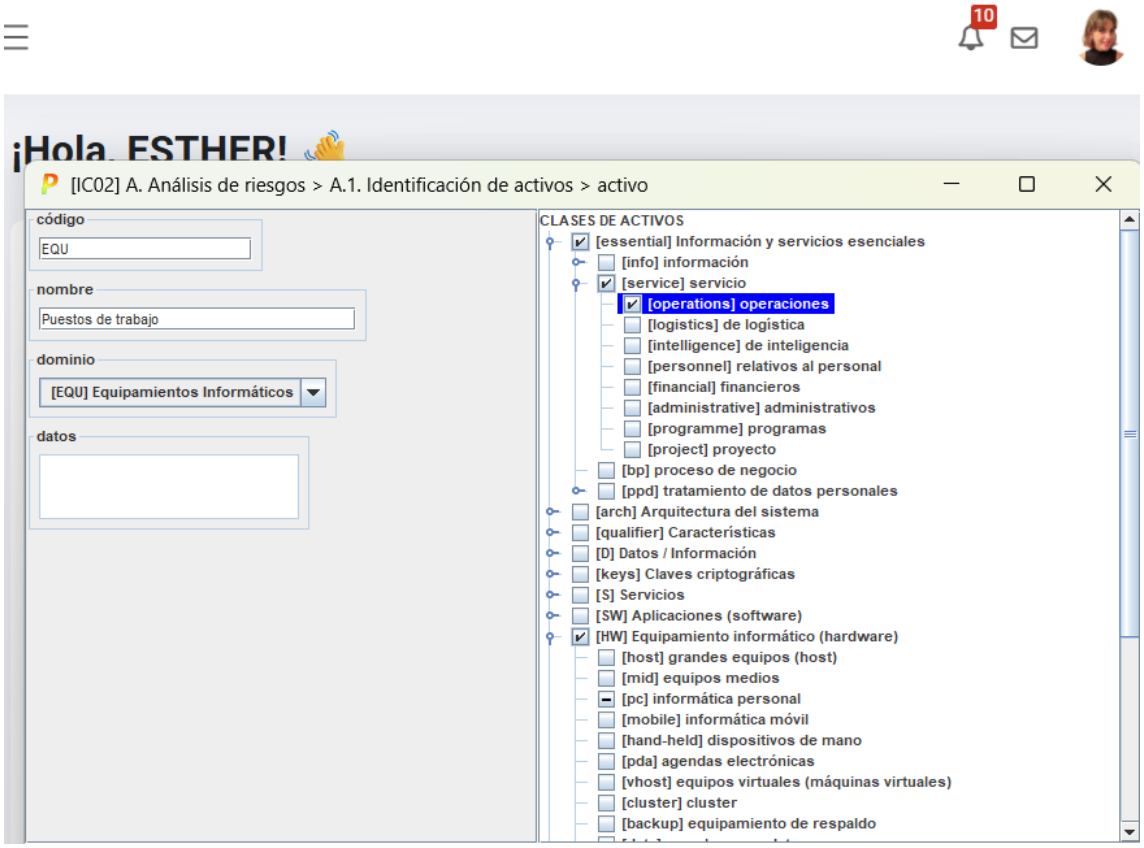


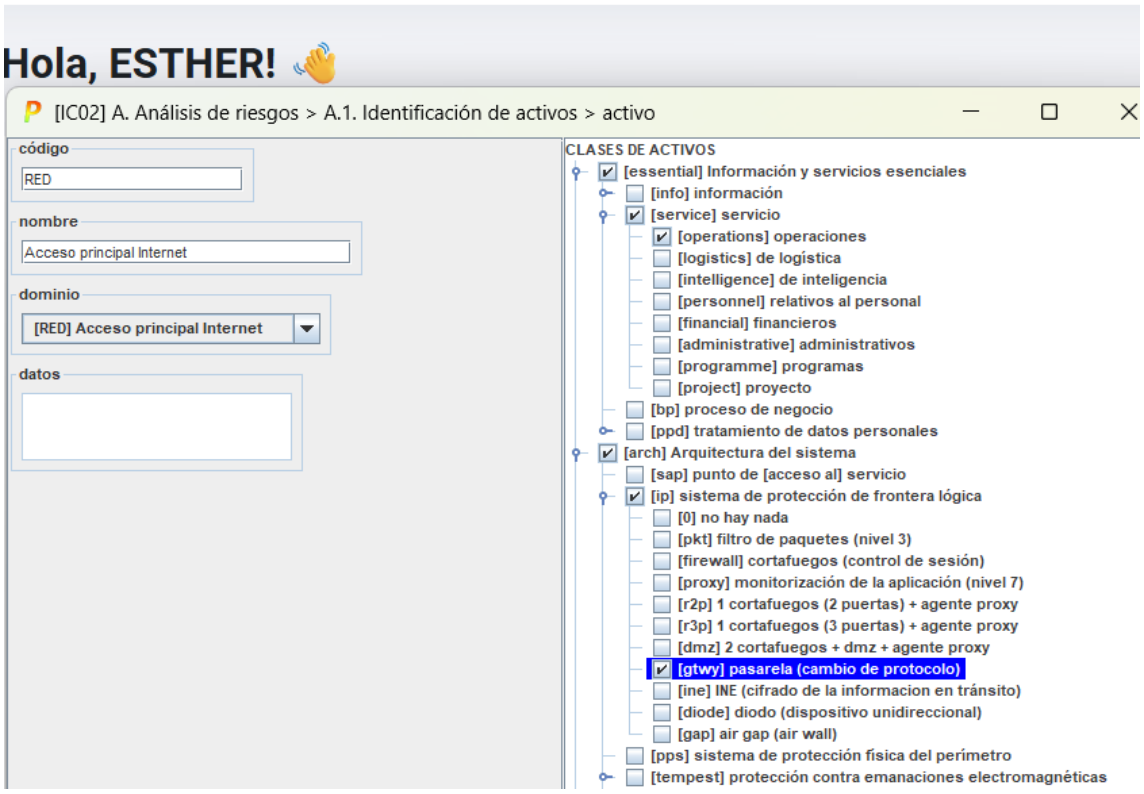
Se seleccionan los cuatro activos indicados en la tabla para su previo uso en la herramienta PILAR (Proceso Informático de Localización y Análisis de Riesgos)




¡Hola, ESTHER!
[IC02] A. Análisis de riesgos > A.1. Identificación de activos > activo
código
BD ECO/FIN
nombre
Bases de datos económico y financieros
dominio
[INF] Información
datos
CLASES DE ACTIVOS
[essential] Información y servicios 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
[Media] Soportes de información
[AUX] Equipamiento auxiliar
[L] Instalaciones
[P] Personal
[other] Otras clases


¡Hola, ESTHER!
[IC02] A. Análisis de riesgos > A.1. Identificación de activos > activo
código
SER
nombre
Soporte Gestor Empresarial
dominio
[SER] Servicios
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)
[COM] Redes de comunicaciones
[Media] Soportes de información
[AUX] Equipamiento auxiliar
[L] Instalaciones
[P] Personal
[other] Otras clases

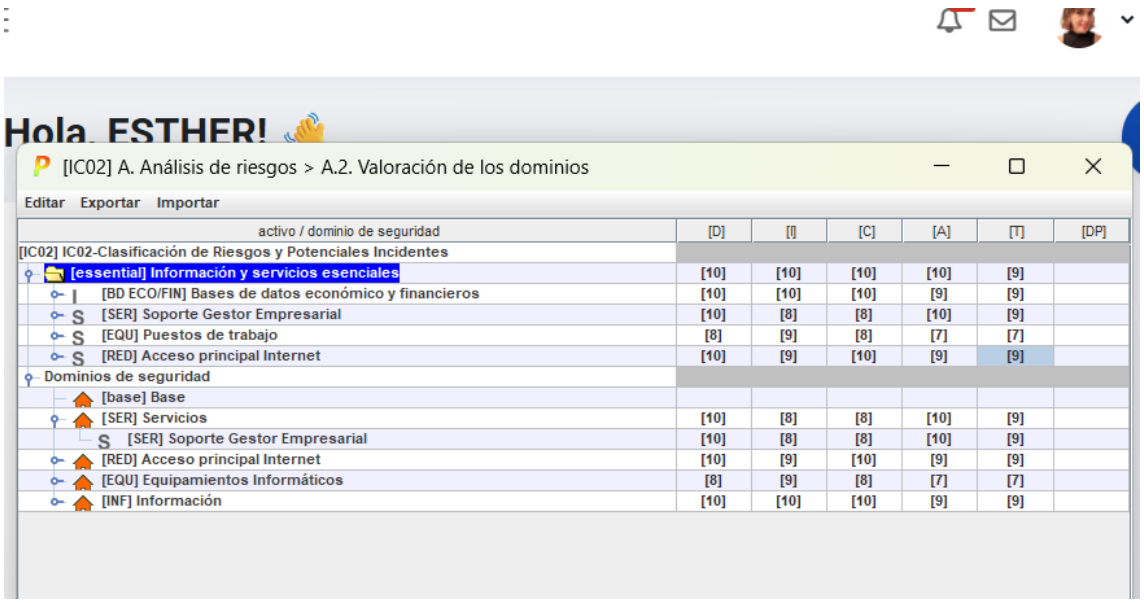

¡Hola, ESTHER!
[IC02] A. Análisis de riesgos > A.1. Identificación de activos > activo
código
EQU
nombre
Puestos de trabajo
dominio
[EQU] Equipamientos Informáticos
datos
CLASES DE ACTIVOS
[essential] Información y servicios esenciales
[info] información
[service] servicio
[operations] operaciones
[logistics] 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!
[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 informacion 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.

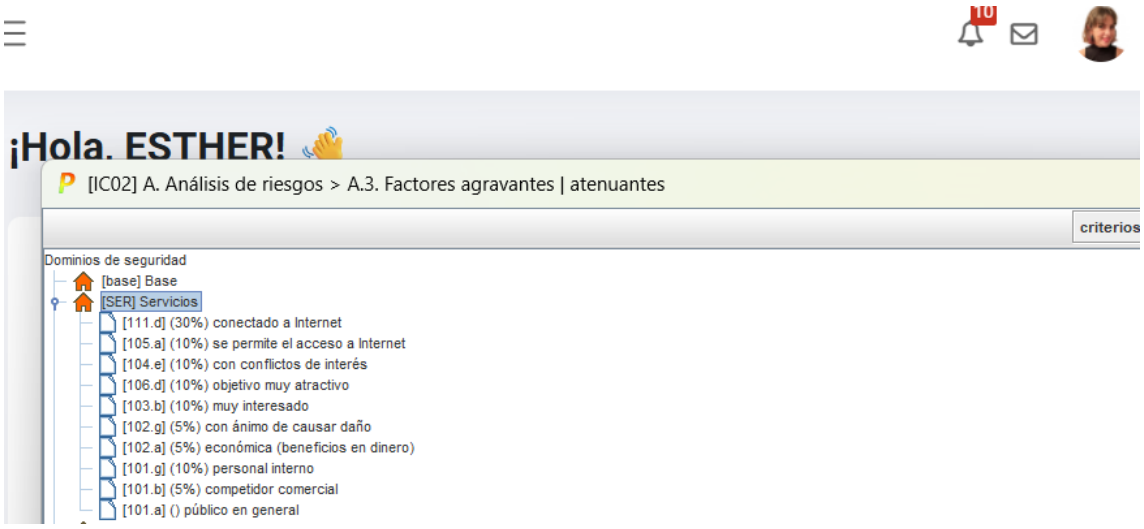
En este apartado se determina el nivel de importancia que tienen los activos esenciales en sus diferentes dominios de seguridad definidos. Además, se indican un par de factores atenuantes por cada dominio.

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

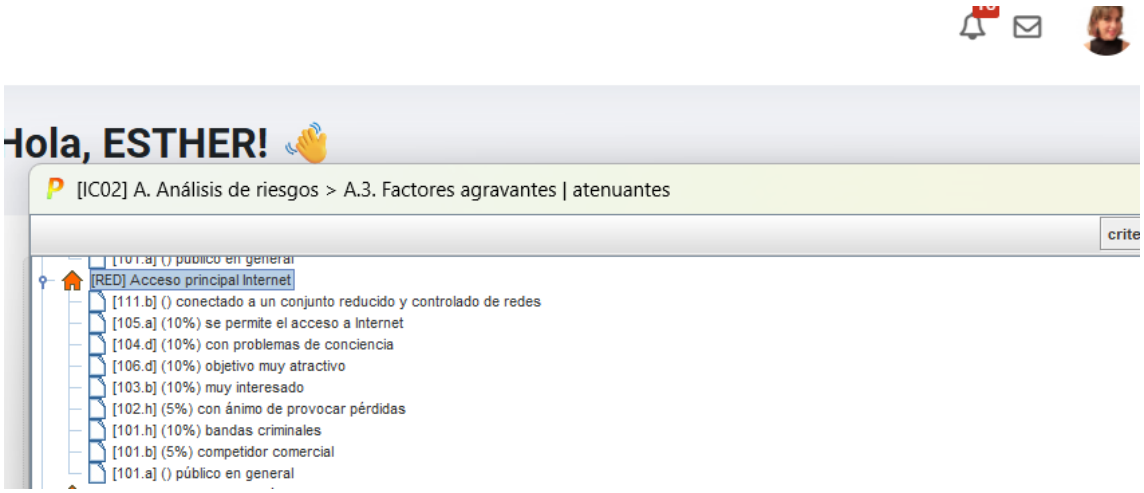


Se identifican los factores agravantes y atenuantes de cada uno de los dominios de seguridad de la empresa.

Dominio Servicios [SER]



Dominio Acceso principal Internet [RED]



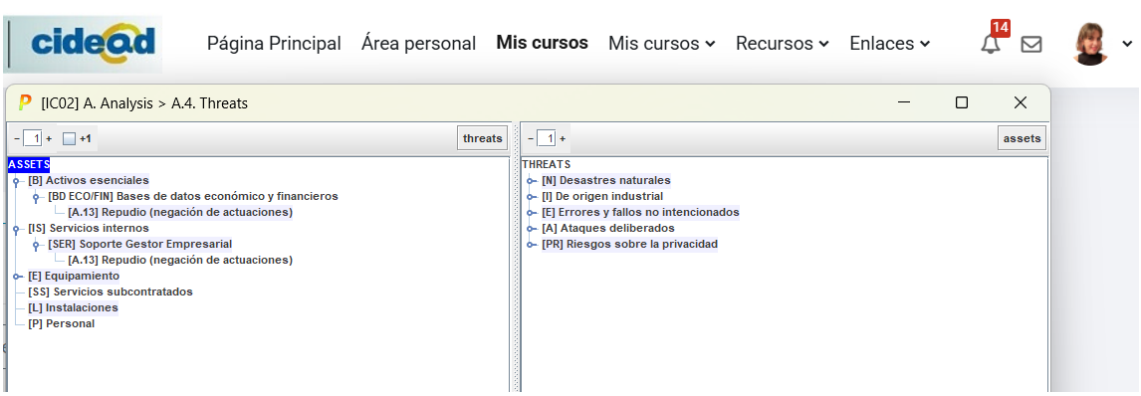
Dominio Equipamientos Informáticos [EQU]

Dominio Información [INF]

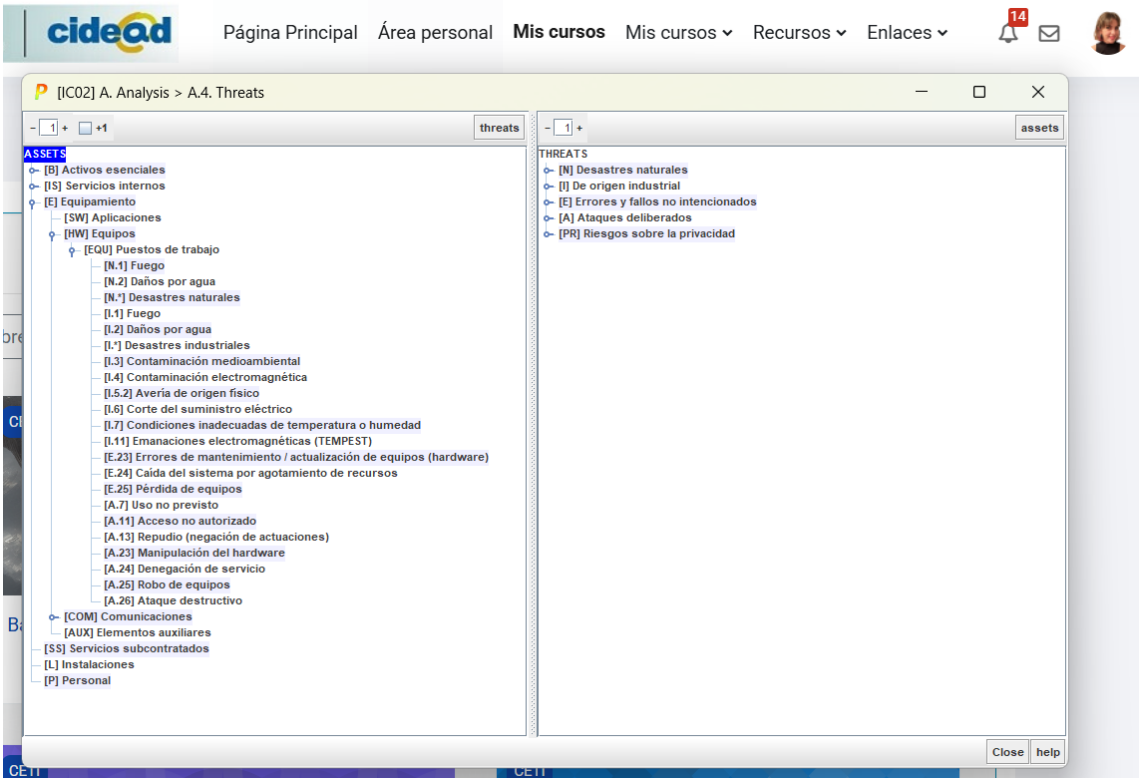
Apartado 3: Determinación de las amenazas y sus salvaguardas dispuestas.

Amenazas localizadas en cada uno de los activos:

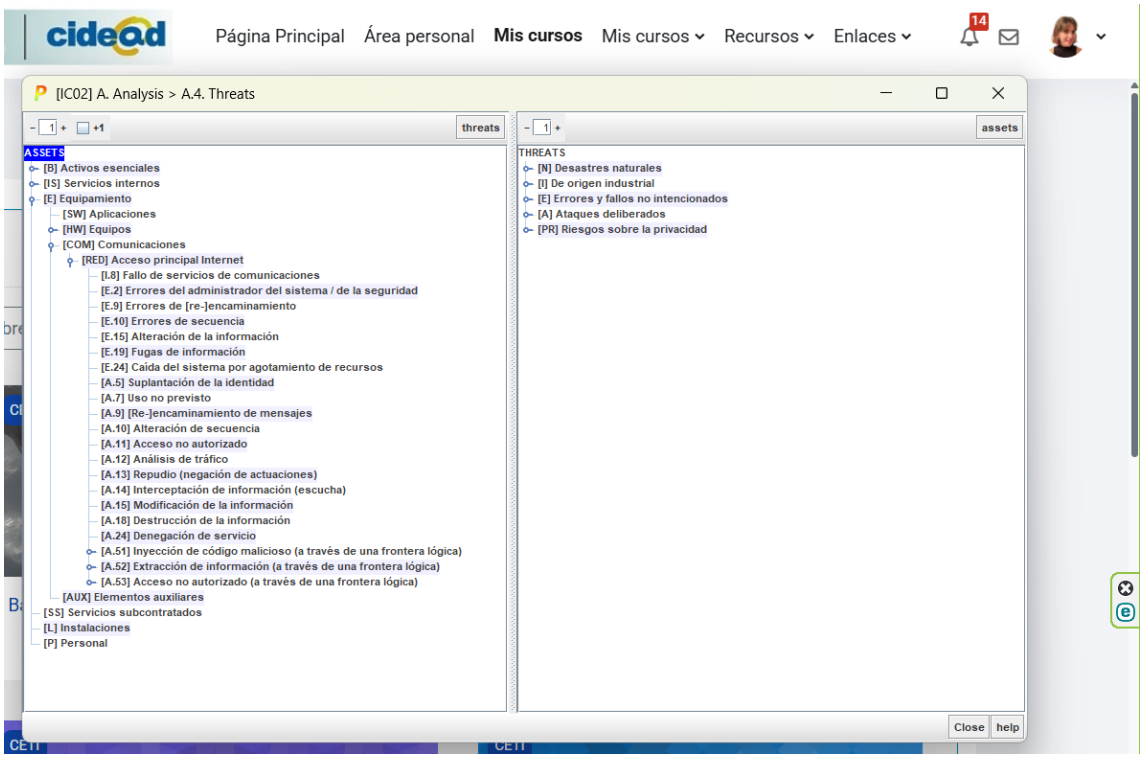
[BD ECO/FIN] Bases de datos económicos y financieros y [SER] Soporte Gestor Empresarial



[EQU] Puestos de Trabajo



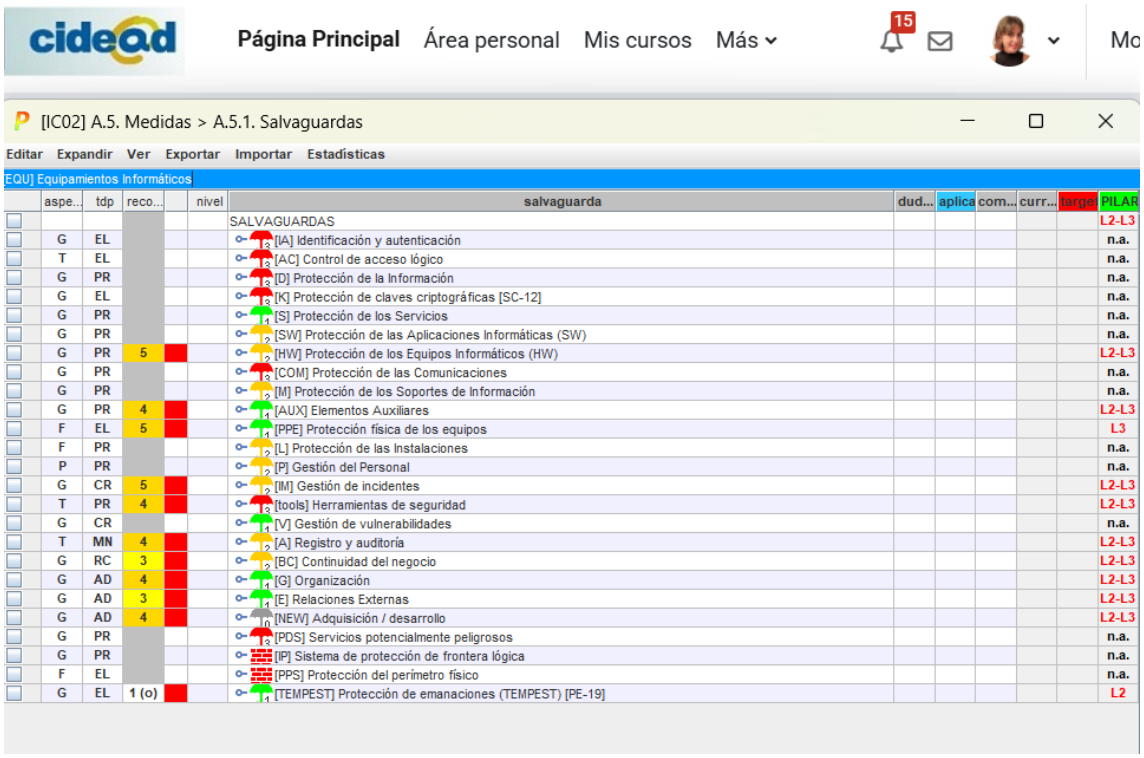
[RED] Acceso principal Internet



Salvaguardas asociadas a cada activo.

Dominio Servicios [SER]

Dominio Equipamientos Informáticos [EQU]



	aspe...	tdp	reco...		nivel	salvaguarda	dud...	aplica	com...	curr...	targe	PILAR
						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				[SW] Protección de las Aplicaciones Informáticas (SW)						n.a.
	G	PR	5			[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				[L] 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

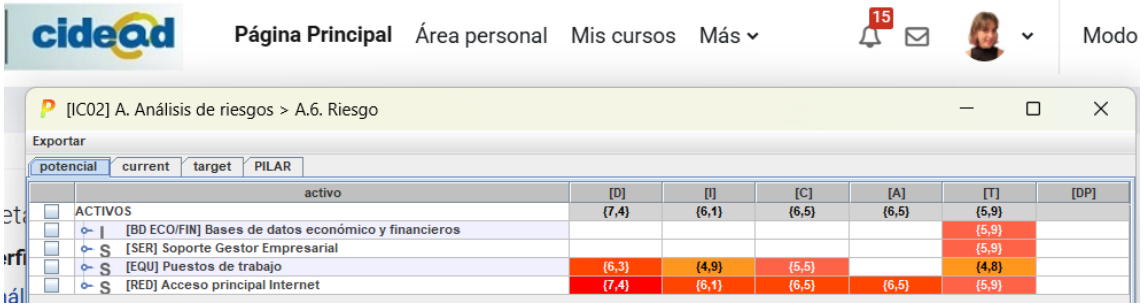
Dominio Acceso principal Internet [RED]

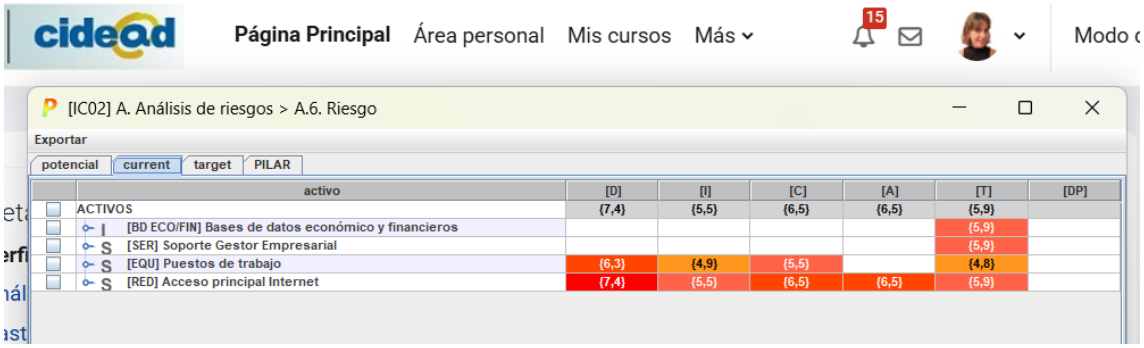
	aspe...	tdp	reco...		nivel	salvaguarda	dud...	aplica	com...	curr...	targe	PILAR
						SALVAGUARDAS						L2-L5
	G	EL				[IA] Identificación y autenticación						n.a.
	T	EL	7			[AC] Control de acceso lógico						L2-L4
	G	PR				[D] Protección de la Información						n.a.
	G	EL				[K] Protección de claves 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				[M] Protección de los Soportes de Información						n.a.
	G	PR				[AUX] Elementos Auxiliares						n.a.
	F	EL				[PPE] Protección física de los equipos						n.a.
	F	PR				[L] 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]

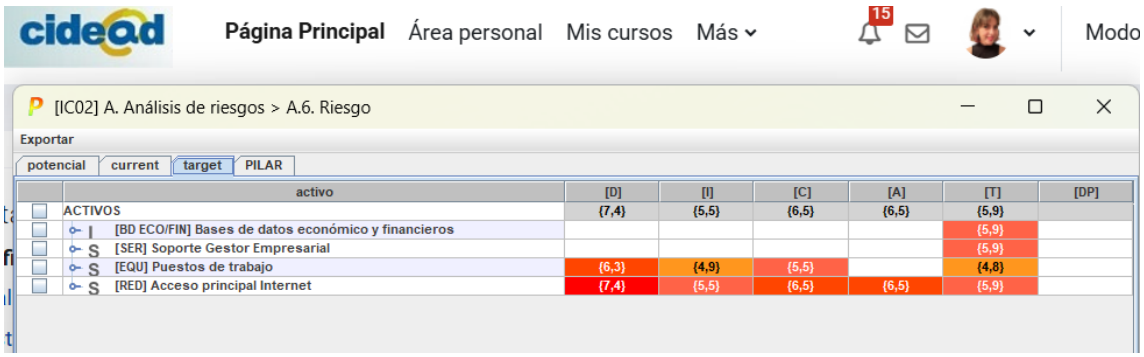
Apartado 4: Estimación del riesgo que tendría que considerar la empresa para su estudio y toma de decisiones.

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.

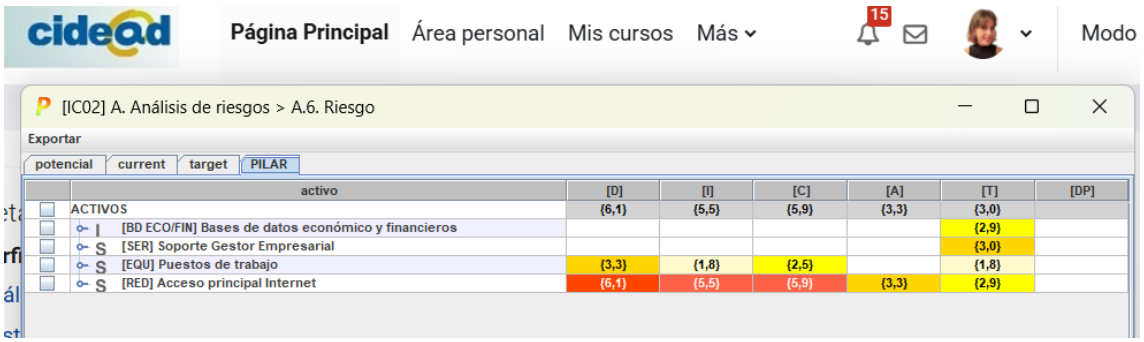




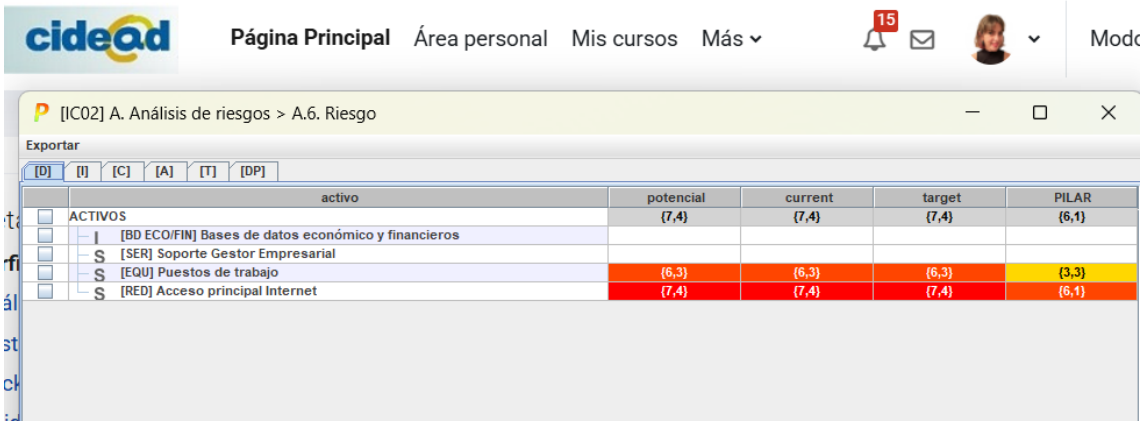
activo	[D]	[I]	[C]	[A]	[T]	[DP]
ACTIVOS	{7,4}	{5,5}	{6,5}	{6,5}	{5,9}	
[BD ECO/FIN] Bases de datos económico y financieros					{5,9}	
[SER] Soporte Gestor Empresarial					{5,9}	
[EQU] Puestos de trabajo	{6,3}	{4,9}	{5,5}		{4,8}	
[RED] Acceso principal Internet	{7,4}	{5,5}	{6,5}	{6,5}	{5,9}	



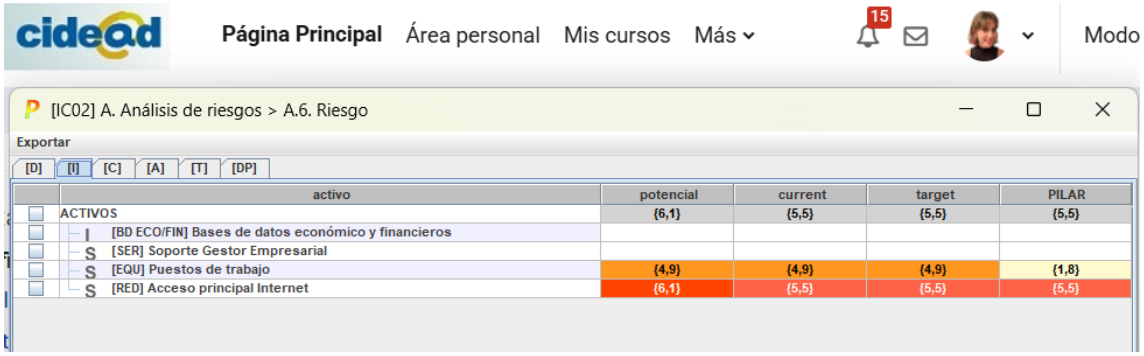
activo	[D]	[I]	[C]	[A]	[T]	[DP]
ACTIVOS	{7,4}	{5,5}	{6,5}	{6,5}	{5,9}	
[BD ECO/FIN] Bases de datos económico y financieros					{5,9}	
[SER] Soporte Gestor Empresarial					{5,9}	
[EQU] Puestos de trabajo	{6,3}	{4,9}	{5,5}		{4,8}	
[RED] Acceso principal Internet	{7,4}	{5,5}	{6,5}	{6,5}	{5,9}	

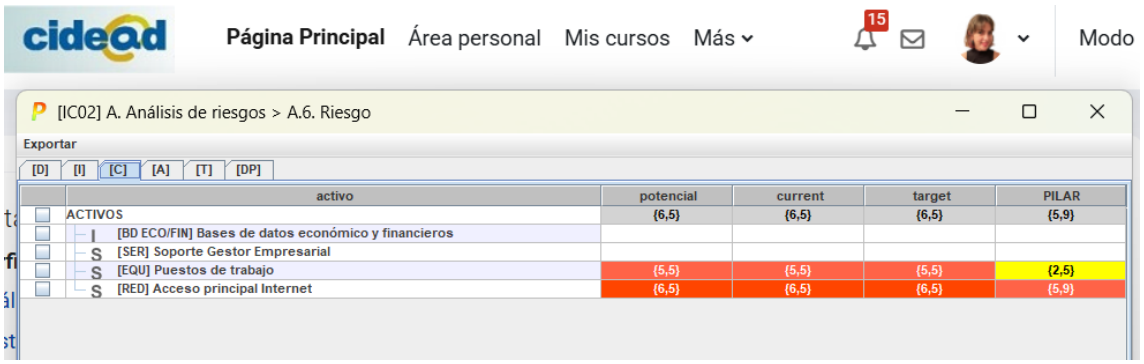


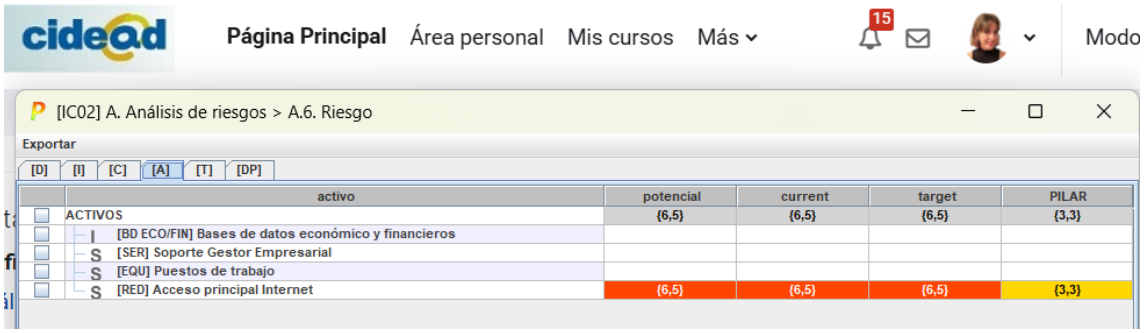
activo	[D]	[I]	[C]	[A]	[T]	[DP]
ACTIVOS	{6,1}	{5,5}	{5,9}	{3,3}	{3,0}	
[BD ECO/FIN] Bases de datos económico y financieros					{2,9}	
[SER] Soporte Gestor Empresarial					{3,0}	
[EQU] Puestos de trabajo	{3,3}	{1,8}	{2,5}		{1,8}	
[RED] Acceso principal Internet	{6,1}	{5,5}	{5,9}	{3,3}	{2,9}	

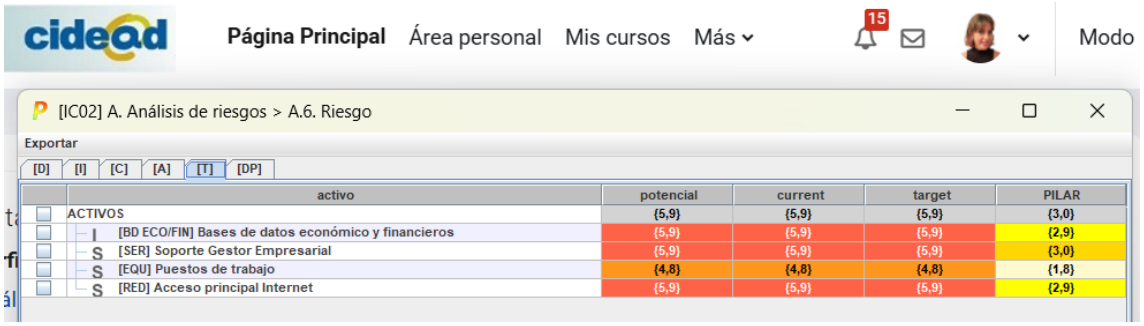


activo	potencial	current	target	PILAR
ACTIVOS	{7,4}	{7,4}	{7,4}	{6,1}
[BD ECO/FIN] Bases de datos económico y financieros				
[SER] Soporte Gestor Empresarial				
[EQU] Puestos de trabajo	{6,3}	{6,3}	{6,3}	{3,3}
[RED] Acceso principal Internet	{7,4}	{7,4}	{7,4}	{6,1}

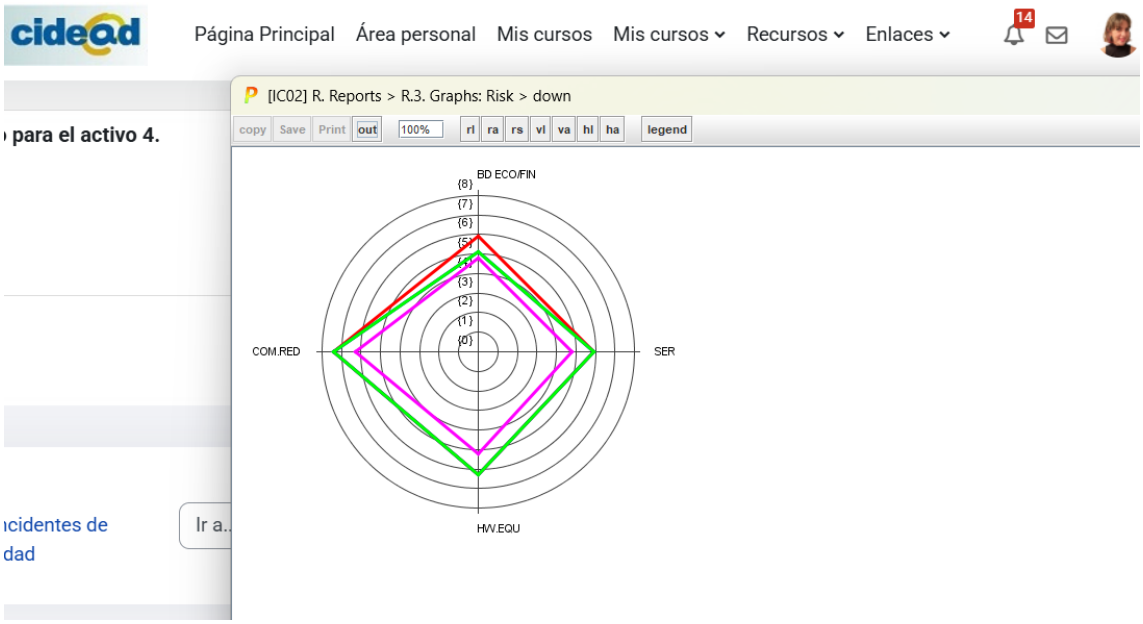

cidead
Página Principal
Área personal
Mis cursos
Más
15
Modo
[IC02] A. Análisis de riesgos > A.6. Riesgo
Exportar
[D] [I] [C] [A] [T] [DP]
activo | potencial | current | target | PILAR
ACTIVOS | {6,1} | {5,5} | {5,5} | {5,5}
[BD ECO/FIN] Bases de datos económico y financieros
[SER] Soporte Gestor Empresarial
[EQU] Puestos de trabajo | {4,9} | {4,9} | {4,9} | {1,8}
[RED] Acceso principal Internet | {6,1} | {5,5} | {5,5} | {5,5}


cidead
Página Principal
Área personal
Mis cursos
Más
15
Modo
[IC02] A. Análisis de riesgos > A.6. Riesgo
Exportar
[D] [I] [C] [A] [T] [DP]
activo | potencial | current | target | PILAR
ACTIVOS | {6,5} | {6,5} | {6,5} | {5,9}
[BD ECO/FIN] Bases de datos económico y financieros
[SER] Soporte Gestor Empresarial
[EQU] Puestos de trabajo | {5,5} | {5,5} | {5,5} | {2,5}
[RED] Acceso principal Internet | {6,5} | {6,5} | {6,5} | {5,9}


cidead
Página Principal
Área personal
Mis cursos
Más
15
Modo
[IC02] A. Análisis de riesgos > A.6. Riesgo
Exportar
[D] [I] [C] [A] [T] [DP]
activo | potencial | current | target | PILAR
ACTIVOS | {6,5} | {6,5} | {6,5} | {3,3}
[BD ECO/FIN] Bases de datos económico y financieros
[SER] Soporte Gestor Empresarial
[EQU] Puestos de trabajo
[RED] Acceso principal Internet | {6,5} | {6,5} | {6,5} | {3,3}


cidead
Página Principal
Área personal
Mis cursos
Más
15
Modo
[IC02] A. Análisis de riesgos > A.6. Riesgo
Exportar
[D] [I] [C] [A] [T] [DP]
activo | potencial | current | target | PILAR
ACTIVOS | {5,9} | {5,9} | {5,9} | {3,0}
[BD ECO/FIN] Bases de datos económico y financieros | {5,9} | {5,9} | {5,9} | {2,9}
[SER] Soporte Gestor Empresarial | {5,9} | {5,9} | {5,9} | {3,0}
[EQU] Puestos de trabajo | {4,8} | {4,8} | {4,8} | {1,8}
[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 rpoducción	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