



**TAREA 02**

# **AUDITORÍA DE INCIDENTES DE CIBERSEGURIDAD**

**INCIDENTES DE CIBERSEGURIDAD**

**ALBA MOREJÓN GARCÍA**

**2024/2025**

**CETI - Ciberseguridad en Entornos de las Tecnologías de la Información**

## Clasificación de riesgos y potenciales incidentes.

Un Sistema de Gestión de Seguridad de la Información debe disponer de un correcto sistema de gestión de riesgos.

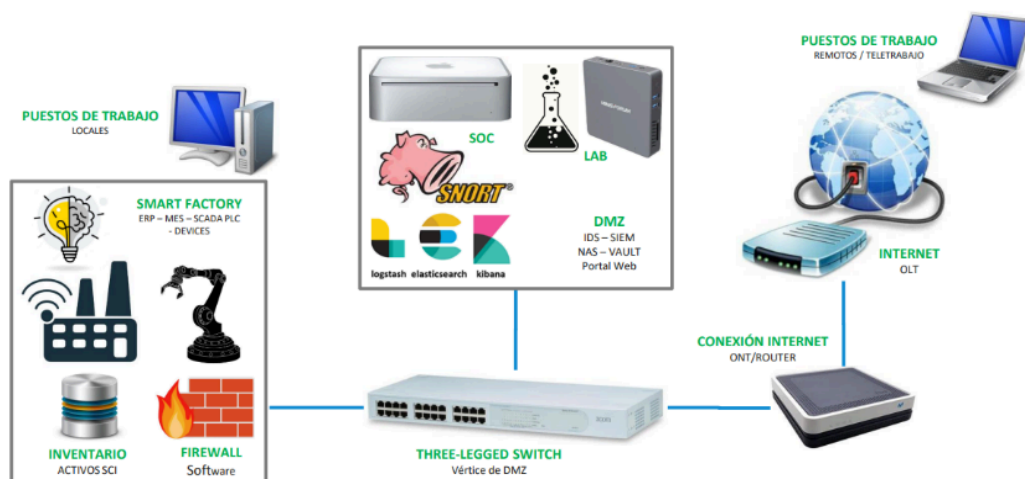
Un proceso de gestión de riesgos de seguridad de la información trata de identificar, comprender, evaluar y mitigar los riesgos.

El concepto de riesgo se corresponde con la probabilidad de que se produzca un incidente de seguridad, materializándose una amenaza y causando pérdidas o daños. El riesgo depende entonces de los siguientes factores: la probabilidad de que la amenaza se materialice aprovechando una vulnerabilidad y produciendo un daño o impacto. El producto de estos factores representa el riesgo. En esta tarea realizaremos un análisis y gestión de riesgos en la empresa ficticia de la unidad anterior para evitar o disminuir la probabilidad de que se produzcan diversos incidentes. Para este análisis seguiremos la metodología [Magerit v.3](#) desarrollada por el gobierno español.

Además, haremos uso de la herramienta [PILAR \(versión Basic\)](#) que implementa la metodología MAGERIT que ha sido desarrollada por el Centro Criptológico Nacional (CCN). Este software es privativo y debe licenciarse, pero provee de una licencia de evaluación de 30 días, que es la que usaremos en este caso práctico.

**Introducción: Diagrama de bloques y detalles de activos de la empresa.**

La empresa tiene el siguiente diagrama de bloques:



La empresa tiene los siguientes activos materiales principales:

Activo	Dirección IP	Sistema Operativo	Modelo Máquina	Función Empresa
Router	192.168.1.1	Askey SO	RTF3505VW	Router conexión Internet
Switch	192.168.1.11	3COM SO	SuperStack 3 3300XM	Three-Legged Switch
SOC	192.168.1.101	MacOS Ventura	Mac Mini M1	IDS/SIEM/NAS/VAULT
Labo_Server	192.168.1.102	Debian 11	MinisForum HM90	Servidor Laboratorio
ERP	192.168.1.25	Debian 11	ProLiant uServer Intel Xeon E	Servidor Gestor Empresarial
MES	192.168.1.24	Raspbian	Raspberry Pi 4B	Servidor Gestor Factoría
SCADA	192.168.1.23	Raspbian	Raspberry Pi 4B	Supervisión / Control / Firewall / Inventario
PLC	192.168.1.22	Raspbian	Raspberry Pi 4B	Controlador lógico
DEVICE	192.168.1.21	Raspbian	Raspberry Pi 4B	Dispositivo fabril
B.D. Inventario	192.168.1.25	MacOS Ventura	Mac Mini M1	Base de datos de Inventario
B.D. ECO/FIN	192.168.1.25	MacOS Ventura	Mac Mini M1	Base de datos ECO / FIN
Puestos trabajo	192.168.1.50-99	Windows 11 Pro	Lenovo ThinkCentre M720t	Puestos de trabajo
Maquetas, Prototipos	192.168.1.102	Debian 11	MinisForum HM90	Maquetas, prototipos, lanzaderas
Portal Web	192.168.1.102	Debian 11	MinisForum HM90	Portales web
Big Data, IA	192.168.1.50-99	Windows 11	Lenovo ThinkCentre M720t	Sistemas Big Data, IA

*Nota: Todos los datos no proporcionados de la empresa deben ser definidos de forma autónoma y libre como si fueras parte de la dirección general de la empresa, justificando su elección. Por ejemplo: se puede decidir si los equipos actualmente disponen de una política de contraseñas seguras o si por el contrario no existen políticas al respecto. En cualquiera de los casos, debe exponerse en el documento de prácticas.*

## Apartado 1: Priorización y jerarquía de activos.

- A partir de la lista de activos de la introducción, se deben priorizar y jerarquizar indicando los que crees que son esenciales para la empresa. Se ordenan desde el de más importancia al de menor, además se deben indicar aquellos que dependen de otros.

Jerarquía de activos según la importancia para la empresa:

- |  |   |
|--|---|
| 1. ERP                                 | depende de: bd eco/fin, puestos trabajo, router, switch     |
| 2. SCADA                               | depende de: PLC y router y switch                           |
| 3. MES                                 | depende de: ERP, SCADA, PLC, router y switch                |
| 4. PLC                                 | depende de: SCADA y router y switch                         |
| 5. Base datos Económica/Financiera     | depende de: ERP, router, switch                             |
| 6. Base de Datos Inventario            | depende de: ERP, router, switch                             |
| 7. SOC                                 | depende de: router, switch                                  |
| 8. Router                              | depende de: switch  |
| 9. Switch                              | depende de: router  |
| 10. Big Data e Inteligencia Artificial | depende de: bd inventario y eco/fin puestos, router, switch |
| 11. Puestos de Trabajo                 | depende de: ERP, MES, router, switch                        |
| 12. Portal Web                         | depende de: router, switch                                  |
| 13. Servidor Laboratorio               | depende de: puestos trabajo, router, switch                 |
| 14. Dispositivos/Device                | depende de: router, switch                                  |
| 15. Maquetas y Prototipos              | depende de: servidor laboratorio y puestos de trabajo       |

El orden que se ha establecido, se basa en la importancia de los activos para la continuidad de las operaciones y eficiencia, teniendo en cuenta el impacto que tendría la pérdida o interrupción de cada uno en las operaciones, la seguridad y los objetivos de la empresa.

Los activos más importantes como ERP, MES y SCADA, son prioritarios debido a su papel central en la gestión de la producción, inventario y recursos. También se ha dado alta prioridad a los PLC y las bases de datos debido a su conexión con la fabricación y las decisiones financieras.

Orden de prioridad:

- Prioridad alta (1-5), activos esenciales para la operación
- Prioridad media-baja (6-9) sirven de soporte a la operación crítica
- Prioridad media (10-12) tienen importancia operativa, pero no son activos críticos inmediatos
- Prioridad baja (13-15) tienen importancia estratégica o de soporte, pero con menor impacto directo.

- De la anterior lista de activos, se debe seleccionar uno por cada uno de estos tipos indicados: **activo esencial de información, activo esencial de servicio, activo de equipamiento informático y un activo de redes de comunicación.**

Activos Información	Activos Servicio	Activos Equipamiento informático	Activos Redes de Comunicación
ERP	SCADA	Puestos Trabajo	Router
BD Eco/Fin	MES	Labo Server	Switch
BD Inventario	PLC	Dispositivos	SOC
Big Data e IA	Portal Web	Maquetas/Prototipo	

Activos Información, engloba los sistemas que manejan y centralizan datos críticos para las operaciones administrativas.

Activos Servicio, sistemas que soportan los procesos operativos y fabriles.

Activos Equipamiento informático, dispositivos físicos utilizados por los empleados o en entornos de prueba.

Activos Redes de Comunicación, incluimos los elementos que garantizan la conectividad y seguridad de la red.

ERP, centraliza la información para la toma de decisiones, además, integra todas las áreas de la empresa (inventario, producción, ventas...). Es importante para la gestión de recursos, planificación y control de las operaciones.

SCADA, tiene un rol crítico en la gestión y seguridad de los procesos a tiempo real, si falla la seguridad, calidad y la producción pueden verse comprometidos de inmediato

Puestos de Trabajo, permite al empleado interactuar con los sistemas de información y gestión. Sin ellos, los empleados no tendrían acceso a las herramientas necesarias para su trabajo, paralizando las operaciones administrativas y productivas.

Router, asegura la conectividad entre las zonas de la empresa y gestiona las conexiones con el exterior, no contar con él bloquearía la operación de los sistemas dependientes de él.

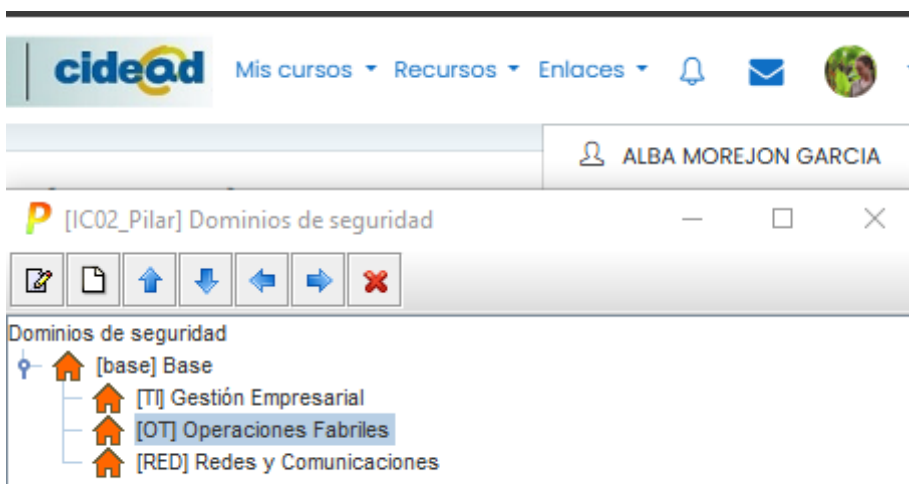
**- Con el uso de la herramienta PILAR se debe recoger la información de los cuatro activos anteriores. Estos activos deben definirse en su capa correcta y en un dominio de seguridad adecuado, por lo que habrá que crear los dominios de seguridad necesarios.**

**Muestra la ventana detallada de información de estos cuatro activos.**

La herramienta PILAR es un software que se utiliza para el análisis y la gestión en sistemas de información, sirve para ayudar a identificar, clasificar y proteger los activos. Su principal enfoque es evaluar los riesgos de seguridad y definir las medidas de protección.

A continuación se muestra la configuración elegida:

- Dominios



- Clases



- Activos

Enseñanzas Regladas a Distancia **cidead** Mis cursos Recursos Enlaces ALBA MOREJON GARCIA

Enlace permanente Mostrar mensajes

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

código: ERP

nombre: ERP

dominio: [TI] Gestión Empresarial

datos:

**CLASES DE ACTIVOS**

- ☒ [essential] Activos esencial...
- ☒ [SW] Aplicaciones (software)
- ☒ [prp] desarrollo propio (in house)

Enseñanzas Regladas a Distancia **cidead** Mis cursos Recursos Enlaces ALBA MOREJON GARCIA

Enlace permanente Mostrar mensajes

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

código: SC

nombre: SCADA

dominio: [OT] Operaciones Fabriles

datos:

**CLASES DE ACTIVOS**

- ☒ [essential] Activos esencial...
- ☒ [SW] Aplicaciones (software)
- ☒ [std] estándar (off the shelf)
- ☒ [app] servidor de aplicaciones
- ☒ [dbms] sistema de gestión de bases de datos

Enseñanzas Regladas a Distancia **cidead** Mis cursos Recursos Enlaces ALBA MOREJON GARCIA

Enlace permanente Mostrar mensajes

[IC02\_Pilar] A. Análisis de riesgos > A.1. Identificación de activos > a...

código: PC

nombre: Puestos Trabajo

dominio: [TI] Gestión Empresarial

datos:

**CLASES DE ACTIVOS**

- ☒ [essential] Activos esenciales
- ☒ [HW] Equipamiento informático (hardware)
- ☒ [pc] informática personal

Enseñanzas Regladas a Distancia **cidead** Mis cursos Recursos Enlaces ALBA MOREJON GARCIA

Enlace permanente Mostrar mensajes

[IC02\_Pilar] A. Análisis de riesgos > A.1. Identificación de activos > a...

código: RT

nombre: Router

dominio: [RED] Redes y Comunicaciones

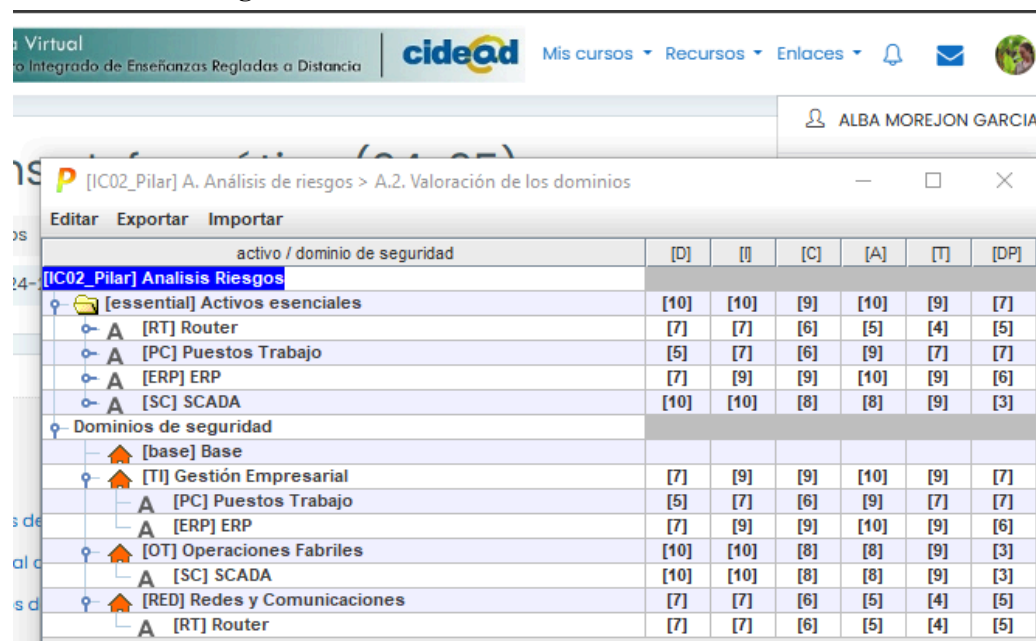
datos:

**CLASES DE ACTIVOS**

- ☒ [essential] Activos esenciales
- ☒ [COM] Redes de comunicaciones
- ☒ [LAN] red local

## Apartado 2: Valoración de los dominios de seguridad.

- Debes determinar el nivel de importancia que tienen los activos esenciales en sus diferentes dominios de seguridad definidos. Muestra una captura de pantalla con la valoración numérica de los activos en sus dominios de seguridad.



The screenshot shows the CIDEAD platform interface. At the top, there's a header with 'Virtual', 'Integrado de Enseñanzas Regladas a Distancia', and the CIDEAD logo. Below this, there's a navigation bar with 'Mis cursos', 'Recursos', 'Enlaces', and a user profile for 'ALBA MOREJON GARCIA'. The main content area displays a window titled '[IC02\_Pilar] A. Análisis de riesgos > A.2. Valoración de los dominios'. Inside this window, there's a table with columns for 'activo / dominio de seguridad' and six security domains: [D], [I], [C], [A], [T], and [DP]. The table lists various assets and their corresponding numerical ratings for each domain.

activo / dominio de seguridad	[D]	[I]	[C]	[A]	[T]	[DP]
[IC02_Pilar] Analisis Riesgos						
[essential] Activos esenciales	[10]	[10]	[9]	[10]	[9]	[7]
A [RT] Router	[7]	[7]	[6]	[5]	[4]	[5]
A [PC] Puestos Trabajo	[5]	[7]	[6]	[9]	[7]	[7]
A [ERP] ERP	[7]	[9]	[9]	[10]	[9]	[6]
A [SC] SCADA	[10]	[10]	[8]	[8]	[9]	[3]
Dominios de seguridad						
[base] Base						
[TI] Gestión Empresarial	[7]	[9]	[9]	[10]	[9]	[7]
A [PC] Puestos Trabajo	[5]	[7]	[6]	[9]	[7]	[7]
A [ERP] ERP	[7]	[9]	[9]	[10]	[9]	[6]
[OT] Operaciones Fabriles	[10]	[10]	[8]	[8]	[9]	[3]
A [SC] SCADA	[10]	[10]	[8]	[8]	[9]	[3]
[RED] Redes y Comunicaciones	[7]	[7]	[6]	[5]	[4]	[5]
A [RT] Router	[7]	[7]	[6]	[5]	[4]	[5]

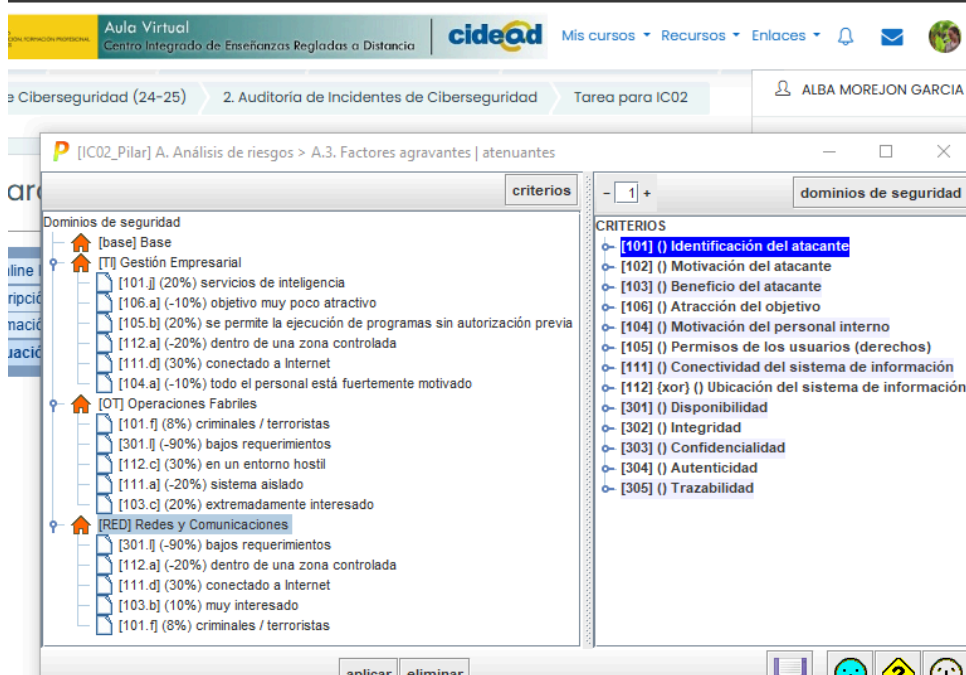
Para el Router se prioriza la importancia en la conectividad y seguridad de la red. La disponibilidad crítica, se refleja en un tiempo de recuperación rápido, ya que su interrupción afecta las operaciones inmediatas. La Integridad y confidencialidad se vincula a la posible manipulación y accesos no autorizados, lo que podría derivar en incidentes graves o problemas legales al procesar datos personales. La autenticidad y trazabilidad son relevantes para investigar accesos indebidos y asegurar la continuidad del servicio.

El impacto en las operaciones de la organización de los Puestos de Trabajo es central. Una interrupción afecta directamente a la productividad y el manejo de información personal, dado que maneja datos confidenciales y accesos críticos, los riesgos de seguridad y autenticidad son altos con potencial de incidentes graves. La trazabilidad asegura el monitoreo de actividades, lo que ayuda en las auditorías y control de riesgos laborales.

El ERP es vital para la gestión empresarial, por lo que su disponibilidad debe ser inmediata. La integridad es crucial porque cualquier error podría generar incumplimientos legales significativos. Su información confidencial tiene alto valor económico y comercial, lo que lo convierte en un objetivo atractivo para ataques. Además, garantizar autenticidad y trazabilidad es esencial para proteger datos sensibles y cumplir normativas.

Finalmente, el SCADA controla los procesos industriales críticos, lo que lo hace indispensable para las operaciones. Su disponibilidad tiene impacto directo en la seguridad física de las infraestructuras, ya que un fallo podría causar pérdidas o interrupciones graves, así como afectar a la integridad de los datos. La confidencialidad y trazabilidad aseguran que las operaciones sean seguras y que los incidentes puedan ser investigados eficazmente.

- Además, debes indicar, al menos, un par de factores atenuantes y/o agravantes por cada dominio de seguridad. Muestra una captura de estos factores.



En el dominio de Gestión Empresarial los principales agravantes seleccionados están relacionados con la alta exposición a ataques debido a la conexión a Internet y la flexibilidad de los permisos que pueden permitir la ejecución de programas no autorizados, lo que eleva significativamente el riesgo. Como atenuantes están la ubicación controlada de los sistemas y la motivación del personal, que reduce la probabilidad de riesgos internos

En el caso de Operaciones Fabriles se prioriza como agravante la ubicación en el entorno hostiles, donde los sistemas están más expuestos a riesgos físicos y lógicos, además del alto interés que puede suscitar en atacantes que buscan interrumpir procesos industriales críticos. Sin embargo, el aislamiento del sistema y los menores requerimientos de disponibilidad, actúan como factores atenuantes al limitar las posibles vías de ataque y tolerar pequeñas interrupciones.

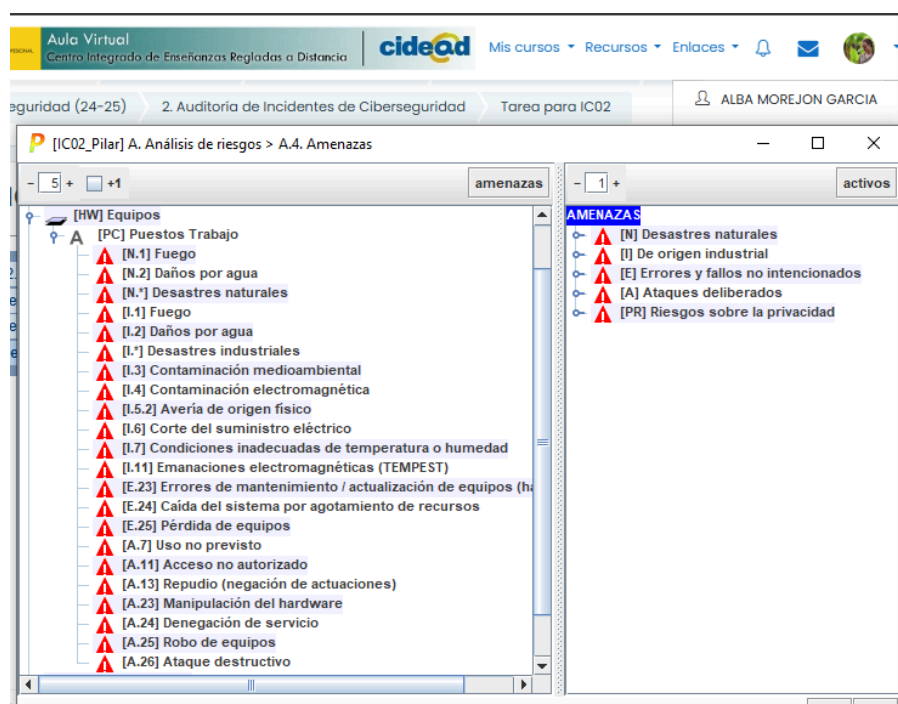
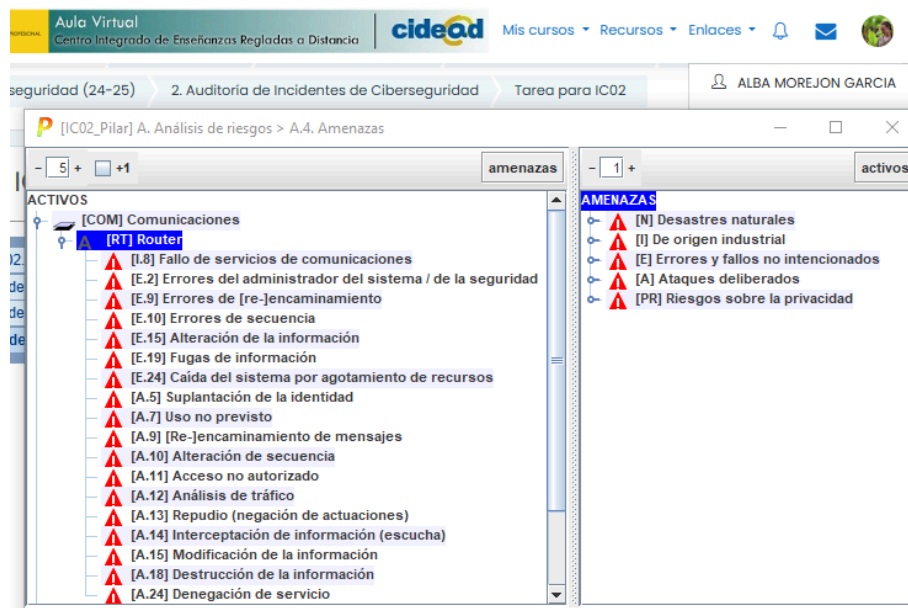
Para Redes y Comunicaciones, los agravantes destacados son la conexión a Internet, que lo expone a amenazas externas y el interés de los atacantes, dado que comprometer el router puede proporcionar acceso a toda la red. Como atenuantes, se ha considerado la ubicación controlada, que protege físicamente el dispositivo y los bajos requerimientos de confidencialidad en la configuración, lo que disminuye la sensibilidad de los datos asociados



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

- Para cada uno de los cuatro activos seleccionados en el apartado uno, indica la lista de amenazas asociada a estos activos. Realiza una captura de cada activo con su lista de amenazas asociada.

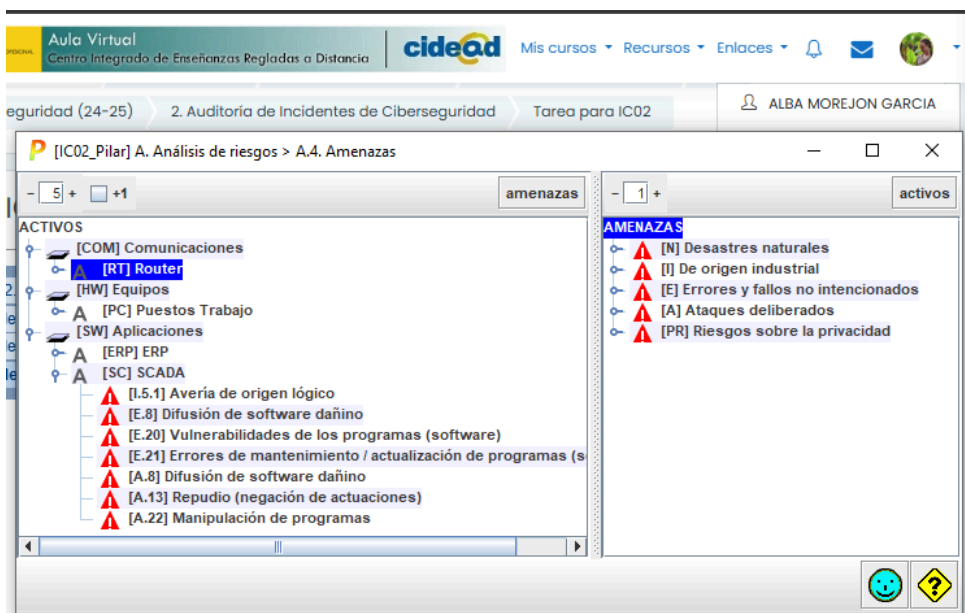
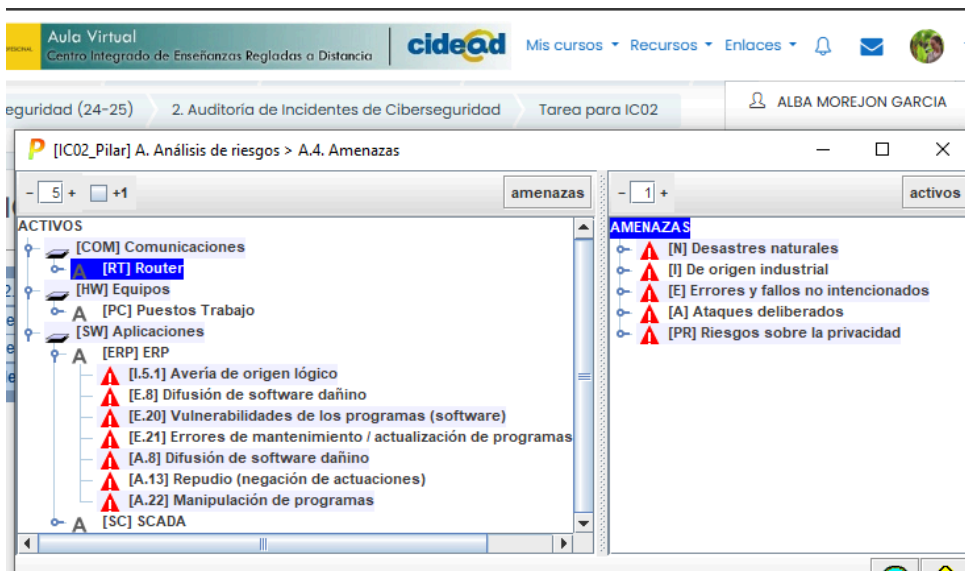
PILAR aplica automáticamente los valores prefijados del fichero TSV



El router tiene vulnerabilidades relacionadas con el acceso no autorizado a la red, ya que un atacante podría intentar obtener acceso a la red interna a través de él. Las amenazas como la interceptación de información y el análisis de tráfico, son comunes en este tipo de equipos. La denegación de servicios también es una amenaza relevante ya que podrían afectar a la disponibilidad de los servicios, además, los routers pueden ser atacados a través de vulnerabilidades de software y fallos en los servicios de comunicaciones lo que hace que la gestión del dispositivo y su actualización sea crucial.

Los puestos de trabajo son puntos de entrada frecuente para los atacantes, debido al abuso de privilegios de acceso y la suplantación de identidad. Las amenazas como la difusión de software dañino o el robo de equipos, son importantes dado que los dispositivos pueden ser comprometidos o sustraídos. Además, las vulnerabilidades de configuración y los errores del administrador, las técnicas de ingeniería social abren las puertas a los atacantes.





En el sistema SCADA la denegación de servicio es una amenaza considerable ya que un ataque puede paralizar la planta, así como, el corte del suministro eléctrico y averías físicas o lógicas son riesgos comunes que podrían afectar la operación del sistema. La destrucción de información también es una amenaza significativa ya que podría alterar los procesos de producción o incluso causar daños materiales. Además, la inyección de código malicioso y el acceso no autorizado pueden ser explotadas por ciberdelincuentes. El sistema ERP, las amenazas de abuso de privilegios o suplantación de identidad son relevantes debido a la cantidad de usuarios que interactúan con el sistema. La manipulación de configuraciones y modificación de información pueden alterar el funcionamiento del sistema comprometiendo su integridad. También, se debe tener en cuenta el riesgo de errores administrativos en la configuración y mantenimiento del sistema que podrían generar vulnerabilidades.

- Además, para cada dominio de seguridad recoge las salvaguardas que te muestra la herramienta ordenadas de mayor a menor prioridad según la herramienta. Para cada una de estas salvaguardas debes indicar una acción concreta que se puede realizar para llevarla a cabo en cierto grado. Incluye también el estado actual y el estado objetivo de esta salvaguarda. Por último realiza una captura de pantalla en la que se muestran estas salvaguardas configuradas.

Hay valores que no permitía modificar como es el caso de Mecanismos de autenticación, que luego más adelante seguirá afectando al desempeño de la práctica.

asp...	tdp	reco...	nivel	salvaguarda	dudas	base	coment...	current	target	PILAR
SALVAGUARDAS										
G	EL	8		[IA] Identificación y autenticación				-L3	-L4	L2-L4
G	STD	2		[IA.1] Se dispone de normativa de identificación y autenticación [IA-1]				-L3	-L4	L2-L4
G	PROC	2		[IA.2] Se dispone de procedimientos para las tareas de identificación y autenticación [IA-1]				L2	L4	L2
G	EL	3		[IA.3] Identificación de los usuarios				L2	L3	L3
G	EL	3		[IA.4] Gestión de la identificación y autenticación de usuario				L2	L3	L2-L3
G	EL	4		[IA.5] Cuentas especiales (administración)				L3	L4	L2-L3
G	PR	7		[IA.6] El mecanismo de autenticación se inhabilita cuando se ve comprometido o hay sospecha de ello				L3	L4	L4
T	EL	5		[IA.7] Canal seguro de autenticación [SC-11]				L2	L3	L3
G	EL	8		[IA.8] {xor} Nivel de garantía de la autenticación						L3
G	EL	3		[IA.9] Biometría - Algo que eres				L1	L3	L3
G				Mecanismo de autenticación (NIST SP 800-63)						
T	EL	7		[AC] Control de acceso lógico				L2	L4	L2-L4
G	PR			[D] Protección de la Información				L2	L4	n.a.
G	EL			[K] Protección de claves criptográficas [SC-12]				L1	L3	n.a.
G	PR			[S] Protección de los Servicios						n.a.
G	PR	5		[SW] Protección de las Aplicaciones Informáticas (SW)				L2	L3	L2-L3
G	PR	4		[HW] Protección de los Equipos Informáticos (HW)				L2	L3	L2-L3
G	PR			[COM] Protección de las Comunicaciones				L2	L4	n.a.
G	PR			[M] Protección de los Soportes de Información						n.a.
G	PR	3		[AUX] Elementos Auxiliares				L1	L3	L2-L3
F	EL	5		[PPE] Protección física de los equipos				L2	L4	L3
F	PR			[L] Protección de las Instalaciones				L2	L4	n.a.
P	PR			[P] Gestión del Personal				L1	L3	n.a.
G	CR	5		[IM] Gestión de incidentes						L2-L3
T	PR	7		[tools] Herramientas de seguridad				L2	L4	L2-L4
G	CR	3		[V] Gestión de vulnerabilidades				L1	L3	L2-L3
T	MN	4		[A] Registro y auditoría				L2	L4	L2-L3
G	RC	1 (o)		[BC] Continuidad del negocio				L1	L4	L2
G	AD	4		[G] Organización						L2-L3
G	AD	3		[E] Relaciones Externas				L1	L3	L2-L3
G	AD	4		[NEW] Adquisición / desarrollo				L1	L3	L2-L3
G	PR			[PDS] Servicios potencialmente peligrosos				L1	L3	n.a.
G	PR			[IP] Sistema de protección de frontera lógica				L2	L4	n.a.
F	EL			[PPS] Protección del perímetro físico				L2	L4	n.a.
G	EL	1 (o)		[TEMPEST] Protección de emanaciones (TEMPEST) [PE-19]				L1	L2	L2

Salvaguardas Gestión Empresarial:

- Se dispone de normativas de identificación y autenticación, crear y publicar una política formal de identificación y autenticación, indicando procedimientos para gestionar usuarios y contraseñas. (L2-L4)
- Registro y auditoría, implementar un sistema centralizado que capture logs de eventos importantes. (L2-L4)
- Gestión de incidentes, diseñar un plan de respuesta a incidentes, incluyendo simulaciones periódicas para asegurar su eficiencia. (L2-L4)
- Continuidad del negocio, desarrollar y mantener un plan con estrategias de recuperación ante desastres naturales y ciberataques. (L1-L4)
- Protección de las aplicaciones informáticas, implementar un programa de revisión y actualización software para garantizar la corrección de vulnerabilidades críticas. (L2-L3)

<

### Salvaguardas Operaciones Fabriles:

- Identificación de usuarios, configurar cuentas individuales para cada operativo cuentas compartidas. (L2-L4)
- Protección física de equipos, instalar cerraduras y controles de acceso para proteger equipos críticos. (L2-L4)
- Protección física de las instalaciones, instalar cámaras de vigilancia y personal de seguridad. (L2-L4)
- Gestión de incidentes, enseñar a los empleados para que reporten incidentes de los sistemas de control. (L1-L4)
- Protección de las comunicaciones, configurar canales cifrados para comunicaciones entre los sistemas de control y centros de operaciones. (L2-L4)

[IC02_Pilar] A.5. Medidas > A.5.1. Salvaguardas									
Editar	Expandir	Ver	Exportar	Importar	Estadísticas				
[RED] Redes y Comunicaciones									
asp...	tdp	reco...	nivel	salvaguarda	dud...	base	co...	surr...	target
				SALVAGUARDAS					
	G	EL		1 [A] Identificación y autenticación				L2	L5
	G	STD		1 [A.1] Se dispone de normativa de identificación y autenticación [A-1]				L1	L4
	G	PROC		1 [A.2] Se dispone de procedimientos para las tareas de identificación y autenticación [A-1]				L1	L4
	G	EL		1 [A.3] Identificación de los usuarios				L2	L5
	G	EL		1 [A.4] Gestión de la identificación y autenticación de usuario				L2	L5
	G	EL		1 [A.5] Cuentas especiales (administración)				L1	L4
	G	PR		1 [A.6] El mecanismo de autenticación se inhabilita cuando se ve comprometido o hay sospecha de ello				L1	L4
	T	EL		1 [A.7] Canal seguro de autenticación [SC-11]				L2	L5
	G	EL		1 [A.8] {xor} Nivel de garantía de la autenticación					
	G	EL		1 [A.9] Biometría - Algo que eres				L1	L3
	G			2 Mecanismo de autenticación (NIST SP 800-63)					
	T	EL	7	1 [A] Control de acceso lógico				L2	L4
	G	PR		1 [D] Protección de la Información				L2	L4
	G	EL		1 [K] Protección de claves criptográficas [SC-12]				L2	L4
	G	PR		1 [S] Protección de los Servicios				L2	L3
	G	PR		1 [SW] Protección de las Aplicaciones Informáticas (SW)				L1	L3
	G	PR		1 [HW] Protección de los Equipos Informáticos (HW)				L2	L4
	G	PR	8	1 [COM] Protección de las Comunicaciones				L2	L5
	G	PR		1 [M] Protección de los Soportes de Información				L2	L4
	G	PR		1 [AUX] Elementos Auxiliares				L1	L3
	F	EL		1 [PPE] Protección física de los equipos				L2	L4
	F	PR		1 [L] Protección de las Instalaciones				L2	L4
	P	PR		1 [P] Gestión del Personal					
	G	CR	4	1 [IM] Gestión de incidentes				L2	L4
	T	PR	4	1 [tools] Herramientas de seguridad				L2	L4
	G	CR		1 [V] Gestión de vulnerabilidades				L2	L4
	T	MN	4	1 [A] Registro y auditoría				L2	L5
	G	RC	1 (o)	1 [BC] Continuidad del negocio				L2	L5
	G	AD	3	1 [G] Organización				L1	L3
	G	AD	3	1 [E] Relaciones Externas				L1	L3
	G	AD	3	1 [NEW] Adquisición / desarrollo				L2	L3
	G	PR		1 [PDS] Servicios potencialmente peligrosos				L1	L4
	G	PR		1 [IP] Sistema de protección de frontera lógica				L2	L5
	F	EL		1 [PPS] Protección del perímetro físico				L2	L4
	G	EL		1 [TEMPEST] Protección de emanaciones (TEMPEST) [PE-19]				L1	L3

## Salvaviduas Redes y Comunicaçoes:

- Canal seguro de autenticación, configurar autenticación a través de protocolos seguros (HTTPS SSH VPN). (L2-L5)
- Control de acceso lógico, implementar listas de control de acceso en dispositivos de red para segmentar y restringir el tráfico no autorizado. (L2-L4)
- Sistemas de protección de frontera lógica, configurar un firewall con políticas de inspección de tráfico y detección de intrusiones. (L2-L5)
- Herramientas de seguridad, instalar y mantener actualizadas herramientas de seguridad como antivirus, IDS/IPS y escáneres de vulnerabilidades en los equipos de red. (L2-L4)
- Registro y auditoría, configurar syslog para centralizar los registros de los dispositivos de red y generar alertas de eventos críticos. (L2-L5)

**Apartado 4: Estimación del riesgo a considerar por la empresa para su estudio y toma de decisiones.**  
**- Para cada uno de los cuatro activos seleccionados en el apartado uno, indica la estimación del estado del riesgo a asumir por la empresa. Se debe indicar la estimación actual (current) y la estimación objetivo (target).**

Virtual Integrado de Enseñanzas Regladas a Distancia cidead Mis cursos Recursos Enlaces ALBA MOREJON GARCIA

amenazas asociada a estos activos Modo d

[IC02\_Pilar] A. Análisis de riesgos > A.6. Riesgo

Exportar

potencial current target PILAR

activo	[D]	[I]	[C]	[A]	[T]	[DP]
ACTIVOS	(4,2)	(5,6)	(4,8)	(2,0)	(5,0)	
[RT] Router	(1,8)	(1,8)	(2,1)	(2,0)	(0,95)	
[D] disponibilidad	(1,8)					
[I] integridad de los datos		(1,8)				
[C] confidencialidad de los datos			(2,1)			
[A] autenticidad de los usuarios y de la información				(2,0)		
[T] trazabilidad del servicio y de los datos					(0,95)	
[DP] Datos personales						
[PC] Puestos Trabajo	(2,5)	(1,5)	(2,2)		(2,4)	
[D] disponibilidad	(2,5)					
[I] integridad de los datos		(1,5)				
[C] confidencialidad de los datos			(2,2)			
[A] autenticidad de los usuarios y de la información					(2,4)	
[T] trazabilidad del servicio y de los datos						
[DP] Datos personales						
[ERP] ERP	(3,3)	(4,5)	(4,7)		(3,5)	
[D] disponibilidad	(3,3)					
[I] integridad de los datos		(4,5)				
[C] confidencialidad de los datos			(4,7)			
[A] autenticidad de los usuarios y de la información					(3,5)	
[T] trazabilidad del servicio y de los datos						
[DP] Datos personales						
[SC] SCADA	(4,2)	(5,6)	(4,8)		(5,0)	
[D] disponibilidad	(4,2)					
[I] integridad de los datos		(5,6)				
[C] confidencialidad de los datos			(4,8)			
[A] autenticidad de los usuarios y de la información					(5,0)	
[T] trazabilidad del servicio y de los datos						
[DP] Datos personales						

gestionar leyenda

Hay espacio sin rellenar porque en las salvaguardas anteriores hubo espacio que no me dejaba rellenar la propia aplicación.

Virtual Integrado de Enseñanzas Regladas a Distancia cidead Mis cursos Recursos Enlaces ALBA MOREJON GARCIA

amenazas asociada a estos activos Modo d

[IC02\_Pilar] A. Análisis de riesgos > A.6. Riesgo

Exportar

potencial current target PILAR

activo	[D]	[I]	[C]	[A]	[T]	[DP]
ACTIVOS	(1,1)	(2,7)	(2,5)	(0,64)	(1,5)	
[RT] Router	(0,55)	(0,56)	(0,65)	(0,64)	(0,40)	
[D] disponibilidad	(0,55)					
[I] integridad de los datos		(0,56)				
[C] confidencialidad de los datos			(0,65)			
[A] autenticidad de los usuarios y de la información				(0,64)		
[T] trazabilidad del servicio y de los datos					(0,40)	
[DP] Datos personales						
[PC] Puestos Trabajo	(0,83)	(0,65)	(0,78)		(0,79)	
[D] disponibilidad	(0,83)					
[I] integridad de los datos		(0,65)				
[C] confidencialidad de los datos			(0,78)			
[A] autenticidad de los usuarios y de la información					(0,79)	
[T] trazabilidad del servicio y de los datos						
[DP] Datos personales						
[ERP] ERP	(1,1)	(2,3)	(2,5)		(1,2)	
[D] disponibilidad	(1,1)					
[I] integridad de los datos		(2,3)				
[C] confidencialidad de los datos			(2,5)			
[A] autenticidad de los usuarios y de la información					(1,2)	
[T] trazabilidad del servicio y de los datos						
[DP] Datos personales						
[SC] SCADA	(0,99)	(2,7)	(1,7)		(1,5)	
[D] disponibilidad	(0,99)					
[I] integridad de los datos		(2,7)				
[C] confidencialidad de los datos			(1,7)			
[A] autenticidad de los usuarios y de la información					(1,5)	
[T] trazabilidad del servicio y de los datos						
[DP] Datos personales						

gestionar leyenda

- **Calcula la bajada que se produce en los riesgos en cada uno de los criterios de seguridad para cada activo.**

Router

- Disponibilidad:  $1,8 - 0,55 = 1,25$
- Integridad:  $1,8 - 0,56 = 1,24$
- Confidencialidad:  $2,1 - 0,65 = 1,45$
- Autenticidad:  $2,0 - 0,64 = 1,36$
- Trazabilidad:  $0,95 - 0,40 = 0,55$

Puestos Trabajo

- Disponibilidad:  $2,5 - 0,83 = 1,67$
- Integridad:  $1,5 - 0,65 = 0,85$
- Confidencialidad:  $2,2 - 0,78 = 1,42$
- Trazabilidad:  $2,4 - 0,79 = 1,61$

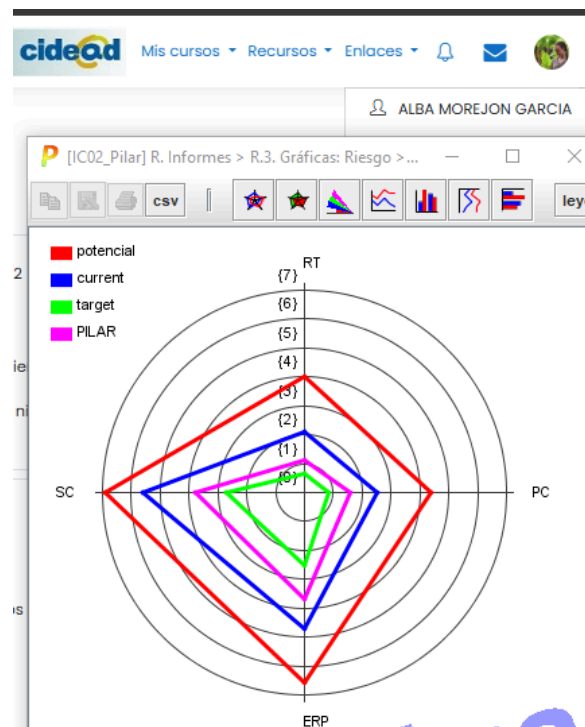
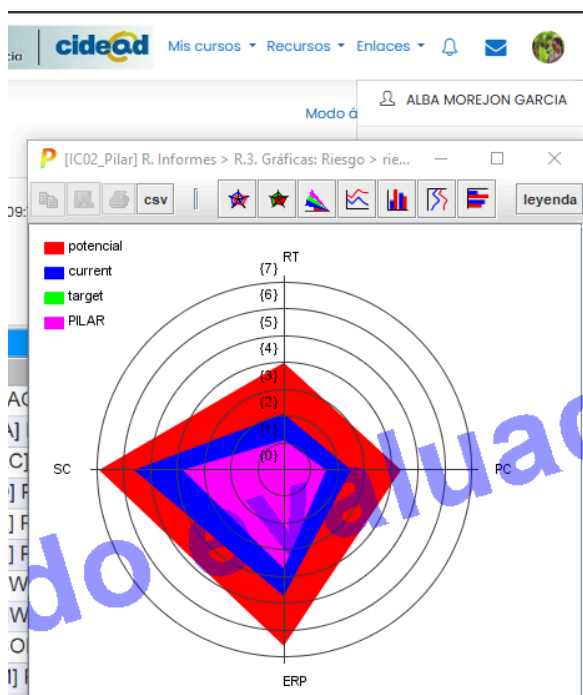
ERP

- Disponibilidad:  $3,3 - 1,1 = 2,2$
- Integridad:  $4,5 - 2,3 = 2,2$
- Confidencialidad:  $4,7 - 2,5 = 2,2$
- Trazabilidad:  $3,5 - 1,2 = 2,3$

SCADA

- Disponibilidad:  $4,2 - 0,99 = 3,21$
- Integridad:  $5,6 - 2,7 = 2,9$
- Confidencialidad:  $4,8 - 1,7 = 3,1$
- Trazabilidad:  $5,0 - 1,5 = 3,5$

- **Además, muestra una captura de la gráfica de riesgos de tipo "Área" en la que se muestran los cuatro activos con sus valores actuales, objetivo y recomendados por PILAR.**





## **Apartado 5: Taxonomía de incidentes.**

**Para cada uno de los cuatro activos seleccionados en el apartado uno y tras el estudio de sus riesgos, determina un tipo de incidente que podría producirse en relación a sus riesgos. Para este tipo de incidente indica el grupo al que pertenece y realiza una pequeña explicación sobre este.**

Router

Tipo de Incidente: Acceso no autorizado

Grupo: Ciberataque

Un atacante podría aprovechar una puerta trasera en el firmware del router o descifrar las contraseñas con técnicas de fuerza bruta. Una vez dentro la red interna se habría visto comprometida, ya que el intruso podría interceptar el tráfico, descifrando mensajes confidenciales o desconfigurando las rutas críticas de la red. Este incidente no sólo pondría en jaque las comunicaciones, sino que abriría las puertas a un ataque más completo en la infraestructura tecnológica

Puestos de trabajo

Tipo de Incidente: Difusión de software

Grupo: Malware

Los puestos de trabajo son un objetivo común para la difusión de malwares, debido a descargas inadvertidas, correos electrónicos de phishing o dispositivos externos infectados, basta con que un empleado haga clic en un archivo adjunto sospechosamente o conecte un USB. Una vez activado el malware se despliega extendiéndose por la red, además si el atacante utiliza ingeniería social las víctimas podrían ayudarse en saberlo abriendo las puertas a sus datos o a los sistemas críticos.

Este tipo de incidentes podría comprometer la confidencialidad y disponibilidad de la información, además de permitir movimientos laterales dentro de la red poniendo en riesgo sistemas críticos como el ERP o SCADA.

ERP

Tipo de Incidente: Abuso de privilegios

Grupo: amenazas internas

Un usuario con permisos elevados podría acceder a datos sensibles de manera indebida, alterar configuraciones o manipular datos financieros, esta acción podría desestabilizar todo el sistema empresarial: facturas, estrategias, pedidos... Este incidente comprometería la integridad y la confidencialidad del sistema, generando posibles pérdidas financieras, dañando a la reputación y causando dificultades operativas en la gestión empresarial.

SCADA

Tipo de Incidente: Denegación de servicios

Grupo: Ciberataque

Un ataque DoS contra un sistema SCADA, supondría la detención de las máquinas, los sensores inutilizados, las líneas de producción paradas, entre otras consecuencias. Este ataque satura los recursos del sistema hasta que el sistema colapsa, puede tener efectos devastadores: interrupción, inhabilitación, pérdida, paralización... Un pequeño comando ejecutado desde un lugar remoto podría afectar a los procesos críticos y detener una operación multimillonaria. Este incidente afecta directamente la disponibilidad del sistema con graves consecuencias económicas y operativas.