RETO FINAL

Fortaleciendo la Red de Empresa XYZ

Ciberseguridad Nivel Explorador

Cristian Camilo Perez Puentes

Bootcamp 2025 | 24 de noviembre de 2025

Temas

- Análisis Inicial
- Configuraciones Aplicadas
- Políticas de Seguridad
- Justificación Teórica
- Conclusiones

Analisis Inicial

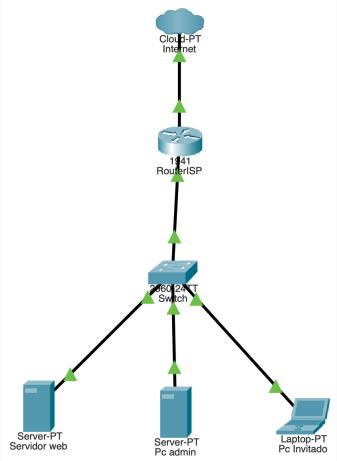
Escenario Inicial

! Situacion Actual:

- Red plana sin segmentacion
- Sin firewall ni controles de acceso
- Puertos abiertos innecesarios
- Vulnerable a ataques

+ Objetivos:

- Evaluar vulnerabilidades
- Redisenar la topologia
- Implementar controles
- Definir politicas



Red inicial

Vulnerabilidades Detectadas

Vulnerabilidad	Prob.	Riesgo
Sin Firewall	Alta	Critico
Puertos Abiertos	Media	Alto
Sin Segmentacion	Media	Alto

Impacto en Triada CIA

C - Acceso no autorizado
I - Modificacion de datos
A - DoS y malware

Sin Firewall

Trafico sin inspeccion. Exposicion total.

Puertos Abiertos

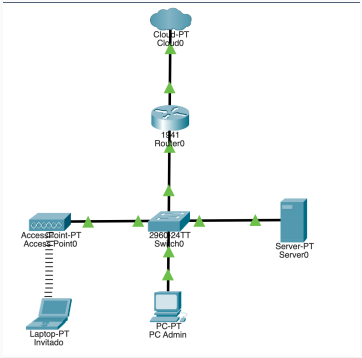
HTTP/HTTPS en PC Admin innecesario.

Red Plana

Movimiento lateral libre.

Configuraciones Aplicadas

Nueva Topologia Segmentada



Red con VLANs

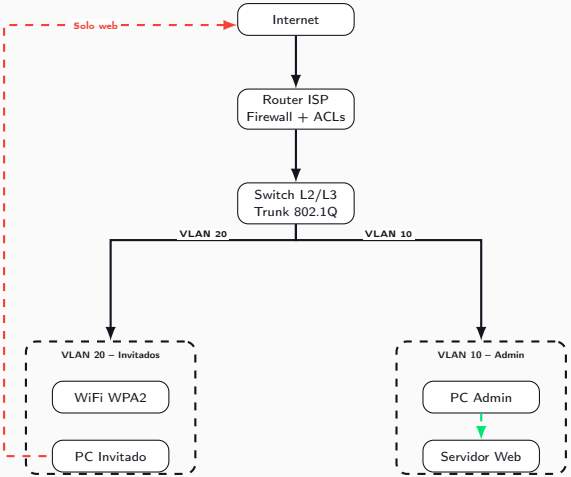
+ Mejoras:

- Segmentacion en 2 VLANs
- Router como gateway y firewall
- ACLs para control de trafico
- Port Security en switch
- WPA2 en red inalambrica

Router-on-a-Stick

Subinterfaces G0/0.10 y G0/0.20 con 802.1Q.

Arquitectura de Red Segmentada



Segmentacion en VLANs

VLAN 10 – Administrativa

- PC Admin + Servidor Web
- Red: `192.168.10.0/24`
- Gateway: `192.168.10.1`

VLAN 20 – Invitados

- Access Point + PC Invitado
- Red: `192.168.20.0/24`
- Solo acceso a Internet

Switch:

- `Fa0/1`: Trunk 802.1Q
- `Fa0/2-3`: VLAN 10
- `Fa0/4`: VLAN 20

ACL en Router:

- Deny: VLAN20 → VLAN10
- Permit: VLAN20 → Internet

Mecanismos de Autenticacion

WPA2-PSK en WiFi

- SSID: `Invitados`
- Cifrado: AES
- Passphrase compleja

Acceso a Dispositivos

- Usuario local privilegio 15
- SSH para gestion remota
- `enable secret`

Port Security

- Max 2 MACs por puerto
- Aprendizaje `sticky`
- Violacion: `restrict`

Beneficios:

- Impide dispositivos no autorizados
- Protege contra MAC spoofing

Politicas de Seguridad

Higiene Digital

Contrasenas

- Minimo 10 caracteres
- Combinacion de tipos
- Cambio cada 90 dias

Buenas Practicas

- Bloqueo de pantalla
- Cuentas individuales
- Cierre de sesiones

Actualizaciones

- Firmware de dispositivos
- Software de servidores
- Pruebas previas

Respaldos

- Configuraciones de red
- Datos criticos
- Almacenamiento externo

Politica de Seguridad

Normas de Uso

- Solo software autorizado
- Uso laboral de recursos
- Proteccion de info confidencial

Control de Acceso

- Minimo privilegio
- Cuentas individuales
- Trazabilidad

Gestion de Incidentes

- Reporte inmediato a TI
- Documentar evento
- Escalamiento

Responsabilidades

- Usuarios: cumplir normas
- Admins: implementar controles

Justificacion Teorica

Triada CIA

Confidencialidad

Segmentacion VLAN
ACLs restrictivas
WPA2-PSK

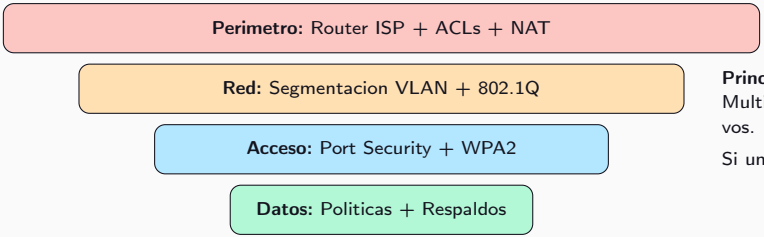
Integridad

Autenticacion local
SSH para gestion
MAC sticky

Disponibilidad

Aislamiento VLANs
Respaldos periodicos
Plan de incidentes

Defensa en Profundidad



Principio:
Multiples capas protegen los activos.

Si una falla, las demas contienen.

Minimo Privilegio

En la Red

- Invitados: solo Internet
- VLAN 10 aislada de VLAN 20
- Servidor: solo HTTPS
- Puertos: MACs conocidas

En Usuarios

- Privilegios especificos
- Solo admins gestionan red
- Acceso segun funcion
- Cuentas individuales

"Solo los privilegios minimos necesarios para la funcion."

Conclusiones

Resumen de Mitigaciones

Vulnerabilidad	Mitigacion	Capa
Sin Firewall	ACLs en RouterISP	Perimetral
Puertos Abiertos	Solo HTTPS en servidor	Config
Sin Segmentacion	VLAN 10 + VLAN 20	Red
Acceso libre	Port Security + WPA2	Acceso
Sin politicas	Documento normativo	Organizacional

Resultado: Red segmentada con controles multinivel, alineada con CIA.

Recomendaciones Futuras

Corto Plazo

- Implementar 802.1X (RADIUS)
- Configurar IDS/IPS
- Centralizar logs
- Automatizar respaldos

Mediano Plazo

- Firewall dedicado (NGFW)
- VPN para acceso remoto
- SIEM centralizado
- Auditorias periodicas

La seguridad es un proceso continuo.