|  |  |  |
| --- | --- | --- |
| sistemas informaticos | | CASO PRACTICO 1 |
|  | | |
|  | | |
|  |  | |
| alumno cesur 24/25  Alejandro Muñoz de la Sierra | PROFESOR  Efren Zurita Alonso | |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| contenido | | | | | | |
| 01 |  | 02 |  | 03 |  | 04 |
| introduccion |  | Identificación y selección del hardware y medios de transmisión |  | Topología de la Red |  | Mapas de la Red |
|  |  |  |  |  |  |  |
| 05 |  | 06 |  | 07 |  | 08 |
| Configuración de Redes y Protocolos |  | Implementación de Seguridad |  | Presupuesto del Sistema |  | Conclusión |
|  |  |  |  |  |  |  |
| 09 |  | 10 |  | 11 |  | 12 |
| Chapter 5 |  | Chapter 6 |  | Chapter 7 |  | Chapter 8 |

|  |  |
| --- | --- |
| 01 introduccion |  |
| 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 |  |

**2. Identificación y selección de hardware y medios de transmisión**

* **Hardware necesario:**
  + 1 Switch con capacidad para 5 o más puertos (preferentemente un switch de 5-8 puertos para futuras expansiones).
  + 5 cables de red Ethernet CAT6 para conectar cada ordenador, servidor e impresora al switch.
  + Router con capacidad para gestionar las conexiones de red local y el acceso a Internet.
  + **Firewall:** Dispositivo o software que protege la red de accesos no autorizados.
  + **Servidor:** Equipamiento que actuará como servidor de archivos y aplicaciones.
* **Justificación de elección:**
  + **Switch Gigabit:** Permite la transmisión de datos a altas velocidades entre los equipos, asegurando un rendimiento óptimo para tareas compartidas en la red.
  + **Cables Ethernet CAT6:** Aseguran un alto rendimiento, con capacidad para transmitir datos a velocidades de hasta 1 Gbps, además de ofrecer durabilidad y estabilidad a largo plazo.
  + **Router:** Facilita la conexión a Internet y permite gestionar la asignación de IPs a los dispositivos conectados a la red.
  + **Firewall:** Es esencial para la seguridad de la red, permitiendo filtrar el tráfico y proteger contra amenazas externas. Puede ser un dispositivo físico o software integrado en el router.
  + **Servidor:** Proporciona recursos compartidos (archivos, aplicaciones, impresoras), centralizando la gestión de datos y facilitando el acceso para todos los usuarios de la red.

**3. Determinación de la topología de red**

* **Topología seleccionada:** Estrella.
* **Justificación:**
  + La topología en estrella permite que cada ordenador esté conectado directamente al switch, facilitando la gestión y resolución de problemas en caso de fallo. Además, esta estructura proporciona un rendimiento más rápido y seguro en comparación con otras topologías como la bus.
  + Esta topología facilita la expansión en el futuro, permitiendo agregar más equipos sin afectar a los existentes.

**4. Creación de mapas físicos y lógicos de la red**

* **Mapa físico:**
  + El mapa debe mostrar la disposición de los tres ordenadores, el switch, el router y el firewall. Debe indicar claramente cómo están conectados entre sí utilizando los cables Ethernet.
* **Mapa lógico:**
  + Este mapa debe reflejar la distribución de las direcciones IP, la asignación del protocolo TCP/IP y cómo se gestiona el tráfico entre los dispositivos conectados, incluido el servidor.

**5. Configuración de redes y protocolos**

* **Configuración del protocolo TCP/IP:**
  + Se debe asignar direcciones IP estáticas o dinámicas a los tres ordenadores y al servidor a través del router. Se configurará el protocolo TCP/IP en cada equipo para que puedan comunicarse entre sí y con el servidor de Internet.
* **Dispositivos de interconexión:**
  + El switch gestionará el tráfico entre los equipos locales, y el router gestionará las conexiones externas a Internet.
  + **Firewall:** Configurado para filtrar el tráfico no deseado y proteger la red interna de amenazas externas.
* **Gestión de puertos de comunicación:**
  + Configuración básica de puertos de red para la asignación de servicios compartidos (como una impresora de red o un servidor de archivos).
* **Verificación de la red:**
  + Uso de herramientas como ping y tracert para verificar la conectividad y la latencia de los equipos.
* **Aplicación de protocolos seguros:**
  + Configuración del cortafuegos y habilitación de VPN para asegurar las conexiones remotas, si se considera necesario.

6. **Implementación de Seguridad**

**Configuración del Firewall**

En la planificación de esta red, es esencial implementar un firewall entre el router y el switch para proteger tanto las comunicaciones internas como las externas de la empresa. El firewall actúa como una barrera de seguridad entre la red interna de la organización y las amenazas potenciales del exterior. Su configuración estará orientada a:

1. **Definir políticas de acceso**:
   * Solo permitir tráfico necesario para la operación de la empresa.
   * Bloquear puertos innecesarios que puedan ser utilizados por actores malintencionados.
   * Permitir tráfico entrante únicamente para los servicios esenciales, como la navegación web (HTTP y HTTPS) y el correo electrónico (SMTP, IMAP, POP3).
2. **Control de tráfico**:
   * Filtrar el tráfico que entra y sale de la red según direcciones IP, puertos y protocolos.
   * Limitar el acceso a recursos internos desde ubicaciones externas, permitiendo solo conexiones VPN seguras en caso de acceso remoto.
3. **Monitoreo en tiempo real**:
   * Utilizar las funcionalidades del firewall para registrar y monitorear el tráfico en tiempo real. Esto permitirá detectar comportamientos anómalos y tomar acciones correctivas de manera inmediata.
   * Configurar alertas automáticas para detectar intentos de intrusión o actividad sospechosa.
4. **Segmentación de la red**:
   * Utilizar el firewall para separar la red interna en subredes o VLANs, lo cual mejora la seguridad al controlar el tráfico entre diferentes departamentos o secciones de la empresa.
5. **Política de actualización y mantenimiento**:
   * Implementar un plan de actualización regular para el firmware y las reglas del firewall, garantizando que siempre se utilicen los mecanismos de seguridad más recientes.

**Justificación del uso del Firewall y Medidas de Seguridad Adicionales**

La instalación de un firewall es fundamental para proteger la red empresarial frente a amenazas externas como ataques DDoS, malware y accesos no autorizados. Sin este dispositivo de seguridad, la empresa quedaría vulnerable a ataques que podrían comprometer la integridad de los datos y la operatividad de los servicios.

* **Protección contra ataques externos**: El firewall actúa como la primera línea de defensa, bloqueando intentos de acceso no autorizados que puedan vulnerar los sistemas internos de la empresa. Esto incluye la prevención de intrusiones y la protección contra ataques automatizados.
* **Seguridad en la red interna**: Además de proteger contra amenazas externas, el firewall ayuda a controlar el tráfico dentro de la red interna, evitando que dispositivos o usuarios no autorizados accedan a áreas críticas de la red.
* **Cumplimiento normativo**: En muchas industrias, se exige el uso de firewalls como parte de las normativas de seguridad (como el GDPR o la ISO 27001). La implementación de este dispositivo asegura que la empresa cumpla con los estándares de protección de datos.
* **Monitoreo y análisis del tráfico**: El firewall proporciona información detallada sobre el tráfico de la red, lo que permite identificar intentos de ataque, gestionar ancho de banda y analizar patrones de uso que podrían ser indicativos de amenazas emergentes.
* **Seguridad adicional**: Además del firewall, se recomienda implementar medidas de seguridad complementarias como:
  + **Uso de VPN** para accesos remotos seguros.
  + **Antivirus y sistemas de detección de intrusos (IDS)** en los equipos conectados a la red.
  + **Políticas de contraseñas seguras** y autenticación de dos factores (2FA) para accesos sensibles.
  + **Cifrado de datos sensibles**, tanto en reposo como en tránsito.

Estas medidas, junto con el firewall, aseguran que la red de la empresa funcione de manera segura y eficiente, protegiendo tanto los datos de los clientes como los activos de la organización.

**7.Presupuesto**

**1. Equipos de Red**

Estos incluyen routers, switches, y puntos de acceso necesarios para configurar la red.

* **Router principal**: El dispositivo que conecta la red interna con Internet y gestiona el **NAT**.
  + Ejemplo: **Router Cisco o TP-Link**.
  + Costo estimado: 100 - 500 € (dependiendo de la marca y las características).
* **Switches de red**: Para interconectar múltiples dispositivos dentro de la red interna.
  + Ejemplo: **Switch de 24 puertos Gigabit**.
  + Costo estimado: 80 - 300 € (dependiendo de la cantidad de puertos y la velocidad).
* **Puntos de acceso Wi-Fi**: Si la red incluye conexiones inalámbricas para dispositivos móviles.
  + Ejemplo: **Access Point Ubiquiti o TP-Link**.
  + Costo estimado: 60 - 200 € cada uno (dependiendo del alcance y las características).

**2. Cableado**

El cableado es necesario para conectar los dispositivos a la red física (si no es completamente inalámbrica).

* **Cable Ethernet Cat6**: Para conexiones rápidas y fiables.
  + Costo estimado: 0,50 - 1 € por metro.
  + Total estimado (para una oficina pequeña-mediana): 200 - 500 € (dependiendo de la cantidad de conexiones).

**3. Hardware adicional**

* **Servidores**: Si se necesita un servidor dedicado para la gestión de la red, la autenticación de usuarios o servicios de almacenamiento centralizado.
  + Ejemplo: **Servidor Dell o HP**.
  + Costo estimado: 1.000 - 3.000 € (dependiendo de la capacidad de almacenamiento, procesador, y RAM).
* **Unidades de backup o almacenamiento externo**: Para copias de seguridad o almacenamiento de datos.
  + Ejemplo: **NAS (Network Attached Storage)**.
  + Costo estimado: 300 - 1.000 €.

**4. Software y Licencias**

* **Software de configuración de red**: Si se requiere un sistema de gestión centralizado o software para la administración de la red.
  + Ejemplo: **Cisco Meraki, Ubiquiti UniFi**.
  + Costo estimado: 100 - 500 € anuales (dependiendo del número de dispositivos gestionados).
* **Firewall y seguridad de red**: Para proteger la red de ataques y malware.
  + Costo estimado (software de firewall y suscripción): 200 - 1.000 € anuales.

**5. Mano de obra**

* **Instalación y configuración**: Mano de obra para el diseño, instalación, y configuración de la red.
  + Costo estimado: 50 - 100 €/hora.
  + Total estimado (para un proyecto de 20-50 horas): 1.000 - 5.000 €.

**6. Mantenimiento y Soporte**

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

**Presupuesto total 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 € |
| **Unidades de backup / NAS** | 300 - 1.000 € |
| **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: 3.540 - 14.000 €**

Este presupuesto varía según la escala del proyecto, las marcas elegidas y las necesidades específicas de la red.

--------------------------------------------------------------------------------------------------------

Vamos a desglosar las primeras cuatro secciones para aclararlas y justificar los pasos relacionados con la configuración de redes y el uso de IPs, comenzando por las secciones 3 y 4.

**Sección 1: Identificación de componentes físicos de la red**

En esta sección, debes identificar los componentes que forman la parte física de la red, como routers, switches, cables, servidores y otros dispositivos conectados. Aquí hablamos de los dispositivos tangibles que permiten la conectividad y que forman el hardware necesario para que la red funcione.

**Sección 2: Identificación de componentes lógicos de la red**

Los componentes lógicos son los que permiten la comunicación entre los dispositivos físicos. Aquí entrarían los protocolos (por ejemplo, TCP/IP), el direccionamiento IP (las IPs asignadas a los dispositivos), y el esquema de la red (cómo están conectados los dispositivos lógicamente). Aquí también puedes detallar la segmentación de la red, por ejemplo, la separación en subredes.

**Sección 3: Diseño de la red física y lógica**

Esta sección implica diseñar tanto el mapa físico como el lógico de la red. Veamos cómo hacer esto.

**Mapa físico de la red:**

Este es un diagrama que muestra cómo están conectados los dispositivos entre sí a nivel físico. Los dispositivos incluyen servidores, ordenadores, impresoras, routers y switches, y cómo se conectan usando cables (Ethernet) o de forma inalámbrica. El objetivo es mostrar la estructura de la red, con cada dispositivo ubicado en su espacio físico (por ejemplo, diferentes oficinas o plantas de un edificio).

Justificación:

* El mapa físico es esencial para planificar la infraestructura de la red y evitar interferencias o fallos físicos.
* Facilita la gestión y el mantenimiento de los dispositivos, pues muestra de forma clara dónde se encuentra cada uno.

**Mapa lógico de la red:**

El mapa lógico, por otro lado, muestra cómo se comunican los dispositivos entre sí, independientemente de su ubicación física. Este mapa representa aspectos como:

* **IPs de los dispositivos**: Cada dispositivo en una red tiene asignada una dirección IP única, que sirve para identificarlo. En redes internas (como la que montarías en una empresa), se utilizan direcciones IP privadas (por ejemplo, 192.168.x.x).
* **Rutas de comunicación**: Cómo fluyen los datos entre los dispositivos. Aquí también es importante ver cómo están segmentadas las subredes si es necesario.

Justificación:

* Un mapa lógico es crucial para entender cómo se comporta la red, asegurarse de que los dispositivos se pueden comunicar sin problemas, y planificar la red de manera eficiente.
* Permite implementar seguridad al identificar dónde se pueden aplicar cortafuegos y qué partes de la red deben estar aisladas o protegidas.

**Sección 4: Configuración de la red**

Aquí es donde configuramos las IPs y otros protocolos. Vamos a explicar cómo funcionan y cómo debes abordar esta parte:

**Direcciones IP:**

Una dirección IP es un número único que identifica un dispositivo en la red. Piensa en las IPs como las direcciones postales de los dispositivos. Hay dos tipos de direcciones IP:

* **IP pública**: La que identifica tu red en Internet.
* **IP privada**: La que se usa dentro de una red local (LAN).

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

**Configuración de IPs:**

1. **Estática**: Asignas una dirección IP fija a un dispositivo. Esta IP no cambiará a menos que lo hagas manualmente.
2. **Dinámica**: Las IPs se asignan automáticamente usando el protocolo DHCP. Este es más flexible, pero no siempre adecuado para dispositivos que necesitan una IP fija (como servidores o impresoras).

**Subredes:**

Dividir la red en subredes (o segmentos más pequeños) puede mejorar el rendimiento y la seguridad. Por ejemplo, puedes separar la red de empleados de la red de invitados, usando distintas subredes como 192.168.1.x para empleados y 192.168.2.x para invitados.

**Protocolos:**

Además de las IPs, los protocolos (como **TCP/IP**) definen cómo se comunican los dispositivos en la red. Algunos protocolos a configurar son:

* **TCP/IP**: Es el protocolo básico para la comunicación en Internet y redes internas.
* **DHCP**: Asigna IPs automáticamente.
* **DNS**: Traduce nombres de dominio (como google.com) a direcciones IP.

**Justificación**:

* La correcta configuración de las IPs y protocolos es fundamental para que los dispositivos puedan comunicarse sin interferencias.
* El uso de subredes mejora la seguridad y organiza mejor la red.
* Los protocolos de red permiten que los dispositivos entiendan cómo deben intercambiar los datos, asegurando la correcta transmisión de la información.

Con esta información deberías tener una idea clara para abordar las secciones 3 y 4 en tu caso práctico, enfocando la justificación en cómo estas configuraciones mejoran la comunicación, la seguridad y el rendimiento de la red.

El rango de direcciones **192.168.0.x** pertenece a un conjunto de direcciones IP definidas como **privadas** según los estándares de la **IETF (Internet Engineering Task Force)** en el documento **RFC 1918**. Estas direcciones privadas están reservadas para su uso en redes locales (LAN), lo que significa que no se pueden enrutar directamente en Internet. Aquí te explico por qué se utiliza este rango:

**1. Direcciones IP Privadas**

Las direcciones IP privadas se utilizan para identificar dispositivos dentro de una red interna, como una red doméstica o la red de una empresa. Existen tres rangos de direcciones IP 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 uno de los más comunes y se suele utilizar en pequeñas redes domésticas y oficinas.

**2. Uso del rango 192.168.0.x**

Dentro de este rango, **192.168.0.x** o **192.168.1.x** es muy popular para redes locales porque:

* **Simplicidad y Estándar**: Muchos routers y dispositivos de red vienen configurados por defecto para usar direcciones dentro del rango 192.168.0.x o 192.168.1.x, como **192.168.0.1** o **192.168.1.1** para el propio router.
* **Facilidad de Configuración**: Para pequeños entornos de red (hogares, pequeñas empresas), este rango es sencillo de implementar sin chocar con otras configuraciones comunes.

**3. Separación de Redes Públicas y Privadas**

Las direcciones IP privadas, como las **192.168.x.x**, no pueden ser accedidas directamente desde Internet. Esto añade una capa de seguridad porque no puedes enviar datos directamente desde una IP pública a una IP privada sin que exista un router que actúe como intermediario, normalmente usando **NAT (Network Address Translation)**.

**4. Traducción de Direcciones de Red (NAT)**

El **NAT** se utiliza en los routers para traducir las direcciones IP privadas (por ejemplo, **192.168.0.5**) en una única dirección IP pública que permite que los dispositivos en la red interna accedan a Internet. Cuando el tráfico regresa, el NAT vuelve a traducir la IP pública a la IP privada correspondiente en la red interna.

**Resumen**

El rango **192.168.0.x** se utiliza en redes internas porque:

* Está reservado para uso privado (según el RFC 1918).
* Es uno de los rangos predeterminados en muchos routers.
* Ayuda a separar las redes privadas de las públicas.
* Facilita la configuración de redes pequeñas y medianas.

Para elaborar un presupuesto para la implementación de un sistema de red basado en el caso práctico, que utilice el rango de direcciones IP privadas **192.168.0.x**, podemos considerar los siguientes elementos clave:

La colocación del firewall en una red empresarial es crucial para la seguridad, y puede hacerse de las siguientes maneras:

**1. Entre el Router y el Switch**

* **Descripción**: El firewall se conecta directamente al router, y luego el switch se conecta al firewall.
* **Ventajas**:
  + **Control centralizado**: Permite inspeccionar y filtrar todo el tráfico que entra y sale de la red antes de llegar a los dispositivos internos.
  + **Seguridad adicional**: Ofrece una capa de seguridad que protege todos los dispositivos conectados al switch, ya que todos deben pasar por el firewall.
  + **Facilidad para gestionar políticas de seguridad**: Puedes establecer reglas de seguridad que apliquen a todos los dispositivos conectados a la red.

**2. Entre el Firewall y el Router**

* **Descripción**: En este caso, el firewall está conectado a Internet y el router se conecta al firewall.
* **Ventajas**:
  + **Aislamiento**: Ayuda a proteger el router de ataques externos, permitiendo que solo el firewall interactúe directamente con Internet.
  + **Protección adicional para el router**: En caso de que el router tenga vulnerabilidades, el firewall actúa como una barrera de protección.
  + **Gestión de tráfico de red**: Puedes gestionar el tráfico y aplicar políticas de seguridad antes de que llegue al router.

**Recomendación General**

* **Implementación común**: En entornos empresariales, es común tener un firewall **entre el router y el switch**. Esto permite proteger toda la red interna, controlar el tráfico y gestionar la seguridad de manera eficiente.
* **Configuraciones avanzadas**: En algunas implementaciones más complejas, puede ser necesario tener firewalls adicionales en diferentes puntos de la red para proteger segmentos específicos.

**Consideraciones Finales**

* **Tipo de firewall**: Es importante elegir un firewall adecuado, que pueda manejar el tráfico de red, ofrezca características de seguridad robustas (como filtrado de paquetes, detección de intrusiones, VPN, etc.) y que sea escalable para futuras necesidades.
* **Configuración**: Asegúrate de configurar adecuadamente las políticas de seguridad del firewall para proteger la red de amenazas externas, permitiendo solo el tráfico necesario.

7. Presupuesto

Si decides ubicar el firewall entre el router y el switch, protegerá el tráfico que va hacia y desde el switch, lo que también es efectivo, pero menos común.

**Presupuesto y Configuración**

Aquí hay una propuesta de presupuesto y configuración que incluye un firewall:

**1. Equipos de red:**

* **Router:** 1 unidad (ejemplo: Cisco, TP-Link, etc.)
* **Switch:** 1 unidad (ejemplo: 24 puertos, marca específica)
* **Firewall:** 1 unidad (ejemplo: Fortinet, pfSense, etc.)
* **Cables de red (Cat6 o superior):** Cantidad según la configuración (ejemplo: 20 cables de 1 metro)

**2. Costos estimados:**

* **Router:** $100 - $300
* **Switch:** $150 - $500
* **Firewall:** $200 - $600 (dependiendo del modelo y las capacidades)
* **Cables de red:** $50 - $100
* **Otros (instalación, configuración):** $100 - $300 (opcional, si decides contratar a un profesional)

**Total estimado**

**Total:** $700 - $1800 (dependiendo de las marcas y modelos elegidos)

**Configuración básica**

* **Ubicación del Firewall:**
  + Colocarlo entre el router e Internet, para proteger toda la red local.
* **Configuración del Firewall:**
  + Definir reglas para permitir o bloquear el tráfico basado en IP, puertos y protocolos.
  + Configuración de VPN, si es necesario, para acceso remoto seguro.
* **Configuración del Router:**
  + Asignación de IPs estáticas para servidores o equipos críticos.
  + Configuración de DHCP para equipos que no requieren IP fija.

**Consideraciones adicionales**

* **Seguridad:** Asegúrate de que el firewall tenga características de seguridad avanzadas, como detección de intrusiones (IDS/IPS).
* **Monitoreo:** Implementar un sistema de monitoreo para revisar el tráfico y las alertas de seguridad.

Sí, en una configuración de red típica para una empresa, es común tener un servidor que actúe como un recurso centralizado para varios propósitos. Aquí te explico la función y la ubicación de un servidor en la red:

**Funciones del Servidor**

1. **Servidor de archivos:**
   * Almacena y gestiona documentos y archivos compartidos entre los usuarios de la red.
   * Permite que varios usuarios accedan a los mismos archivos simultáneamente.
2. **Servidor de aplicaciones:**
   * Aloja aplicaciones empresariales, como sistemas de gestión (ERP, CRM, etc.).
   * Permite que los usuarios accedan a aplicaciones a través de la red.
3. **Servidor web:**
   * Aloja sitios web internos (intranet) o externos.
   * Proporciona contenido a través del protocolo HTTP/HTTPS.
4. **Servidor de base de datos:**
   * Almacena y gestiona bases de datos utilizadas por aplicaciones empresariales.
   * Permite la consulta y manipulación de datos desde otros sistemas.
5. **Servidor de correo:**
   * Gestiona el envío y recepción de correos electrónicos dentro de la organización.

**Ubicación en la Red**

* **Entre el Router y los Equipos:**
  + El servidor generalmente se conecta al switch, que a su vez está conectado al router.
  + Esto permite que todos los dispositivos en la red local (PCs, impresoras, etc.) se comuniquen con el servidor de manera eficiente.

**Ejemplo de Configuración de Red**

Markdown

Copiar código

Internet

|

Router

|

Firewall

|

Switch

/ | \

PC1 PC2 Servidor

**Presupuesto Adicional para el Servidor**

Si decides incluir un servidor en tu red, aquí hay un ejemplo de presupuesto para un servidor básico:

**1. Servidor:**

* **Servidor físico:** $500 - $2000 (dependiendo de la capacidad y la marca).
* **Sistema operativo:** $100 - $300 (licencias de Windows Server o Linux).
* **Software adicional:** $200 - $500 (dependiendo de las aplicaciones que necesites).

**Total estimado para el Servidor**

**Total:** $800 - $2800 (dependiendo de la configuración y necesidades).

**Consideraciones**

* **Mantenimiento:** Asegúrate de incluir un plan de mantenimiento para el servidor.
* **Seguridad:** Implementa medidas de seguridad como copias de seguridad regulares y actualizaciones de software.

Si necesitas más detalles sobre la configuración del servidor o el presupuesto, no dudes en preguntar.