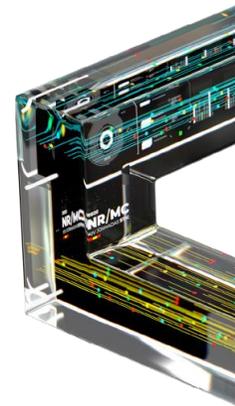


# #XIVJORNADASCCNCERT

**ePULPO: Inteligencia de  
seguridad global y  
cumplimiento normativo**





***Félix García Romero***

***Ingenia***

***fgarcia@ingenia.es***

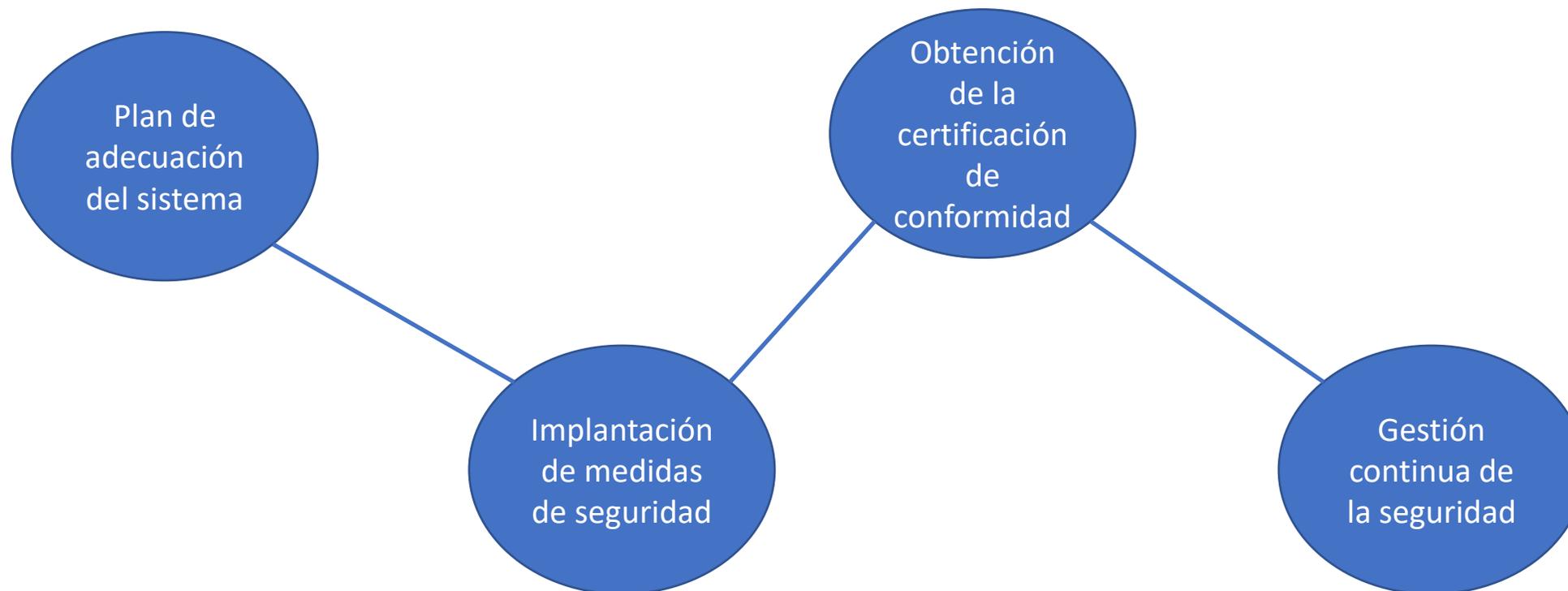
# Un entorno cambiante de amenazas



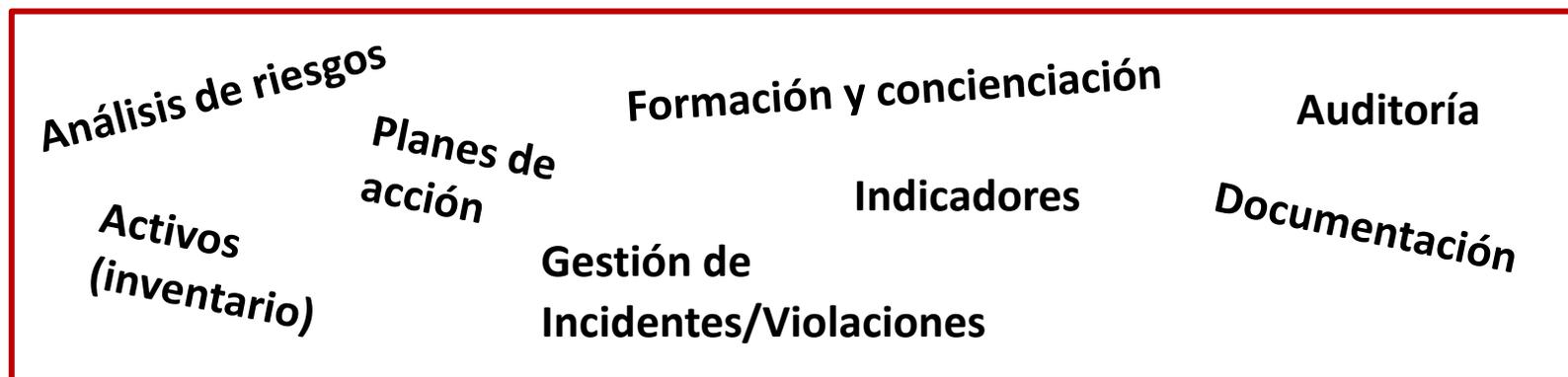
# Inteligencia de seguridad



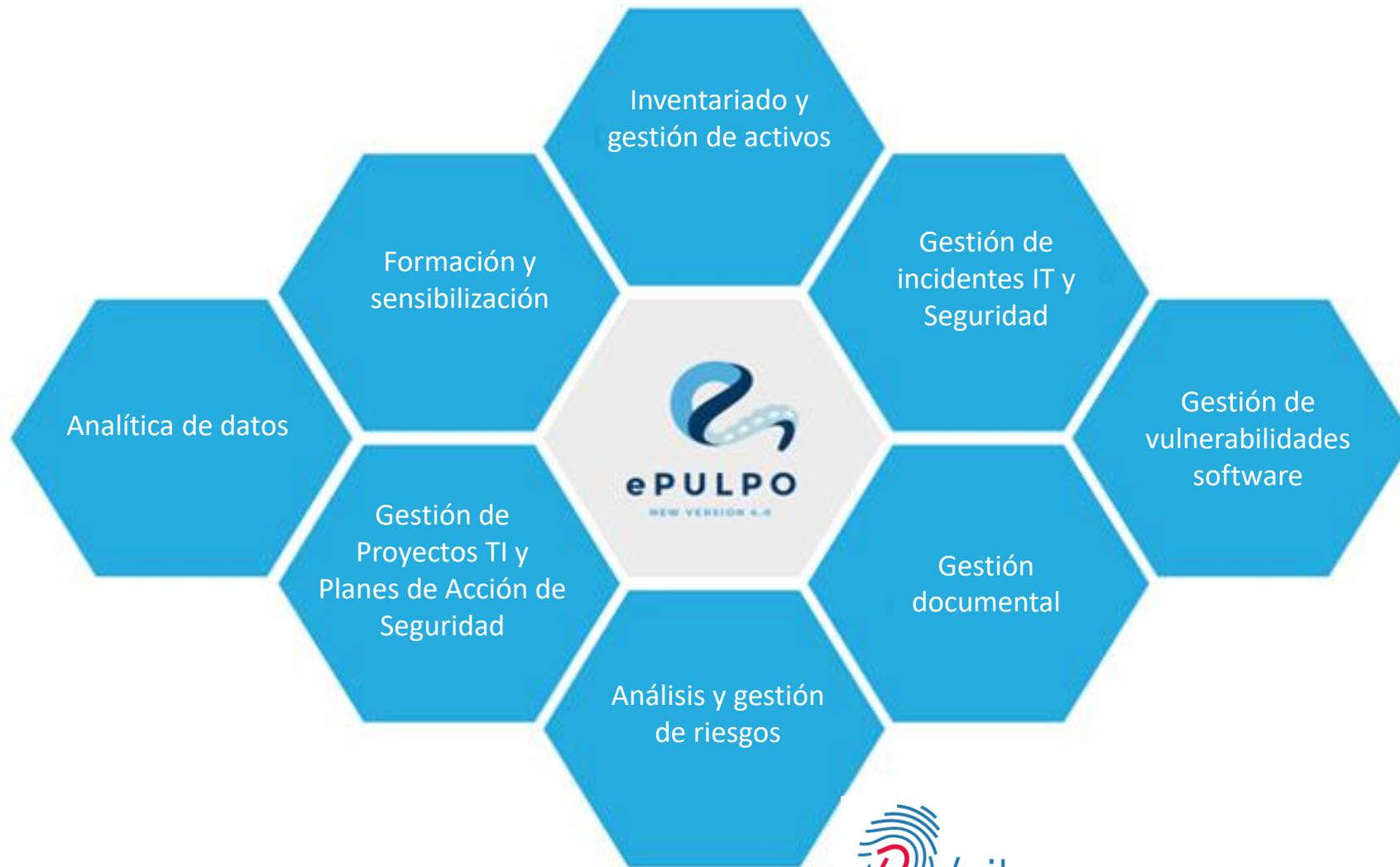
# Aterrizando el plan al ENS



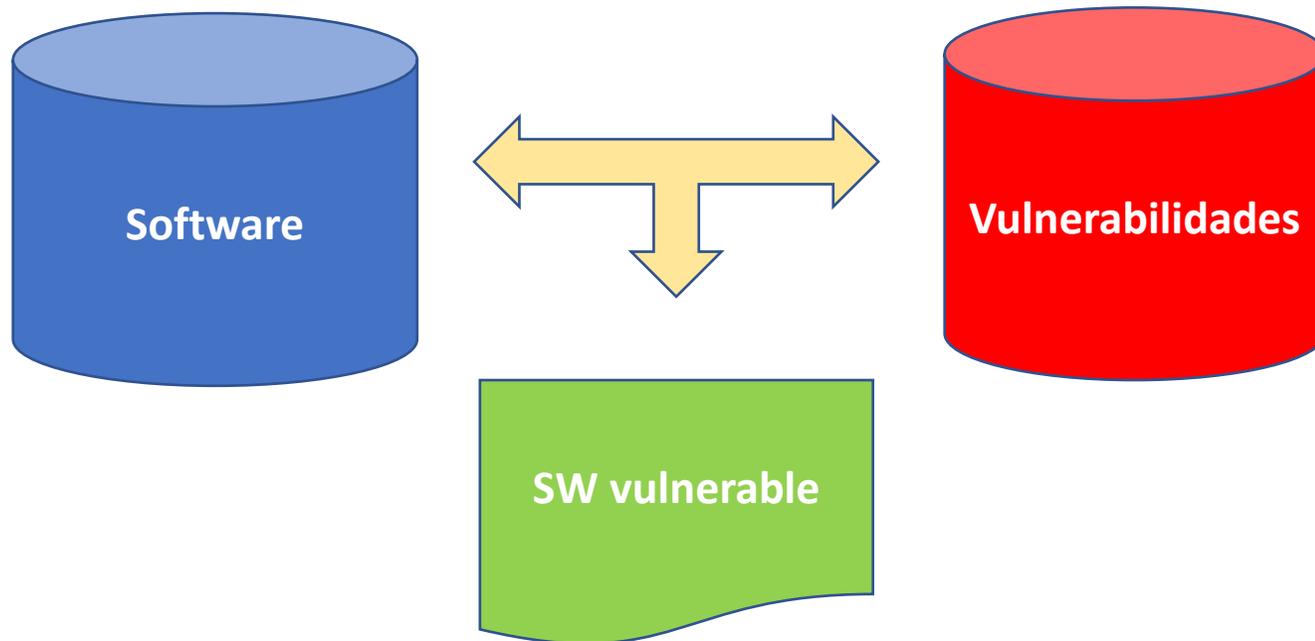
# Cumplimiento normativo y sinergias



# ¿ePULPO?



# Saneando el inventario software



# Identificación automática y tratamiento de una vulnerabilidad software



[Alerta](#) ▾ [Incidentes](#) ▾ [Servicios](#) [Publicaciones](#) ▾ [Sobre INCIBE-CERT](#) ▾



[Inicio](#) / [Alerta Temprana](#) / [Vulnerabilidades](#) / CVE-2020-0655

## Vulnerabilidad en Remote Desktop Services de Microsoft (CVE-2020-0655)

**Tipo:** Validación incorrecta de entrada

**Gravedad:** Alta ■■■■

**Fecha publicación :** 11/02/2020

**Última modificación:** 13/02/2020

### Descripción

Se presenta una vulnerabilidad de ejecución de código remota en Remote Desktop Services (anteriormente se conoce como Terminal Services), cuando un atacante autenticado abusa del redireccionamiento del portapapeles, también se conoce como "Remote Desktop Services Remote Code Execution Vulnerability".

### Impacto

**Vector de acceso:** A través de red

**Complejidad de Acceso:** Media

**Autenticación:** No disponible

**Tipo de impacto:** Compromiso total de la integridad del sistema + Compromiso total de la confidencialidad del sistema + Compromiso total de la disponibilidad del sistema

# Identificación automática y tratamiento de una vulnerabilidad software

Reporte CVE - CVE

Muestra (número de elementos) 
🌐 🔧 🗑️ 🌑

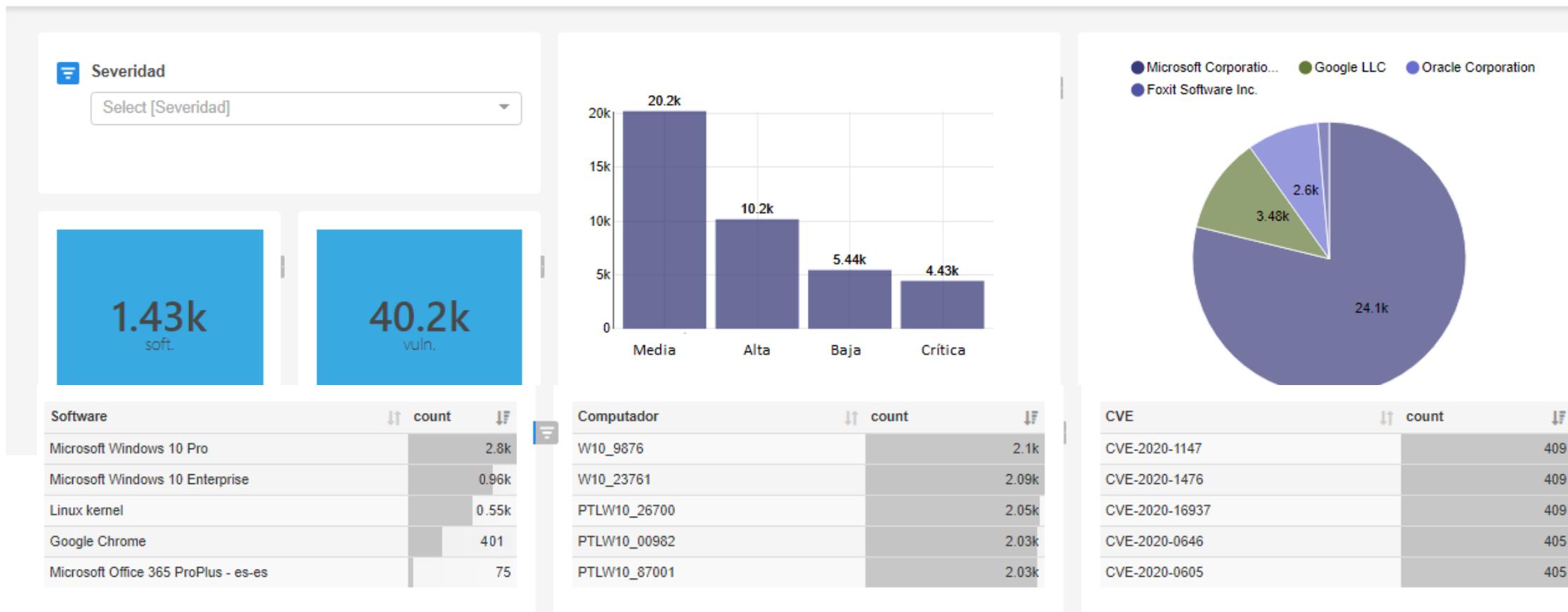
📄
 Desde 1 hasta :

⏴
Acciones

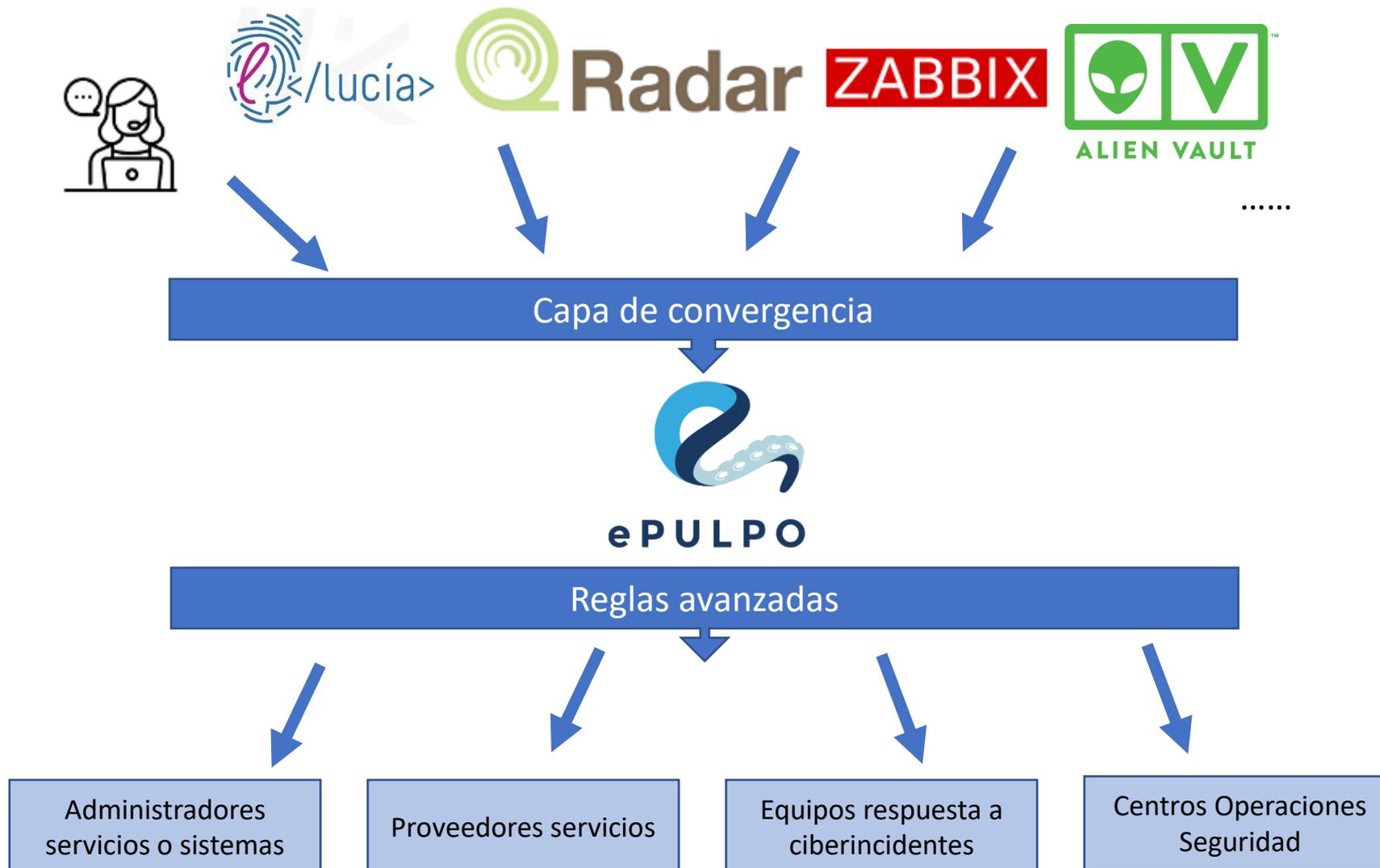
ID	Título	Entidad	Estado	Fecha de apertura	Última actualización	Prioridad	Solicitante - Solicitante	Asignada a - Técnico	Asignada a - Grupo técnico	Categoría
22 359	Vulnerabilidad en Remote Desktop Services de Microsoft (CVE-2020-0655)	Entidad base	<span style="color: green;">○</span> En curso (asignada)	26-11-2020 12:58	26-11-2020 12:58	Alta	admin admin <span>ⓘ</span>		GOM > GOM-SEGURIDAD	Vulnerabilidad*,* *,*
Nombre	Número de serie	Número de inventario	Ubicación	Estado	Grupo	Usuario	Licencias	Fecha de instalación		

# Identificación automática y tratamiento de una vulnerabilidad software

## Vulnerabilidades software



# Centralizando la gestión de ciberincidentes



# Centralizando la gestión de ciberincidentes

Gestión de tickets 🔍 ☆

Edit dashboard

[Tickets] Filtro entidad

Time range

2019-11-30 : 2020-06-30

Entidad

Select [Entidad]

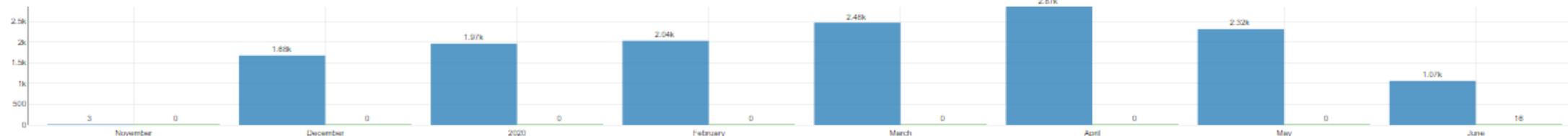
[Tickets] Total

14.4k  
tickets

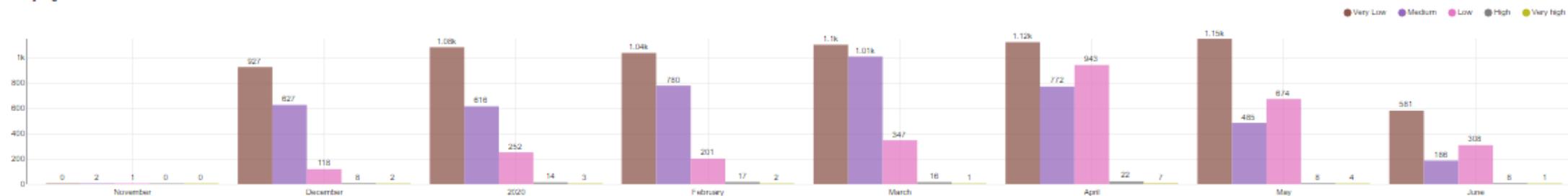
[Tickets] Abiertos

16  
open

[Tickets] Estado



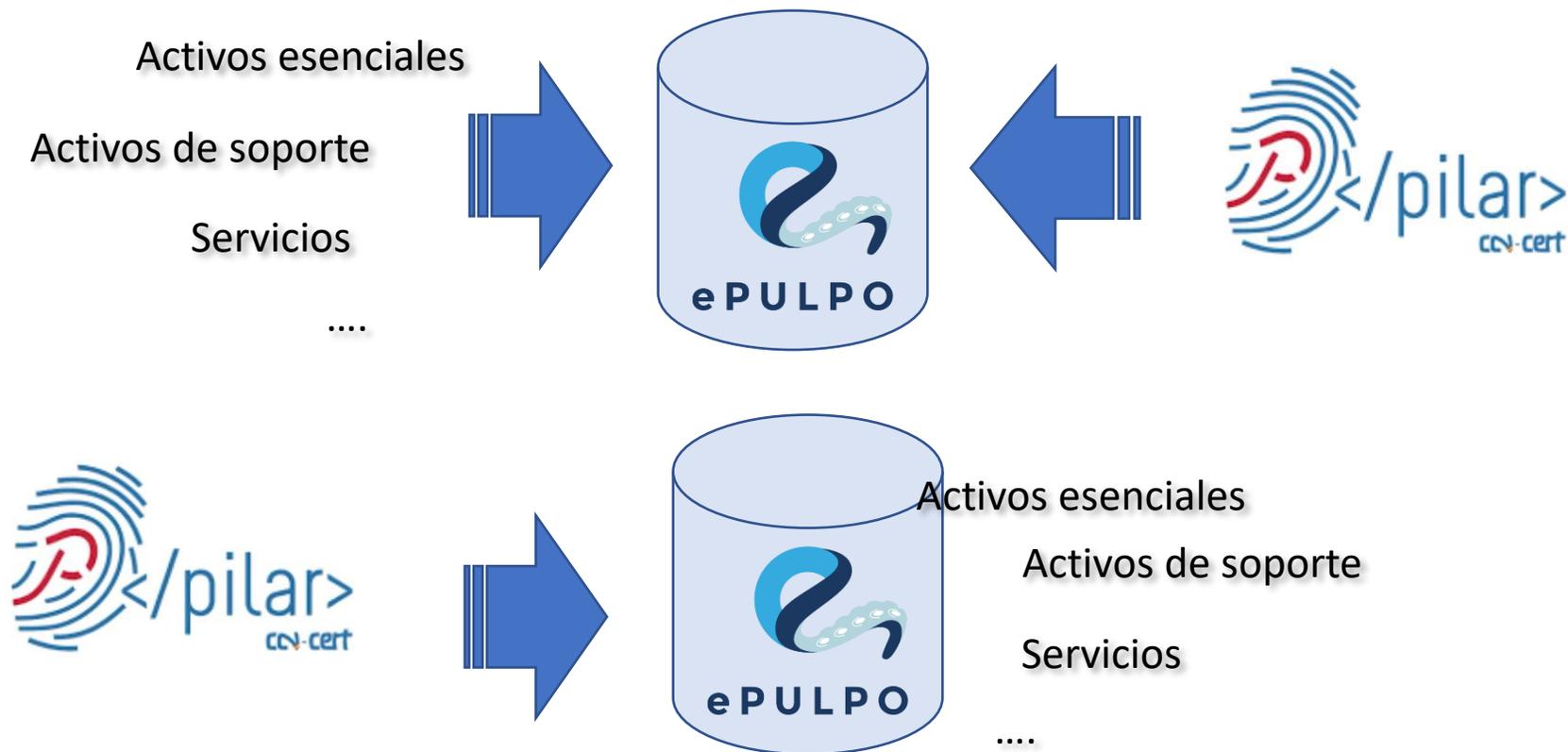
[Tickets] Urgencia



[Tickets] Prioridad

Very Low Medium Low High Very high

# Agilizando la gestión de riesgos



# Beneficios



Facilita la gestión de las tareas de Seguridad y TI

Alineado con cumplimiento normativo (ENS, RGPD, ISO 27001)



Activos más securizados.

Saneamiento del software inventariado



Centraliza la gestión de ciberincidentes.

Capa de convergencia.

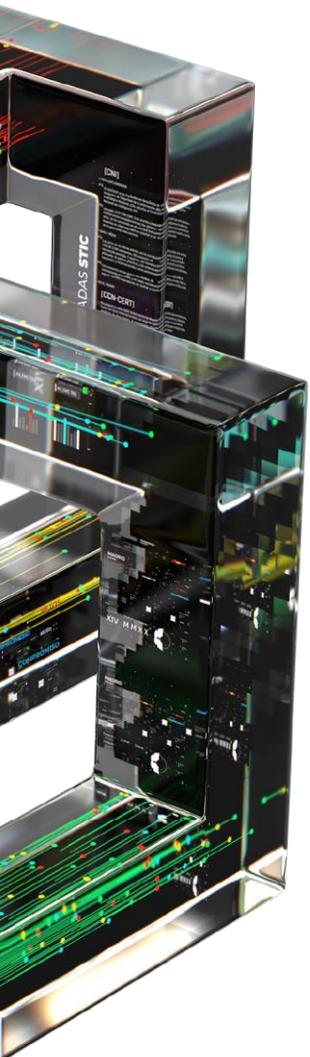
Integrable con herramientas del CCN y de terceros



Centraliza el análisis y gestión de riesgos.

Integración con PILAR

Fuente de datos única



**MUCHAS GRACIAS**

**#XIVJORNADASCCNCERT**