

# GUIÓN REDES

Arantxa Quijada López

(Diapositiva 1)

# Diseño e Implementación de una Red Informática para una Empresa

¡Hola! ¿Qué tal? Bienvenidos a este recorrido por nuestro proyecto de redes.

Hoy vamos a hablar sobre cómo diseñamos e implementamos una red simulada para una empresa de unas 75 personas, usando Cisco Packet Tracer. Sí, ese simulador que a veces **nos da dolores de cabeza**, pero que nos ayuda muchísimo a visualizar y probar redes sin gastar un solo cable en la vida real.

El reto era conectar **50 estaciones de trabajo por cable** y **25 dispositivos inalámbricos**, como portátiles, tablets o incluso smartphones. Todo esto gestionado desde un **servidor centralizado**, que no solo organiza los servicios esenciales, sino que también mantiene el orden en toda la red.

¿Cómo lo organizamos? Pues siguiendo un **modelo de red jerárquico**, dividiendo por **VLANs** para separar departamentos y controlar mejor el tráfico. También aplicamos políticas de **control de acceso**, configuramos un esquema de **direccionamiento IP ordenado**, y montamos servicios como **DHCP** y **DNS**, que son básicos para que la red funcione de forma dinámica.

Por supuesto, no dejamos de lado la seguridad. Usamos listas de control de acceso, conocidas como **ACLs**, para limitar quién puede acceder a qué. Todo esto buscando algo clave: que la red sea **eficiente, segura y escalable**.

Este proyecto no fue solo armar cables virtuales. Fue aplicar conocimientos reales de diseño y administración de redes, con los principios de siempre en mente: **confidencialidad, integridad y disponibilidad** de la información. Ya sabes, la famosa triada de la seguridad.

Así que si estás empezando a trabajar con redes o simplemente quieres ver cómo se arma una infraestructura de este tipo desde cero, quédate. Vamos a ir paso a paso, y también te iré mostrando capturas y simulaciones en Packet Tracer. ¡Vamos allá!

**VIDEO 1**

Aquí tienen la vista general de la red que diseñamos. Tranquilos, que la iremos desglosando por partes en los próximos capítulos.

(Diapositiva 2)

# Plano y Distribución de la Infraestructura Básica

Vamos ahora con la parte física del proyecto: la **distribución de la infraestructura dentro de la empresa**.

Y sí, aunque estemos trabajando en un entorno simulado, pensamos como si esto fuera un espacio real, con personas trabajando, moviéndose y usando la red todo el día.

Lo primero que hicimos fue diseñar un **plano de la empresa** que optimizara tanto el flujo de trabajo como la instalación de la red. Imagina entrar por la recepción —ese es el punto central— desde donde se accede al resto de las áreas: oficinas, salas de reunión, incluso los baños. Todo bien conectado, tanto física como lógicamente.

Ahora, en cuanto al corazón operativo, el **área de trabajo principal** se divide en dos zonas:

* Por un lado, tenemos **50 estaciones de trabajo cableadas**, que marcamos en color lila. Esta zona está pensada para los puestos más estáticos, como administrativos, diseñadores o contadores, que necesitan una conexión más estable y rápida.
* Por otro lado, tenemos una zona con **25 estaciones inalámbricas**, marcadas en verde, pensadas para usuarios más móviles. Aquí se conectan a través de WiFi, lo que les da más flexibilidad, ideal para reuniones rápidas, tareas en movimiento o dispositivos como laptops y tablets.

Si seguimos avanzando hacia la parte derecha del plano, nos encontramos con las **salas técnicas**. Aquí está todo el hardware que da soporte a la red: una zona dedicada a los **switches**, bien organizados, y más allá, una sala cerrada que funciona como el **Centro de Procesamiento de Datos (CPD)**.

En el CPD ubicamos los **servidores y equipos críticos**, todos protegidos y en un ambiente de temperatura controlada, porque sí, mantener la temperatura baja no es un lujo, ¡es una necesidad para que los equipos no colapsen!

En resumen: organizamos el plano para que tanto el personal como la red puedan operar de forma eficiente. Cada zona tiene su propósito y su tipo de conexión, todo alineado con las necesidades reales de una empresa moderna.

(Diapositiva 3)

# Hardware y Software de los Equipos y Servidores

Pasamos ahora a lo que hace funcionar todo este sistema: el **hardware, el software y los equipos de red**.

Empezamos con los **equipos de los usuarios**. Usamos una combinación de **PCs de escritorio y portátiles**. Por ejemplo, modelos como el HP ProBook 450 o Dell OptiPlex, que vienen equipados con procesadores potentes como el Intel i5-12400 o el Ryzen 5 5600U. Todos con **16 GB de RAM** y **un SSD de 512 GB NVMe**, para que las aplicaciones vuelen.

Todos estos equipos corren con **Windows 11 Pro**, activado y legal, y están organizados en tres estados: operativos, en mantenimiento o con fallas. Esto facilita muchísimo el seguimiento del inventario técnico.

A nivel de **software**, tenemos una configuración bastante completa:

* Para el día a día, usamos **Microsoft 365**: Word, Excel, Outlook y Teams, que permiten trabajar y comunicarse sin problema.
* En navegación y reuniones, usamos **Chrome, Edge, Teams y Zoom**.
* Para **seguridad**, tenemos tanto **Windows Defender** como ESET, y para soporte remoto y comunicación usamos **AnyDesk** y **TeamViewer**.
* Y claro, también usamos herramientas de colaboración en la nube como **OneDrive, SharePoint y Planner**, e incluso algo de automatización con Power Automate.
* Finalmente, algunos departamentos usan **sistemas ERP como SAP Business One**, y para la gestión de la red tenemos **UniFi**.

**VIDEO 2**

Aquí pueden ver cómo se distribuyen los diferentes dispositivos dentro del entorno de Packet Tracer. Tenemos laptops y PCs conectados a sus respectivos switches, y en el CPD están los servidores y puntos de control de red.

Ahora sí, hablemos de la **columna vertebral de la red**: los equipos Cisco que hacen todo esto posible.

* En la capa de acceso usamos el **switch Cisco C2960**, con 24 puertos Fast Ethernet. Es perfecto para segmentar la red con **VLANs**, aplicar **QoS** y controlar el tráfico básico.
* Para el core de la red usamos un **switch Capa 3 Cisco C3650**. Este sí que es un monstruo: 24 puertos Gigabit PoE+ para alimentar puntos de acceso y teléfonos IP, soporte para **VLANs avanzadas**, **ACLs**, y un montón de características de seguridad. Incluso puede gestionar tráfico inalámbrico desde el mismo equipo.
* Y como routers principales, tenemos **Cisco 2911**. Este modelo no solo maneja el enrutamiento, también tiene funciones de **firewall**, control de tráfico con **IDS/IPS**, y una interfaz de administración bastante amigable. Ideal para una empresa de este tamaño que necesita rendimiento y seguridad.

(Diapositiva 4)

# Esquema de la Red y Distribución de Dispositivos

El esquema lógico de la red se basa en una arquitectura jerárquica que integra routers, switches multilayer y de acceso, estaciones de trabajo (PCs y laptops), impresoras y servidores. Cada departamento está segmentado mediante VLANs, lo que facilita una gestión eficiente y segura del tráfico de red.

Se han implementado rutas redundantes entre los routers principales y los servidores centrales, que alojan servicios esenciales como DHCP, DNS y correo electrónico. Asimismo, se mantiene una separación clara entre los dispositivos conectados por cable y aquellos que acceden a la red vía WiFi, optimizando tanto el rendimiento como la seguridad.

En la vista física de Cisco Packet Tracer, se ha replicado fielmente la disposición real del plano de oficinas: los switches se encuentran ubicados en su sala técnica correspondiente, mientras que los servidores están alojados en el Centro de Procesamiento de Datos (CPD), con control adecuado de temperatura. El cableado sigue rutas lógicas a lo largo de las paredes, respetando la infraestructura física.

Esta representación permite verificar la coherencia entre el diseño lógico de la red y la distribución física del cableado y los dispositivos en la instalación, facilitando la planificación y el mantenimiento.

(Diapositiva 5)

# Configuración de la infraestructura de red

Para asegurar una segmentación adecuada de la red y un uso eficiente del espacio de direcciones IP, se diseñó un plan de subredes utilizando bloques de máscara /27, lo que permite hasta 30 hosts útiles por subred.

Se definieron un total de 23 subredes, cada una asignada a una VLAN específica, enlaces entre routers, conexiones a proveedores de servicios de internet (ISPs) y enlaces con switches multilayer.

La tabla de subredes detalla información clave, incluyendo la dirección de subred, el rango de direcciones IP utilizables, la dirección de broadcast y el propósito asignado a cada segmento.

La configuración IP de cada interfaz se realizó de acuerdo al plan de subredes establecido. En el entorno de Cisco Packet Tracer, las direcciones IP fueron asignadas manualmente a las interfaces de los routers y switches multilayer, utilizando comandos desde el modo de configuración global.

Para la propagación dinámica de rutas dentro de la red, se implementó el protocolo OSPF (Open Shortest Path First) en los switches multilayer y routers principales, garantizando una actualización eficiente y rápida de las tablas de enrutamiento.

(Diapositiva 6)

# Instalación y configuración del servidor

Los servidores críticos de la red, incluyendo DHCP, DNS y correo electrónico, fueron configurados con direcciones IP estáticas asignadas dentro del rango correspondiente a la VLAN del Centro de Procesamiento de Datos (CPD), asegurando así su correcta identificación y accesibilidad dentro de la infraestructura.

Esta asignación fija de direcciones IP garantiza la estabilidad en la resolución de nombres, la correcta entrega de servicios esenciales y una comunicación eficiente con los dispositivos cliente. Asimismo, se configuró una puerta de enlace predeterminada común para todos los servidores, asegurando el enrutamiento adecuado hacia el resto de la red.

Para facilitar la asignación automática de direcciones IP a los dispositivos finales, se habilitó el servicio DHCP en uno de los servidores. Se definieron múltiples pools de direcciones, cada uno asociado a una VLAN específica, con su correspondiente rango de direcciones IP, máscara de subred, puerta de enlace y servidor DNS, optimizando así la gestión y administración del direccionamiento IP en la red.

(Diapositiva 7)

# Permisos y políticas de seguridad para los usuarios

(Diapositiva 8)

# Conectividad y acceso a los recursos compartidos

Para verificar la correcta conectividad entre los dispositivos de la red y el acceso a los recursos compartidos, se realizaron pruebas mediante el comando ping desde diversas estaciones de trabajo hacia servidores, impresoras y otros equipos ubicados en distintas VLANs. Estas pruebas confirmaron que la comunicación interdepartamental es efectiva y que los servicios esenciales, como DHCP, DNS y compartición de archivos, se encuentran disponibles y operativos. Adicionalmente, se puede emplear el modo de simulación de Cisco Packet Tracer, que permite observar de manera visual el flujo de paquetes y validar el comportamiento esperado del tráfico en la red. Esta herramienta facilita la identificación de posibles fallos y optimiza la configuración mediante un análisis detallado del funcionamiento de la infraestructura