MINISTERIO DEL PODER POPULAR PARA LA EDUCACIÓN UNIVERSITARIA

UNIVERSIDAD RAFAEL URDANETA

FACULTAD DE INGENIERÍA

CÁTEDRA: PLANIFICACION Y ADMINISTRACION DE REDES DE COMUNICACIONES

PERIODO: 2024-A

PROFESOR: HALLER BRACHO

PROYECTO

PLANIFICACION Y ADMINISTRACION DE REDES DE COMUNICACIONES

Integrantes

Vargas, Wanfredo - C.I. 29.977.093

Jaraba, Luis - C.I. 30.200.228

Crespo, Luis - C.I. 30.167.842

TOPOLOGIA DE LA RED

La topología es la forma en que se conectan los dispositivos de red entre sí, y es necesario el tener que conectar cinco oficinas que usan diferentes medios de transmisión (fibra óptica, Fast Ethernet, inalámbrico y ADSL) y que estos tienen diferentes números de usuarios y equipos. Además, es necesario tener en cuenta la seguridad, la segmentación y los servicios externos que se quieren ofrecer.

La topología consiste en conectar cada oficina con el centro de datos mediante un router y un switch. El router se encarga de establecer la conexión WAN con el centro de datos, usando el medio de transmisión adecuado para cada oficina. El switch se encarga de distribuir la conexión LAN entre los equipos de cada oficina, usando la tecnología Gigabit Ethernet. El centro de datos se conecta con el ISP de fibra, que a su vez se conecta con Internet. El centro de datos también aloja el servidor DNS que provee de servicio a todas las oficinas.

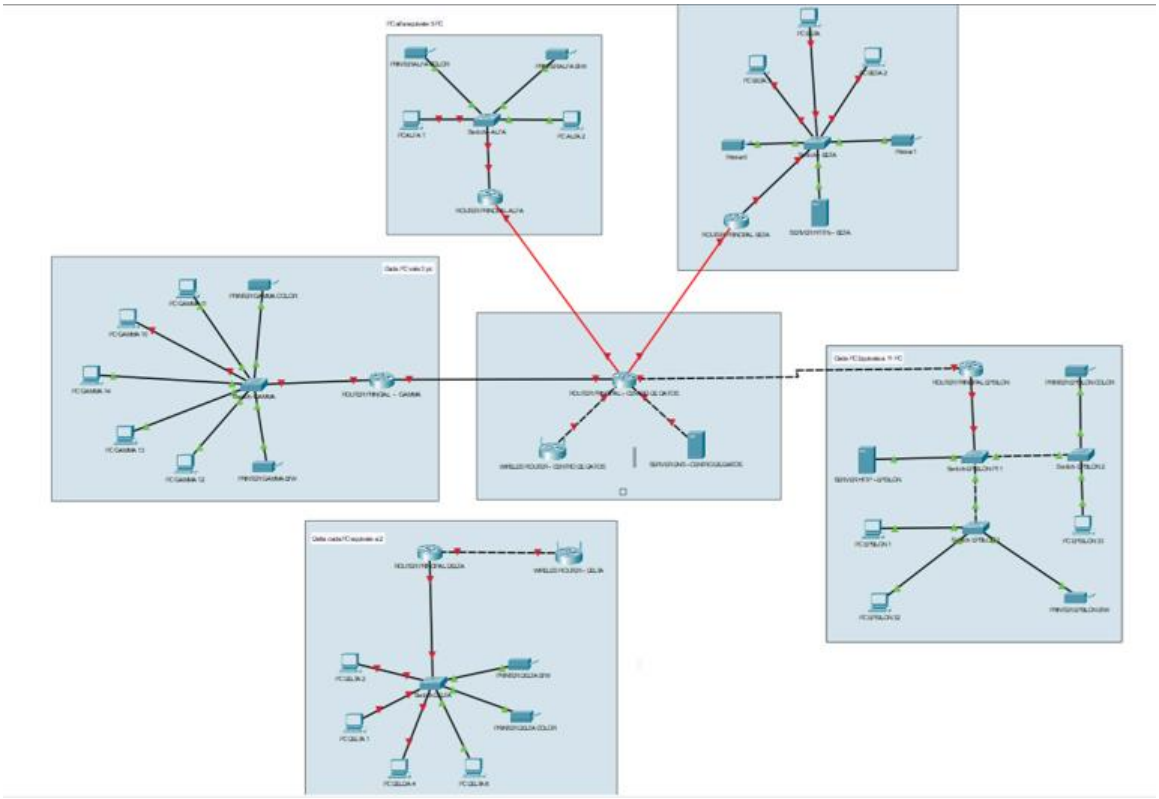
Esta topología tiene varias ventajas:

- Permite aprovechar las diferentes tecnologías WAN disponibles para cada oficina, sin necesidad de homogeneizarlas.
- Permite tener una conexión LAN de alta velocidad y calidad en cada oficina, usando el estándar Gigabit Ethernet.
- Permite tener un punto centralizado de gestión y control de la red, el centro de datos, donde se puede implementar la seguridad, la segmentación y los servicios externos.
- Permite tener una escalabilidad y flexibilidad de la red, ya que se puede añadir o quitar oficinas, equipos o servicios sin afectar al resto de la red.

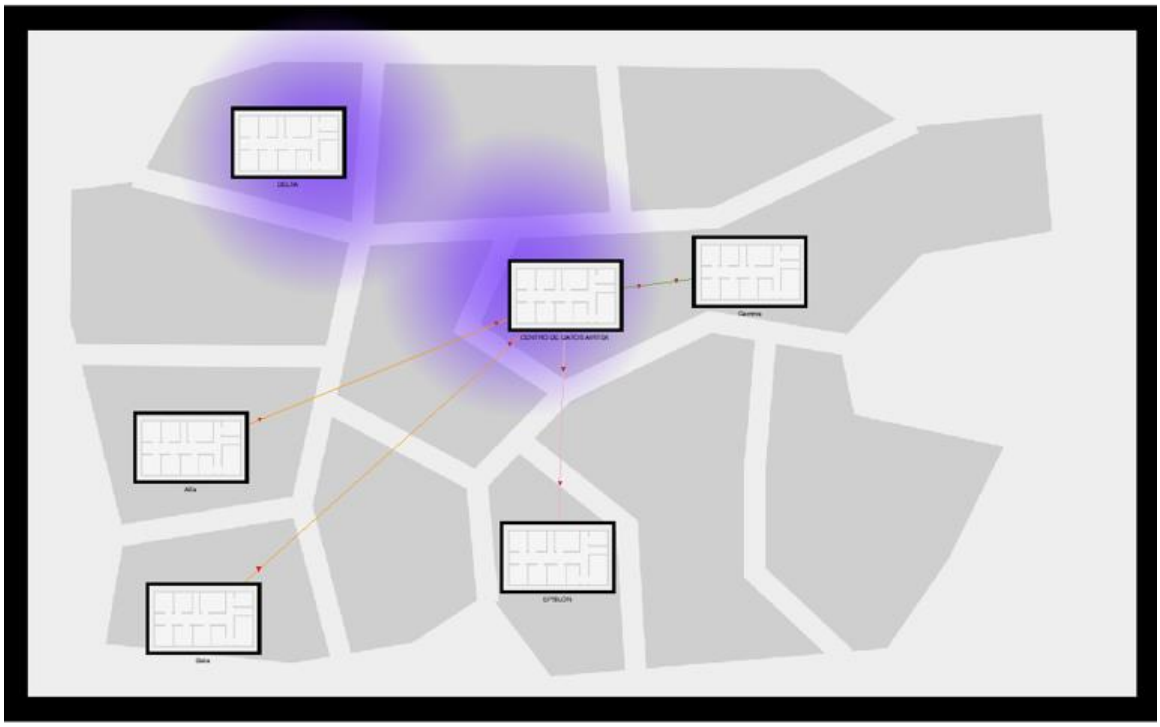
Esta topología también tiene algunos inconvenientes:

- Requiere de una inversión inicial en dispositivos de red, como routers, switches y servidores, así como en el alquiler de las líneas WAN y el espacio en el centro de datos.
- Requiere de un mantenimiento y una configuración adecuados de los dispositivos de red, para garantizar el funcionamiento óptimo y la seguridad de la red.
- Requiere de una coordinación y una comunicación entre las diferentes oficinas y el centro de datos, para resolver posibles incidencias o cambios en la red.

DIAGRAMA COMPLETO



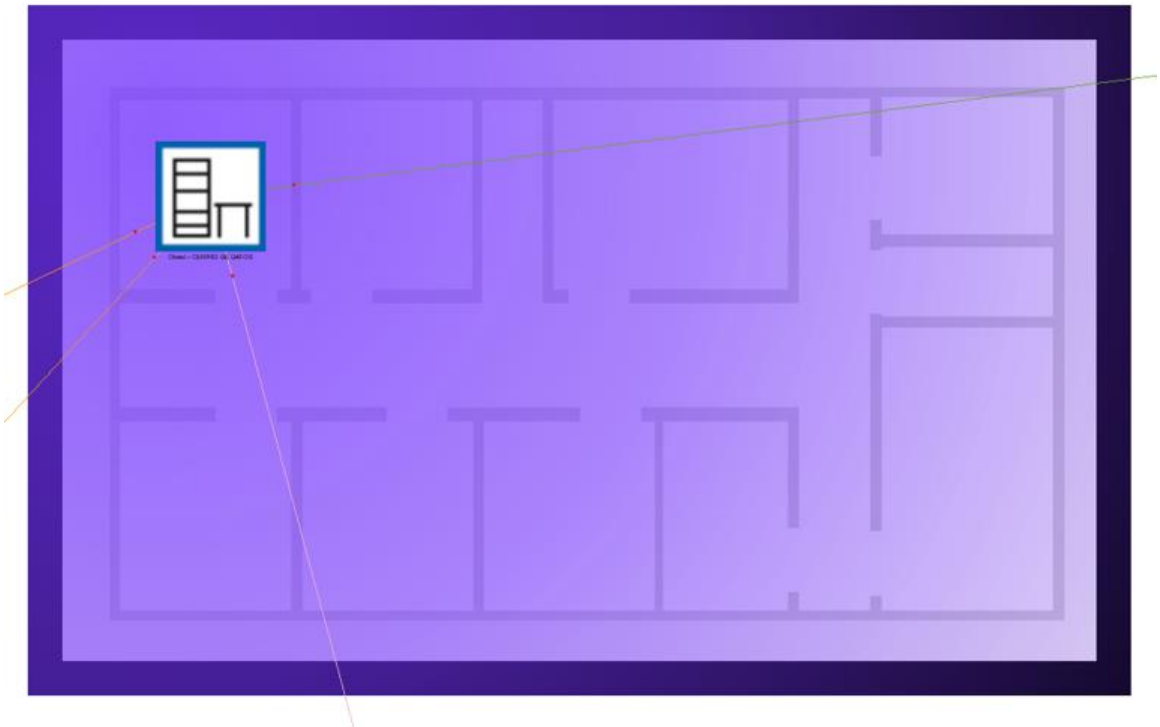
TOPOLOGIA LOGICA



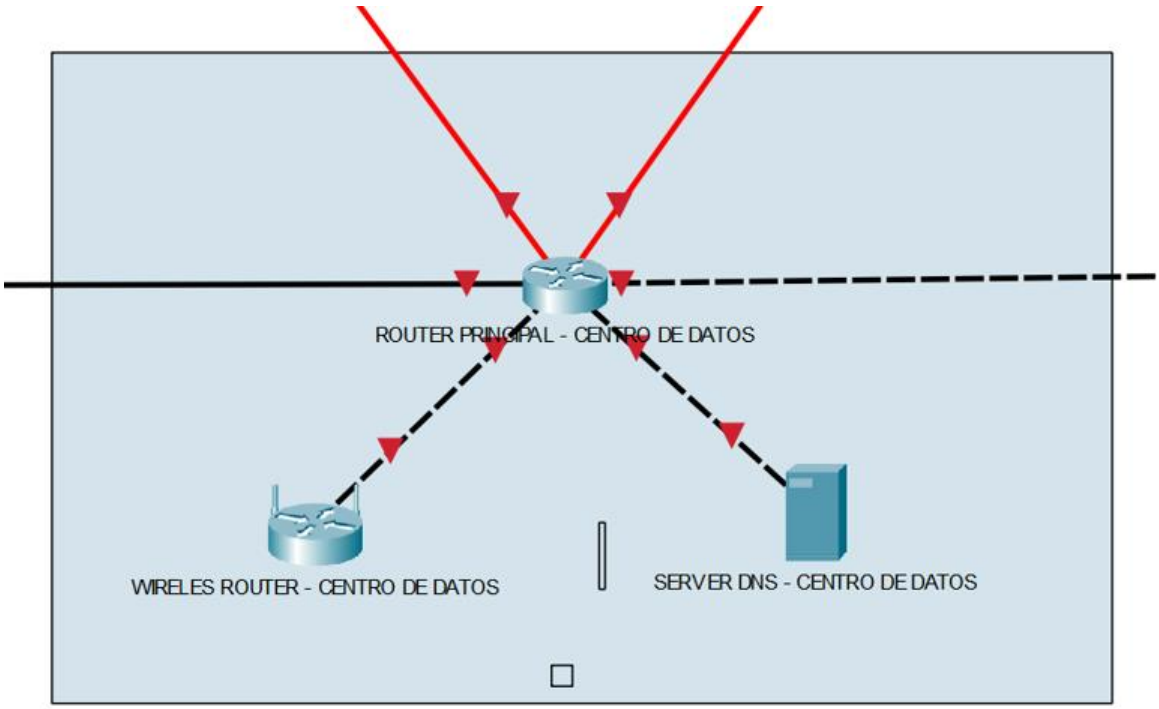
TOPOLOGIA FISICA - CABLEADO

DIAGRAMA ESPECIFICO

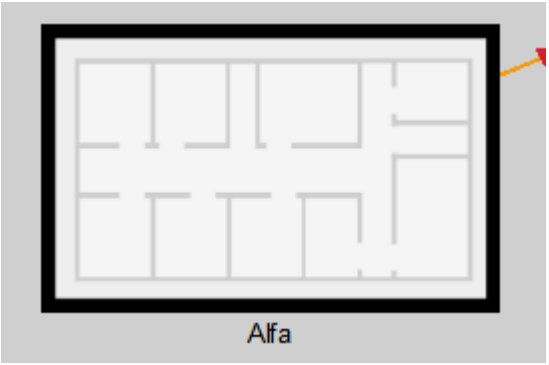
OFICINA DE CENTRO DE DATOS - FISICA



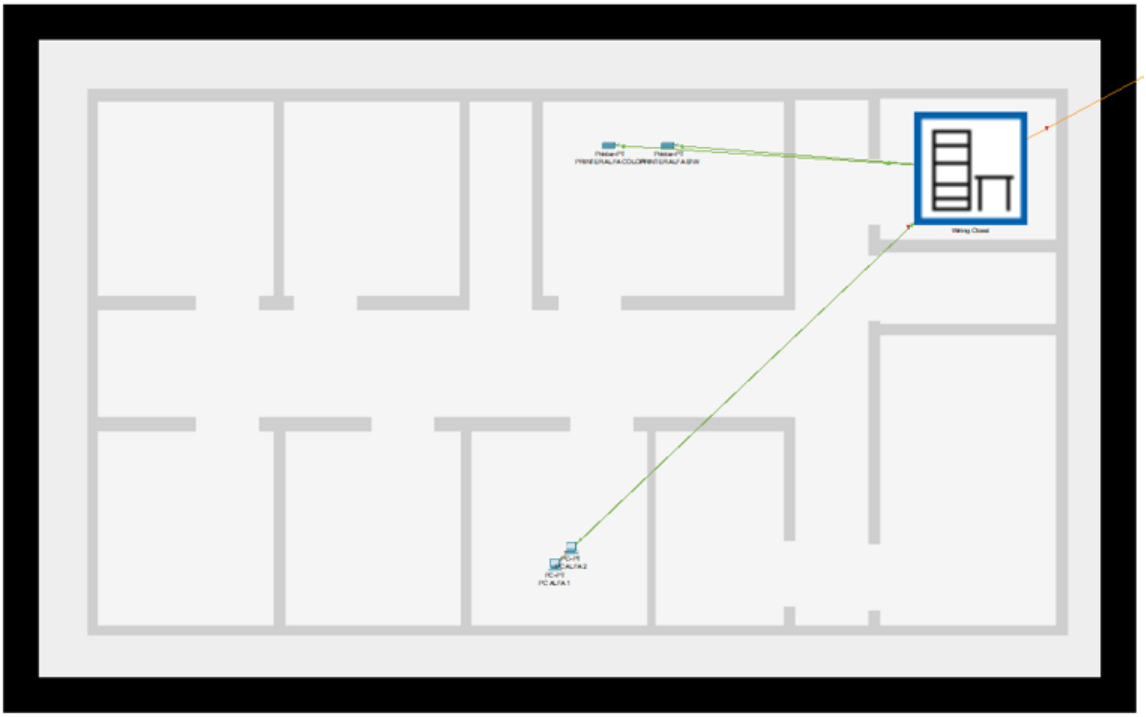
OFICINA DE CENTRO DE DATOS - INTERNA



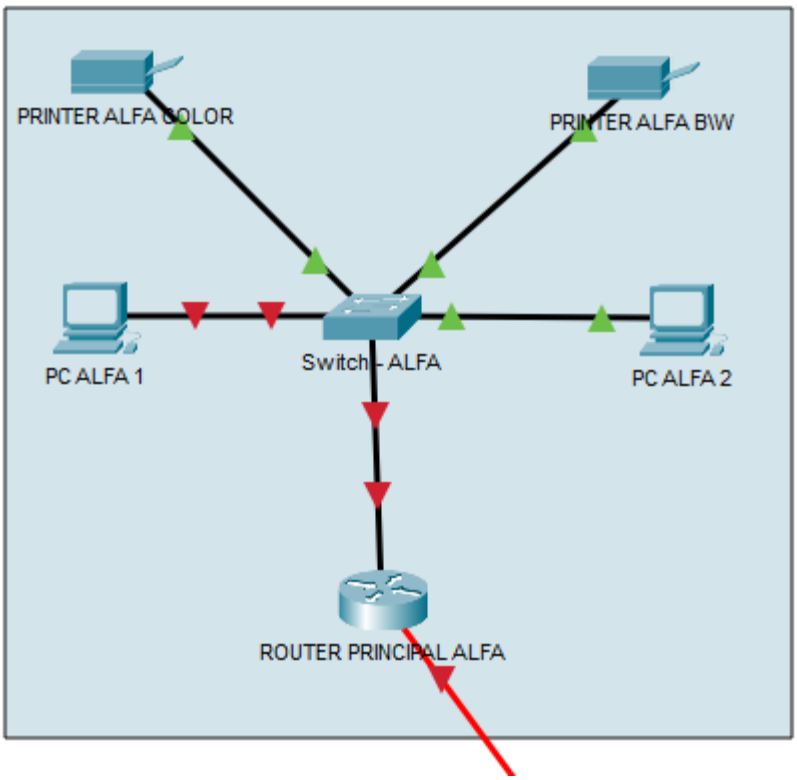
OFICINA DE CENTRO DE DATOS - LOGICA



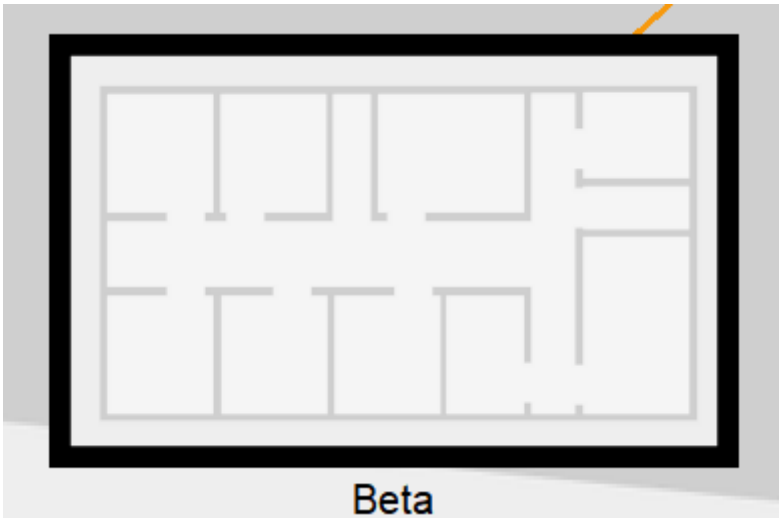
OFICINA ALFA - FISICA



OFICINA ALFA - INTERNA

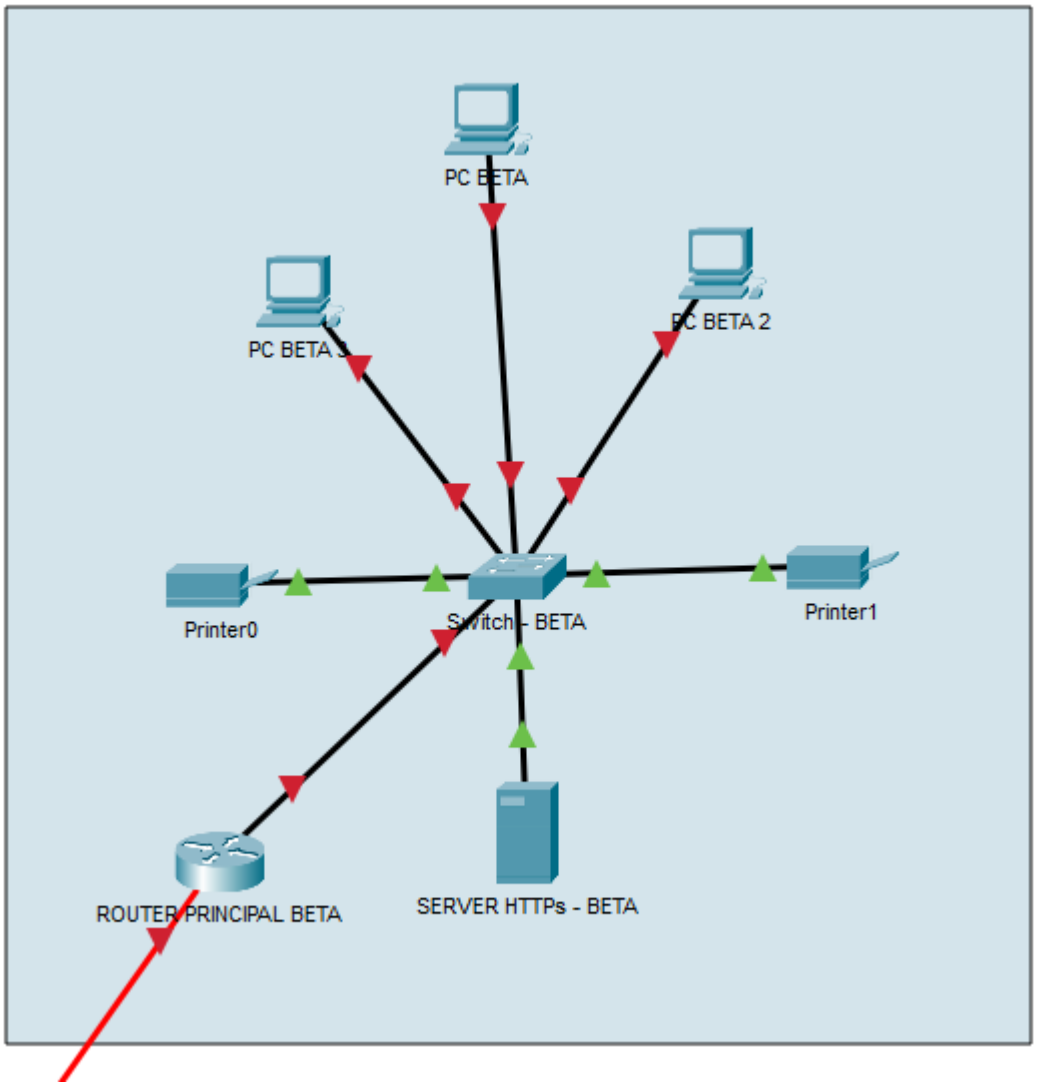


OFICINA ALFA - LOGICA

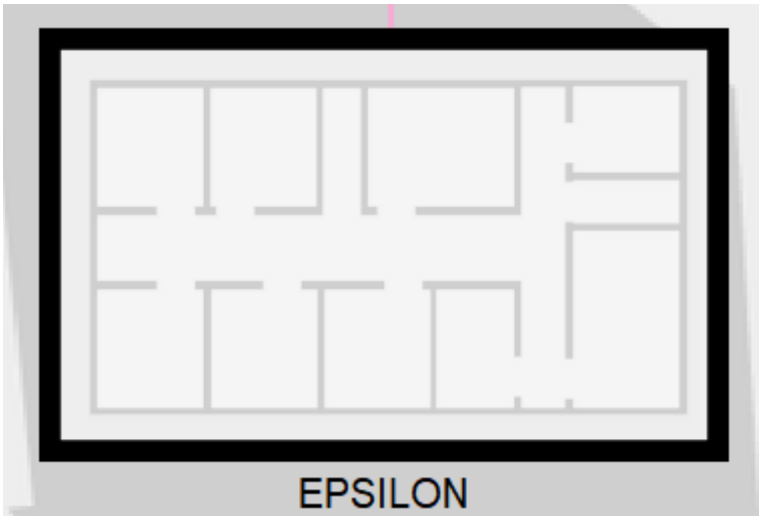


OFICINA BETA - FISICA

OFICINA BETA - INTERNA

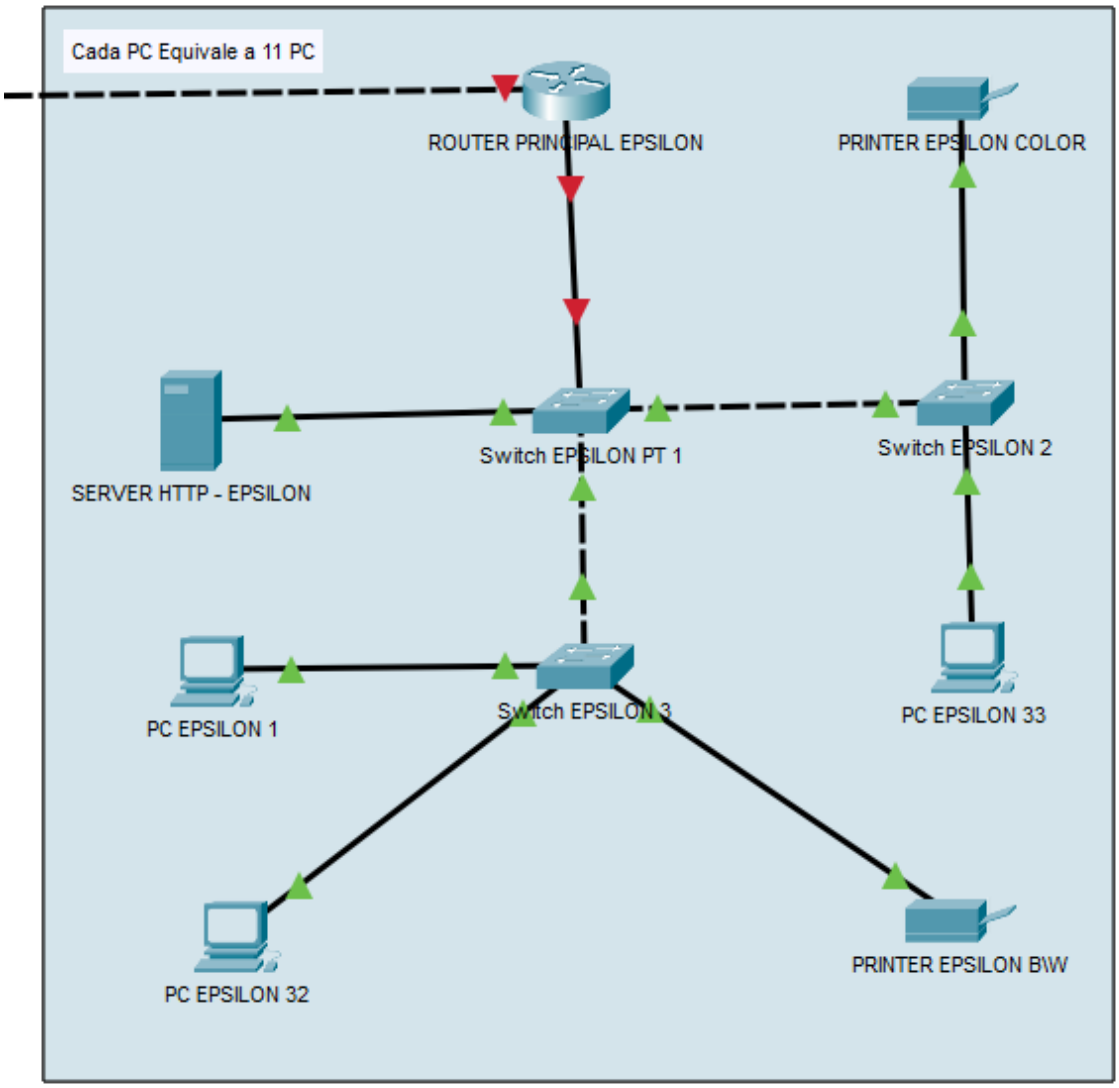


OFICINA BETA - LOGICA



OFICINA EPSILON FISICA

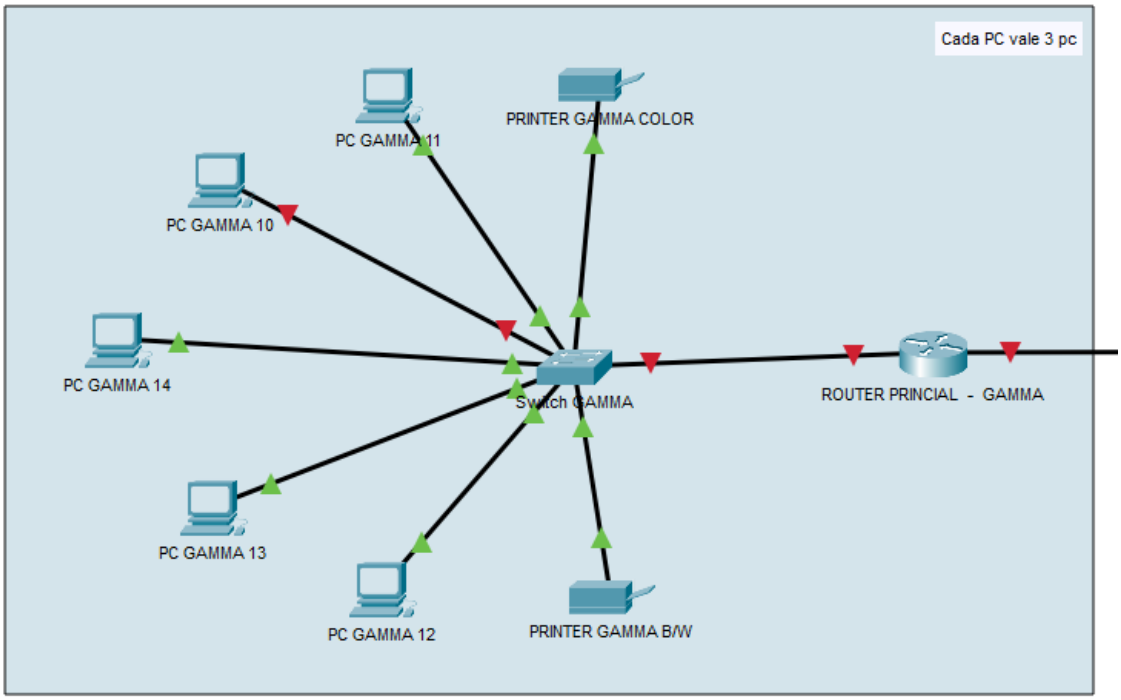
OFICINA EPSILON - INTERNA



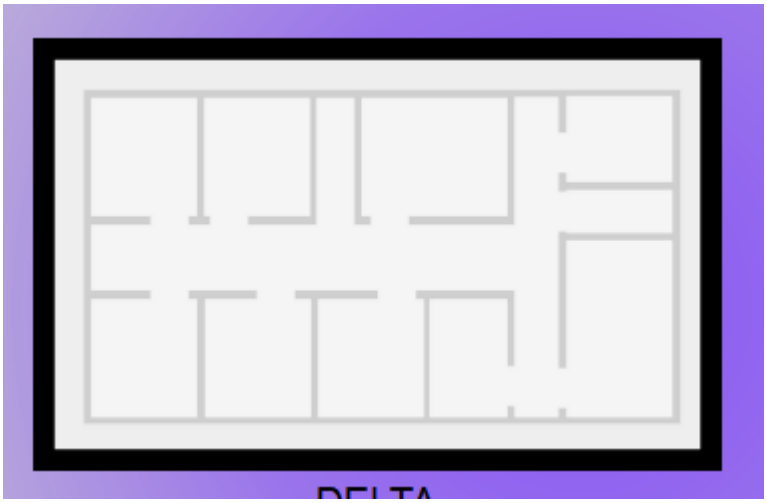
OFICINA EPSILON - LOGICA

OFICINA GAMMA - FISICA

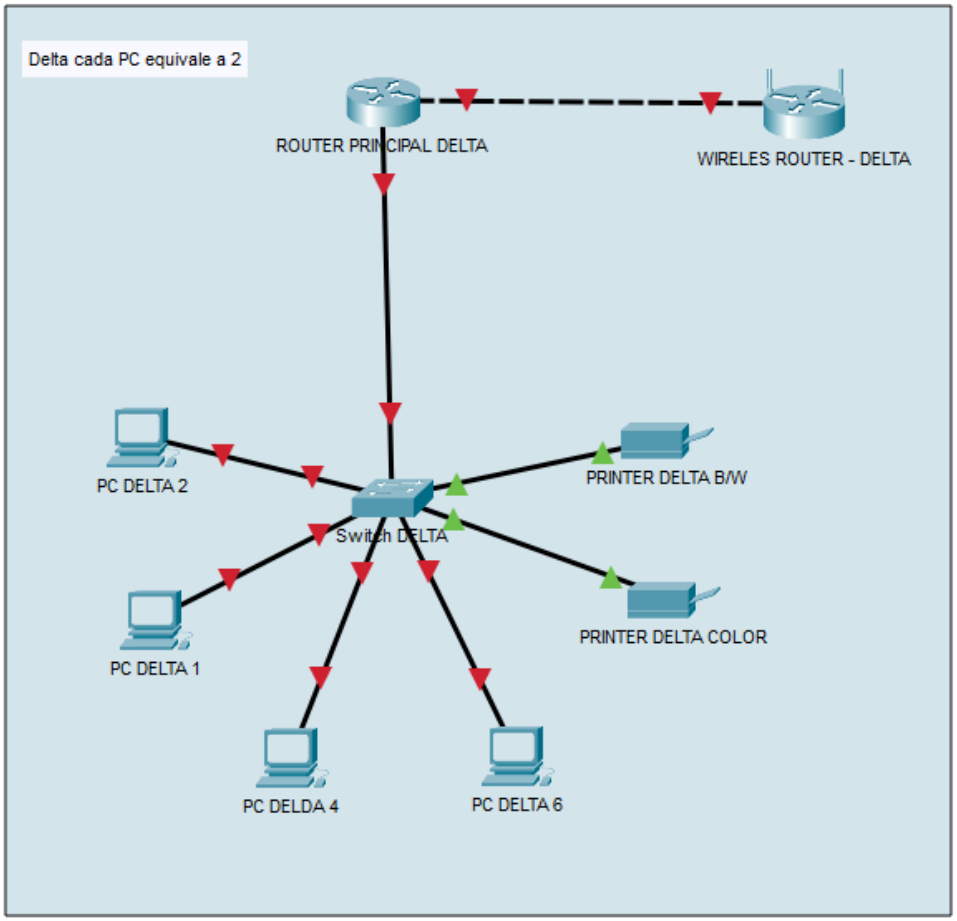
OFICINA GAMMA - INTERNA



OFICINA GAMMA - LOGICA



OFICINA DELTA - FISICA



OFICINA DELTA – LOGICA

ELEMENTOS DE LA RED

Los dispositivos de interconexión aquellos que permiten conectar los equipos de una red entre sí, y con otras redes. Los principales dispositivos de interconexión que se usarán en este proyecto son los siguientes:

- Router: Es un dispositivo que se encarga de enrutar los paquetes de datos entre redes diferentes, usando direcciones IP. Los routers se usan para establecer las conexiones WAN entre las oficinas y el centro de datos, y entre el centro de datos y el ISP de fibra. Los routers también se usan para implementar la seguridad y la segmentación de la red, mediante el uso de listas de control de acceso (ACL), NAT y subredes. Los routers que se usarán en este proyecto son los siguientes:
    - Router Delta: La oficina Delta al ser de enlace inalambrico, utiliza el router wrt300n es un router inalámbrico que soporta el estándar 802.11n draft, que ofrece velocidades de hasta 300 Mbps y un mayor alcance que el 802.11g. El router wrt300n tiene 4 puertos LAN Fast Ethernet y un puerto WAN Fast Ethernet para conectar con el centro de datos. El router wrt300n también tiene una antena MIMO de tres elementos que mejora la cobertura y la calidad de la señal inalámbrica. El router wrt300n funciona con el software Linksys y ofrece funciones de configuración y seguridad de la red, como la interfaz web, el asistente de instalación, el filtrado MAC, el firewall SPI, el VPN pass-through, el WPA2 y el WPS. El router wrt300n también permite el control parental, el QoS, el UPnP y el DDNS.
    - Router alfa: Es el router que conecta la oficina alfa con el centro de datos, usando un enlace de fibra óptica. Este router tiene dos interfaces: una interfaz GigabitEthernet que se conecta con el switch alfa, y una interfaz Serial que se conecta con el centro de datos. Este router tiene asignada la dirección IP 172.16.0.1/23 en su interfaz GigabitEthernet, y la dirección IP 150.185.222.1/29 en su interfaz Serial. Este router también hace NAT con sobrecarga para permitir el acceso a Internet de los equipos de la oficina alfa, usando la dirección IP pública 150.185.222.1.
    - Router beta: Es el router que conecta la oficina beta con el centro de datos, usando un enlace de fibra óptica. Este router tiene dos interfaces: una interfaz GigabitEthernet que se conecta con el switch beta, y una interfaz Serial que se conecta con el centro de datos. Este router tiene asignada la

dirección IP 172.16.2.1/23 en su interfaz GigabitEthernet, y la dirección IP 150.185.222.2/29 en su interfaz Serial. Este router también hace NAT con sobrecarga para permitir el acceso a Internet de los equipos de la oficina beta, usando la dirección IP pública 150.185.222.2. Además, este router tiene configuradas unas ACL para permitir el acceso externo al servidor HTTPS de la oficina beta, usando la dirección IP pública 150.185.222.3.

- Router gamma: Es el router que conecta la oficina gamma con el centro de datos, usando un enlace Fast Ethernet. Este router tiene dos interfaces: una interfaz FastEthernet que se conecta con el switch gamma, y una interfaz Serial que se conecta con el centro de datos. Este router tiene asignada la dirección IP 172.16.4.1/23 en su interfaz FastEthernet, y la dirección IP 150.185.222.4/29 en su interfaz Serial. Este router también hace NAT con sobrecarga para permitir el acceso a Internet de los equipos de la oficina gamma, usando la dirección IP pública 150.185.222.4.
- Router epsilon: Es el router que conecta la oficina epsilon con el centro de datos, usando un enlace ADSL. Este router tiene dos interfaces: una interfaz Ethernet que se conecta con el switch epsilon, y una interfaz ATM que se conecta con el centro de datos. Este router tiene asignada la dirección IP 172.16.8.1/23 en su interfaz Ethernet, y la dirección IP 150.185.222.6/29 en su interfaz ATM. Este router también hace NAT con sobrecarga para permitir el acceso a Internet de los equipos de la oficina epsilon, usando la dirección IP pública 150.185.222.6. Además, este router tiene configuradas unas ACL para permitir el acceso externo al servidor HTTP de la oficina epsilon, usando la dirección IP pública 150.185.222.7.
- Router centro de datos: Es el router que conecta el centro de datos con el ISP de fibra, usando un enlace de fibra óptica. Este router tiene dos interfaces: una interfaz GigabitEthernet que se conecta con el servidor DNS, y una interfaz Serial que se conecta con el ISP de fibra. Este router tiene asignada la dirección IP 172.16.10.1/23 en su interfaz GigabitEthernet, y la dirección IP 150.185.222.8/29 en su interfaz Serial. Este router también hace NAT con sobrecarga para permitir el acceso a Internet del servidor DNS, usando la dirección IP pública 150.185.222.8. Además, este router tiene configuradas unas ACL para permitir el acceso externo al servidor DNS, usando la dirección IP pública 150.185.222.8.

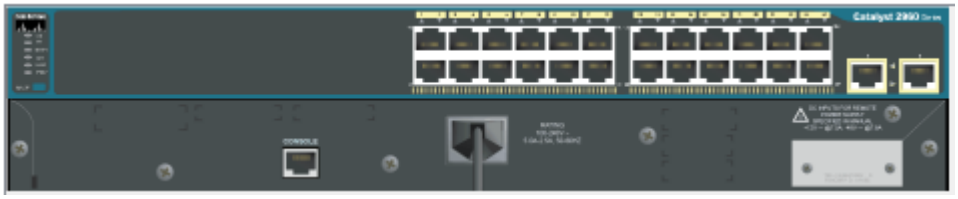
- Switch: Es un dispositivo que se encarga de conmutar los paquetes de datos entre los equipos de una misma red, usando direcciones MAC. Los switches se usan para distribuir la conexión LAN entre los equipos de cada oficina, usando la tecnología Gigabit Ethernet. Los switches también se usan para implementar la segmentación de la red, mediante el uso de VLANs. Los switches que se usarán en este proyecto son los siguientes:
    - El switch utilizado para cada oficina es el Cisco 2960 es un conmutador de capa 2 que ofrece 24 o 48 puertos Gigabit Ethernet con una velocidad de línea. También tiene 4 puertos SFP fijos de 1 Gigabit o 2 puertos SFP+ fijos de 10 Gigabit para conectar con otros dispositivos de red. El switch Cisco 2960 soporta PoE+ con un presupuesto de hasta 740W y PoE perpetuo, lo que permite alimentar dispositivos como teléfonos IP, cámaras de seguridad o puntos de acceso inalámbricos. El switch Cisco 2960 funciona con el software Cisco IOS y ofrece funciones de gestión de dispositivos y de red, como la interfaz web, el acceso por Bluetooth, el CLI, el SNMP y la consola RJ-45 o USB. El switch Cisco 2960 también permite el apilamiento con FlexStack-Plus y FlexStack-Extended, lo que aumenta la escalabilidad y la redundancia de la red. El switch Cisco 2960 ofrece características de capa 3 con acceso enrutado (OSPF), enrutamiento estático y RIP. Además, el switch Cisco 2960 proporciona visibilidad con DNS-AS y NetFlow, seguridad con 802.1X, SPAN y BPDU Guard, fiabilidad con un alto MTBF y una garantía limitada de por vida mejorada, y resiliencia con fuentes de alimentación redundantes opcionales.
- Servidor HTTPS: Es un servidor web que usa el protocolo HTTPS para cifrar y autenticar las comunicaciones entre el cliente y el servidor. Este protocolo requiere un certificado digital emitido por una autoridad de certificación (CA) para establecer una conexión segura. El servidor HTTPS de la oficina beta tiene la dirección IP pública 150.185.222.2 y el nombre de dominio
- Servidor HTTP: Es un servidor web que usa el protocolo HTTP para transferir datos entre el cliente y el servidor. Este protocolo no ofrece ningún mecanismo de seguridad. El servidor HTTP de la oficina epsilon tiene la dirección IP pública 150.185.222.3 y el nombre de dominio

- Servidor DNS: Es un servidor que usa el protocolo DNS para resolver los nombres de dominio en direcciones IP y viceversa. Este protocolo permite que los usuarios accedan a los recursos de la red usando nombres más fáciles de recordar que las direcciones numéricas. El servidor DNS del centro de datos tiene la dirección IP pública 150.185.222.1 y el nombre de dominio empresa.com. Este servidor provee el servicio DNS a todas las oficinas de la empresa.

DISPOSITIVOS A UTILIZAR

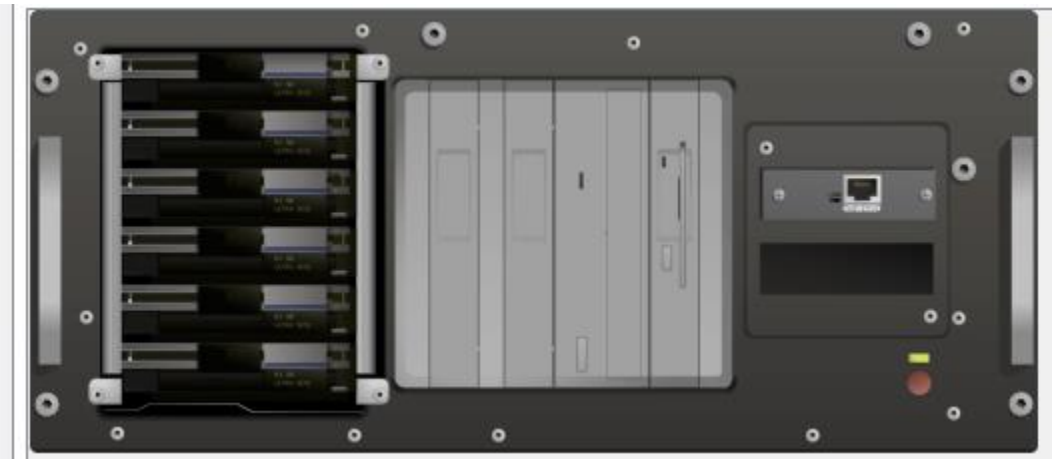
Routers PT

Switch Cisco 2960



PCs

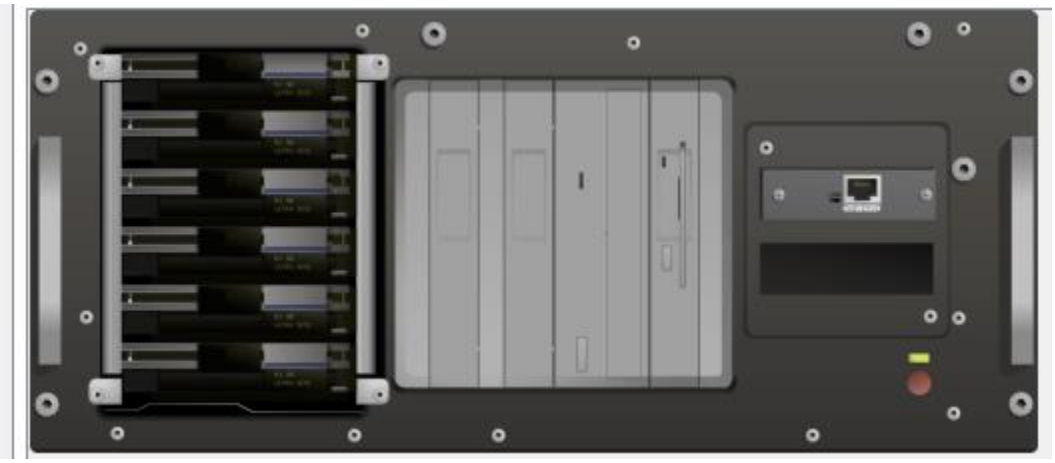
Servidor DNS



Router Inalambrico WRT300N

Impresoras

Servidor HTTP y HTTPS



CONFIGURACION DE LA RED

Conectividad WAN

La empresa cuenta con cinco oficinas en Maracaibo: Alfa, Beta, Gamma, Delta y Epsilon, conectadas a Internet a través de un centro de datos usando diferentes tecnologías WAN. Alfa y Beta utilizan enlaces de Fibra Óptica por su alta velocidad y fiabilidad, ideales para grandes anchos de banda y baja latencia. Gamma se conecta mediante Fast Ethernet, adecuado para requisitos moderados de ancho de banda y menor costo. Delta opta por un enlace inalámbrico para flexibilidad y reducción de cableado físico, mientras que Epsilon usa ADSL, una solución rentable para demandas de ancho de banda más bajas.

- Alfa y Beta: Enlaces de Fibra Óptica.
- Gamma: Enlace Fast Ethernet.
- Delta: Enlace inalámbrico.
- Epsilon: Enlace ADSL.
- Fibra Óptica (Alfa y Beta): Se eligió por su alta velocidad y fiabilidad. Es ideal para conectar oficinas que requieren un gran ancho de banda y una baja latencia.
- Fast Ethernet (Gamma): Ofrece una velocidad decente a un costo menor en comparación con la fibra óptica, adecuado para oficinas con requisitos moderados de ancho de banda.
- Enlace Inalámbrico (Delta): Proporciona flexibilidad y reduce la necesidad de cableado físico. Útil para oficinas que pueden estar en ubicaciones difíciles de cablear.
- ADSL (Epsilon): Una solución rentable para oficinas con demandas de ancho de banda más bajas.

Conectividad LAN

- Todas las oficinas: Conectividad Gigabit Ethernet.
- Usuarios: Cada oficina tiene un número variable de usuarios con computadoras individuales.
- Impresoras: Dos por oficina, una a color y otra en blanco y negro.
- Gigabit Ethernet: Se utiliza para redes LAN debido a su capacidad para manejar grandes cantidades de datos, lo cual es esencial para mantener la productividad empresarial.

Direccionamiento IP

Todas las oficinas tienen conectividad Gigabit Ethernet en sus redes LAN para manejar grandes cantidades de datos, esencial para la productividad empresarial. Se utiliza el bloque de direcciones privadas 172.16.0.0/23, con un margen del 20% para futuras expansiones. La asignación de direcciones IP se automatiza mediante DHCP para reducir la carga administrativa y los errores humanos.

- Bloque Privado: 172.16.0.0/23.
- Margen: 20% de reserva en cada subred para expansión futura.
- Asignación Automática: DHCP implementado en cada oficina.
- Bloque Privado 172.16.0.0/23: Se seleccionó para permitir una amplia gama de direcciones IP dentro de la red privada de la empresa.
- Margen del 20%: Se reserva para permitir la expansión futura sin la necesidad de reestructurar toda la red.
- DHCP: Automatiza la asignación de direcciones IP, reduciendo la carga administrativa y los errores humanos.

VLANs en Oficina Beta

En la oficina Beta, se crearon VLANs (10, 20, 30 y 40) para segmentar el tráfico de red y mejorar la seguridad y el rendimiento, correspondiendo cada una a un departamento diferente. Se implementó VLAN Trunking para permitir la comunicación entre VLANs a través de un solo router. Para la seguridad, se utiliza NAT con sobrecarga, permitiendo que múltiples dispositivos compartan una única dirección IP pública y ocultando las direcciones IP internas.

- VLAN 10: Administración.
- VLAN 20: Gerencia.
- VLAN 30: Operaciones.

- VLAN 40: Atención al Cliente.
- VLAN Trunking: Implementado para permitir la comunicación entre VLANs a través de un solo router.
- VLANs 10, 20, 30, 40: Se crearon para segmentar el tráfico de red y mejorar la seguridad y el rendimiento. Cada VLAN corresponde a un departamento diferente, asegurando que los recursos y datos sean accesibles solo para el personal relevante.
- VLAN Trunking: Permite que múltiples VLANs compartan un enlace físico común, lo que simplifica la infraestructura de red y reduce costos.

Seguridad y NAT

- NAT con Sobrecarga: Implementado para permitir el acceso a Internet manteniendo la red interna segura.
- Acceso Externo: Restringido, excepto para ciertos servicios.
- NAT con Sobrecarga: Se implementa para permitir que múltiples dispositivos compartan una única dirección IP pública. Esto mejora la seguridad al ocultar las direcciones IP internas y permite el ahorro de direcciones IP públicas.
- Acceso Externo Restringido: Asegura que los recursos internos estén protegidos de accesos no autorizados desde Internet.

Servicios Externos

Se configuran servidores HTTPS en Beta y HTTP en Epsilon para ser accesibles desde el exterior, utilizando el bloque de direcciones públicas 150.185.222.0/29. Esto permite la interacción con clientes y socios mientras se mantiene la seguridad de la red interna. El servidor DNS en el centro de datos proporciona servicio DNS a todas las oficinas, y todos los servicios son accesibles mediante nombres de dominio, excepto DHCP.

- Servidor HTTPS: Oficina Beta.
- Servidor HTTP: Oficina Epsilon.
- Servidor DNS: Centro de datos.
- Servidores HTTPS, HTTP y DNS: Se configuran para ser accesibles desde el exterior utilizando un conjunto limitado de direcciones IP públicas. Esto permite la interacción con clientes y socios mientras se mantiene la seguridad de la red interna.
- Bloque de Direcciones Públicas 150.185.222.0/29: Se asigna para estos servicios externos. La elección de un bloque pequeño se debe a la limitada necesidad de direcciones públicas y al alto costo de estas.

Bloque de Direcciones Públicas

- Asignado: 150.185.222.0/29.
- Servidor DNS: Proporciona servicio DNS a todas las oficinas.

Dominio y Nombres de Servicio

- Dominio: (Escoge un nombre de dominio y justifícalo).
- Acceso a Servicios: Todos los servicios son accesibles mediante nombres de dominio, excepto DHCP.

Simulación y Pruebas en Packet Tracer

Se realizarán pruebas en Packet Tracer para asegurar que la configuración cumple con los requisitos de seguridad y conectividad, incluyendo el acceso al servidor HTTPS de Beta y al servidor DNS y HTTP de Epsilon, tanto desde la red interna como externa, y la comprobación de las tablas NAT y el funcionamiento general.

- Acceso a Servidor HTTPS: Desde la red interna y externa de la oficina Beta.
- Acceso a Servidor DNS y HTTP: Desde la red interna y externa de la oficina Epsilon.
- Comprobación: Tablas NAT y funcionamiento general.
- Pruebas de Acceso y Funcionamiento de NAT: Se realizan para asegurar que la configuración cumple con los requisitos de seguridad y conectividad.

Restricciones de Acceso en Oficina Beta

El departamento de administración en Beta tiene acceso a Internet pero no a las redes de otros departamentos, manteniendo la confidencialidad y la integridad de los datos.

- Departamento de Administración: Acceso a Internet sin acceso a otras redes internas.
- Departamento de Administración: Se le permite el acceso a Internet pero se restringe el acceso a las redes de otros departamentos para mantener la confidencialidad y la integridad de los datos.

PROCEDIMIENTOS DE SEGURIDAD, PLANES DE CONTINGENCIAS Y OTRAS INFORMACIONES RELEVANTES

Procedimientos de Seguridad, Planes de Contingencia y Otras Informaciones Relevantes

En el contexto de la infraestructura informática de la empresa, es fundamental implementar procedimientos de seguridad robustos, planes de contingencia efectivos y herramientas de monitoreo de red para garantizar la integridad, disponibilidad y confidencialidad de los datos. A continuación, se detallan los aspectos clave de estas áreas:

Procedimientos de Seguridad:

1. Autenticación y Autorización:
   - Se establecerá un sistema centralizado de autenticación y autorización para gestionar el acceso a la red y sus recursos. Cada usuario recibirá credenciales únicas que les permitirán acceder a los recursos pertinentes según su rol en la empresa. Se implementarán políticas de contraseñas robustas y se realizarán auditorías periódicas para garantizar la seguridad de las cuentas de usuario.
2. Firewalls y Listas de Control de Acceso (ACL):
   - Se configurarán firewalls en los routers y switches para controlar el tráfico de red tanto en el perímetro como dentro de la red. Las ACL se utilizarán para restringir el acceso a recursos sensibles y proteger la red contra posibles amenazas externas e internas. Se establecerán reglas específicas para permitir o denegar el tráfico según la dirección IP, el puerto y el protocolo.
3. Detección y Prevención de Intrusiones (IDS/IPS):
   - Se implementarán sistemas de detección y prevención de intrusiones para monitorear el tráfico de red en busca de actividades maliciosas y responder de manera proactiva a posibles amenazas. Se configurarán alertas para notificar al personal de seguridad sobre posibles intentos de intrusión, y se tomarán medidas correctivas según sea necesario para mitigar los riesgos.
4. Cifrado de Datos:
   - Se utilizarán protocolos de cifrado como SSL/TLS para proteger la comunicación entre los clientes y los servidores, garantizando la confidencialidad e integridad de los datos transmitidos. Se implementarán políticas de cifrado para asegurar que la información confidencial se almacene y transmita de manera segura en toda la red.
5. Respaldo y Recuperación de Datos:

- Se establecerán políticas de respaldo periódico de los datos críticos de la empresa, utilizando soluciones de respaldo automatizadas y redundantes. Se desarrollarán planes de recuperación de desastres detallados para restaurar rápidamente los datos y la funcionalidad de la red en caso de fallos graves o incidentes de seguridad.

Planes de Contingencia:

1. Plan de Respuesta a Incidentes:
   - Se elaborará un plan detallado que describa los procedimientos a seguir en caso de incidentes de seguridad, incluyendo la notificación de las partes interesadas, la contención de la amenaza, la investigación forense y la restauración de la operatividad normal. Se designarán roles y responsabilidades específicos para cada miembro del equipo de seguridad, y se realizarán simulacros periódicos para garantizar una respuesta eficaz en situaciones de emergencia.
2. Backup y Replicación de Datos:
   - Se establecerán políticas de respaldo frecuente de los datos críticos de la empresa, utilizando tecnologías de respaldo incrementales y completas. Se implementará la replicación de datos en ubicaciones geográficamente dispersas para garantizar la disponibilidad y la integridad de la información en caso de fallos catastróficos. Se realizarán pruebas periódicas de los procedimientos de respaldo y recuperación para validar su eficacia.
3. Simulacros y Entrenamiento del Personal:
   - Se llevarán a cabo simulacros periódicos de seguridad y entrenamiento del personal para familiarizarlos con los procedimientos de seguridad y los protocolos de respuesta a incidentes. Se proporcionará formación específica sobre la identificación y gestión de amenazas, así como sobre el uso adecuado de herramientas y sistemas de seguridad. Se documentarán los resultados de los simulacros y se realizarán revisiones periódicas para mejorar continuamente los procesos de seguridad.

Monitoreo de Red:

El monitoreo de red es una práctica esencial para mantener la salud, el rendimiento y la seguridad de la infraestructura informática de la empresa. A continuación, se presentan las herramientas y protocolos clave utilizados para esta función:

- Syslog:** Se utilizará el protocolo Syslog para recopilar mensajes de registro de sistema, permitiendo la identificación y resolución de problemas de manera eficiente.
- SNMP (Simple Network Management Protocol):** Se empleará SNMP para facilitar el intercambio de información de gestión entre dispositivos de red, permitiendo el monitoreo y control de la infraestructura de manera centralizada.
- NETFLOW: Se implementará NETFLOW para registrar información detallada sobre el tráfico de datos que atraviesa la red, lo que permitirá realizar análisis exhaustivos y detectar posibles problemas de rendimiento o seguridad.

La integración de estas herramientas de monitoreo con los procedimientos de seguridad y los planes de contingencia garantizará una respuesta eficaz ante posibles amenazas o incidentes, salvaguardando la continuidad operativa y la seguridad de la infraestructura informática de la empresa.

ESPECIFICACIONES Y DETALLES TECNICOS SOBRE PRODUCTOS Y SERVICIOS UTILIZADOS EN LA RED

Dispositivos de Red:

1. Routers:
   - Router Delta (WRT300N):** Este router inalámbrico de la oficina Delta funciona con el estándar 802.11n draft, ofreciendo velocidades de hasta 300 Mbps y un mayor alcance que el 802.11g. Cuenta con 4 puertos LAN Fast Ethernet y un puerto WAN Fast Ethernet para conectar con el centro de datos. Además, dispone de una antena MIMO de tres elementos para mejorar la cobertura y calidad de la señal inalámbrica. Se utiliza el software Linksys para la configuración y seguridad de la red, ofreciendo funciones como la interfaz web, filtrado MAC, firewall SPI, entre otros.
2. Switches:
   - Switch Cisco 2960: Este conmutador de capa 2 ofrece 24 o 48 puertos Gigabit Ethernet con una velocidad de línea. Además, cuenta con 4 puertos SFP fijos de 1 Gigabit o 2 puertos SFP+ fijos de 10 Gigabit para conectar con otros dispositivos de red. Soporta PoE+ con un presupuesto de hasta 740W y PoE perpetuo, lo que permite alimentar dispositivos como teléfonos

IP, cámaras de seguridad o puntos de acceso inalámbricos. Funciona con el software Cisco IOS y ofrece características de capa 3 con acceso enrutado (OSPF), enrutamiento estático y RIP, así como otras funcionalidades avanzadas de gestión y seguridad.

3. Servidores:
    - Servidor DNS: Alojado en el centro de datos, este servidor proporciona el servicio DNS a todas las oficinas de la empresa. Tiene la dirección IP pública 150.185.222.1 y el nombre de dominio empresa.com. Utiliza el protocolo DNS para resolver nombres de dominio en direcciones IP y viceversa, permitiendo que los usuarios accedan a los recursos de la red utilizando nombres de dominio más fáciles de recordar.
4. Servidor HTTPS (Oficina Beta): Este servidor web utiliza el protocolo HTTPS para cifrar y autenticar las comunicaciones entre el cliente y el servidor. Tiene la dirección IP pública 150.185.222.2 y ofrece acceso seguro a los servicios web de la oficina Beta.
    - Servidor HTTP (Oficina Epsilon): Este servidor web utiliza el protocolo HTTP para transferir datos entre el cliente y el servidor. Tiene la dirección IP pública 150.185.222.3 y proporciona servicios web no cifrados a la oficina Epsilon.

Dirección IP y DHCP:

- Se utiliza el bloque de direcciones privadas 172.16.0.0/23 para asignar direcciones IP a los dispositivos de la red.
- Se reserva un margen del 20% en cada subred para futuras expansiones.
- Se implementa DHCP en cada oficina para automatizar la asignación de direcciones IP a los dispositivos de la red, reduciendo la carga administrativa y los errores humanos.

VLANs (Oficina Beta):

- Se han creado VLANs (10, 20, 30, 40) para segmentar el tráfico de red y mejorar la seguridad y el rendimiento.
- Cada VLAN corresponde a un departamento diferente, como administración, gerencia, operaciones y atención al cliente.

- Se ha implementado VLAN Trunking para permitir la comunicación entre VLANs a través de un solo router, simplificando la infraestructura de red y reduciendo costos.

Seguridad y NAT:

- Se implementa NAT con sobrecarga para permitir el acceso a Internet manteniendo la red interna segura.
- Se restringe el acceso externo a ciertos servicios mediante la configuración de ACLs en los routers.
- Se utilizan firewalls y listas de control de acceso (ACL) para controlar el tráfico de red tanto en el perímetro como dentro de la red, protegiendo contra posibles amenazas externas e internas.

Servicios Externos y Bloque de Direcciones Públicas:

- Los servidores HTTPS, HTTP y DNS son accesibles desde el exterior utilizando un conjunto limitado de direcciones IP públicas del bloque 150.185.222.0/29.
- Se implementa NAT con sobrecarga para permitir que múltiples dispositivos compartan una única dirección IP pública, mejorando la seguridad al ocultar las direcciones IP internas y permitiendo el ahorro de direcciones IP públicas.

Dominio y Nombres de Servicio:

- Todos los servicios son accesibles mediante nombres de dominio, excepto DHCP, facilitando el acceso y la identificación de los recursos de la red.
- Se utiliza el nombre de dominio empresa.com para el servidor DNS alojado en el centro de datos, permitiendo a los usuarios acceder a los recursos de la red utilizando nombres de dominio fáciles de recordar.

INTERACCION NO TECNICA Y RELEVANTE COMO POLITICAS DE LA EMPRESA

En el contexto de la implementación de la red empresarial para nuestras cinco oficinas ubicadas en la ciudad de Maracaibo, es esencial establecer políticas de interacción no técnica que regulen el comportamiento de los empleados, promuevan la seguridad de la información, y garanticen el cumplimiento de las normativas de uso de la red. Este documento detalla las políticas clave que deben seguirse para asegurar un entorno de trabajo eficiente, seguro y ético.

Política de Acceso a la Red

1. Objetivo: Garantizar que el acceso a la red empresarial se realice de manera segura y autorizada.
2. Procedimientos:
    - Todos los empleados deben tener credenciales de acceso únicas y seguras para utilizar la red.
    - El acceso a la red desde dispositivos personales solo está permitido mediante autorización previa del departamento de TI.
    - El acceso remoto a la red empresarial debe realizarse a través de una conexión VPN segura y autorizada.

Política de Uso Aceptable de la Red

1. Objetivo: Establecer reglas claras sobre el uso apropiado de los recursos de red de la empresa.
2. Procedimientos:
    - El uso de la red está reservado exclusivamente para actividades relacionadas con el trabajo.
    - Está prohibido el acceso a sitios web no relacionados con el trabajo durante el horario laboral, excepto por razones comerciales legítimas.
    - El intercambio de archivos y datos debe cumplir con las políticas de seguridad de la empresa y las leyes de protección de datos.

Política de Seguridad de la Información

1. Objetivo: Proteger la confidencialidad, integridad y disponibilidad de la información empresarial.
2. Procedimientos:
    - Los empleados deben cumplir con las políticas de seguridad de la información al manejar datos sensibles o confidenciales.
    - Se deben utilizar medidas de cifrado adecuadas para proteger la información confidencial durante su transmisión y almacenamiento.
    - Cualquier incidente de seguridad o brecha de datos debe ser reportado inmediatamente al departamento de TI.

Política de Privacidad de los Datos

1. Objetivo: Garantizar el tratamiento ético y legal de los datos personales de empleados, clientes y terceros.
2. Procedimientos:
    - La recopilación, almacenamiento y procesamiento de datos personales debe cumplir con las leyes y regulaciones de privacidad de datos aplicables.
    - Se debe obtener el consentimiento explícito de los individuos antes de recopilar o procesar sus datos personales.
    - Los empleados tienen la responsabilidad de proteger la privacidad de los datos personales y garantizar su uso adecuado.

Política de Acceso a Servicios Externos

1. Objetivo: Facilitar el acceso seguro a servicios externos esenciales para las operaciones comerciales.
2. Procedimientos:
    - El acceso a servicios externos, como servidores web y DNS, debe realizarse utilizando métodos seguros y autorizados.
    - Se deben implementar medidas de autenticación y cifrado para proteger la comunicación con los servicios externos.
    - El acceso a servicios externos debe limitarse a empleados autorizados y para fines comerciales legítimos.

La implementación efectiva de estas políticas de interacción no técnica es fundamental para mantener un entorno de trabajo seguro, eficiente y ético en el uso de la red empresarial. Todos los empleados tienen la responsabilidad de cumplir con estas políticas y contribuir a la protección de la información empresarial y la privacidad de los datos.