ESCUELA SUPERIOR DE GUERRA
"General Rafael Reyes Prieto"
Colombia

Modelamiento de Amenazas Cibernéticas con STRIDE y Zabbix

CC Diego Edison Cabuya Padilla
MY Víctor López Salguero
MY Sergio Cruz Baudín
CC Yerson Torres Bueno

Versión: 2025

UNIÓN, PROYECCIÓN, LIDERAZGO

AGENDA

01 Introducción

02 Descripción del escenario

03 Arquitectura de red

04 Análisis de riesgos y amenazas

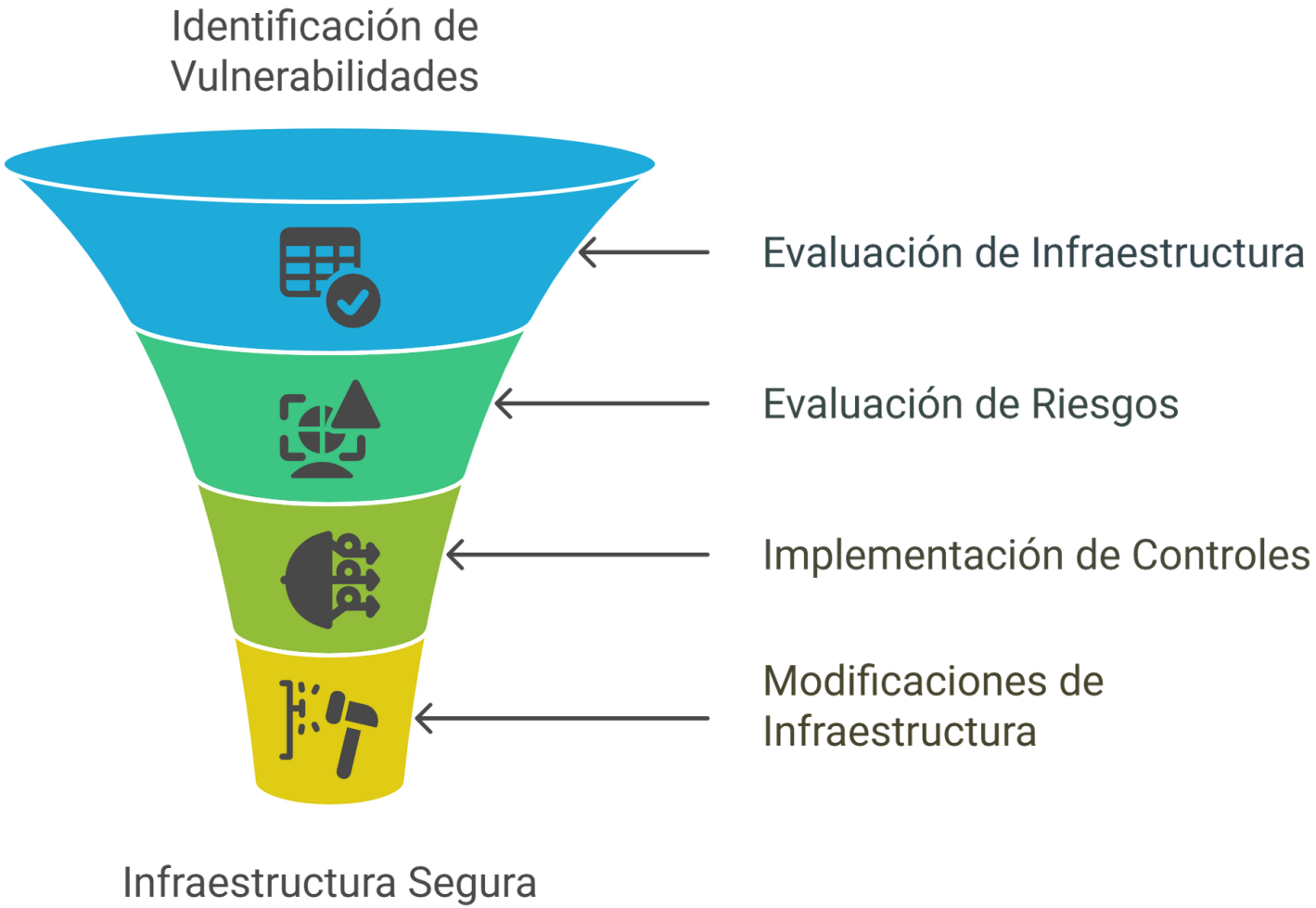
05 Diseño de controles de seguridad

06 Matriz RACI

07 Conclusiones y recomendaciones

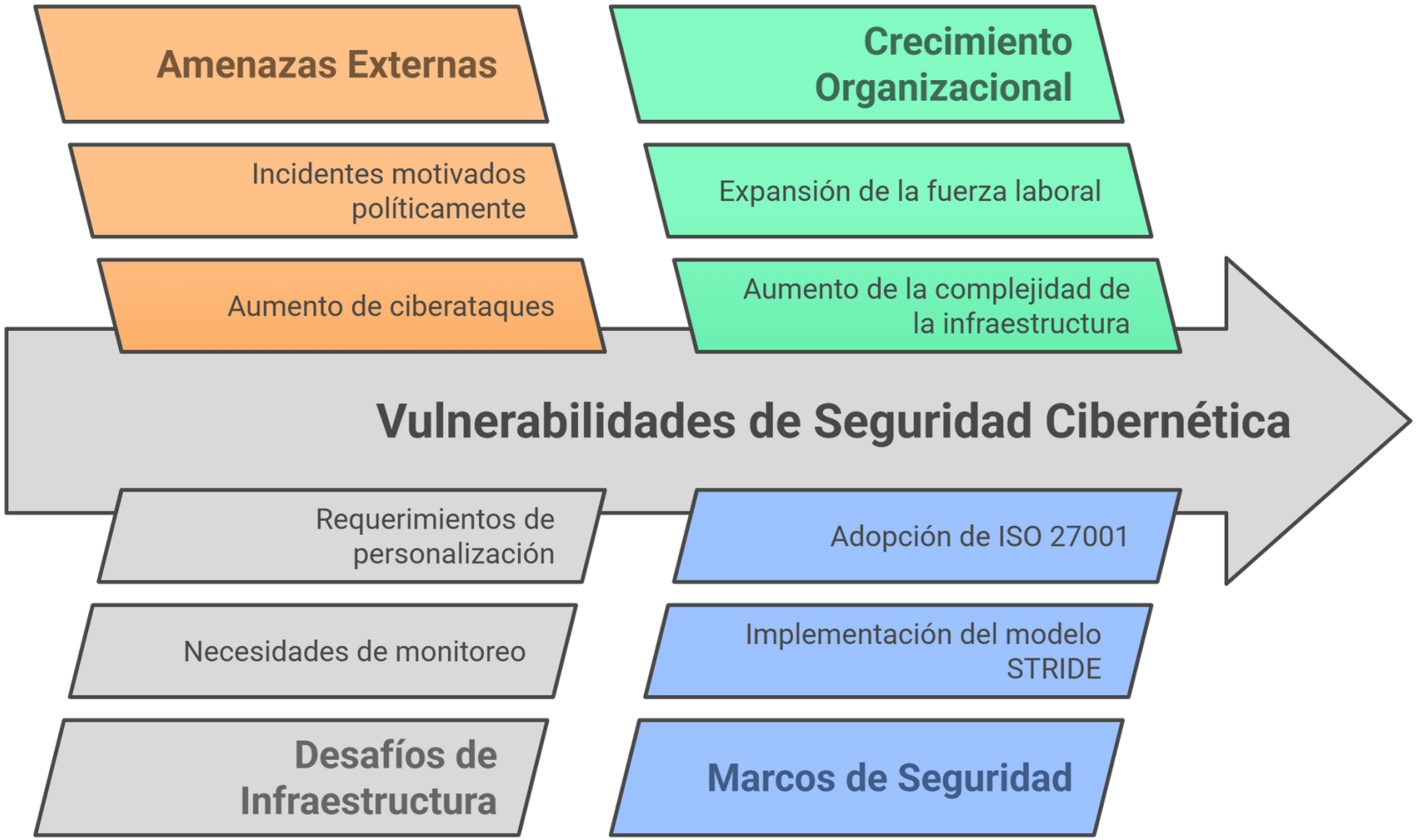
Introducción

Compumundohipermegared



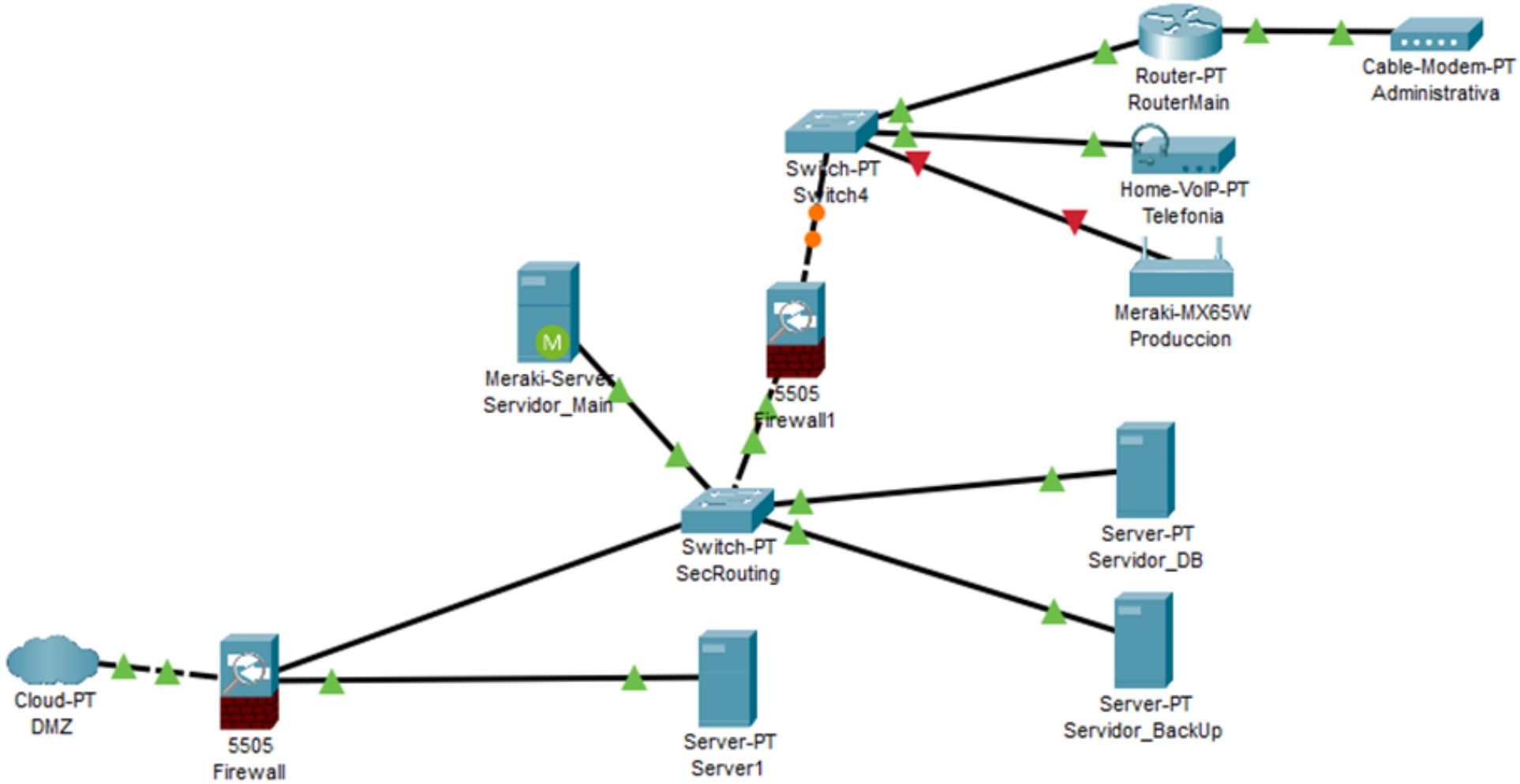
Escenario

Compumundohipermegared



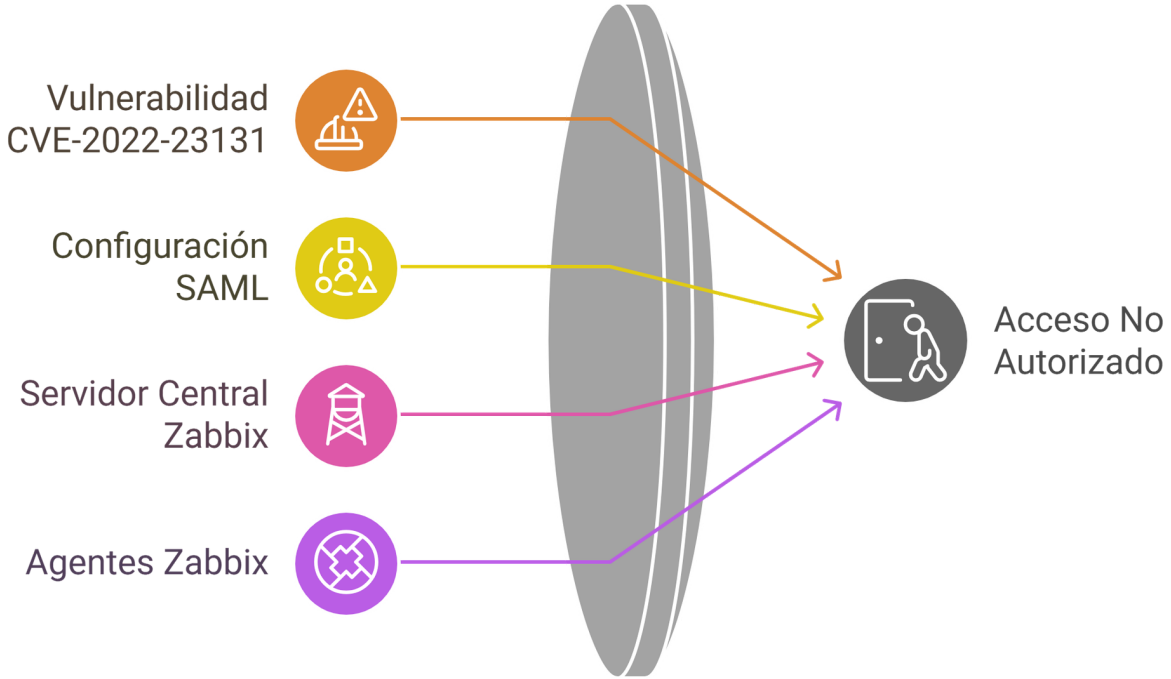
Arquitectura de red de la empresa

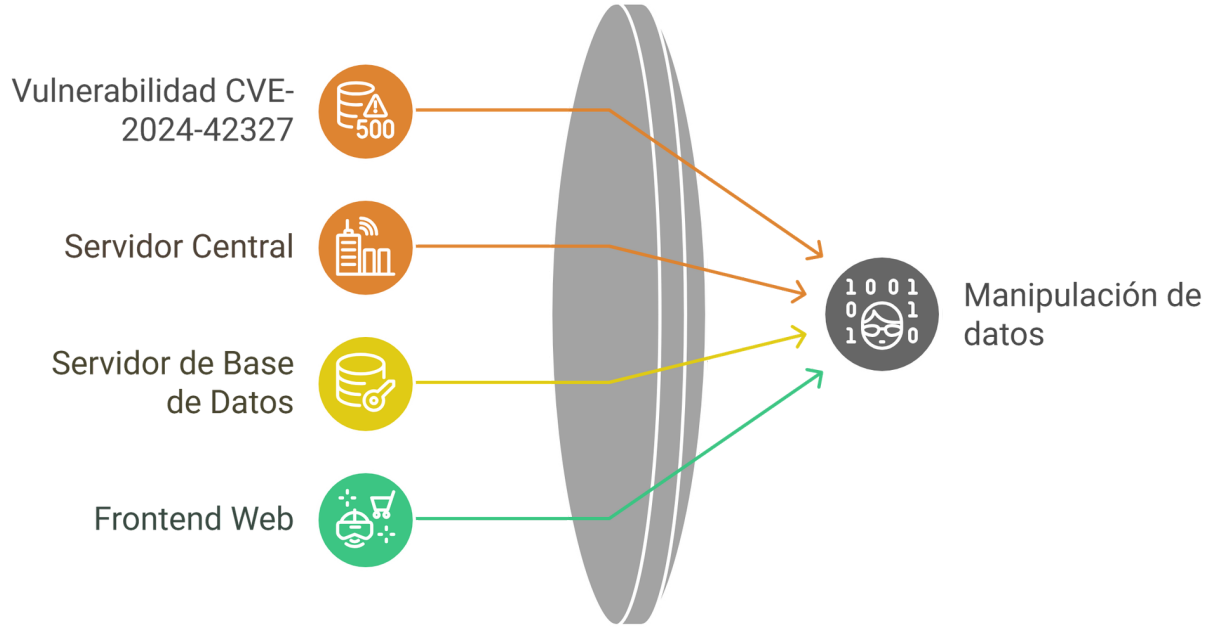
Compumundohipermegared



Análisis de riesgos y amenazas

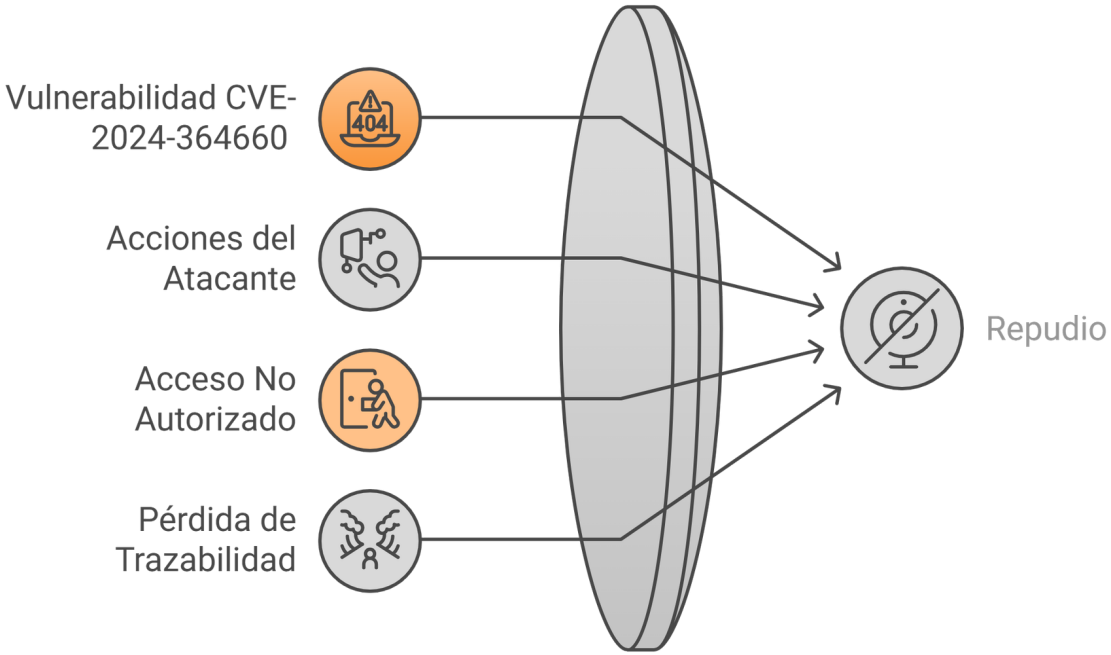
Modelo STRIDE

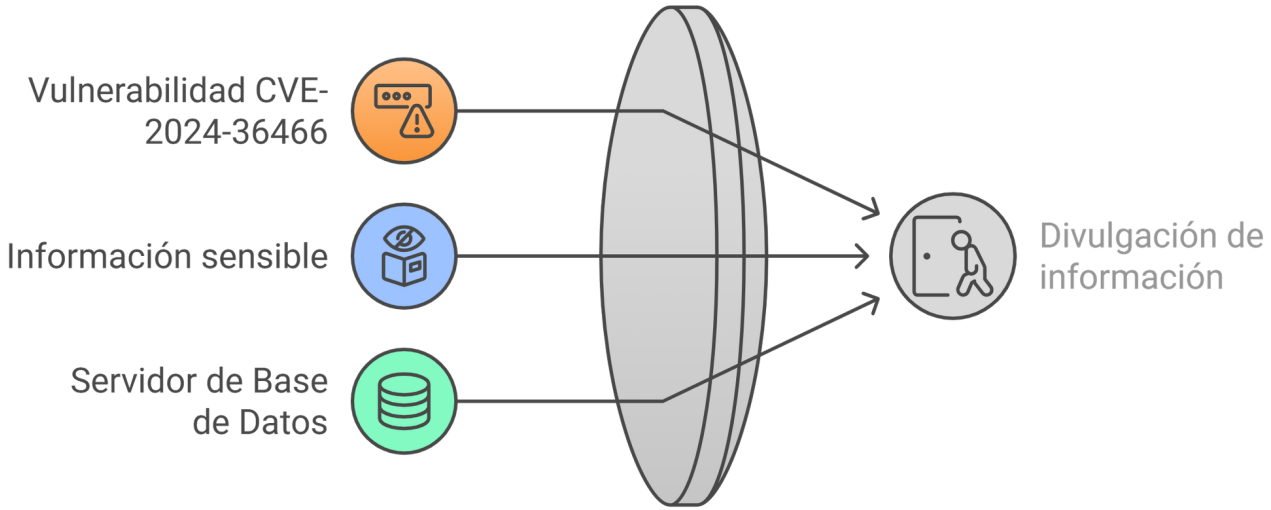




Análisis de riesgos y amenazas

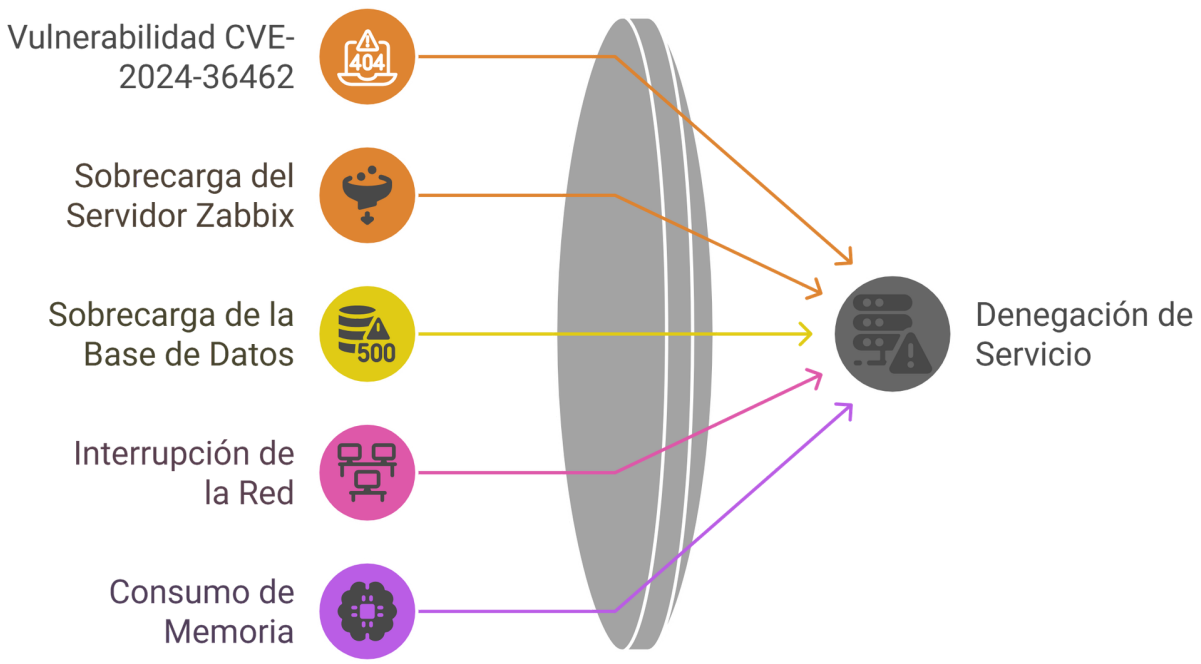
Modelo STRIDE

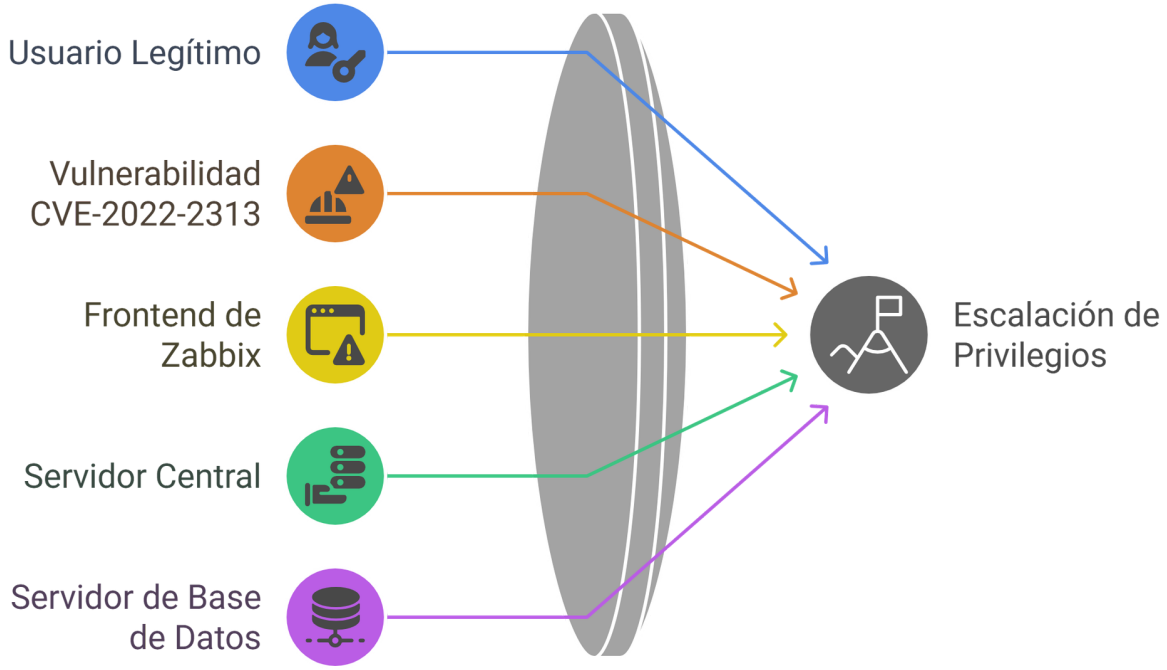




Análisis de riesgos y amenazas

Modelo STRIDE





Diseño de controles de seguridad

Controles organizacionales

Protección de Registros

Asegurar que los registros estén cifrados y almacenados de forma segura

Roles de Seguridad

Definición clara de roles de seguridad para reducir riesgos

Planificación de Incidentes

Preparación para gestionar y mitigar incidentes de seguridad

Participación en la Industria

Participación en foros de seguridad para mantenerse actualizado

Integración de Proyectos

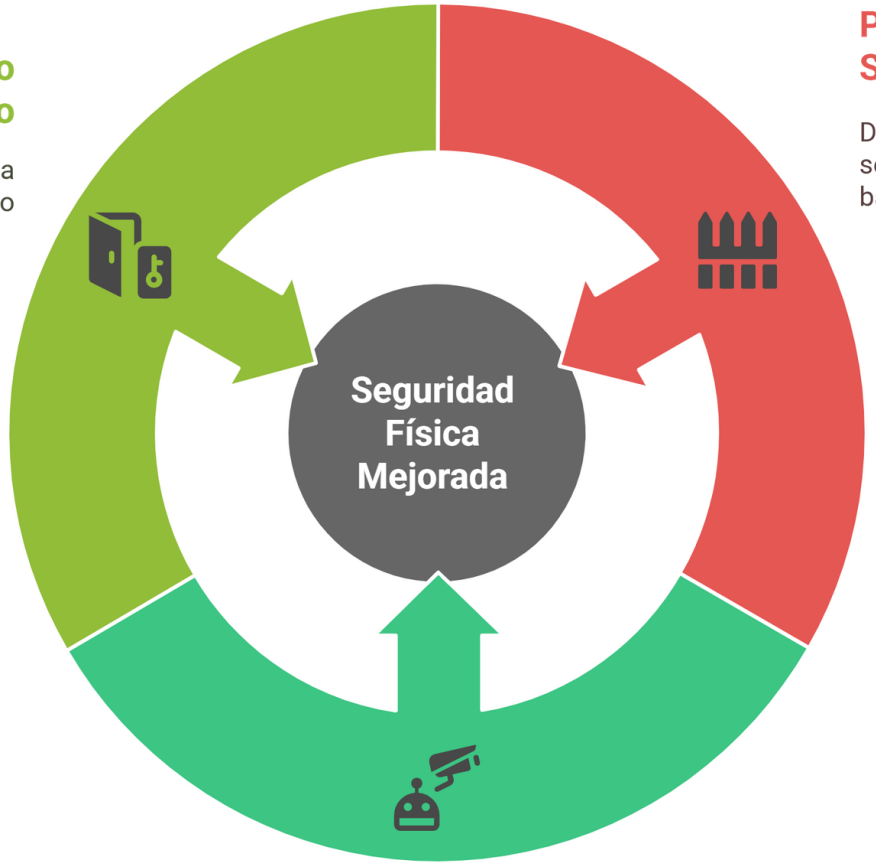
Integración de medidas de seguridad en la gestión de proyectos

Diseño de controles de seguridad

Controles fisicos

Acceso Restringido

Acceso controlado a personal autorizado



Perímetros de Seguridad

Definición de áreas seguras con barreras físicas

Monitoreo de Seguridad

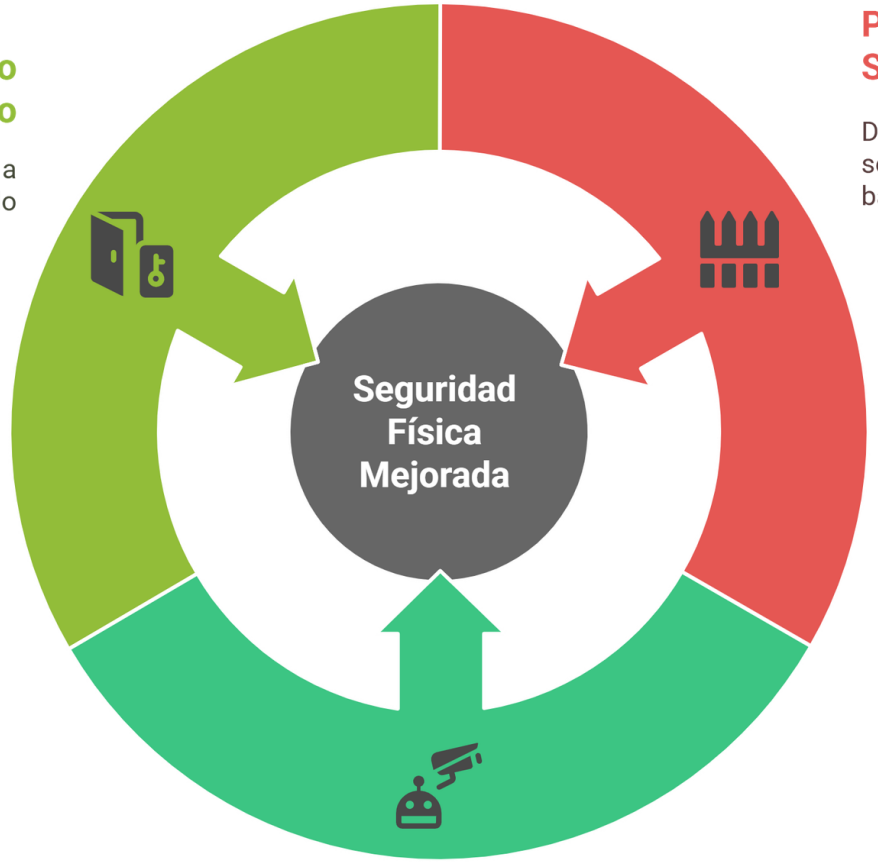
Monitoreo continuo con cámaras y alarmas

Diseño de controles de seguridad

Controles fisicos

Acceso Restringido

Acceso controlado a personal autorizado



Perímetros de Seguridad

Definición de áreas seguras con barreras físicas

Monitoreo de Seguridad

Monitoreo continuo con cámaras y alarmas

Diseño de controles de seguridad

Controles tecnológicos

Autenticación Segura

Procedimientos para acceso seguro

Protección de Puntos Finales

Medidas para dispositivos de usuario

Derechos de Acceso

Gestión de acceso privilegiado

Matriz RACI

Modelo STRIDE

Amenaza	Componentes Afectados	Administrador de Zabbix (AZ)	Equipo de Seguridad TI (ES)	Administrador de Base de Datos (ABD)	Equipo de Red (ER)	Gerente de TI (GTI)	Auditor de Seguridad (AS)
Suplantación (Spoofing)	Servidor central, agentes Zabbix	R	A	C	I	I	C
Manipulación (Tampering)	Servidor central, DB, frontend web	R	A	R	I	I	C
Repudio (Repudiation)	Servidor central, servidor de DB	R	A	R	I	I	C

Matriz RACI

Modelo STRIDE

Amenaza	Componentes Afectados	Administrador de Zabbix (AZ)	Equipo de Seguridad TI (ES)	Administrador de Base de Datos (ABD)	Equipo de Red (ER)	Gerente de TI (GTI)	Auditor de Seguridad (AS)
Divulgación (Information Disclosure)	Servidor central, servidor de DB	R	A	R	I	I	C
Denegación (DoS)	Servidor central, DB, dispositivos de red	R	A	R	R	I	C
Elevación (Elevation)	Servidor central, servidor de DB	R	A	R	I	I	C

Conclusiones

Referencias

Aguilar Antonio, J. M. (2020). La brecha de ciberseguridad en América Latina rente al contexto global de ciberamenazas. Revista de estudios de seguridad internacional, 6(2), 17-43.

Arghire, I. (2024, diciembre 2). Critical Vulnerability Found in Zabbix Network Monitoring Tool. SecurityWeek. https://www.securityweek.com/critical-vulnerability-found-in-zabbix-network-monitoring-tool/

Haworth, J. (2022, febrero 18). Critical vulnerabilities in Zabbix Web Frontend allow authentication bypass, code execution on servers. The Daily Swig | Cybersecurity News and Views. https://portswigger.net/daily-swig/critical-vulnerabilities-in-zabbix-web-frontend-allow-authentication-bypass-code-execution-on-servers

Lambert, Dmitr., Baekel, B. van., & Lambert, D. Natha. (2022). Zabbix 6 IT Infrastructure Monitoring Cookbook.

SOC team OGMA. (2024, octubre 8). Mitigating CVE-2024-36460: Plaintext Password Exposure in Zabbix Front-End Audit Log. Mitigating CVE-2024-36460: Plaintext Password Exposure in Zabbix Front-End Audit Log. http://ogma.in/mitigating-cve-2024-36460-plaintext-password-exposure-in-zabbix-front-end-audit-log

Preguntas

@EsdegCol

Escuela Superior de Guerra

Escuela Superior de Guerra

Escuela Superior de Guerra

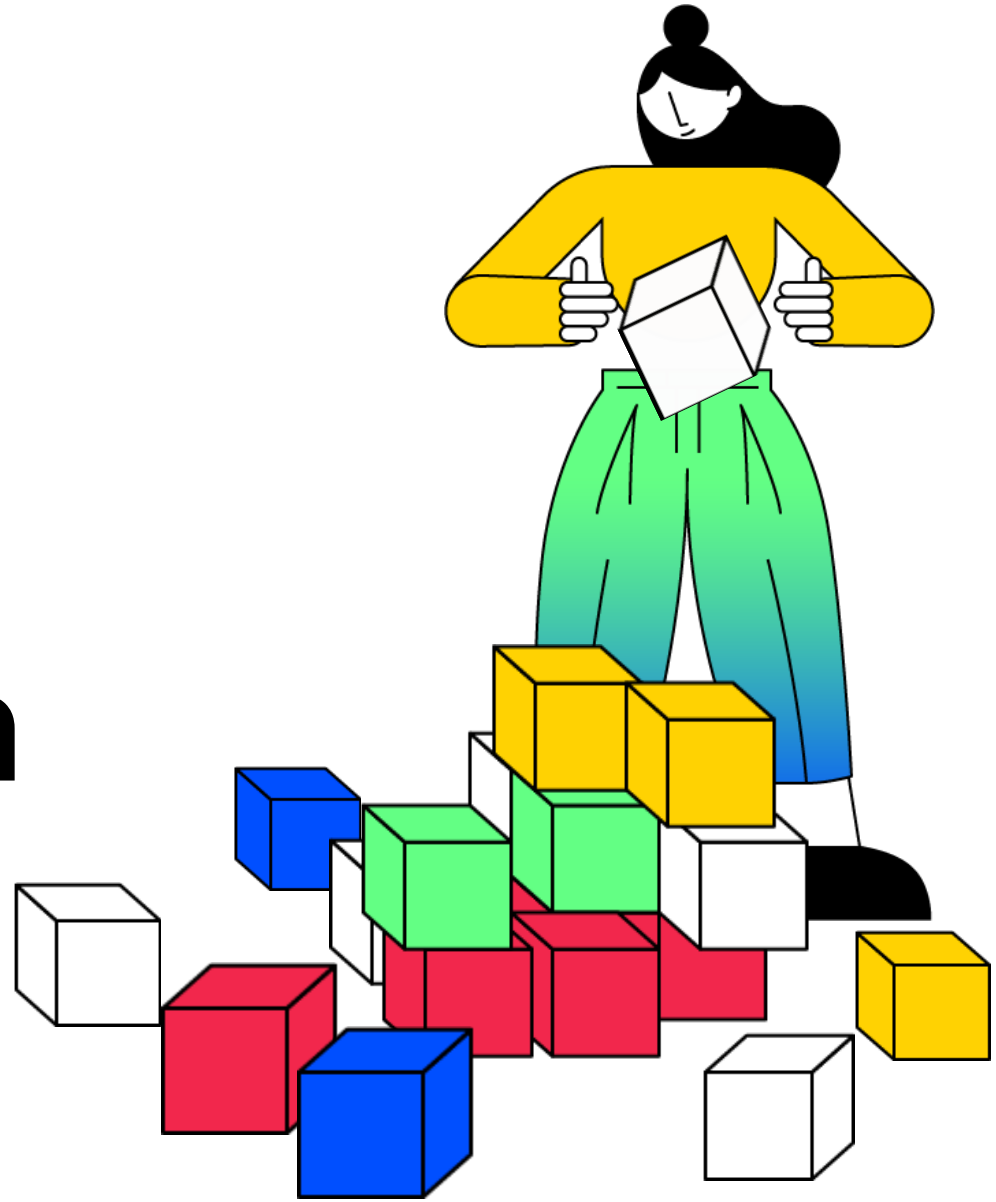
www.esdegue.edu.co

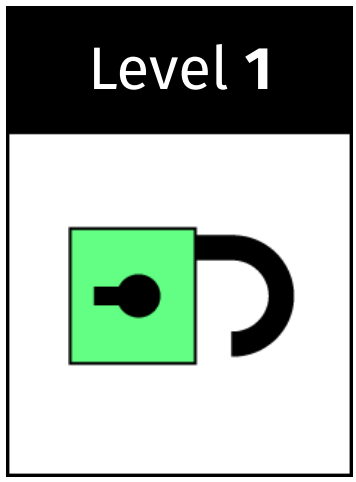
La ***Escuela Superior de Guerra "General Rafael Reyes Prieto"*** está certificada bajo las normas internacionales **ISO 9001:2015** e **ISO 21001:2018.**

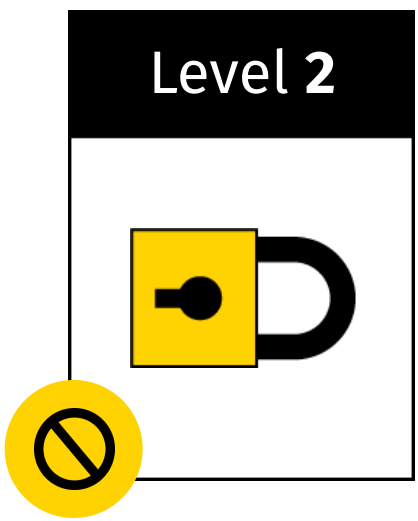
STRIDE - SABBIX

Escape room

start



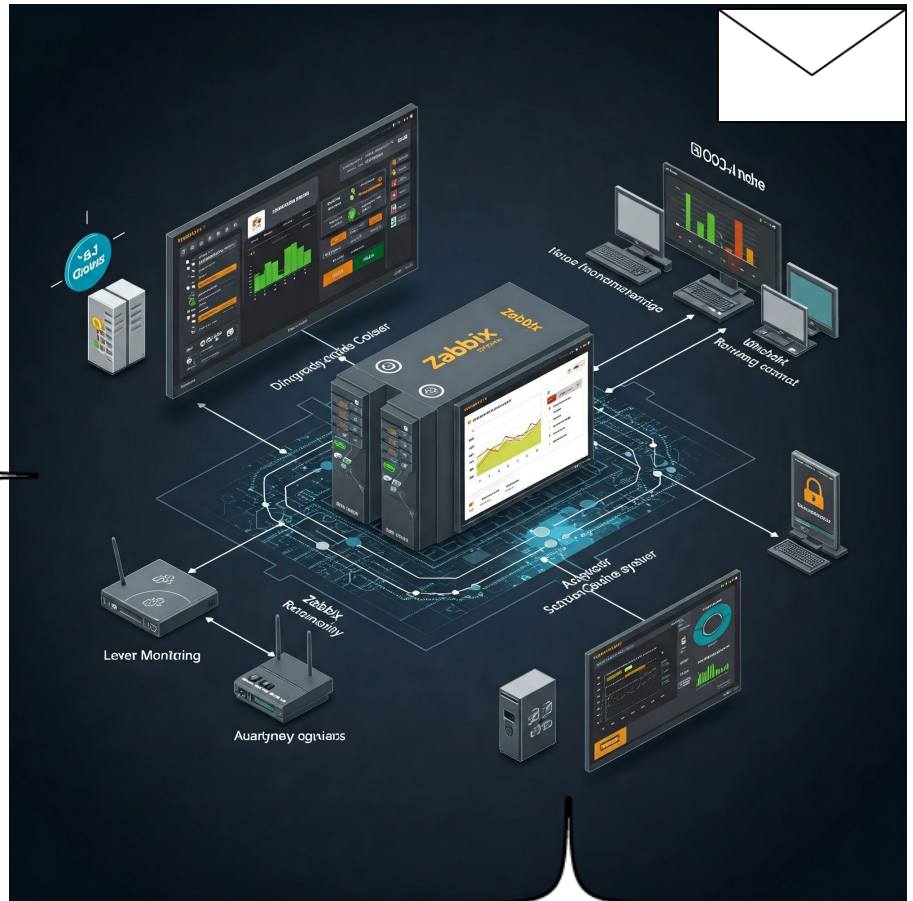

Level 1


Level 2

¿Cuál es la principal razón para realizar un estudio completo de la infraestructura tecnológica de Compumundohipermegared?

- Implementar nuevas tecnologías.
- Identificar vulnerabilidades y proteger la información de clientes y proveedores
- Reducir costos operativos.
- Cumplir con regulaciones gubernamentales.

Send



Zabbix solo permite el monitoreo básico de la infraestructura TI, sin opciones de personalización.

True

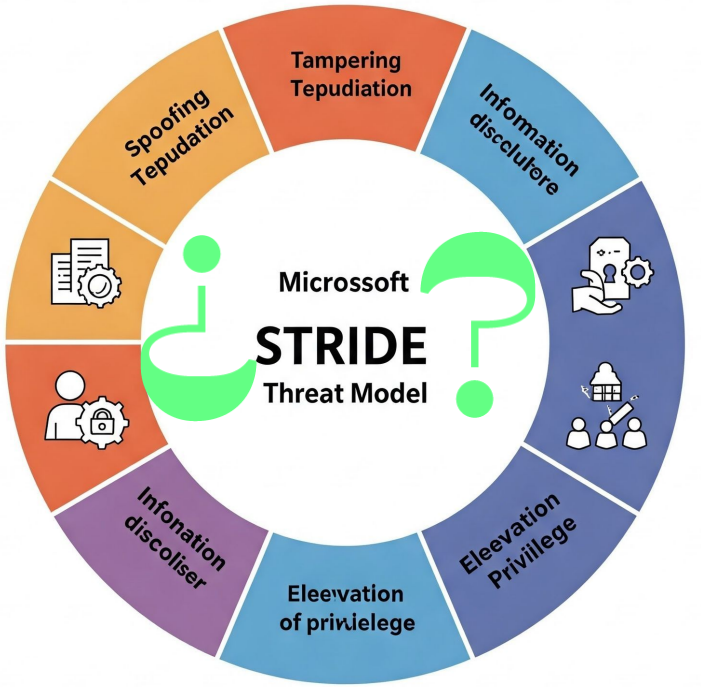
False

Send

¿Qué modelo de amenazas se utiliza como guía para identificar vulnerabilidades?

- COBIT
- ITIL
- STRIDE
- NIST

Send



Menu

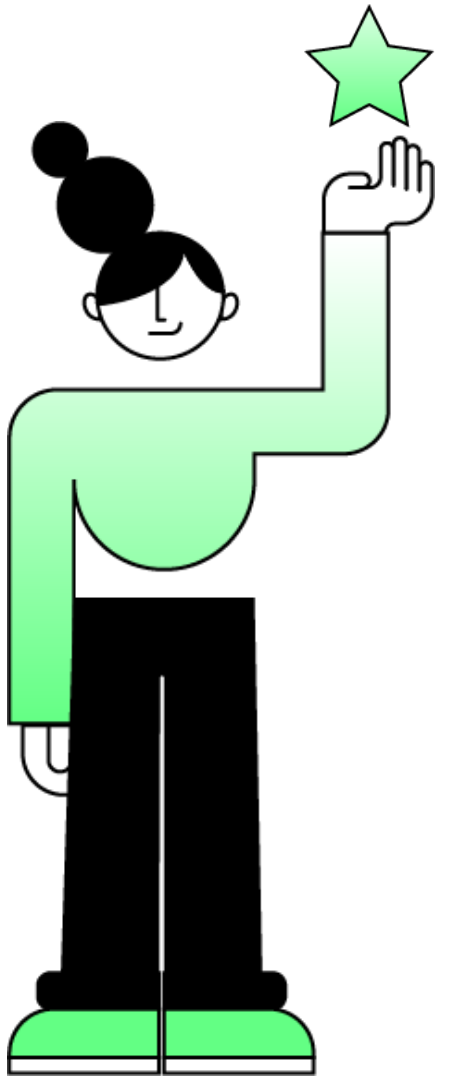
Level 1

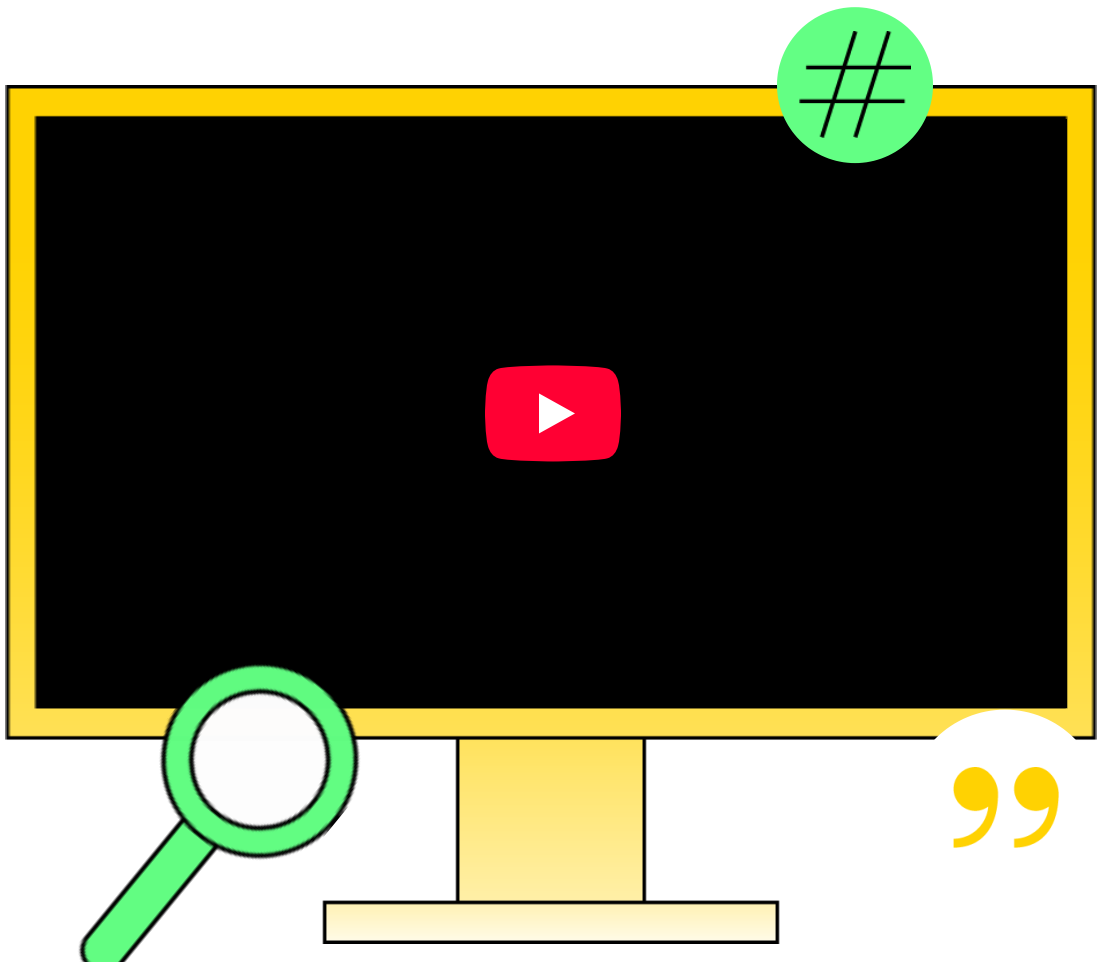
Level 2

Great!

You have passed **level 1** and earned the **green star**.

Keep going to the next level!





La suplantación de identidad (Spoofing) no representa una amenaza para el sistema Zabbix

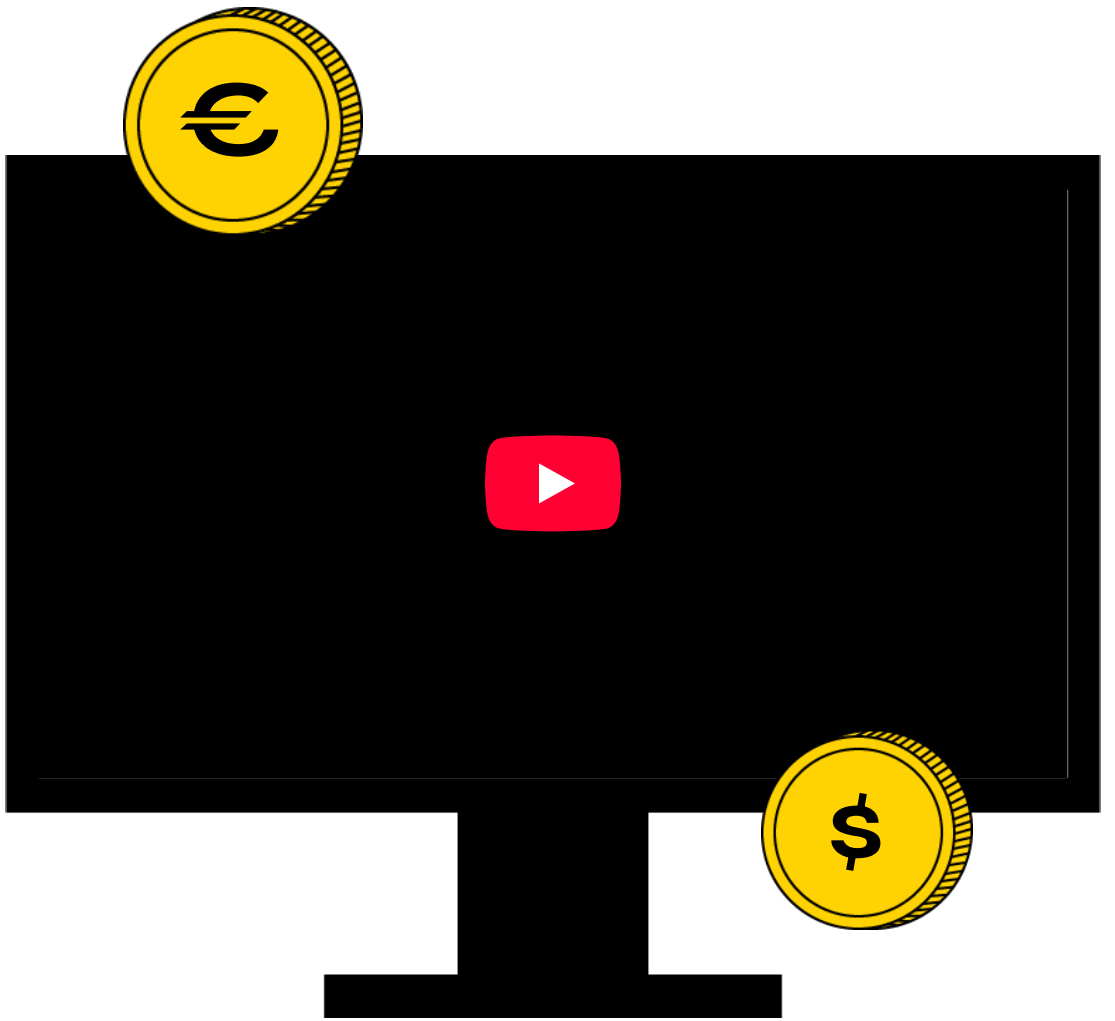
- True
- False

Send

¿Cuál es el orden de las amenazas que forman el modelo STRIDE?

- Spoofing
- Information Disclosure
- Elevation of Privilege
- Denial of Service
- Tampering
- Repudiation

Send



¿Cuál de las siguientes opciones describe mejor el propósito de los controles físicos de seguridad?

- Gestionar los derechos de acceso a los sistemas
- Monitorear la actividad del usuario en la red
- Proteger las áreas que contienen información y activos asociados
- Cifrar los registros del sistema

Send

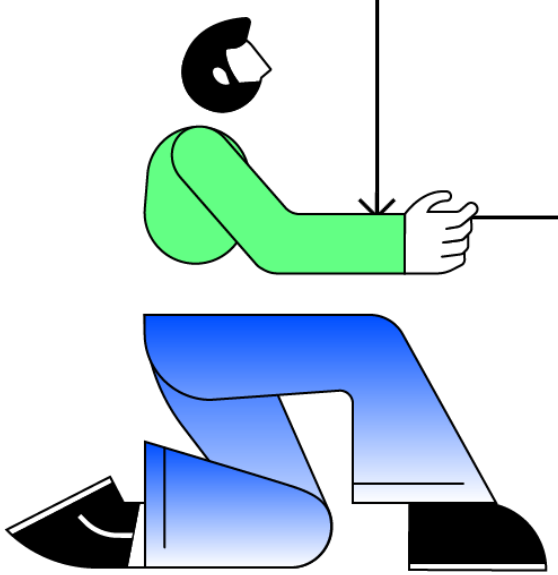
Certificate of

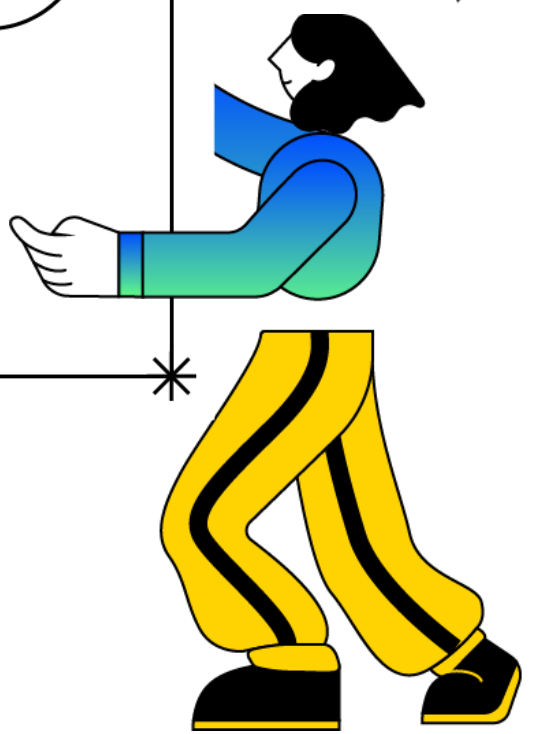
STRIDE expert

Gracias por participar

Es importante tomar estos conocimientos para implementar en cada una de nuestras Fuerzas

ESDEG - MAECI	
Marzo 2025	





Gracias

@EsdegCol

Escuela Superior de Guerra

Escuela Superior de Guerra

Escuela Superior de Guerra

www.esdegue.edu.co