RETO FINAL

CIBERSEGURIDAD NIVEL EXPLORADOR

Fortaleciendo la Red de Empresa XYZ en 6 Horas

Preparado por:

Cristian Camilo Perez Puentes

Fecha:
30 de noviembre de 2025

Bootcamp de Ciberseguridad - 2025

Índice

Escenario

La Empresa XYZ es una compañía pequeña que ha detectado problemas de seguridad en su red interna. La red actual es plana, sin segmentación, y carece de controles básicos de seguridad, lo que la hace vulnerable a ataques y accesos no autorizados. Se te ha asignado el rol de consultor de ciberseguridad para evaluar, rediseñar y aplicar medidas de protección en un entorno simulado (por ejemplo, utilizando Cisco Packet Tracer, GNS3 o una herramienta similar).

Objetivos del Reto

Los participantes deberán demostrar lo siguiente:

- **Conceptos Fundamentales y Modelos de Seguridad:** Identificar y explicar la relevancia de la tríada CIA (Confidencialidad, Integridad y Disponibilidad) y otros modelos básicos de seguridad en la red.
- **Higiene Digital:** Proponer y aplicar acciones de higiene digital (por ejemplo, gestión de contraseñas, actualizaciones, segmentación y respaldos) que protejan la información.
- **Análisis de Vulnerabilidades, Amenazas y Riesgos:** Detectar y documentar al menos tres vulnerabilidades o riesgos presentes en la red actual.
- **Medios de Transmisión y Autenticación:** Reconocer y configurar mecanismos de autenticación y protocolos seguros para la transmisión de datos (por ejemplo, configuración de WPA2 en redes inalámbricas o autenticación en puertos).
- **Configuración de Redes LAN y VLAN:** Diseñar y configurar una red LAN segmentada en al menos dos VLAN (por ejemplo, una para el área administrativa y otra para invitados) y definir reglas de acceso.
- **Política de Seguridad de la Información:** Elaborar un documento breve que contenga las políticas, normas y procedimientos básicos para la protección de los recursos informáticos de la empresa.

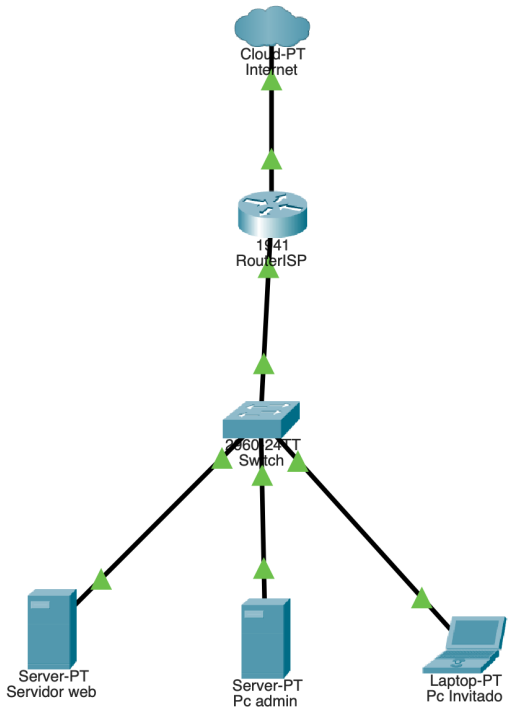

Figura 1: Diagrama de la red inicial de la Empresa XYZ

Descripción de la topología:

La topología inicial de la red de la Empresa XYZ se modelo en Cisco Packet Tracer, con los siguientes componentes principales:

- **Modulo cloud**: Representa la conexión a Internet.
- **Router**: Gestiona el tráfico entre la red interna e Internet.
- **Switch**: Conecta todos los dispositivos dentro de la red local.
- **Laptop**: Representa a los usuarios invitados.
- **Servidores:** Uno representa el servidor web y otro el PC administrativo; ambos exponen servicios HTTP/HTTPS configurados, como se muestra en las figuras de puertos abiertos (Firgura 2).

Figura 2: Puertos HTTP y HTTPS abiertos en el servidor

0.1 Identificación de Vulnerabilidades

0.1.1. Matriz de Riesgos

Vulnerabilidad	Probabilidad	Impacto	Nivel de riesgo
Ausencia de Firewall y reglas de filtrado	Alta	Alto	Critico
Puerto Abierto	Media	Alto	Alta
Falta de Segmentación de Red	Media	Alto	Alta

Cuadro 1: Matriz de riesgos para las vulnerabilidades identificadas

0.1.2. Ausencia de Firewall y reglas de filtrado

- **Descripción:** El sistema no cuenta con un firewall activo ni con reglas de filtrado configuradas. Esto permite que cualquier tráfico entrante o saliente llegue directamente al equipo sin ser inspeccionado o limitado.
- **Tipo:** Vulnerabilidad de configuración / Punto de entrada expuesto.

- **Impacto Potencial:** Exposición total del sistema a tráfico malicioso sin ningún tipo de bloqueo.
- **Riesgo:** Critico, ya que la ausencia de un firewall permite diversidad de ataques, desde accesos no autorizados, malware, hasta ataques de denegación de servicio (DoS), lo cual determina una probabilidad e impactos altos.
- **Relación con la Tríada CIA:**
  - **Confidencialidad:** Acceso no autorizado a datos al no existir barreras de filtrado.
  - **Integridad:** Un atacante podría modificar información o configuración del sistema.
  - **Disponibilidad:** Riesgo elevado de ataques de denegación de servicio (DoS) o interrupciones por malware.

0.1.3. Vulnerabilidad, Puerto Abierto

- **Descripción:** Los puertos HTTP (80) y HTTPS (443) están abiertos en el PC Administrativo, lo cual expone servicios web que no deberían ejecutarse en un equipo de usuario interno.
- **Tipo:** Vulnerabilidad de configuración / Punto de entrada expuesto
- **Impacto Potencial:** Amplía la superficie de ataque del sistema, permitiendo que posibles atacantes interactúe con servicios web no necesario t aumenta el riesgo de acceso no autorizado o movimiento lateral dentro de la red.
- **Riesgo:** Alto, ya que depende de la medidas de seguridad en otras capas de red y del software del servidor web, pero puede tener un impacto significativo si se explotan vulnerabilidades en esos servicios.
- **Relación con la Tríada CIA:**
  - **Confidencialidad:** Riesgo de acceso no autorizado a datos a través de vulnerabilidades en los servicios web.
  - **Integridad:** Posibilidad de manipulación de datos o configuración del sistema mediante ataques dirigidos a los servicios web.
  - **Disponibilidad:** Riesgo de interrupciones del servicio debido a ataques dirigidos a los puertos abiertos.

0.1.4. Falta de Segmentación de Red

- **Descripción:** La red no cuenta con segmentación entre dispositivos, permitiendo que todos los equipos se comuniquen libremente entre sí sin restricciones.
- **Tipo:** Vulnerabilidad de arquitectura / configuración.
- **Impacto Potencial:**

    - Facilita el movimiento lateral de un atacante dentro de la red e incrementa la probabilidad de que malware o exploits se propaguen entre equipos, ademas dificulta la detección y el aislamiento de incidentes.

- **Riesgo:** Alto, ya que la falta de segmentación aumenta la probabilidad de compromisos múltiples dentro los cual es de un alto impacto, la probabilidad de ser explotada depende la protection de la red en otras capas.

- **Relación con la Tríada CIA:**

    - **Confidencialidad:** Datos sensibles pueden ser accesibles desde cualquier dispositivo de la red.
    - **Integridad:** Un atacante que comprometa un equipo puede modificar información en otros sistemas.
    - **Disponibilidad:** Malware o ataques DoS pueden propagarse sin barreras, interrumpiendo múltiples servicios.

0.2 Análisis de Amenazas

0.3 Herramientas Utilizadas para el Análisis

1 Rediseño y Configuración de la Red

1.1 Diseño de la Nueva Topología

1.1.1. Diagrama de Red Actualizado

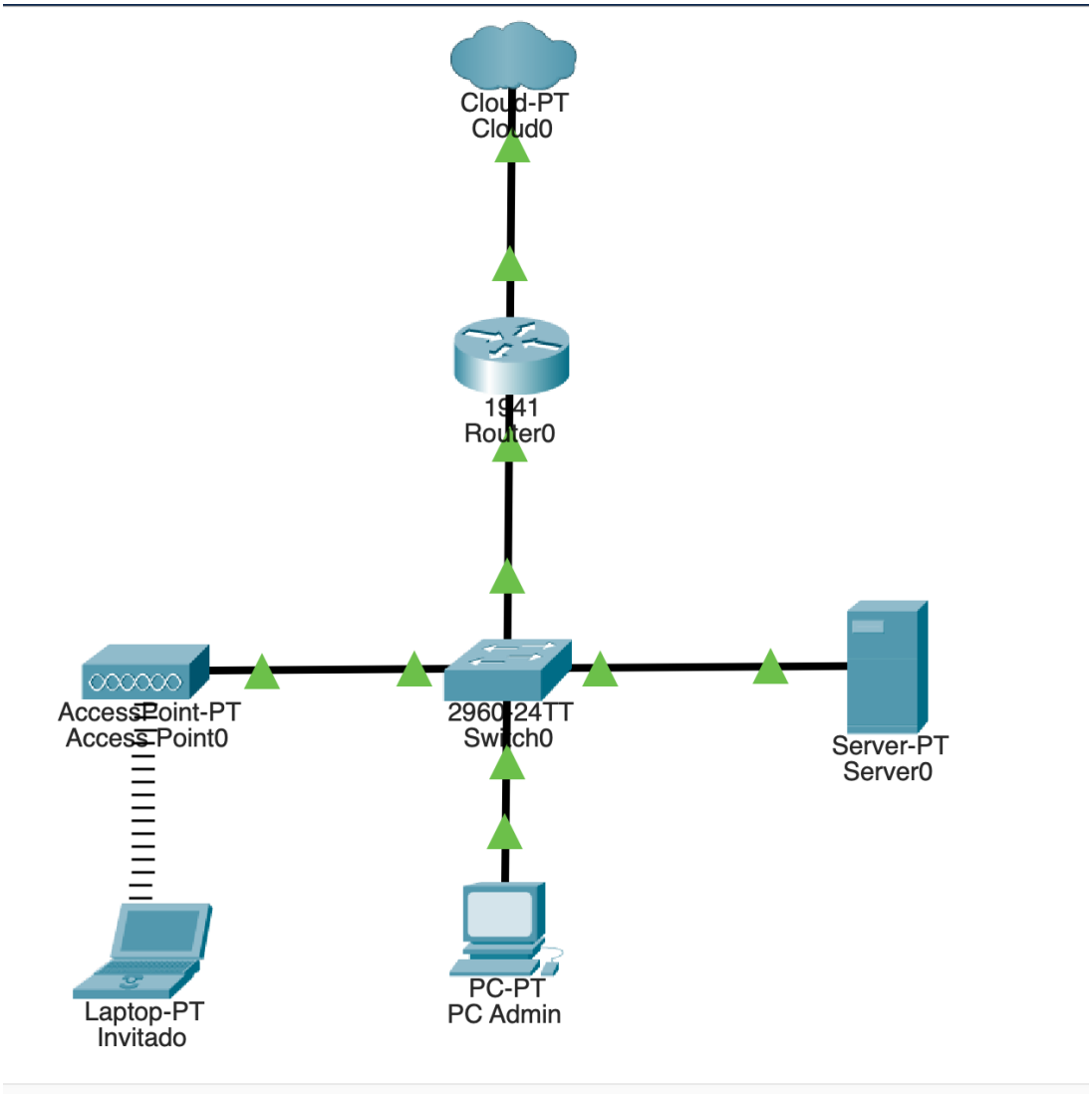

Figura 3: Diagrama de la red rediseñada de la Empresa XYZ

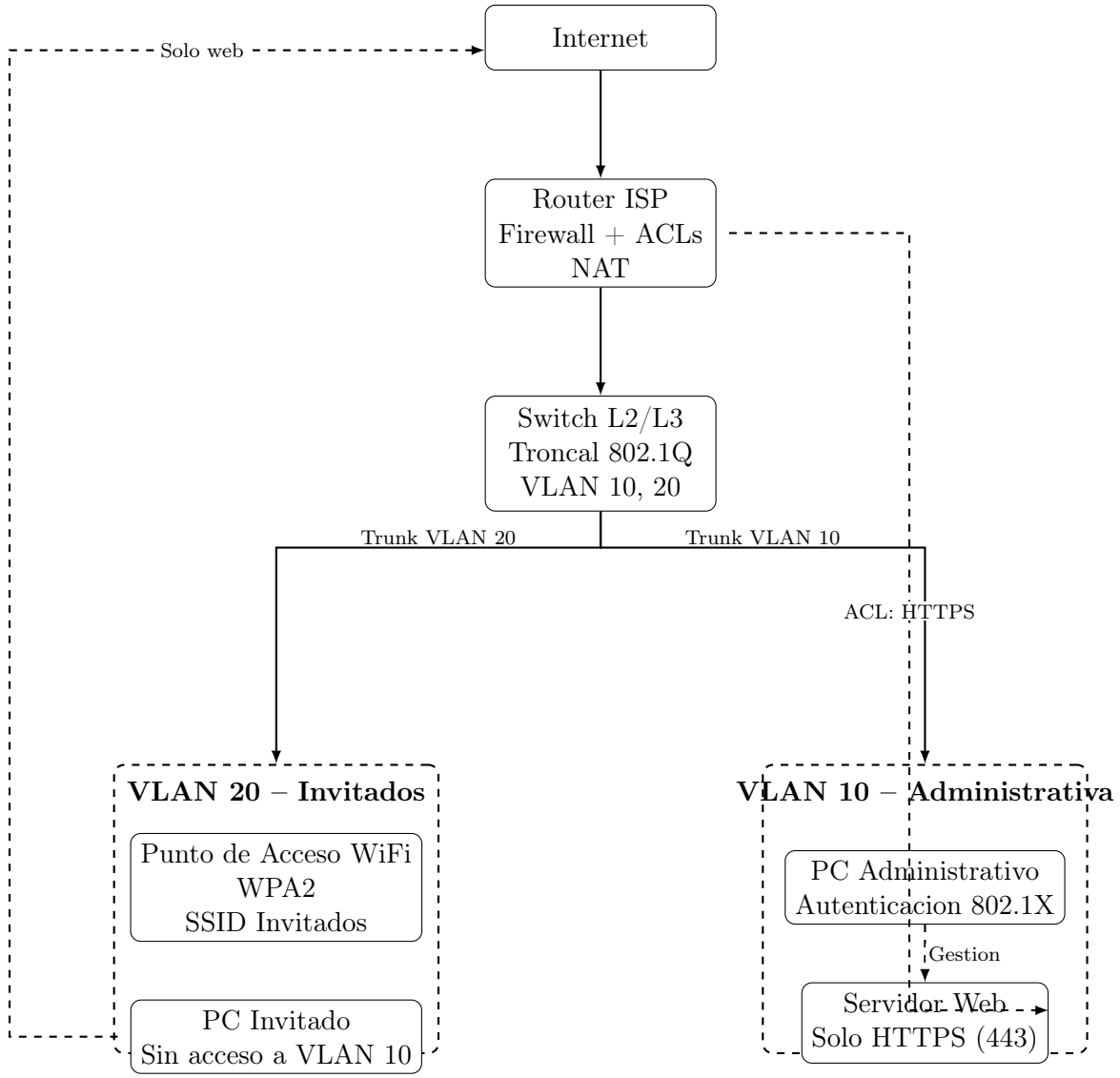

Figura 4: Red de la Empresa XYZ segmentada en VLAN 10 (Administrativa) y VLAN 20 (Invitados)

1.2 Configuración de Dispositivos

1.2.1. Configuración del Switch

Listing 1: Comandos de configuracion del switch

```
enable
conf t
hostname Switch

! Crear VLANs
```

```
vlan 10
 name ADMIN
vlan 20
 name INVITADOS
exit

! Puerto hacia el router: TRUNK 802.1Q
interface fa0/1
 switchport mode trunk
 switchport trunk allowed vlan 10,20
 no shutdown

! Puertos acceso VLAN 10 (Pc Admin + Servidor Web)
interface fa0/2
 switchport mode access
 switchport access vlan 10
 ! Medida basica de autenticacion de puerto (Port Security)
 switchport port-security
 switchport port-security maximum 2
 switchport port-security violation restrict
 switchport port-security mac-address sticky
 no shutdown

interface fa0/3
 switchport mode access
 switchport access vlan 10
 ! Medida basica de autenticacion de puerto (Port Security)
 switchport port-security
 switchport port-security maximum 2
 switchport port-security violation restrict
 switchport port-security mac-address sticky
 no shutdown

! Puerto acceso VLAN 20 (AP invitados)
interface fa0/4
 switchport mode access
 switchport access vlan 20
 ! Medida basica de autenticacion de puerto (Port Security)
 switchport port-security
 switchport port-security maximum 2
 switchport port-security violation restrict
 switchport port-security mac-address sticky
 no shutdown

end
```

1.2.2. Configuración del Router

Listing 2: Comandos de configuracion del router

```
enable
conf t
hostname RouterISP

! Enlace al switch (trunk)
interface GigabitEthernet0/0
 no shutdown
 no ip address

interface GigabitEthernet0/0.10
 encapsulation dot1Q 10
 ip address 192.168.10.1 255.255.255.0
 no shutdown

interface GigabitEthernet0/0.20
 encapsulation dot1Q 20
 ip address 192.168.20.1 255.255.255.0
 no shutdown

! Enlace a Internet
interface GigabitEthernet0/1
 ip address 200.0.0.1 255.255.255.252
 no shutdown
end

! Autenticacion basica para acceso al router (consola y VTY)
username admin privilege 15 secret Admin123
line console 0
 login local
 logging synchronous
line vty 0 4
 login local
 transport input ssh
exit

! ACL para que no invitados NO accedan a VLAN 10
conf t
ip access-list extended GUEST_TO_INSIDE
 deny ip 192.168.20.0 0.0.0.255 192.168.10.0 0.0.0.255
 permit ip 192.168.20.0 0.0.0.255 any
exit
```

1.2.3. Configuración de Dispositivos Finales

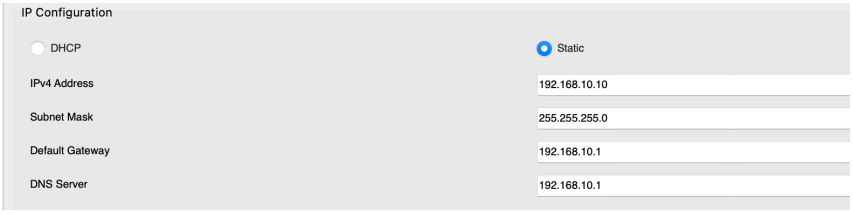

Figura 5: Configuración del PC Administrativo (VLAN 10)

Figura 6: Configuración del PC Invitado (VLAN 20)

Figura 7: Configuración del Servidor Web (VLAN 10)

1.2.4. Justificación del Diseño

- **Segmentación en VLAN 10 y VLAN 20:** Se crearon dos VLAN lógicas en el switch: `VLAN 10` (ADMIN) para el PC administrativo y el servidor web, y `VLAN 20` (INVITADOS) para el punto de acceso inalámbrico y el PC invitado. Esta separación reduce el dominio de broadcast y limita el movimiento lateral de un atacante, mitigando el riesgo asociado a la falta de segmentación identificada en la red original.
- **Puertos de acceso y troncal 802.1Q en el switch:** El puerto `Fa0/1` se configuró como enlace troncal 802.1Q hacia el RouterISP, permitiendo transportar simultáneamente las VLAN 10 y 20. Los puertos `Fa0/2` y `Fa0/3` se definieron como puertos de acceso en VLAN 10 para el PC Admin y el Servidor Web, mientras que `Fa0/4` se asignó a VLAN 20 para el AP de invitados. Esto garantiza que cada dispositivo se incorpore al segmento lógico que le corresponde según su función.

- **Subinterfaces en el RouterISP como puerta de enlace por VLAN:** Sobre la interfaz física `G0/0` se crearon las subinterfaces `G0/0.10` y `G0/0.20`, etiquetadas con `encapsulation dot1Q 10` y `dot1Q 20` respectivamente, y con direcciones IP `192.168.10.1` y `192.168.20.1`. Cada subinterfaz actúa como *default gateway* de su VLAN, permitiendo el enrutamiento entre segmentos de forma controlada y preparada para aplicar políticas de filtrado.
- **Control de acceso de invitados mediante ACL:** Se definió la lista de acceso extendida `GUEST_TO_INSIDE`, que bloquea explícitamente el tráfico IP desde la red de invitados (`192.168.20.0/24`) hacia la red administrativa (`192.168.10.0/24`) y solo permite que los invitados se comuniquen con el exterior (`any`). Con esto se cumple el requisito de que los usuarios invitados puedan navegar por Internet pero no acceder a recursos internos sensibles.
- **Alineación con las vulnerabilidades detectadas:** En conjunto, estas decisiones de diseño abordan las vulnerabilidades iniciales: se introduce segmentación lógica de la red, se restringe el alcance de los puertos abiertos únicamente al servidor que debe exponer servicios, y se implementa un punto de control centralizado (RouterISP) donde aplicar ACLs y futuras políticas de firewall y NAT.

1.3 Implementación de Mecanismos de Autenticación

La red rediseñada no solo se apoya en la segmentación mediante VLAN, sino también en mecanismos de autenticación que reducen la probabilidad de accesos no autorizados tanto a nivel de medios de transmisión (WiFi) como de puertos físicos de switch y acceso a los dispositivos de red. A continuación se describe cómo se implementaron estos controles.

1.3.1. Configuración de WPA2 en Punto de Acceso

Para proteger el medio inalámbrico se configuró el punto de acceso de invitados con el protocolo **WPA2-PSK**, sustituyendo cualquier modo abierto o WEP, que se consideran inseguros. En el entorno de Packet Tracer, la configuración se realizó de la siguiente forma:

- Se definió el SSID `Invitados` asociado a la VLAN 20, de modo que todo el tráfico inalámbrico de los usuarios se encamine correctamente hacia la red de invitados.
- En la pestaña de configuración inalámbrica del AP se seleccionó el modo de seguridad **WPA2-PSK** con cifrado fuerte (AES) y se configuró una *passphrase* robusta, evitando contraseñas triviales o por defecto.
- En el equipo *PC/Laptop Invitado* se instaló la interfaz inalámbrica (módulo WPC/WMP en Packet Tracer), se escaneó la red y se asoció al SSID `Invitados` introduciendo la misma clave WPA2 configurada en el AP.

- Se validó la autenticación inalámbrica verificando que el PC invitado obtiene conectividad IP en la red 192.168.20.0/24 y puede comunicarse con su puerta de enlace (192.168.20.1), mientras permanece aislado de la VLAN administrativa.

Con esta configuración, el acceso al medio inalámbrico queda restringido únicamente a quienes conocen la clave WPA2, reduciendo el riesgo de que agentes externos se conecten a la red de invitados y utilicen la infraestructura como punto de entrada a la organización.

1.3.2. Autenticación en Puertos (Port Security)

Además de la protección en la red inalámbrica, se implementaron medidas básicas de autenticación a nivel de puertos del switch utilizando la funcionalidad de **Port Security** en los puertos de acceso `Fa0/2`, `Fa0/3` y `Fa0/4`. En la configuración mostrada en el listado del switch se aplican las siguientes directrices:

- **Activación de Port Security:** El comando `switchport port-security` habilita el control de seguridad sobre el puerto, permitiendo limitar qué direcciones MAC pueden utilizarlo.
- **Límite de direcciones MAC por puerto:** Con `switchport port-security maximum 2` se restringe el número de dispositivos que pueden conectarse simultáneamente a cada puerto, evitando que se utilicen como puntos de concentración no autorizados.
- **Aprendizaje "sticky" de MAC:** El comando `switchport port-security mac-address sticky` permite que el switch aprenda automáticamente las direcciones MAC legítimas que se conectan por primera vez y las guarde en la configuración en ejecución, simplificando la administración.
- **Acción ante violaciones:** La opción `switchport port-security violation restrict` indica que, si se detecta una MAC no autorizada o se supera el máximo configurado, el puerto restringirá el tráfico de la MAC infractora y generará registros, sin derribar completamente el puerto (*shutdown*), lo que equilibra seguridad y disponibilidad.

En conjunto, estas medidas contribuyen a que los puertos de acceso solo sean utilizados por los dispositivos previstos (PC administrativo, servidor y punto de acceso), dificultando que un atacante conecte un equipo adicional al switch para realizar ataques de sniffing, suplantación o movimiento lateral dentro de la red.

2 Implementación de Medidas de Higiene Digital

La higiene digital en la Empresa XYZ se enfocó en cuatro ejes principales: contraseñas seguras, actualización de software, buenas prácticas de acceso y gestión de respaldos y segmentación.

2.1 Políticas de Contraseñas Seguras

Se configuraron contraseñas robustas para el RouterISP, el switch y los equipos críticos, usando `enable secret` y usuarios locales con combinación de mayúsculas, minúsculas, números y símbolos. Se definió una longitud mínima de 10 caracteres, cambio periódico (cada 90 días) y la prohibición de compartir credenciales o reutilizar contraseñas por defecto.

2.2 Actualización de Firmware y Software

Se estableció un procedimiento periódico para revisar y aplicar actualizaciones en router, switch, servidor web y equipos finales, aprovechando mecanismos de actualización automática cuando es posible. Antes de un cambio mayor se recomienda una prueba controlada para evitar indisponibilidades.

2.3 Buenas Prácticas de Acceso

El acceso administrativo a dispositivos de red se realiza mediante sesiones autenticadas, tiempos de expiración de sesión y límite de intentos fallidos. A nivel de usuario se fomenta el bloqueo de pantalla al ausentarse, el uso de cuentas individuales y el cierre de sesiones administrativas en el PC Admin.

2.4 Gestión de Respaldos y Segmentación

Se definieron respaldos periódicos de configuraciones de RouterISP y switch, así como de la información crítica del servidor y del PC administrativo, almacenándolos en un repositorio seguro externo. La segmentación en VLAN 10 (administrativa) y VLAN 20 (invitados), combinada con ACLs, Port Security y WPA2 en la red WiFi, limita el movimiento lateral de un atacante y facilita la recuperación ante incidentes.

3 Política de Seguridad de la Información

3.1 Propósito y Alcance

Esta política establece las directrices mínimas de seguridad de la información para la Empresa XYZ. Aplica a todo el personal (empleados, contratistas y terceros autorizados) y a todos los recursos informáticos de la organización, incluyendo equipos de usuario, servidores, dispositivos de red y servicios accesibles desde la red interna o Internet. Su objetivo es proteger la confidencialidad, integridad y disponibilidad (CIA) de la información y reducir la probabilidad e impacto de incidentes de seguridad.

3.2 Normas de Uso de Recursos Informáticos

El uso de los equipos y sistemas de la Empresa XYZ debe estar vinculado a actividades laborales autorizadas. De forma resumida:

- Está prohibido instalar software sin licencia o no autorizado, utilizar recursos para actividades ilícitas o conectar dispositivos personales a la red administrativa sin aprobación.
- El acceso a Internet y al correo electrónico se utilizará con fines laborales; se evitará visitar sitios de dudosa reputación y abrir enlaces o adjuntos sospechosos.
- La información confidencial (datos de clientes, información financiera, credenciales, configuraciones de red) se almacenará solo en ubicaciones autorizadas y se compartirá únicamente con personal que la necesite para su función.

Los usuarios deben bloquear o cerrar sesión al ausentarse, especialmente en el PC Administrativo y sistemas críticos.

3.3 Contraseñas y Control de Acceso

Las contraseñas empleadas en dispositivos de red, servidores y cuentas de usuario deben:

- Tener al menos 10 caracteres y combinar mayúsculas, minúsculas, números y símbolos.
- Cambiarse de forma periódica (por ejemplo, cada 90 días) y siempre ante sospecha de compromiso.
- No compartirse ni almacenarse en lugares visibles o accesibles por terceros.

Cuando sea posible, se priorizará el uso de autenticación fuerte para accesos críticos (administración remota de dispositivos, servicios expuestos a Internet).

El control de acceso se basará en el principio de mínimo privilegio:

- Solo cuentas administrativas específicas podrán gestionar RouterISP, switch y puntos de acceso.

- Los usuarios de la VLAN de invitados solo tendrán salida a Internet, sin acceso a la VLAN administrativa.
- Se favorecerán cuentas individuales frente a cuentas genéricas, para garantizar trazabilidad de acciones.

Además, el acceso físico y lógico a dispositivos de red se protegerá mediante ubicación en áreas controladas, uso de Port Security en puertos de acceso del switch y administración remota mediante protocolos seguros como SSH.

3.4 Incidentes, Respaldos y Responsabilidades

Se considerará incidente de seguridad cualquier evento que comprometa o pueda comprometer la CIA de la información o de los sistemas (accesos no autorizados, malware, pérdida de dispositivos, fallos graves de configuración, etc.). Todo el personal deberá reportar de inmediato cualquier sospecha al responsable de TI, indicando descripción del evento, equipos afectados y momento de detección.

La Empresa XYZ realizará respaldos periódicos de configuraciones de dispositivos críticos (RouterISP, switch, puntos de acceso) y de la información de negocio en el servidor web y PC administrativo. Estos respaldos se almacenarán en ubicaciones seguras separadas de los sistemas de producción, con acceso restringido, y se validarán mediante pruebas periódicas de restauración.

Los usuarios finales son responsables de cumplir estas normas, proteger sus credenciales y reportar actividades sospechosas. Los administradores de sistemas y redes deberán implementar y mantener las configuraciones de seguridad (segmentación, ACL, autenticación, respaldos) y revisar periódicamente registros y estados de copia de seguridad.

3.5 Mitigación de Riesgos Identificados

Esta política consolida en un marco normativo las medidas técnicas aplicadas en la red de la Empresa XYZ. Al establecer reglas claras sobre uso aceptable, contraseñas, control de acceso, gestión de incidentes y respaldos, contribuye a mitigar las vulnerabilidades iniciales (ausencia de firewall efectivo, puertos abiertos donde no corresponde, falta de segmentación) y limita el impacto de posibles ataques. En conjunto con la segmentación en VLAN, el uso de ACL, Port Security, WPA2 y las prácticas de higiene digital descritas, se refuerza la protección de los servicios críticos de la organización y se mejora la capacidad de respuesta ante incidentes.