



ESCUELA SUPERIOR
DE GUERRA

"General Rafael Reyes Prieto"

Colombia

INFORME AMENAZAS CIBERNETICAS



MY DIEGO CASALLAS– MY YURLEWINSON CASTRO
MY JOSE CALDERON –MY JOAN CONTRERAS

Nuestro equipo reúne a expertos que trabajan juntos para analizar y aprender de las lecciones del pasado, aportando perspectivas únicas para superar desafíos históricos.



Descripción del Escenario

Sistema Híbrido

Acceso desde ordenadores en la empresa y dispositivos personales.

Infraestructura

Servidor central, puntos de venta, routers, cables, computación.

Usuarios

Administradores, personal de ventas, distribuidores, clientes.

Análisis de Riesgos con STRIDE

1 Spoofing

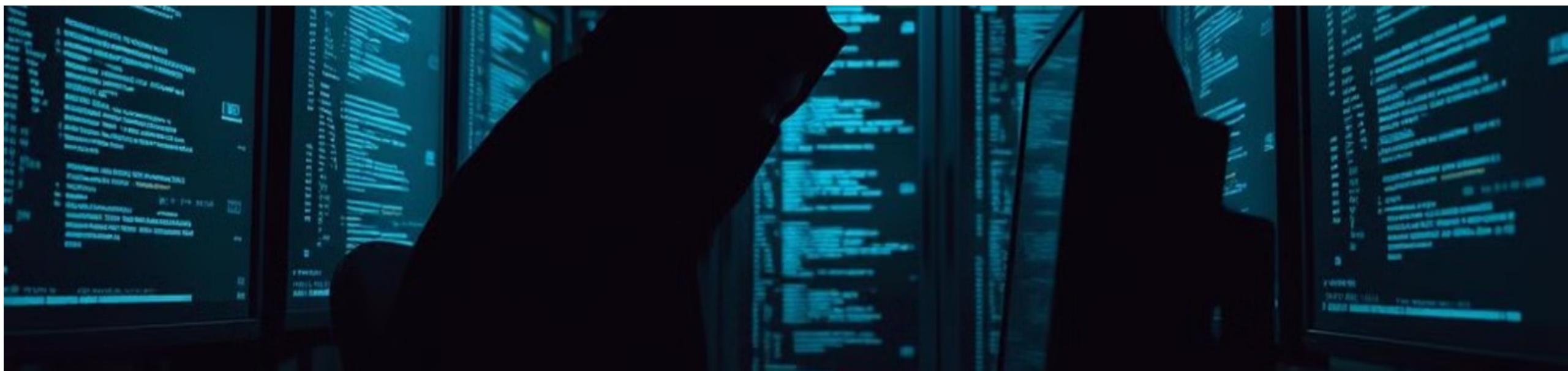
Suplantación de identidad mediante ingeniería social.

2 Tampering

Manipulación de datos de pedidos e inventario.

3 Repudiation

actor malicioso puede modificar datos sin dejar evidencia, esto evita que se identifique responsabilidad.



Análisis de Riesgos con STRIDE

4 Information Disclosure

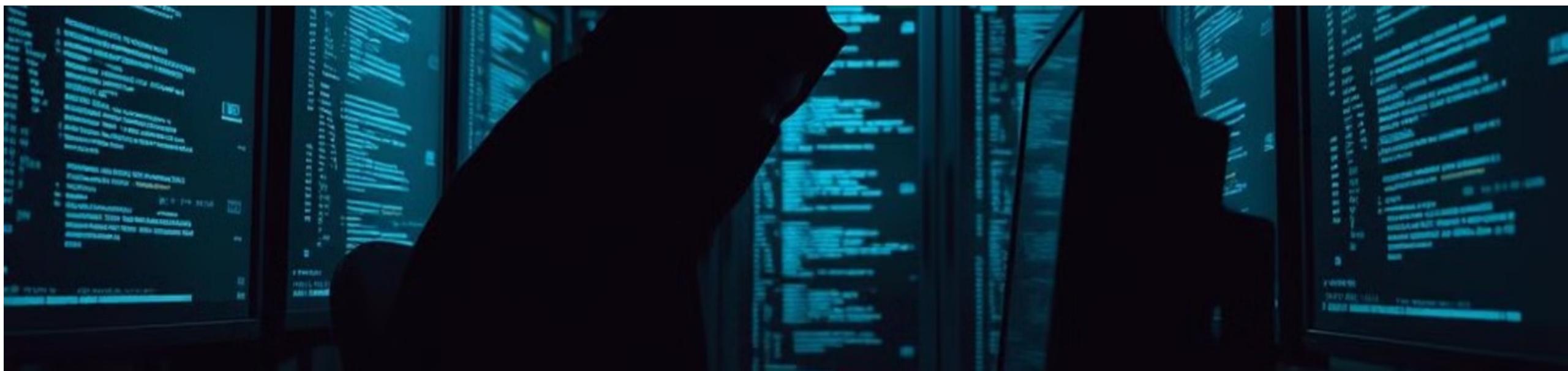
Filtración de información sensible de clientes.

5 Denial of servise

Podria inhabilitar el sistema de pedidos que salen y llegan, esto genera pérdidas monetarias y de fiabilidad del cliente

6 Elevation of Privilege

El atacante puede ingresar y obtener privilegios mayores que le daran el control.



Mitigación de Amenazas



MFA

Autenticación multifactor para prevenir spoofing.



Cifrado

Cifrado de datos para evitar information disclosure.



Firewall

Firewalls para mitigar denial of service.

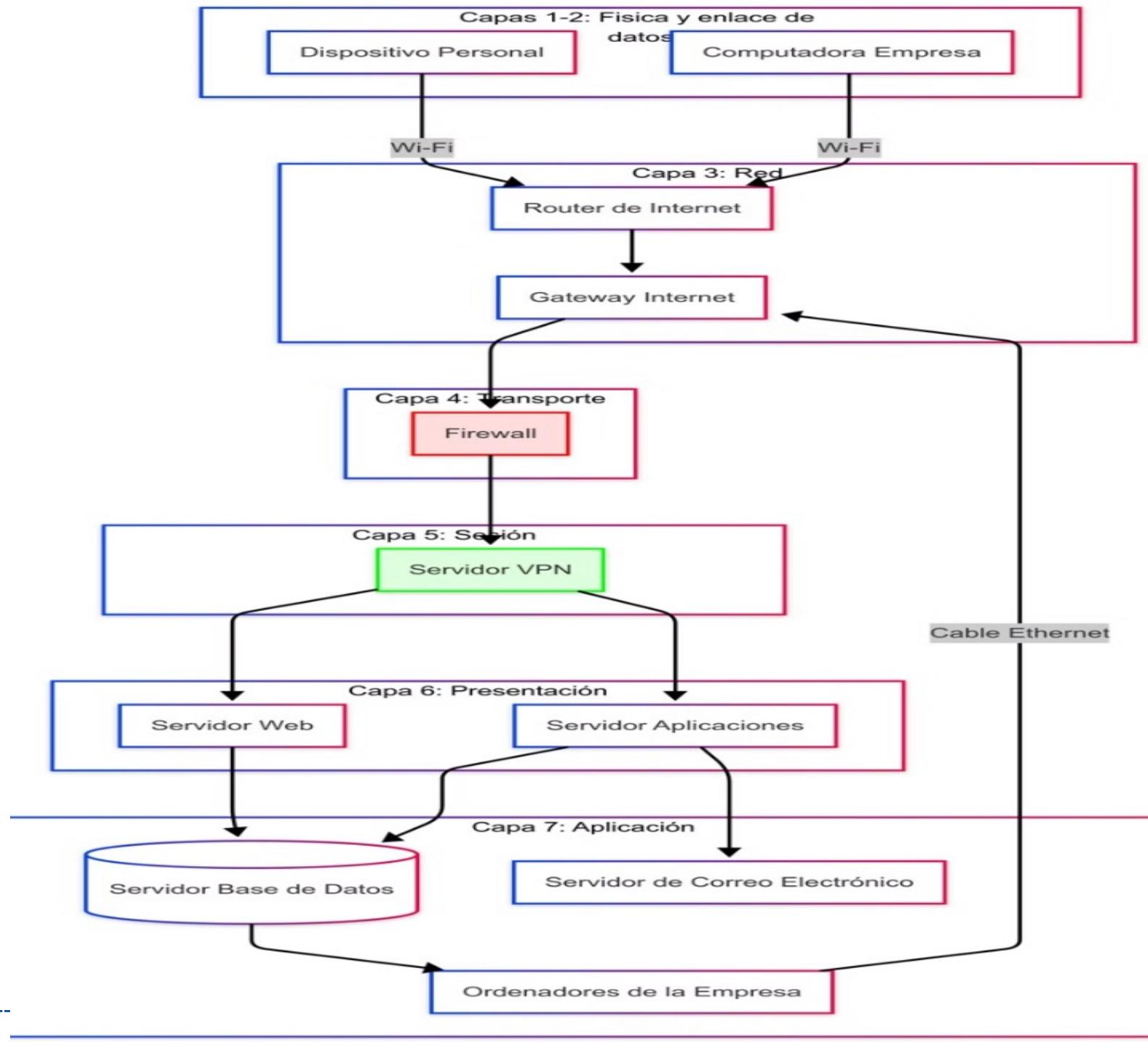


Matriz de Riesgos

Tipo Amenaza	Probabilidad	Impacto	Mitigación
Spoofing	Alta	Alto	MFA, segmentación de red, firewalls, antivirus
Tampering	Media	Alto	monitoreo, auditoría del sistema, permisos necexarios
Repudiation	Baja	Medio	Control versiones, firma digital
Information Disclosure	Alta	Muy Alto	Cifrado de datos, monitoreo de datos, políticas de confidencialidad
Denial of Service	Media	Alto	Firewalls, red por fragmentos, monitoreo
Elevation of Privilege	Alta	Crítico	Privilegios mínimos por usuario, autenticar doble factor, auditoria de los sistemas, actualización de sistemas, alertas

Arquitectura

Diagrama de la arquitectura de seguridad propuesta para Crem Helado.



Políticas de Seguridad Propuestas

1

Autenticación

Doble factor y biométrica.

2

Cifrado

Cifrado de bases de datos.

3

Monitoreo

Detección de actividades inusuales.

4

Capacitación

Entrenar al personal en ciberseguridad.

Conclusiones y Recomendaciones

Amenazas Críticas

Identificación de amenazas en sistemas de gestión.

Políticas de Seguridad

Aplicar protocolos y políticas propuestas.

Cultura de Protección

Incrementar la protección de la información.





Preguntas



@EsdeCol



Escuela Superior
de Guerra



Escuela Superior
de Guerra



Escuela Superior
de Guerra



www.esdecol.edu.co



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



@EsdegCol



Escuela Superior
de Guerra



Escuela Superior
de Guerra



Escuela Superior
de Guerra



www.esdegue.edu.co