Análisis de riesgos – herramienta PILAR del CCN-CERT

María del Carmen Zarcero García-Risco - TCu

XV Encuentros Técnicos OCEX 2023

Proceso de Gestión de Riesgo

Recordemos que el proceso de Gestión de Riesgo, aun tratándose de un proceso iterativo, consta de dos partes bastante diferenciadas: el análisis y el tratamiento de riesgos.

Análisis de Riesgos: analizar nuestra situación con respecto a los riesgos determinados.

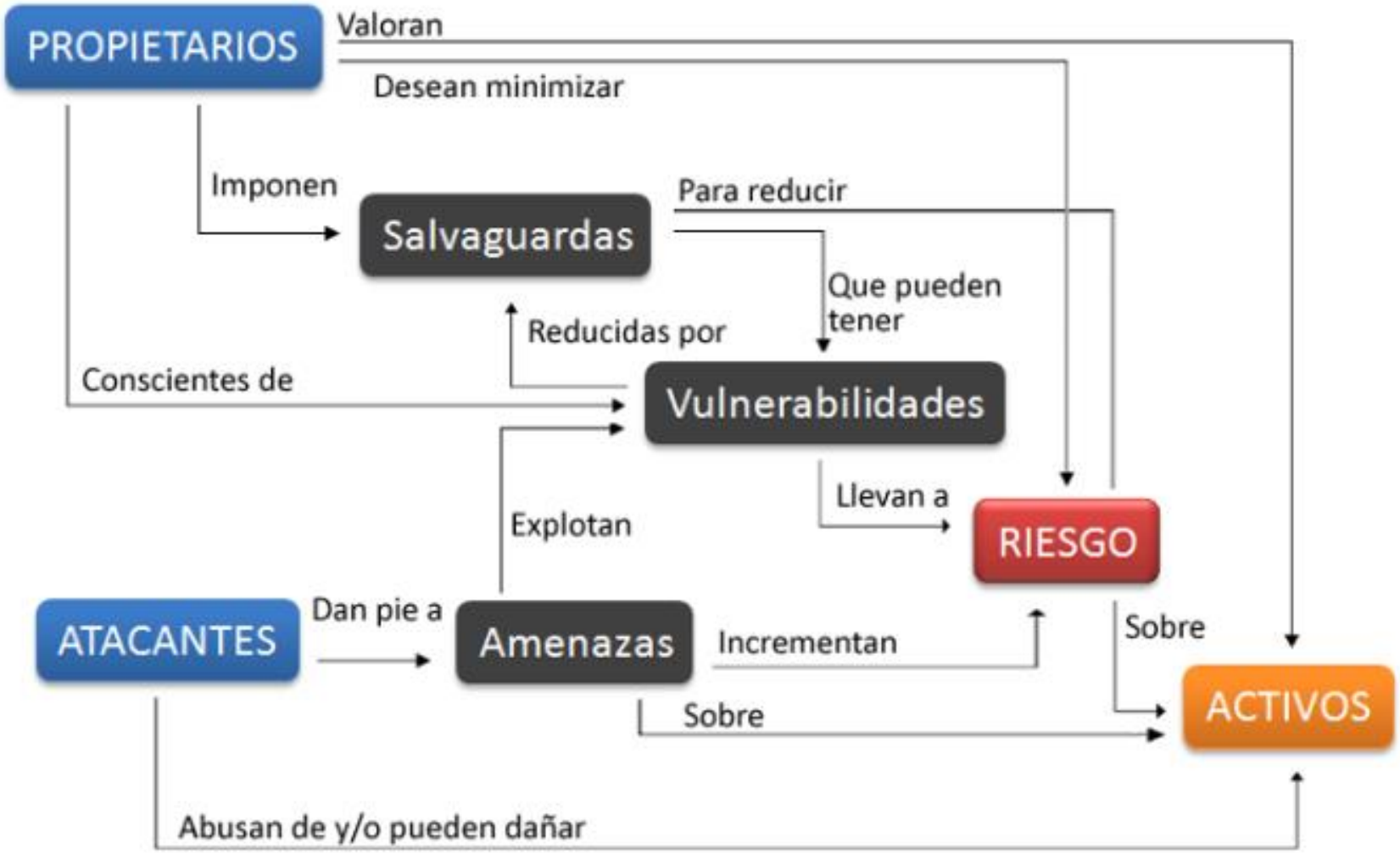
Actividad compleja que requiere de una **ejecución metódica** para llevarla a cabo de forma efectiva.

¿Qué quiere decir Metódicamente?

- Gestionándola como un proyecto con tareas, entregas y puntos de control.
- Ajustándonos a una metodología que nos guíe y nos permita explicar y comparar los resultados.

Fuente CCN-CERT

CONCEPTOS IMPORTANTES DE RIESGO



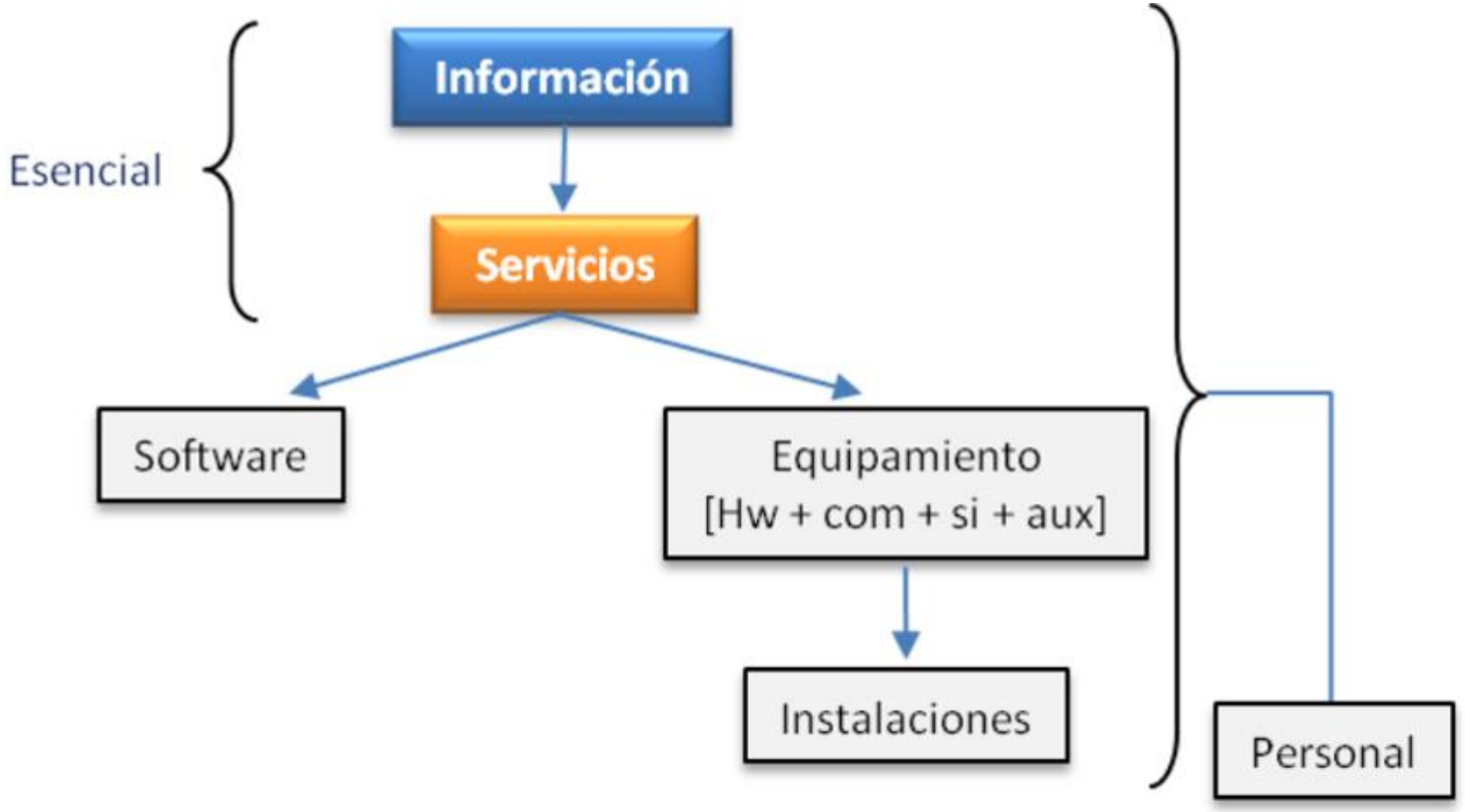
Fuente CCN-CERT

¿Qué es PILAR?

PILAR es un conjunto de herramientas EAR (Entorno de Análisis de Riesgos) cuya función es el **análisis y la gestión de riesgos de un sistema de información** siguiendo la metodología **Magerit** (Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información) y está desarrollada y financiada parcialmente por el CCN. Se actualizan periódicamente y existen diversas variantes.

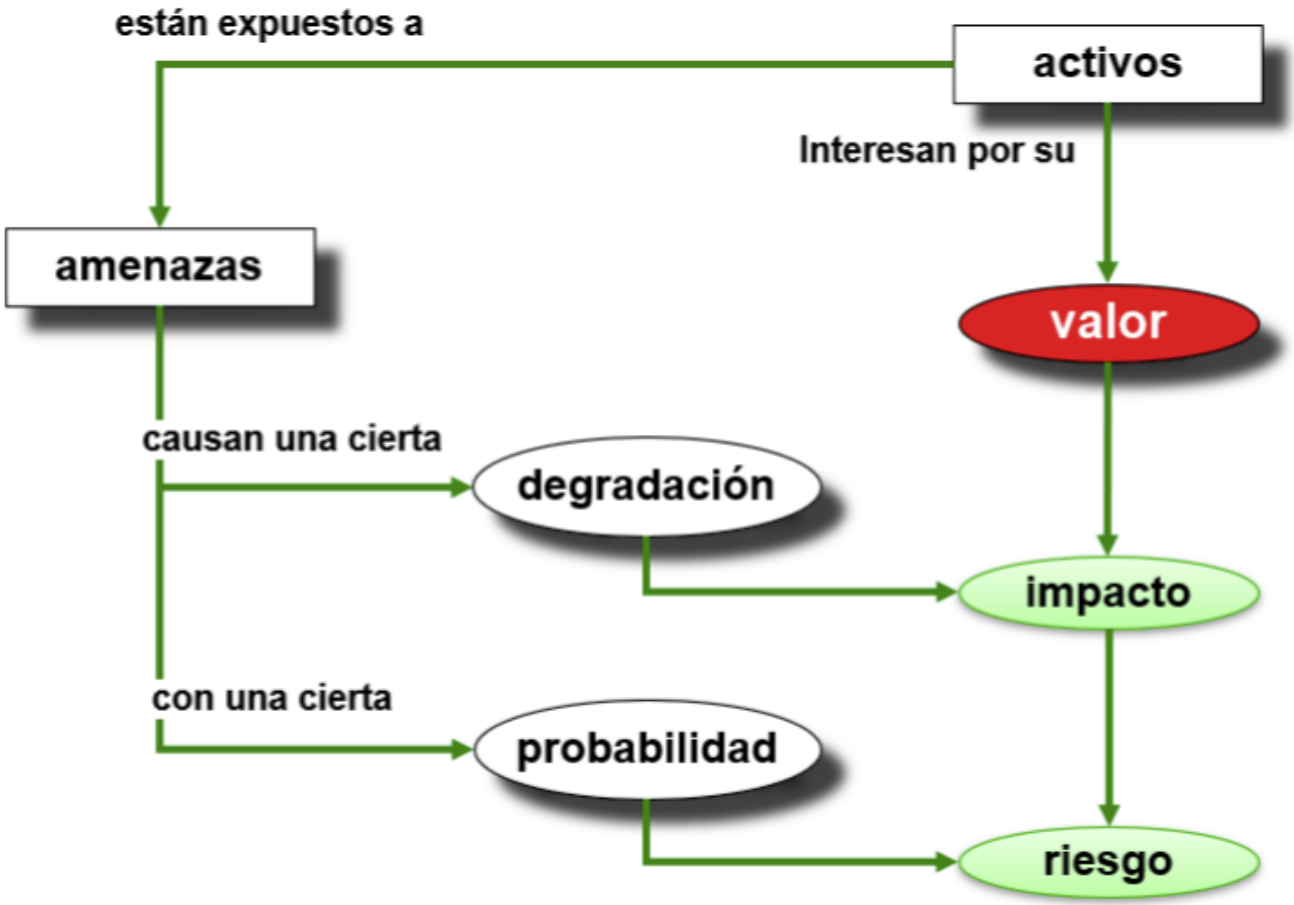
PILAR está **dirigida a** todas aquellas **organizaciones/organismos** que cuentan con infraestructuras de TIC y que tienen la necesidad de gestionar de forma eficiente sus **activos**, realizando Análisis de Impacto y Continuidad de Operaciones, tanto cuantitativos como cualitativos.

Fuente CCN-CERT

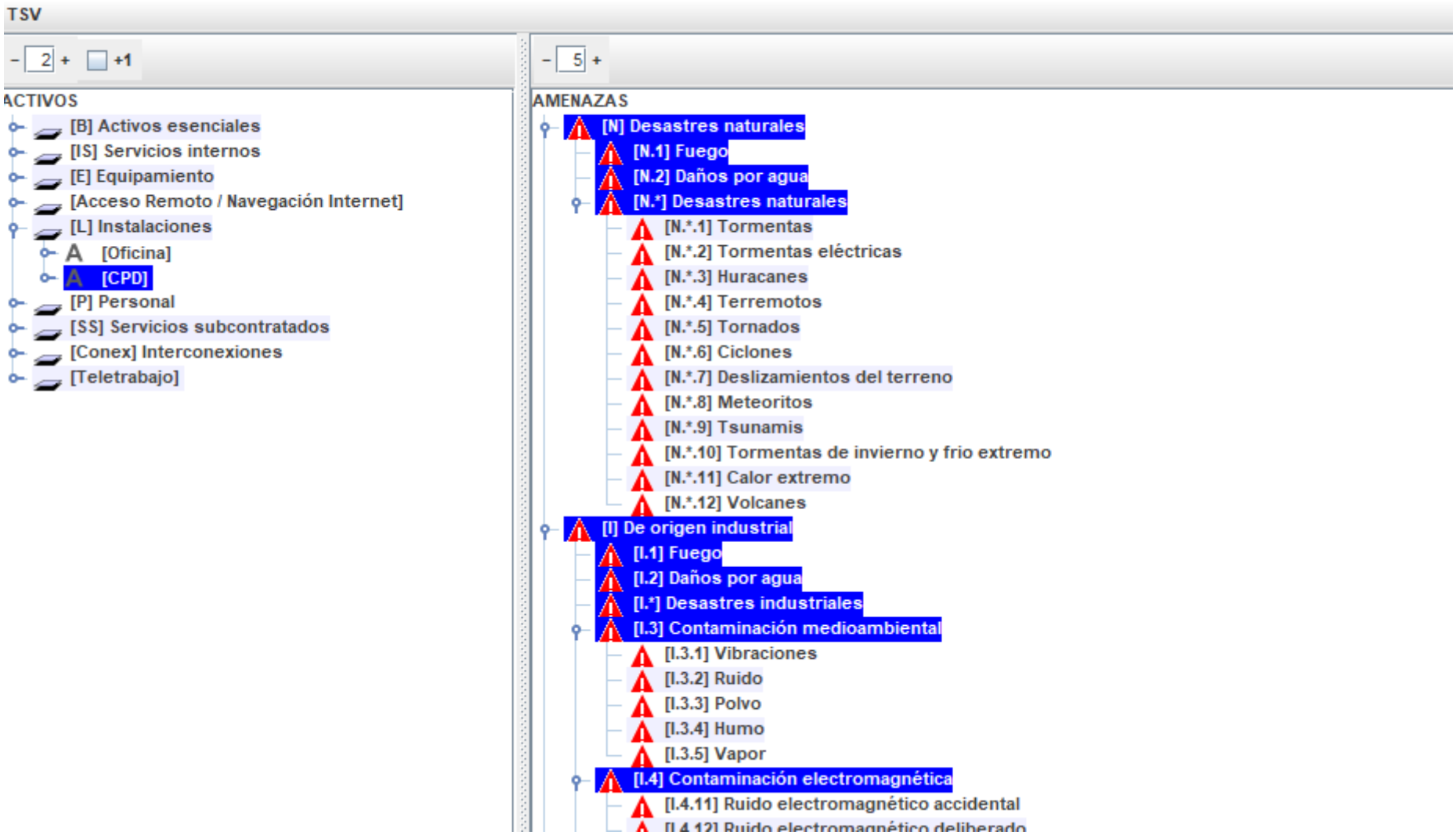


Fuente CCN-CERT

ACTIVOS					
[B] Activos esenciales					
[Info] Información Negocio Fiscalización	[M]	[M]	[M]	[M]	[M]
[S] Servicios de Acceso Información Fiscalización	[M]	[M]	[M]	[M]	[M]
[SI_R] Acceso Remoto	[B]	[M]	[M]	[M]	[M]
[SI_2] Acceso Servicios NUBE	[M]	[M]	[M]	[M]	[M]
[IS] Servicios internos					
[Bus] Bus de servicios	[M]	[M]	[M]	[M]	[M]
[E] Equipamiento					
[SW] Aplicaciones					
[APP1] Aplicaciones para la fiscalización	[M]	[M]	[M]	[M]	[M]
[HW] Equipos					
[HW_Portatil] Portátiles	[M]	[M]	[M]	[M]	[M]
[HW_Portatil_Admin] Portátiles Administradores	[M]	[M]	[M]	[M]	[M]
[Conf] Configuración del Sistema		[M]		[M]	
[HW_Serv] Servidores	[M]	[M]	[M]	[M]	[M]
[Logs] Registro de Actividad del Sistemas		[M]		[M]	
[COM] Comunicaciones					
[HW Router] Router	[M]	[M]	[M]	[M]	[M]
[LAN]	[M]	[M]	[M]	[M]	[M]
[Acceso Remoto / Navegación Internet]					
[HW_VPN] Servidor VPN	[M]				
[HW_Proxy] Proxy de Navegación	[M]	[M]	[M]	[M]	[M]
[HW Router_2] Router Externo	[M]	[M]	[M]	[M]	[M]
[DMZ]	[M]	[M]	[M]	[M]	[M]
[Logs_DMZ] Registro de Actividad Frontera		[M]		[M]	
[Frontera] Border Protection System	[M]	[M]	[M]	[M]	[M]
[Conf_DMZ] Configuración del Sistema		[M]		[M]	
[L] Instalaciones					
[Oficina]	[M]	[M]	[M]	[M]	[M]
[CPD]	[M]	[M]	[M]	[M]	[M]
[P] Personal					
[Usuarios]	[M]	[M]	[M]	[M]	[M]
[Administradores]	[M]	[M]	[M]	[M]	[M]
[SS] Servicios subcontratados					
[Servicios Nube] Fisconex/Office365	[M]	[M]	[M]	[M]	[M]
[Conex] Interconexiones					
[Internet]	[M]	[M]	[M]	[M]	[M]
[Interconexiones] Proveedores	[M]				
[Teletrabajo]					
[HW Router 3] Router WIFI	[B]	[M]	[M]	[M]	[M]
[Hogar]	[B]	[M]	[M]	[M]	[M]
[VPN] Cliente VPN	[B]				
[HW_Portatil_2] Portátiles	[B]	[M]	[M]	[M]	[M]



Fuente CCN-CERT


TSV
- 2 + +1
ACTIVOS
[B] Activos esenciales
[IS] Servicios internos
[E] Equipamiento
[Acceso Remoto / Navegación Internet]
[L] Instalaciones
[Oficina]
[CPD]
[P] Personal
[SS] Servicios subcontratados
[Conex] Interconexiones
[Teletrabajo]
- 5 +
AMENAZAS
[N] Desastres naturales
[N.1] Fuego
[N.2] Daños por agua
[N.*] Desastres naturales
[N.*.1] Tormentas
[N.*.2] Tormentas eléctricas
[N.*.3] Huracanes
[N.*.4] Terremotos
[N.*.5] Tornados
[N.*.6] Ciclones
[N.*.7] Deslizamientos del terreno
[N.*.8] Meteoritos
[N.*.9] Tsunamis
[N.*.10] Tormentas de invierno y frio extremo
[N.*.11] Calor extremo
[N.*.12] Volcanes
[I] De origen industrial
[I.1] Fuego
[I.2] Daños por agua
[I.*] Desastres industriales
[I.3] Contaminación medioambiental
[I.3.1] Vibraciones
[I.3.2] Ruido
[I.3.3] Polvo
[I.3.4] Humo
[I.3.5] Vapor
[I.4] Contaminación electromagnética
[I.4.11] Ruido electromagnético accidental

Fuente CCN-CERT

[base] OCEX/TCu - Redes corporativas | sólo si ...

rec...		nivel	control	du...	fue...	ens	base	co...	current	target	ENS
			[ens:2022] Esquema Nacional de Seguridad (RD 311/2022)						L1	L2	L3 (L2-...
1			[org] Marco organizativo /PR AD						L1	L2	L3 (L2-...
1		B	[org.1] Política de seguridad /AD			M			L1	L2	L3 (L2)
1		B	[org.2] Normativa de seguridad /AD			M			L1	L2	L3
1		B	[org.3] Procedimientos de seguridad /AD			M			L1	L2	L3
1		B	[org.4] Proceso de autorización /PR			M			L1	L2	L3 (L2-...
1			[op] Marco operacional /						L1	L2	L3 (L2-...
			El marco operacional está constituido por las medidas a tomar para proteger la operación del sistema como conjunto integral de componentes para un fin.								
1			[op.pl] Planificación /PR						L1	L2	L3 (L2-...
1			[op.acc] Control de acceso /PR						L1	L2	L3 (L2-...
1			[op.exp] Explotación /PR						L1	L2	L3 (L2-...
1			[op.ext] Recursos externos /PR IM						L1	L2	L3 (L2-...
			[op.nub] Servicios en la nube /PR IM						L1	L2	n.a.
1			[op.cont] Continuidad del servicio /RC MN AD						L1	L2	L3 (L2)
1			[op.mon] Monitorización del sistema /MN						L1	L2	L3 (L2-...
1			[mp] Medidas de protección /PR						L1	L2	L3 (L2-...
1			[mp.if] Protección de las instalaciones e infraestructuras /PR IM						L1	L2	L3 (L2-...
1			[mp.per] Gestión del personal /AW						L1	L2	L3 (L2-...
1			[mp.eq] Protección de los equipos /PR IM						L1	L2	L3 (L2-...
1			[mp.com] Protección de las comunicaciones /PR IM						L1	L2	L3 (L2-...
1			[mp.si] Protección de los soportes de información /EL AD						L1	L2	L3 (L2-...
1			[mp.sw] Protección de las aplicaciones informáticas /PR IM						L1	L2	L3 (L2-...
1			[mp.info] Protección de la información /						L1	L2	L3 (L2-...
1			[mp.s] Protección de los servicios /						L1	L2	L3 (L2-...

potencial | current | target | ENS

activo	[D]	[I]	[C]	[A]	[T]
ACTIVOS	{4,5}	{5,1}	{5,1}	{4,2}	{4,5}
I [Info] Información Negocio Fiscalización		{4,2}	{4,5}	{4,2}	{4,5}
S [S] Servicios de Acceso Información Fiscalizació	{4,5}				
is [SI_R] Acceso Remoto	{2,7}	{5,1}	{5,1}	{4,2}	{2,8}
is [SI_2] Acceso Servicios NUBE	{4,2}	{4,2}	{4,2}	{2,7}	{4,2}

potencial | current | target | ENS

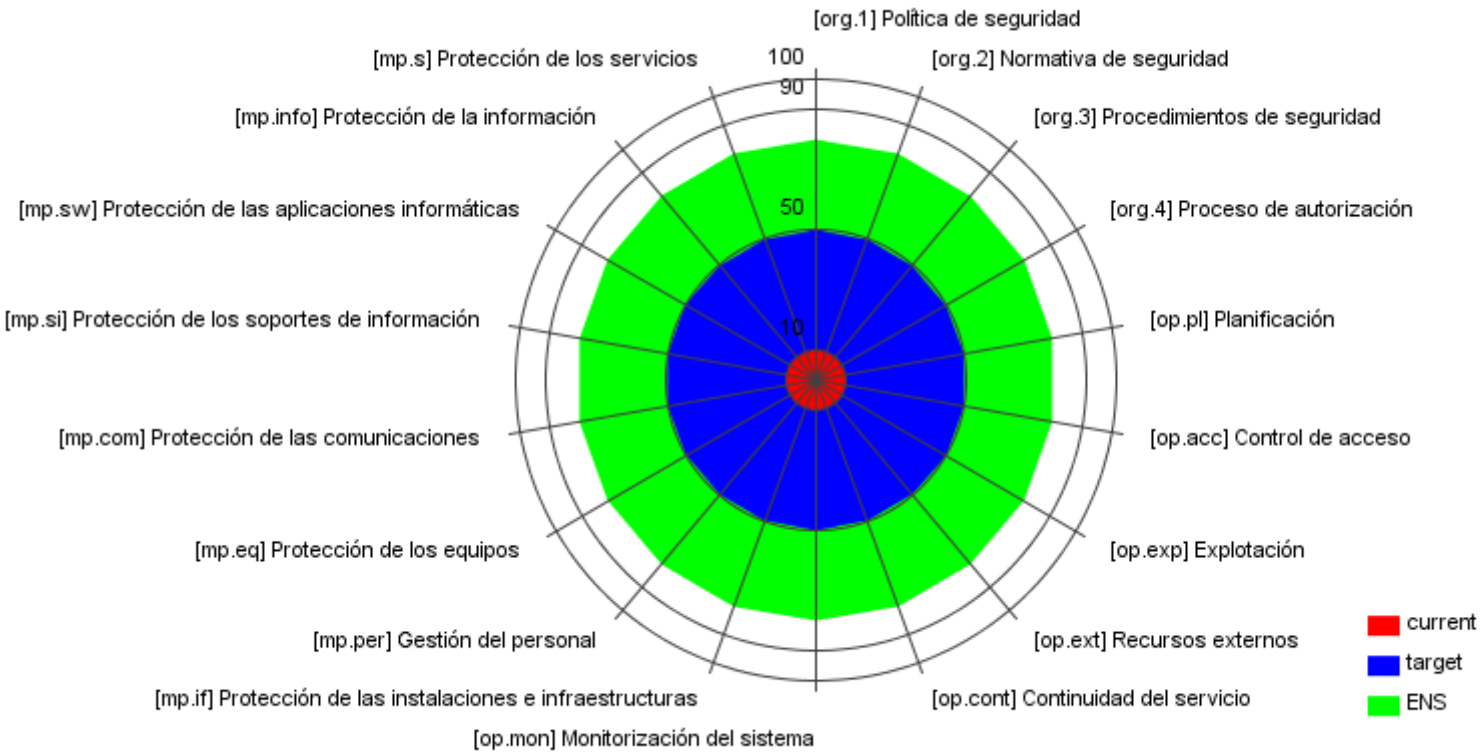
activo	[D]	[I]	[C]	[A]	[T]
ACTIVOS	{3,9}	{4,5}	{4,5}	{3,6}	{3,9}
I [Info] Información Negocio Fiscalización		{3,6}	{3,9}	{3,6}	{3,9}
S [S] Servicios de Acceso Información Fiscalizació	{3,9}				
is [SI_R] Acceso Remoto	{2,2}	{4,5}	{4,5}	{3,6}	{2,2}
is [SI_2] Acceso Servicios NUBE	{0,92}	{0,91}	{0,92}	{0,61}	{0,91}

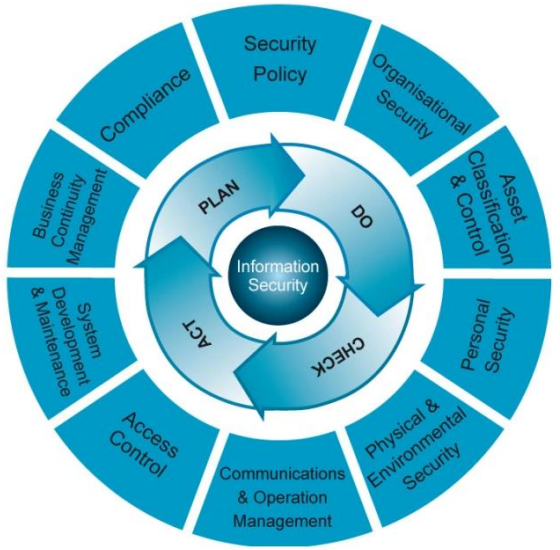
potencial | current | target | ENS

activo	[D]	[I]	[C]	[A]	[T]
ACTIVOS	{2,2}	{2,8}	{2,8}	{1,8}	{2,2}
I [Info] Información Negocio Fiscalización		{1,8}	{2,2}	{1,8}	{2,2}
S [S] Servicios de Acceso Información Fiscalizació	{2,2}				
is [SI_R] Acceso Remoto	{0,89}	{2,8}	{2,8}	{1,8}	{0,88}
is [SI_2] Acceso Servicios NUBE	{0,92}	{0,91}	{0,92}	{0,61}	{0,91}

potencial | current | target | ENS

activo	[D]	[I]	[C]	[A]	[T]
ACTIVOS	{1,3}	{1,8}	{1,8}	{0,99}	{1,3}
I [Info] Información Negocio Fiscalización		{0,99}	{1,3}	{0,99}	{1,3}
S [S] Servicios de Acceso Información Fiscalizació	{1,3}				
is [SI_R] Acceso Remoto	{0,70}	{1,8}	{1,8}	{0,98}	{0,70}
is [SI_2] Acceso Servicios NUBE	{1,0}	{0,99}	{1,0}	{0,70}	{0,99}


[org.1] Política de seguridad
[org.2] Normativa de seguridad
[org.3] Procedimientos de seguridad
[org.4] Proceso de autorización
[op.pl] Planificación
[op.acc] Control de acceso
[op.exp] Explotación
[op.ext] Recursos externos
[op.cont] Continuidad del servicio
[op.mon] Monitorización del sistema
[mp.if] Protección de las instalaciones e infraestructuras
[mp.per] Gestión del personal
[mp.eq] Protección de los equipos
[mp.com] Protección de las comunicaciones
[mp.si] Protección de los soportes de información
[mp.sw] Protección de las aplicaciones informáticas
[mp.info] Protección de la información
[mp.s] Protección de los servicios
100
90
50
10
current
target
ENS


Security Policy
Organisational Security
Asset Classification & Control
Personal Security
Physical & Environmental Security
Communications & Operation Management
Access Control
System Development & Maintenance
Business Continuity Management
Compliance
PLAN
DO
CHECK
ACT
Information Security

Muchas gracias