UNITEC

Seguridad y redes de área amplia

Profesora: Ana María Galindo Juárez

Fecha de entrega 08/08/24

proyecto final

Por: Daniel Ascencio

# Índice

[Índice 1](#_Toc174051624)

[Introducción 2](#_Toc174051625)

[Objetivos 2](#_Toc174051626)

[Hipótesis 3](#_Toc174051627)

[Desarrollo 3](#_Toc174051628)

[Escalabilidad 3](#_Toc174051629)

[Redundancia 3](#_Toc174051630)

[Seguridad 4](#_Toc174051631)

[Control de tráfico 4](#_Toc174051632)

[Telefonía IP 4](#_Toc174051633)

[Monitoreo 4](#_Toc174051634)

[Conectividad 5](#_Toc174051635)

[Uso óptimo de los recursos 5](#_Toc174051636)

[Resultados 5](#_Toc174051637)

[Conclusiones 5](#_Toc174051638)

[Referencias 6](#_Toc174051639)

# Introducción

Este documento explica el desarrollo de una topología propuesta para una empresa ficticia “Z” que opera en la industria farmacéutica. La empresa se acercó con Daniel Ascencio, ingeniero en redes, con la siguiente problemática:

“La empresa (Z) tiene un problema de conectividad. La empresa opera en varios estados de México, y se tienen diversos problemas. Necesitamos que exista conectividad en las oficinas secundarias en los estados de CDMX, Monterrey y Guadalajara con la oficina principal y el call center, manteniendo siempre velocidad, escalabilidad y seguridad. De momento las 3 áreas funcionan bien independientemente y se necesita una solución cohesiva que permita comunicación tanto administrativa como de uso diario. Además, se requiere establecer redundancia en las oficinas secundarias ya que a menudo se caen las redes por falta de mantenimiento. Por último, requerimos que la solución sea escalable y se mantenga útil por un plazo mínimo de 10 años. ¿Nos puede ayudar?”

* *Héctor Hernández, IT Manager en Z*

## Objetivos

En comunicaciones posteriores, se remarcó que la empresa está en constante perdida de ingresos por la situación. Por lo tanto, se postularon los siguientes objetivos:

1. Encontrar una solución a la problemática implementable en 2 meses o menos.
2. No pasar del precio total acordado de la solución de $250,000 pesos.
3. Brindar una propuesta de red a la semana del inicio del proyecto para comparar y confirmar las necesidades de la empresa.
4. La solución debe ocupar los recursos que ya se tienen en la empresa, en donde sea posible.

## Hipótesis

La solución se llevará a cabo después de 1 semana de aceptada la propuesta. Se tardará mes y medio aproximadamente en terminar y costará alrededor de $180,000 pesos, sin contar la infraestructura ya en funcionamiento de la empresa.

# Desarrollo

Con base en la comunicación anterior el Ing. Daniel creó una propuesta de solución para la empresa, utilizando el software “Cisco Packet Tracer” para mostrar el diseño lógico de la red. Daniel identificó los siguientes puntos clave para la propuesta, que se desarrollan a continuación:

## Escalabilidad

La topología debe contar con escalabilidad, es decir que se pueden aumentar equipos en los diversos puntos de la red sin perder funcionalidad. Los dos puntos clave son el call center y las oficinas secundarias, que deben tener la capacidad de duplicar o incluso triplicar la cantidad de equipos en la red, en este caso pueden ser: Servidores, computadoras, celulares y teléfonos.

Para lograr este punto se un cambio tanto en direcciones IP como ancho de banda, para agregar más espacio y velocidad.

Del otro lado en HQ se recomendaron enlaces redundantes entre varios switches, una redundancia para el servidor maestro ya que solía caerse el enlace, y otra en el área de ventas y marketing por solicitud de la empresa ya que planean expandir esta área en un futuro cercano.

## Redundancia

Ya que la comunicación se estableció con un manager de IT con conocimiento en redes, se propuso redundancia como solución a las caídas de las oficinas secundarias. El ing. Daniel estuvo de acuerdo con la propuesta y se implementó en forma de dos switches multicapa por región que funcionan con HSRP para habilitar dos posibles rutas de salida del tráfico al resto de la red.

En las otras áreas de la red no se implementó redundancia por costos y porque no se requería, incluso tomando en cuenta necesidades de escalabilidad.

## Seguridad

En el área de seguridad se establecieron listas de control de acceso para limitar el uso de la red a los usuarios comunes, por ejemplo, a las computadoras de call center y de las áreas de marketing. También se agregaron accesos seguros con contraseña a todos los equipos de red como routers y switches.

El cliente reportó que HQ recibe ataques cibernéticos constantes, pero declinó las diversas recomendaciones.

## Control de tráfico

Siguiendo de cerca el punto anterior se recomendó agregar listas de control de acceso para limitar parte del tráfico de los usuarios. También, por solicitud del cliente se limitó la conectividad de las oficinas secundarias con el resto de la red, solo pudiendo ser alcanzadas desde las oficinas secundarias en Monterrey.

## Telefonía IP

En el área de call center se expandieron recientemente los cubículos y se les agregó una computadora y teléfono a cada uno. Por eso se proponen agregar vlans para dividir el tráfico en datos para las computadoras y VOIP para los teléfonos.

## Monitoreo

En la oficina principal se propuso un servidor maestro que registra todos los cambios de la red. Este servidor lleva un documento de logs con todas las alertas de cambios con fecha y nivel de alerta. También se eligió EIGRP para call center como HQ para tener más métricas de monitoreo.

## Conectividad

Se propone un router frontera para conectar el call center con las oficinas secundarias de Monterrey para interconectar los diversos puntos de la empresa mediante un enlace WAN, y también se estableció conexión entre las otras dos oficinas secundarias con la de Monterrey. HQ y el call center ya tenían conexión directa mediante el departamento de marketing, pero se agregó un router para no saturar de tráfico esa área.

## Uso óptimo de los recursos

Este punto fue clave para todas las propuestas y recomendaciones de los puntos anteriores. En varios casos la empresa pidió que se usaran los equipos existentes para reducir costos y desperdicios. En cuanto a protocolos, se decidió utilizar OSPF para las oficinas secundarias ya que no requieren altos estándares de ninguna métrica, e incluso con las necesidades de escalabilidad no se deberían tener problemas. El resto de la red maneja EIGRP ya que maneja un volumen de tráfico considerable además de necesitar 99% de uptime. HQ diariamente sufre ataques cibernéticos por lo cual se requiere saber al instante cualquier problema.

# Resultados

Se obtuvieron resultados positivos en general y se lograron los 4 objetivos, aunque para el objetivo #3 se tomó 2 semanas en que la empresa estuviera de acuerdo con la propuesta. La implementación tomó 41 días, y hasta el momento de la escritura de este reporte no se han reportado caídas.

# Conclusiones

La solución aborda aspectos clave como escalabilidad, redundancia, seguridad y control de tráfico, utilizando los recursos existentes para optimizar costos. Se implementaron cambios en la topología de la red, incluyendo la adición de routers y switches redundantes, y la configuración de listas de control de acceso. Aunque la implementación del plan fue exitosa y cumplió con la mayoría de los objetivos, hubo un retraso en la aceptación de la propuesta. En general, la red mejorada ha operado sin problemas desde su implementación.

# Referencias

* Bourne, R. (n.d.). *Redistribution between EIGRP and OSPF*. NetworkLessons. Recuperado el 8 de agosto, 2024, desde <https://networklessons.com/cisco/ccie-enterprise-infrastructure/redistribution-between-eigrp-and-ospf>
* Techystudy Best Learning Online. (2021, 7 de diciembre). *WAN Setup in Cisco Packet Tracer WAN configuration in CPT using router and Switches* [Video]. YouTube. <https://www.youtube.com/watch?v=YnYkj4C-mwQ>
* Precios de equipos Cisco recuperados el 8 de agosto, 2024, desde: <https://itprice.com/es/cisco-gpl>