SISTEMAS INFORMATICOS

CASO PRACTICO 1

ALUMNO CESUR 24/25

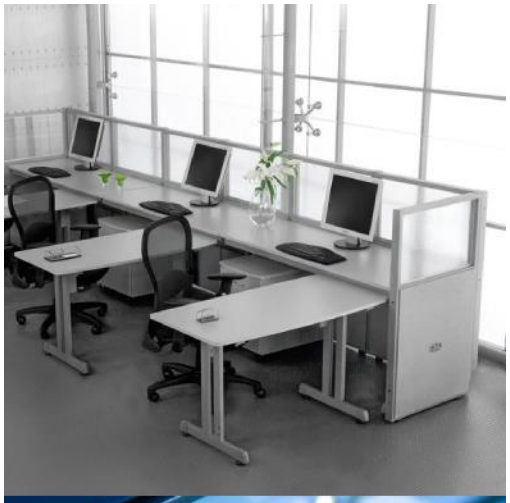
Alejandro Muñoz de la Sierra

PROFESOR

Efren Zurita Alonso

CONTENIDO

0 1
I N T R O D U C C I O N



Este caso práctico tiene como misión planificar una red local para una pequeña empresa que busca mejorar su infraestructura tecnológica y optimizar tanto la comunicación interna como el acceso a recursos compartidos de manera más eficiente.

La empresa cuenta con varios empleados que necesitan acceder a información y herramientas para realizar su trabajo de manera fluida. Para cubrir estas necesidades, proponemos diseñar una red que conecte ordenadores, impresoras y otros dispositivos, garantizando una gestión adecuada del tráfico de datos y, lo más importante, asegurando la protección de la información. Se explorarán aspectos esenciales, como la selección del hardware adecuado, la topología de la red más efectiva, la configuración de protocolos y la implementación de medidas de seguridad sólidas, incluyendo la instalación de un firewall y un servidor para gestionar los recursos de forma centralizada.

El objetivo de este proyecto no es solo establecer una red funcional, sino también asegurarnos de que sea escalable y adaptable a las futuras necesidades de la empresa, respetando siempre las mejores prácticas tanto de diseño como de seguridad. A lo largo de este documento, desglosaremos los elementos clave para llevar a cabo esta planificación.

02

IDENTIFICACIÓN Y SELECCIÓN DEL HARDWARE Y MEDIOS DE TRANSMISIÓN

Para implementar una red eficiente y segura, es imperativo seleccionar el hardware adecuado que permita una comunicación ininterrumpida entre los diferentes nodos de la empresa. El equipo a continuación es necesario:

- **Hardware necesario:**
  - 1 switch de 5+ puertos, recomendados entre 5 – 8 puertos el switch conectará todos los dispositivos.
  - 7 cables Ethernet CAT6: conectarán cada ordenador, servidor e impresora en la oficina, directamente al switch.
  - 1 Router que gestionará la red de área local y las conexiones a Internet.
  - 1 Firewall seguridad de la red, ya sea un dispositivo independiente o un software.
  - 1 servidor como parte central de la red, almacenará todo el contenido compartido.

- **Justificación de elección:**
  - **Switch Gigabit:** la transferencia rápida de datos es necesaria ya que garantiza un rendimiento perfecto cuando se comparten tareas en red, como la impresión desde impresoras o la navegación en archivos remotos.
  - **Cables Ethernet CAT6 :** la tasa de transferencia permitida por cable es de 1Gbps, lo cual es excelente para manejar grandes cantidades de contenido continuamente.

- **Router:** además de gestionar nuestra conexión de Internet, proporcionará direcciones IP a todas las computadoras conectadas. Esto permite que los dispositivos en red se vean entre sí y se comuniquen de manera eficiente.
- **Firewall :** la red debe protegerse de las conexiones externas no autorizadas. El firewall decidirá si una respuesta entrante está permitida o no y desconectará la conexión en caso de intrusiones.
- **Servidor:** será nuestra única fuente compartida de archivos. Será el recurso para las aplicaciones y los periféricos de impresoras.

0 3

DETERMINACIÓN DE LA TOPOLOGÍA DE RED

- **Topología seleccionada: Estrella**

- **Justificación:**
  - El motivo de la elección de la topología en estrella fue que esta topología implica que cada dispositivo, ya sea ordenador o impresora, esté cableado individualmente al switch central. Por lo tanto, con esta topología, la gestión de la red se simplifica enormemente. Así, en caso de problemas, por ejemplo, con uno de los dispositivos, no se afectará el resto del dispositivo conectado.
  - Además, esta topología permite obtener un rendimiento más eficiente y seguro que las topologías de bus. Más conexiones directas al switch garantizan un flujo de datos más rápido.
  - El siguiente beneficio es que esta topología es fácilmente escalable. Así, si la empresa desea conectar más equipos a la red, lo puede hacer sin desconectar los dispositivos antiguos.

0 4

CREACIÓN DE MAPAS FÍSICOS Y LÓGICOS DE LA RED

- **Mapa físico:**
  - En el mapa físico se debe representar la ubicación y conexión de los tres ordenadores, el switch, el router y el firewall. Cada dispositivo estará conectado mediante cables Ethernet, y el esquema debe dejar claro cómo están distribuidos y enlazados físicamente en la oficina. Esto ayuda a visualizar el diseño real de la red y facilita el mantenimiento y la solución de problemas.

Router:

- Conectado a **Internet** mediante el cable de fibra óptica u otro tipo de conexión proporcionada por el proveedor de servicios (ISP).
- Conectado directamente al **firewall**, formando el punto de entrada a la red interna.

Firewall:

- Colocado entre el **router** y el **switch**. Se encarga de filtrar y monitorear el tráfico entrante y saliente, proporcionando seguridad a la red.
- Conectado al **switch** para controlar las comunicaciones entre los dispositivos dentro de la red local.

Switch:

- Conectado al **firewall** y encargado de distribuir las conexiones de red hacia los distintos dispositivos de la red interna.
- Proporciona conexiones mediante cables **Ethernet** (CAT6) a los dispositivos, como ordenadores, impresoras y servidores.

Ordenadores o Dispositivos:

- Conectados físicamente al **switch** a través de cables **Ethernet**, asegurando una conexión estable y rápida.

- Si la red es Wi-Fi, los dispositivos estarían conectados al **router** mediante la señal inalámbrica en lugar de cables.

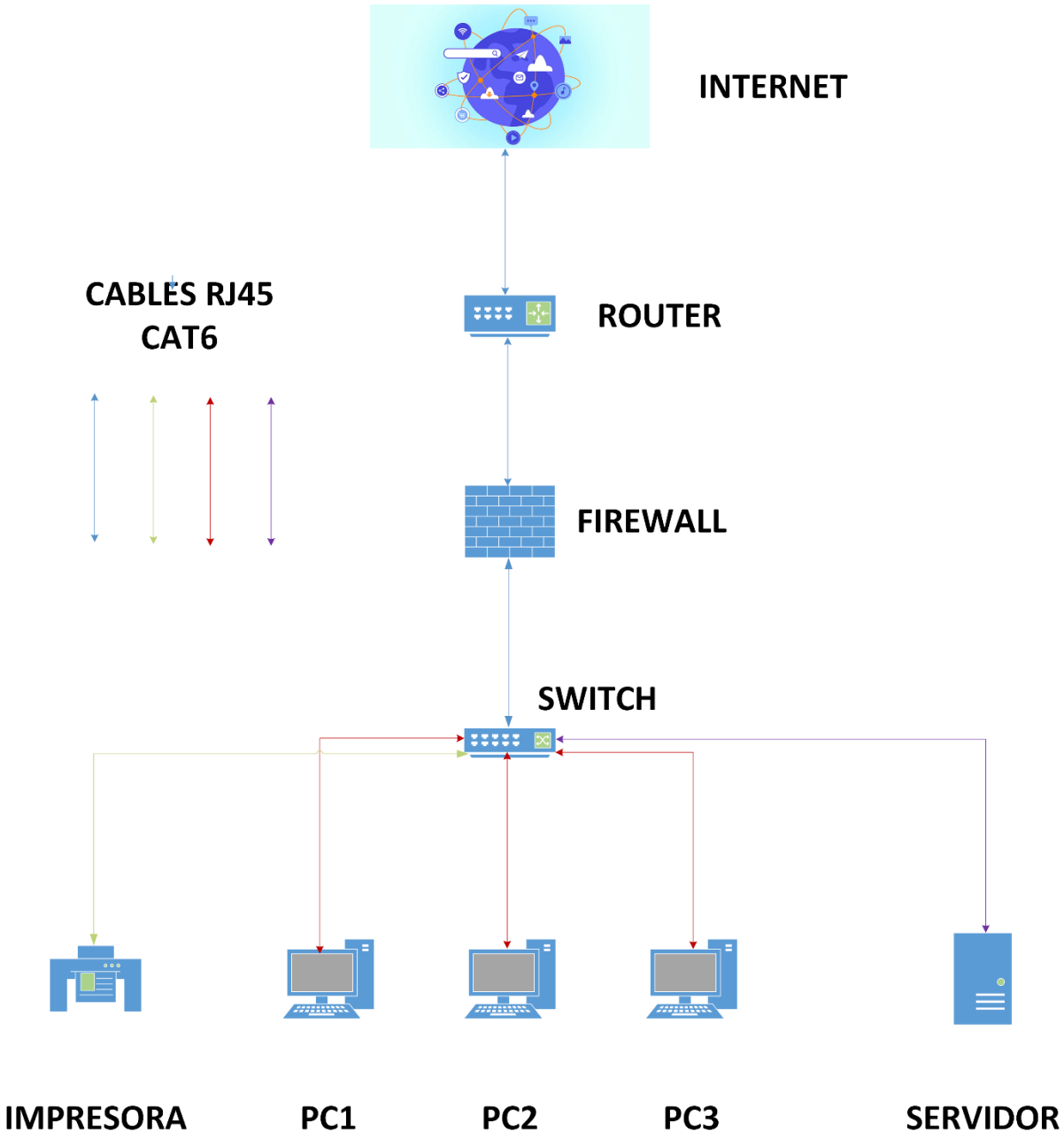
Resumen del Mapa Físico:

- El **router** es el punto central que conecta la red a Internet.
- El **firewall** está posicionado entre el router y el switch para proteger la red interna.
- El **switch** distribuye las conexiones a los dispositivos de la red mediante cables **Ethernet**.
- Los dispositivos, como ordenadores, impresoras y servidores, están conectados físicamente al switch, mientras que los dispositivos Wi-Fi se conectan al router de manera inalámbrica.

Este **mapa físico** describe la disposición de los cables y dispositivos, complementando el **mapa lógico**, que se centra en la configuración de direcciones IP y la estructura de la red.

Este formato resalta las conexiones físicas y su propósito en la red de manera clara y organizada.

SWITCH


INTERNET
CABLES RJ45
CAT6
ROUTER
FIREWALL
SWITCH
IMPRESORA
PC1
PC2
PC3
SERVIDOR

- **Mapa lógico:**
  - El mapa lógico, por otro lado, debe mostrar cómo fluye la información dentro de la red. Este esquema reflejará la asignación de direcciones IP para cada dispositivo, el uso del protocolo TCP/IP para la comunicación entre ellos, y cómo el servidor gestiona y distribuye los recursos. Esto es crucial para garantizar que el tráfico de datos sea eficiente y seguro, permitiendo un control preciso del acceso a la red y a los recursos compartidos.

Direcciones IP Privadas (Red Interna):

- **Ordenadores o dispositivos conectados**: Usan direcciones IP privadas en el rango 192.168.0.x (por ejemplo, 192.168.0.2, 192.168.0.3, etc.).

- **Router**: Suele tener una IP privada como 192.168.1.1 dentro de la red interna, actuando como puerta de enlace para los dispositivos conectados.

- **Firewall**: Tendría una dirección IP dentro del mismo rango de la red interna, como 192.168.0.254, para ser accesible desde dentro de la red y controlar el tráfico.

- **Switch**: Los switches no suelen tener una IP asignada, ya que solo distribuyen el tráfico de red. Sin embargo, si es un switch gestionable, podría tener una IP para su administración, como 192.168.0.253.

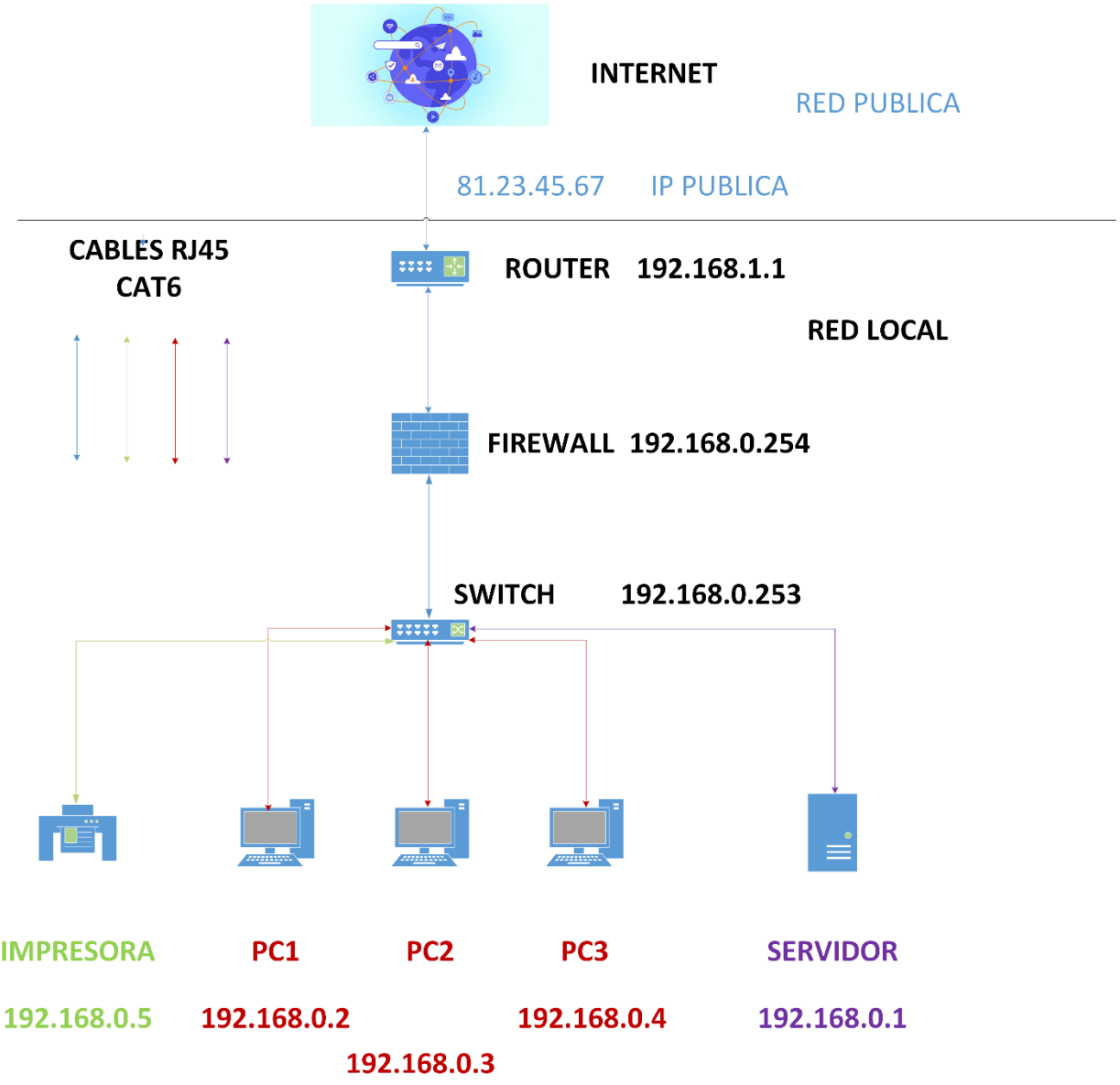
Dirección IP Pública (Red Externa):

- **IP pública del router**: Proporcionada por el ISP (Proveedor de Servicios de Internet), esta dirección IP es la que permite a tu red interna conectarse a Internet. Normalmente tiene el formato de una dirección pública como **81.23.45.67**. A menos que el ISP proporcione una IP estática, esta dirección suele ser dinámica y cambia con el tiempo.

Resumen:

El router es el encargado de gestionar la conversión de las direcciones IP privadas de la red interna (por ejemplo, 192.168.x.x) en una IP pública (como 81.23.45.67) mediante la técnica de **NAT** (Network Address Translation). El **firewall**, ubicado entre el router y la red interna, se encarga de filtrar y proteger el tráfico que entra y sale, asegurando la seguridad de los dispositivos dentro de la red.

De esta forma, los dos mapas combinados ofrecen una visión completa y detallada de la red, tanto en su estructura física como en su funcionamiento lógico, lo que facilita una gestión más eficiente y escalable a medida que la empresa crezca.



05

CONFIGURACIÓN DE REDES Y PROTOCOLO

- **Configuración del protocolo TCP/IP:**
  - Se asignarán direcciones IP a los tres ordenadores y al servidor, utilizando el router para decidir si estas direcciones serán estáticas o dinámicas. Cada equipo será configurado con el protocolo TCP/IP, permitiendo que se comuniquen tanto entre sí como con servidores externos en Internet.

- **Dispositivos de interconexión:**
  - El switch se encargará de gestionar el tráfico entre los dispositivos conectados dentro de la red local, mientras que el router controlará el acceso y las conexiones a Internet desde la red.
  - Además, el firewall será configurado para monitorear y filtrar cualquier tráfico no deseado, protegiendo la red interna de posibles amenazas desde el exterior.

- **Gestión de puertos de comunicación:**
  - Se realizará una configuración básica de los puertos de red, permitiendo que servicios compartidos, como impresoras o servidores de archivos, puedan operar correctamente dentro de la red.

- **Verificación de la red:**
  - Para asegurar que todo funcione de manera óptima, se utilizarán herramientas como ping y tracert que nos permitirán medir la conectividad entre los equipos y la latencia, garantizando que la red esté bien configurada.

- **Aplicación de protocolos seguros:**
  - Se configurará el cortafuegos, y si se considera necesario, se habilitará una VPN (Red Privada Virtual) para asegurar cualquier conexión remota a la red, protegiendo los datos de los usuarios y manteniendo la red segura.

- Este enfoque garantiza que la red funcione de manera eficiente y segura, cumpliendo con los requisitos de la empresa.

- **<u>Configuración y protocolos en detalle:</u>**

  - **Direcciones IP**
    Una dirección IP es un número único que identifica a cada dispositivo dentro de una red. Es similar a una dirección postal que permite localizar cada dispositivo. Existen dos tipos de direcciones IP:
    - **IP pública:** Identifica tu red en Internet, visible desde el exterior.
    - **IP privada:** Utilizada dentro de una red local (LAN) para identificar dispositivos internamente.

    Cada dispositivo en la red necesita una IP única. Por ejemplo, puedes asignar el rango de IPs privadas 192.168.1.x, donde "x" cambia para cada dispositivo (como 192.168.1.1 para el router, 192.168.1.2 para un ordenador, y así sucesivamente).

  - **Configuración de IPs**
    1. **Estática:** Se asigna una dirección IP fija a un dispositivo, que no cambia a menos que lo hagas manualmente. Es ideal para servidores o impresoras.
    2. **Dinámica:** Las IPs se asignan automáticamente mediante el protocolo DHCP, que es más flexible. Sin embargo, no siempre es adecuado para dispositivos que necesitan una IP fija.

  - **Subredes**
    Dividir la red en subredes mejora tanto el rendimiento como la seguridad. Por ejemplo, puedes separar la red de empleados de la red de invitados, usando diferentes subredes: 192.168.1.x para empleados y 192.168.2.x para invitados.

  - **Protocolos**
    Los protocolos son fundamentales para la comunicación en la red. Algunos de los más importantes incluyen:
    - **TCP/IP:** Protocolo básico para la comunicación en Internet y redes internas.

- **DHCP:** Protocolo que asigna direcciones IP de forma automática.
- **DNS:** Traduce los nombres de dominio (como google.com) a direcciones IP.

- **Justificación**:
  La correcta configuración de las IPs y los protocolos es esencial para garantizar que los dispositivos puedan comunicarse sin problemas ni interferencias. Dividir la red en subredes aumenta la seguridad y facilita su gestión. Además, los protocolos permiten que los dispositivos intercambien datos correctamente, asegurando una transmisión fluida de la información.

Explicación en detalle del Rango de direcciones 192.168.0.x

Este rango de direcciones IP pertenece a un conjunto de IPs privadas, según el estándar de la IETF (Internet Engineering Task Force) en el documento RFC 1918. Estas direcciones están reservadas para su uso en redes locales (LAN), lo que significa que no se pueden acceder directamente desde Internet. A continuación, explicamos por qué se usa este rango:

1. **Direcciones IP Privadas**
   Las IPs privadas identifican dispositivos dentro de una red interna, como una red doméstica o empresarial. Existen tres rangos de IPs privadas:
   - 10.0.0.0 – 10.255.255.255 (Clase A)
   - 172.16.0.0 – 172.31.255.255 (Clase B)
   - 192.168.0.0 – 192.168.255.255 (Clase C)

   El rango 192.168.x.x (Clase C) es el más común y suele usarse en redes domésticas o pequeñas oficinas.

2. **Uso del rango 192.168.0.x**
   Este rango, especialmente 192.168.0.x o 192.168.1.x, es muy popular para redes locales por varias razones:
   - Simplicidad: Muchos routers vienen preconfigurados para usar este rango por defecto.
   - Facilidad de configuración: En pequeños entornos de red, este rango es sencillo de implementar.

3. **Separación de redes públicas y privadas**
   Las IPs privadas como las 192.168.x.x no pueden ser accedidas directamente desde Internet, lo que añade una capa de seguridad. Un router actúa como intermediario, usando NAT (Network Address Translation) para gestionar la conexión entre redes privadas y públicas.

4. **Traducción de Direcciones de Red (NAT)**
   El NAT se utiliza en los routers para traducir las IPs privadas (por ejemplo, 192.168.0.5) a una única dirección IP pública que permite a los dispositivos acceder a Internet. Cuando el tráfico regresa, el NAT lo redirige al dispositivo correcto dentro de la red interna.

- **Resumen**
  El rango 192.168.0.x se usa en redes internas porque:
  - Está reservado para uso privado, según el estándar RFC 1918.
  - Es el rango predeterminado en muchos routers.
  - Facilita la configuración de redes pequeñas o medianas.
  - Ayuda a separar las redes privadas de las públicas, mejorando la seguridad y gestión.

ROUTER

0 6

I M P L E M E N T A C I Ó N D E S E G U R I D A D

• **Configuración del Firewall** El firewall se posicionará entre el router y el switch, protegiendo tanto las comunicaciones internas como las externas de la empresa. Su configuración incluirá las siguientes medidas:

1. **Políticas de acceso**:
    - Solo se permitirá el tráfico esencial, como HTTP, HTTPS y SMTP, bloqueando los puertos que no sean necesarios para el funcionamiento de la red.

2. **Control de tráfico**:
    - Se filtrarán los datos según la IP, los puertos y los protocolos, limitando el acceso externo solo a través de una VPN para mayor seguridad.

3. **Monitoreo**:
    - El firewall realizará un monitoreo en tiempo real del tráfico de la red, con registro de actividad y configuración de alertas automáticas para detectar cualquier intento de intrusión.

4. **Segmentación de la red**:
    - La red se dividirá en subredes, lo que permitirá un control más preciso del acceso a las diferentes áreas de la empresa.

5. **Actualizaciones**:
    - El firewall se mantendrá actualizado con las últimas reglas de seguridad para garantizar una protección constante frente a nuevas amenazas.

Justificación del Firewall y Medidas Adicionales

El firewall es esencial para proteger la red contra ataques como el malware y accesos no autorizados. Además de bloquear amenazas externas, también controla el acceso dentro de la propia red, asegurando que las áreas más críticas estén protegidas. Cumple con normativas de seguridad, como el GDPR, y ofrece monitoreo constante del tráfico, con la opción de habilitar VPN para accesos remotos seguros. Para reforzar la seguridad, se complementará con medidas adicionales, como la instalación de antivirus, la aplicación de políticas de contraseñas seguras y el cifrado de datos sensibles.

Con esta combinación de herramientas y prácticas de seguridad, la empresa puede garantizar una red protegida y en cumplimiento con los estándares actuales.

FIREWALL

0 7

P R E S U P U E S T O

1. **Equipos de Red**
   Para crear una red eficiente, se necesita contar con routers, switches y puntos de acceso.
   - **Router principal**: El dispositivo que conecta la red interna a Internet y gestiona el NAT (traducción de direcciones de red).
     - Ejemplo: Router Cisco o TP-Link.
     - **Costo estimado**: Entre 100 y 500 € (dependiendo de la marca y las características). Aunque si contratamos un servicio de fibra, puede ir incluido sin coste.
   - **Switches de red**: Usados para interconectar varios dispositivos en la red interna.
     - Ejemplo: Switch Gigabit de 8+ puertos.
     - **Costo estimado**: De 80 a 300 €, dependiendo de la cantidad de puertos y la velocidad.
   - **Puntos de acceso Wi-Fi**: Si se requiere una red inalámbrica para móviles y otros dispositivos.
     - Ejemplo: Ubiquiti o TP-Link Access Points.
     - **Costo estimado**: Entre 60 y 200 € cada uno (según el alcance y las funciones). Este elemento puede venir incluido en el Router si contratamos un servicio de fibra.

2. **Cableado** Si no es completamente inalámbrica, la red necesita cableado para conectar los dispositivos físicamente.
   - **Cable Ethernet Cat6**: Garantiza conexiones rápidas y estables.
     - **Costo estimado**: De 0,50 a 1 € por metro.
     - **Costo total estimado**: Entre 200 y 500 € para una oficina pequeña o mediana, dependiendo del número de conexiones.

3. **Hardware adicional**
    - **Servidores**: Si se necesita un servidor para gestionar la red, autenticación de usuarios o almacenamiento centralizado.
        - Ejemplo: Servidores Dell o HP.
        - **Costo estimado**: Entre 1.000 y 3.000 €, según la capacidad de almacenamiento, procesador y memoria RAM.

4. **Software y Licencias**
    - **Software de configuración de red**: Si se requiere una gestión centralizada de la red o software de administración.
        - Ejemplo: Cisco Meraki o Ubiquiti UniFi.
        - **Costo estimado**: De 100 a 500 € anuales, según el número de dispositivos gestionados.
    - **Firewall y seguridad de red**: Software para proteger la red de amenazas y malware.
        - **Costo estimado**: De 200 a 1.000 € anuales por las licencias y suscripciones del firewall.

5. **Mano de obra**
    - **Instalación y configuración**: El coste de la mano de obra para diseñar, instalar y configurar la red.
        - **Costo estimado**: Entre 50 y 100 € por hora.
        - **Costo total estimado**: Entre 1.000 y 5.000 € para un proyecto de 20 a 50 horas.

6. **Mantenimiento y Soporte**
    - **Mantenimiento anual**: Incluye actualizaciones de software, monitoreo de la red y soporte técnico.
        - **Costo estimado**: Entre 500 y 2.000 € anuales, dependiendo del tamaño de la red.

Resumen del presupuesto estimado:

Concepto	Costo estimado
Router principal	*100 - 500 €
Switches de red	80 - 300 €
Puntos de acceso Wi-Fi	*60 - 200 € (c/u)
Cableado Ethernet Cat6	200 - 500 €
Servidores	1.000 - 3.000 €
Software de red y licencias	100 - 500 €
Firewall y seguridad	200 - 1.000 €
Mano de obra (instalación)	1.000 - 5.000 €
Mantenimiento anual	500 - 2.000 €

Total estimado: Entre 3.540 y 14.000 €

* Elementos que pueden venir incluidos si contratamos un servicio de fibra.

Este presupuesto puede variar en función de la escala del proyecto, las marcas seleccionadas y las necesidades específicas de la red.
En **nuestro caso**, especificando que contratamos un servicio de fibra y una oficina pequeña, nos **acercamos más a un precio de unos 3500e con un coste mensual de 200e.**

0 8

C O N C L U S I Ó N

En este caso práctico sobre sistemas informáticos, hemos diseñado una red integral para una pequeña empresa, cubriendo tanto sus necesidades de conectividad como de seguridad. Con una cuidadosa selección de hardware, como routers, switches, servidores y cables Ethernet, se ha establecido una infraestructura de red confiable y escalable, preparada para el crecimiento futuro de la empresa.

La elección de una topología en estrella garantiza una estructura organizada y eficiente, lo que facilita el mantenimiento y permite ampliar la red sin mayores complicaciones.

En cuanto a la seguridad, se ha implementado un firewall estratégico entre el router y el switch, asegurando la protección tanto del tráfico interno como de las conexiones externas. La configuración de este firewall, combinada con la segmentación de la red en subredes, ofrece un control detallado sobre los accesos, asegurando la protección de datos sensibles. Además, se han tomado otras medidas de seguridad, como el monitoreo constante del tráfico, la gestión de VPN para un acceso remoto seguro y la aplicación de actualizaciones regulares, lo que protege a la red de amenazas externas e internas.

El diseño propuesto no solo cumple con los requisitos de funcionalidad y seguridad, sino que sigue las mejores prácticas en términos de eficiencia y facilidad de mantenimiento. Este proyecto ofrece una solución robusta y flexible que permitirá a la empresa operar de manera segura y eficiente, al mismo tiempo que le otorga la capacidad de adaptarse a futuras necesidades tecnológicas.

0 9

R E F E R E N C I A S

https://ccnadesdecero.es/router-direccion-192-168-0-1-o-192-168-1-1/

https://www.redeszone.net/tutoriales/configuracion-routers/activar-configurar-firewall-cortafuegos-router-pc/

https://community.fs.com/es/article/network-switch-vs-network-router-vs-network-firewall.html

https://www.fortinet.com/lat/resources/cyberglossary/firewall-configuration

https://miro.com/es/diagrama/que-es-diagrama-red/

https://www.youtube.com/watch?v=Y2L_7ewQteI

https://www.pccomponentes.com/search/?query=redes&fm-390

https://mundowin.com/configuracion-de-redes-informacion-basica-y-conexiones/

https://www.youtube.com/watch?v=awLJkNHBoms

https://www.youtube.com/watch?v=hP459L3FIZ0

https://www.youtube.com/watch?v=1pB2kan_AFk

https://www.dte.us.es/personal/sivianes/TC/P1Enunciado.pdf