

INFORME DE SEGURIDAD CON ZABBIX A EMPRESA DE SERVICIOS DE ENTREGA DE PRODUCTOS QUE EMPLEA EL SISTEMA “SAP” EN LA CADENA DE ABASTECIMIENTOS



**MY. FONSECA RODRÍGUEZ
IVÁN DARÍO**



**MY. NOYA DUARTE
JOHN KEVIN**



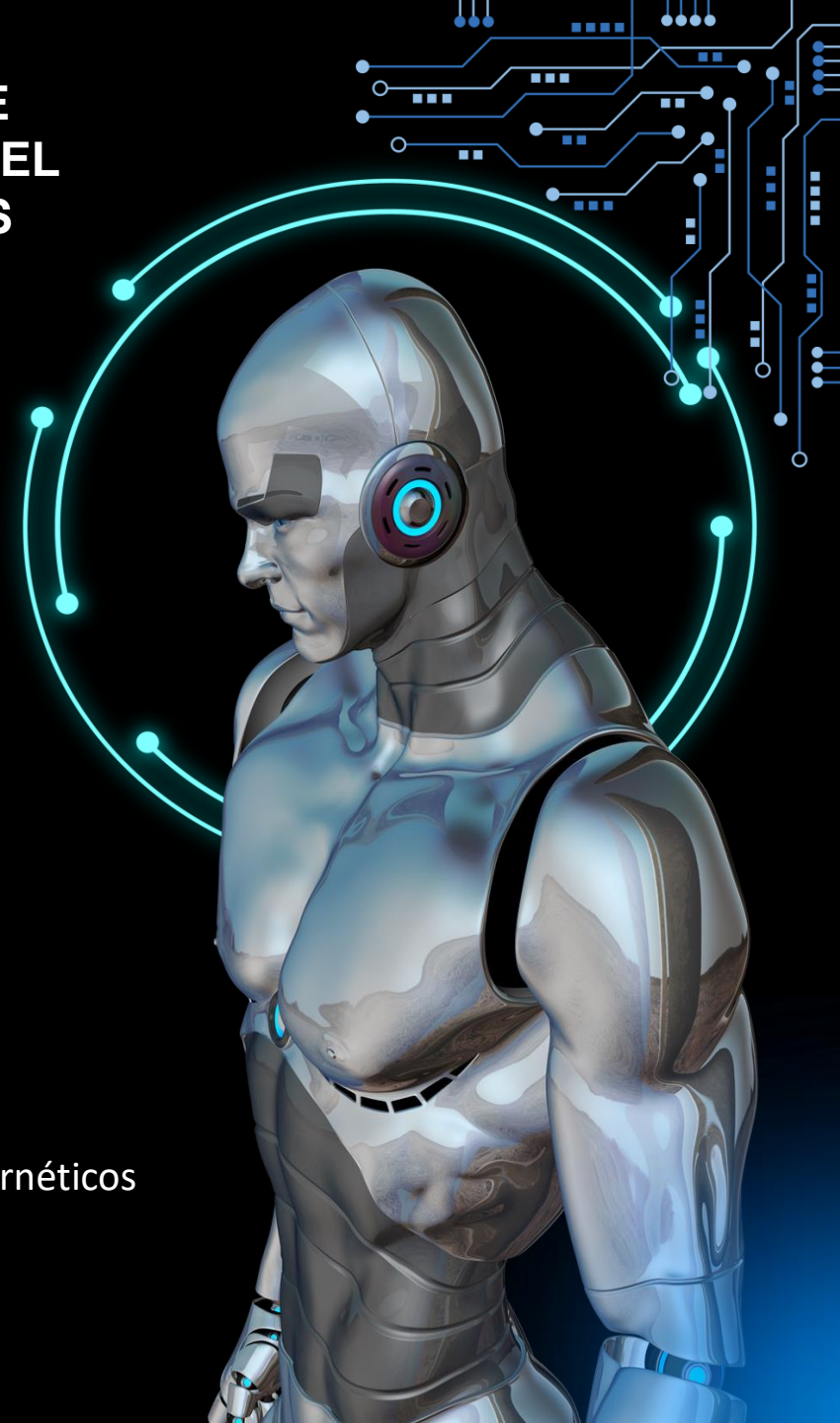
**MY. PEÑA PARRALES
DORLANDY ALBERTO**



**MY. DURÁN VILLANUEVA
RICHARD EDUARDO**



MATERIA: Gestión de Riesgos Cibernéticos
DOCENETE: Jaider Ospina Navas
CURSO: CEM-2025
AULA: “Q”



AGENDA



- 01 Introducción
- 02 Definición del sistema
- 03 Descripción del escenario
- 04 Análisis del riesgo
- 05 Diseño de controles de seguridad
- 06 Conclusiones y recomendaciones
- 07 Referencias



INTRODUCCIÓN



Análisis de Riesgos Cibernéticos en la Integración SAP-Zabbix

Las empresas deben ser conscientes de los riesgos cibernéticos y tomar medidas preventivas. Esta presentación analiza los riesgos en la integración entre SAP y Zabbix, utilizando un enfoque integral que combina los modelos STRIDE, PASTA y DREAD. Se definirán controles de seguridad alineados con la norma ISO/IEC 27001: 2022 para mitigar las amenazas y proteger la información.

DEFINICIÓN DEL SISTEMA

Contamos con un excelente sistema de monitoreo, para que sea utilizado por las **empresas de servicios de entrega de productos**, utilizamos el modelo de **Zabbix**; una plataforma de código abierto que permite la supervisión de la infraestructura de TI. Dado que **SAP** es el sistema central para la logística de la empresa, necesitamos mitigar las vulnerabilidades.

ZABBIX

- Servidor central, agentes en servidores críticos, base de datos y frontend web.

INFRAESTRUCTURA

- Servidores para almacenamiento y procesamiento de datos, redes de interconexión con proveedores y clientes, dispositivos de monitoreo.

USUARIOS

- Administradores de TI y empleados con permisos limitados según su función.

DESCRIPCIÓN DEL ESCENARIO

Infraestructura Tecnológica de Empresa de servicios de entrega de producto.



La integración de SAP con Zabbix permite una supervisión proactiva, pero también introduce vulnerabilidades críticas que deben ser gestionadas.

ANÁLISIS DE RIESGO

Análisis de amenaza con modelo STRIDE, donde se identifico.

S

Spoofing

-Amenaza: Uso de credenciales robadas para acceder a SAP mediante vulnerabilidades.

-Ejemplo : Escalada de privilegios en SAMR/LSAD mediante degradación de protocolo

-Mitigación: Implementación de autenticación multifactor.

T

Tampering

-Amenaza: Modificación de registros en SAP a través de vulnerabilidades en Zabbix.

-Ejemplo: Inyección SQL almacenada en MySQL

-Mitigación: Uso de consultas SQL parametrizadas y monitoreo de logs en tiempo real.

R

Repudiation

-Amenaza: Eliminación de registros de auditoría en SAP, comprometida en Zabbix.

-Ejemplo: Corrupción de memoria en el motor de secuencias de comandos (CVE-2019-0884)

-Mitigación: Implementación de registros inmutables con Blockchain.

I

Disclosure

Amenaza: Robo de credenciales mediante ataques Man-in-the-Middle.

Ejemplo: Vulnerabilidad POODLE en SSLv3 (CVE-2014-3566)

Mitigación: Uso exclusivo de TLS 1.3 para cifrado de comunicaciones.

D

Service

Amenaza: Ataques DDoS dirigidos a los servidores de Zabbix para desactivar el monitoreo.

Ejemplo: Denegación de servicio en Apple iWork

Mitigación: Implementación de sistemas de prevención de intrusiones (IDS/IPS) y balanceo de carga.

E

Privilege

Amenaza: Un usuario con permisos básicos compromete SAP.

Ejemplo: Vulnerabilidad en Cisco IOS que permite ejecución de comandos con privilegios elevados.

Mitigación: Implementar segmentación de red y revisión continua de permisos.

ANÁLISIS DE RIESGO

El modelo PASTA (Process for Attack Simulation and Threat Analysis) permite dividir el análisis en diferentes fases del ciclo de vida de la información.



Identificar la arquitectura de SAP y su monitoreo en Zabbix.
Documentar riesgos asociados.



Evaluar autenticación y control de acceso en SAP y Zabbix (MFA, RBAC).



Revisar seguridad en bases de datos de SAP y registros en Zabbix.



Analizar cifrado de comunicaciones y riesgos de interceptación.



Evaluar vulnerabilidades en integraciones de SAP y Zabbix.

Impacto en la Empresa: Un atacante podría interceptar tráfico entre Zabbix y SAP si la comunicación no está protegida.

Mitigación: Implementar TLS 1.3 y eliminar compatibilidad con versiones antiguas de SSL.

ANÁLISIS DE RIESGO

El modelo **DREAD** nos ayuda a cuantificar el riesgo de cada vulnerabilidad identificada con **STRIDE** y **PASTA** mediante cinco factores.



AMENAZA	D (DAÑO)	R (REPRODUCIBILIDAD)	E (EXPLOTABILIDAD)	A (USUARIOS AFECTADOS)	D (DETECTABILIDAD)	PUNTAJE TOTAL
Escalada de privilegios en SAP	9	8	7	9	5	38 (Crítica)
Inyección SQL	7	9	8	7	6	37 (Alta)
Denegación de servicio DDoS	6	7	9	8	5	35 (Alta)
Robo de credenciales (MITM - POODLE)	8	6	7	8	7	36 (Alta)

Puntaje DREAD: 38 (Crítica)

Impacto: Acceso completo a la base de datos de la Empresa.

Acción: Implementar MFA y RBAC, restringir acceso a cuentas privilegiadas.

ANÁLISIS DE RIESGO

IDENTIFICACIÓN DE AMENAZAS	
Componente	Posibles amenazas
Zabbix	Inyección SQL, escalamiento de privilegios, acceso indebido a logs.
SAP	Ataques de phishing, vulnerabilidades en API, ransomware.
Infraestructura	Ataques DDoS dirigidos, acceso físico no autorizado.

PRIORIZACIÓN DE AMENAZAS SEGÚN SU IMPACTO			
Amenaza	Probabilidad	Impacto	Prioridad
Escalada de privilegios en SAP	Alta	Alta	Crítica
Inyección SQL en Zabbix	Media	Alta	Alta
Denegación de servicio	Alta	Media	Alta
Robo de credenciales por ataque MITM	Media	Alta	Alta

INTEGRACIÓN CON MATRIZ DAFO		
Debilidad/Amenaza	Medida de mitigación (PASTA)	Priorización (DREAD)
Inseguridad en redes (D2)	Implementar TLS 1.3 y VPNs	Alta
Ingeniería social (A3)	Capacitación en seguridad, simulacros de phishing	Alta
Vulnerabilidades en terceros (A2)	Auditorías de seguridad a proveedores de SAP	Media

DISEÑO DE CONTROLES DE SEGURIDAD

Con base en el análisis de riesgos, se proponen las siguientes medidas de mitigación, con base a los controles de al Anexo A (normativo) – Referencia de controles de seguridad de la información – ISO/CEI 27001:2022

1	CONTROLES TECNOLÓGICOS		
	TIPO	CONTROL	METODO
1.1.	Derechos de acceso privilegiado	La asignación y uso de los derechos de acceso privilegiado se restringirá y gestionará.	Restricción de accesos basada en roles (RBAC) para usuarios con privilegios elevados.
1.2	Autenticación segura	Las tecnologías y procedimientos de autenticación segura se implementarán en función de las restricciones de acceso a la información y la política específica del tema sobre el control de acceso.	Autenticación multifactor (MFA) para accesos críticos en Zabbix y en SAP.
1.3	Codificación segura	Los principios de codificación segura se aplicarán al desarrollo de software.	Implementación de TLS 1.3 para cifrado de comunicaciones
1.4	Protección contra malware	La protección contra el malware se implementará y respaldará mediante la conciencia adecuada del usuario.	Sistemas de detección de intrusiones firewall y (IDS/IPS) para prevenir ataques y accesos indebidos.
1.5	Protección de los sistemas de información durante las pruebas de auditoría	Las pruebas de auditoría y otras actividades de aseguramiento que involucren la evaluación de los sistemas operativos deben planificarse y acordarse entre el evaluador y la gerencia correspondiente.	Auditorías periódicas de vulnerabilidades en SAP y Zabbix.
1.6	Restricción de acceso a la información	El acceso a la información y otros activos asociados se restringirá de acuerdo con la política específica del tema establecida sobre el control de acceso.	Restricción de acceso a centros de datos con autenticación biométrica

DISEÑO DE CONTROLES DE SEGURIDAD













Con base en el análisis de riesgos, se proponen las siguientes medidas de mitigación, con base a los controles de al Anexo A (normativo) – Referencia de controles de seguridad de la información – ISO/CEI 27001:2022



2.	CONTROLES DE PERSONAS		
	TIPO	CONTROL	MÉTODO
2.1	Concientización, educación y capacitación en seguridad de la información	El personal de la organización y las partes interesadas relevantes deben recibir la conciencia, educación y capacitación adecuadas en seguridad de la información y actualizaciones periódicas de la política de seguridad de la información de la organización, las políticas y los procedimientos específicos del tema, según sea relevante para su función laboral.	Capacitación en ciberseguridad para reducir el riesgo de ataques de phishing y suplantación de identidad.
3.	CONTROLES ORGANIZACIONALES		
3.1	Políticas de seguridad de la información	La política de seguridad de la información y las políticas específicas del tema deben ser definidas, aprobadas por la gerencia, publicadas, comunicadas y reconocidas por el personal relevante y las partes interesadas relevantes, y revisadas a intervalos planificados y si ocurren cambios significativos.	Políticas de seguridad Zero Trust, para restringir accesos dentro de la red corporativa

CONTROLES DE SEGURIDAD DE LA INFORMACIÓN



Medida	Efectividad	Impacto en seguridad	Costo
MFA y RBAC	Alta 	Alta 	Bajo 
TLS 1.3 y cifrado AES-256	Alta 	Alta 	Medio 
IDS/IPS	Alta 	Media 	Alto 
Auditoria Vulnerabilidades	Media 	Alta 	Alto 



CONCLUSIONES

El seguimiento y monitoreo con la modalidad Zabbix, para el sistema SAP, revela vulnerabilidades que podrían comprometer la continuidad operativa de la empresa, evidenciando que se detecta como las más críticas: el **escalamiento de privilegios, inyección SQL, ataques DDoS y robo de credenciales**.

La combinación de los modelos **STRIDE, PASTA y DREAD** permitió identificar amenazas, y también priorizar su mitigación de manera efectiva.

Las principales recomendaciones incluyen:

Implementar MFA y RBAC para proteger accesos críticos en SAP.

Actualizar protocolos de seguridad eliminando SSLv3 y habilitando TLS 1.3.

Fortalecer la detección de amenazas con IDS/IPS y auditorías constantes.

Capacitar al personal en ciberseguridad para reducir ataques de ingeniería social.

Efectuar auditorías periódicas de vulnerabilidades en SAP.



Esta foto de Autor desconocido está bajo licencia [CC BY-NC-ND](#)

Con estas medidas, empresa de servicios de entrega de productos que emplea el sistema SAP podrá reducir el riesgo de ciberataques, asegurando la protección de su infraestructura y la continuidad de sus operaciones logísticas en la Cadena de Abastecimientos.

REFERENCIAS

- ❖ *Common Vulnerability Scoring System SIG*. (s/f). FIRST — Forum of Incident Response and Security Teams. Recuperado el 18 de febrero de 2025, de <https://www.first.org/cvss/>
- ❖ *Cvss-v31-examples_r1*. (s/f).
- ❖ Jain, S. (2021, abril 22). Threat Modelling Frameworks (SDL, STRIDE, DREAD & PASTA). *Medium*. <https://radiumhacker.medium.com/threat-modelling-frameworks-sdl-stride-dread-pasta-93f8ca49504e>
- ❖ *Software Secured / Comparison of STRIDE, DREAD & PASTA / USA*. (s/f). Recuperado el 18 de febrero de 2025, de <https://www.softwaresecured.com/post/comparison-of-stride-dread-pasta>



Preguntas



@EsdegCol



Escuela Superior
de Guerra



Escuela Superior
de Guerra



Escuela Superior
de Guerra



www.esdegue.edu.co



ESCUELA SUPERIOR
DE GUERRA
"General Rafael Reyes Prieto"
Colombia

ISO 9001:2015
ISO 21001:2018

BUREAU VERITAS
Certification



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



Gracias



AUDITORIO
BICENTENARIO BATALLA DE AYACUCHO
UNIÓN - INTEGRIDAD - VICTORIA



@EsdegCol



Escuela Superior
de Guerra



Escuela Superior
de Guerra



Escuela Superior
de Guerra



www.esdegue.edu.co