Desarollo de Redes 3ra entrega

Escrito Por Nexus

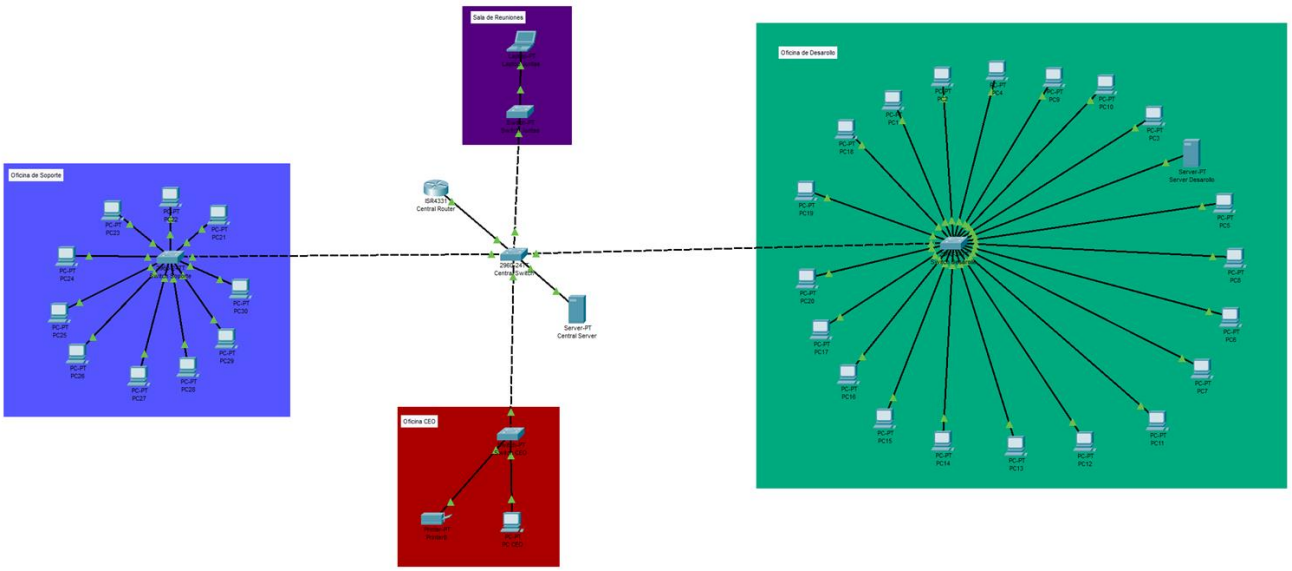
Versión: 1.3
Fecha:12/11/24

Indice

Correccion 2da Entrega

1. Detalle del Esquema Lógico Definitivo por Establecimiento:

- **Oficina Única:** Mantener la oficina con las áreas mencionadas: Oficina de Desarrollo, Oficina de Soporte, Sala de Juntas y Oficina del CEO.
- **Topología de Red:** Se mantendrá la topología de estrella con el switch principal, pero se implementará una **segmentación de red** para dividir las distintas áreas (Desarrollo, Soporte, Sala de Juntas, CEO) con subredes VLAN para mejorar la seguridad y la administración del tráfico.
- **Dispositivos:**
  - **Oficina de Desarrollo:** 20 PCs, 1 switch de 24 puertos, 1 servidor de desarrollo.
  - **Oficina de Soporte:** 10 PCs, 1 switch de 24 puertos.
  - **Sala de Juntas:** 1 PC conectada a un switch de 8 puertos.
  - **Oficina del CEO:** 1 PC conectado a un switch de 8 puertos.
  - **Infraestructura común:** Router principal, switch principal de 48 puertos, servidor principal.



Corrección: La segmentación de la red será clave para mejorar el rendimiento y la seguridad.

2. Cálculo de Materiales por Establecimiento:

- **Cableado estimado:** Se recalcula la longitud total del cableado para asegurar que cubra las nuevas implementaciones, incluida la segmentación de red con VLANs. El cálculo de 404 metros de cable Cat6 es adecuado, pero se adicionan 10% más metros para asegurar que no haya falta de cable en la instalación. Además, el cableado debe estar perfectamente etiquetado para cada área y subred.
- **Equipos:**
    - **Switches adicionales:** En caso de expansión o futura segmentación, se considerará la posibilidad de añadir 1 switch de 24 puertos extra para manejo de carga adicional de dispositivos.
- **Otros materiales:**
    - **Patch panel:** Se incluye un patch panel adicional de 48 puertos para soportar una expansión futura.
    - **Canaletas para cableado estructurado:** Reforzar el plan de cableado con más canaletas si se realizan cambios en la distribución.

Corrección: Recalcular los metros de cableado para cubrir expansión y realizar ajustes en los equipos y materiales.

3. Direccionamiento IP usando VLSM:

- **Red principal:** 192.168.0.0/24 se mantiene.
- **Oficina de Desarrollo:** 192.168.0.0/26 (62 hosts) se mantiene.
- **Oficina de Soporte:** 192.168.0.64/26 (62 hosts) se mantiene.
- **Sala de Juntas:** 192.168.0.128/27 (30 hosts) se mantiene.
- **Oficina del CEO:** 192.168.0.160/28 (14 hosts) se mantiene.
- **Red de infraestructura (routers, switches):** 192.168.0.200/29 (6 hosts) se mantiene.

Corrección: Confirmar que las subredes están correctamente configuradas según las necesidades de los dispositivos y posibles ampliaciones.

4. Documentación del Sistema de Cableado (Normas):

El sistema de cableado estructurado se diseñará y documentará según las **normativas internacionales TIA/EIA-568-C**, que garantizan la correcta transmisión de datos, la seguridad y la organización de las instalaciones. Para lograr esto, se seguirán los siguientes lineamientos:

- **Cableado Cat6 UTP**: Se utilizará cable Cat6 UTP para todas las conexiones de red, garantizando una transmisión de datos de hasta **10 Gbps** en distancias de hasta 55 metros, lo cual es adecuado para las necesidades actuales de la empresa.
- **Distribución y organización**: Se implementarán **canaletas de cableado estructurado** para facilitar la gestión, el mantenimiento y la expansión futura de la infraestructura de red. Cada canaleta se etiquetará adecuadamente para identificar los cables y evitar confusiones durante las labores de mantenimiento.
- **Documentación**: La instalación del cableado se documentará minuciosamente, indicando la longitud exacta del cableado utilizado, las ubicaciones de los puntos de conexión, y los números de puerto en los switches y paneles de parcheo. Además, se creará un **diagrama de cableado estructurado** que visualice la distribución completa de los cables, facilitando futuras expansiones o cambios en la red.
- **Pruebas de calidad**: Se realizarán pruebas de **continuidad y rendimiento** en todo el cableado para asegurar que cumpla con los estándares de velocidad y capacidad. Se incluirán pruebas de **atenuación** y **interferencia** para garantizar la fiabilidad del sistema a largo plazo.

Corrección: Incluir en la documentación un procedimiento para verificar el cumplimiento de las normativas y la correcta instalación del cableado para evitar futuros problemas de interferencia.

5. Interconexión de los Puestos:

La interconexión de los puestos de trabajo en las distintas áreas del establecimiento se llevará a cabo de la siguiente manera, asegurando una **distribución eficiente del tráfico de red** y facilitando la **expansión futura**:

- **Oficina de Desarrollo**: Se instalarán **20 PCs**, todos conectados a un **switch de 24 puertos**, garantizando suficiente capacidad para el tráfico generado por los equipos de desarrollo.
- **Oficina de Soporte**: Los **10 PCs** en esta área estarán conectados a un **switch de 24 puertos**, asegurando que el soporte técnico disponga de la infraestructura necesaria para las operaciones diarias.
- **Sala de Juntas**: Se habilitará un **switch de 8 puertos** para conectar **1 PC** y un proyector, permitiendo una interconexión adecuada para presentaciones y reuniones de equipo.
- **Oficina del CEO**: La **oficina ejecutiva** contará con un **PC conectado a un switch de 8 puertos**, garantizando una conexión segura y eficiente para las operaciones de alto nivel.
- **Infraestructura común**: Todos los switches estarán interconectados al **switch principal** ubicado en el rack central, donde se integrarán los equipos de red y se centralizará la gestión de la red local.

Corrección: Se puede mejorar la interconexión considerando cableado adicional para redundancia y segmentación en caso de expansión de la red.

6. Detalle de la UPS para el Servidor Principal:

Para garantizar la continuidad de las operaciones ante cortes de energía y proteger el servidor principal y los equipos de red esenciales, se seleccionará una **UPS (Fuente de Alimentación Ininterrumpida)** con las siguientes características:

- **Consumo estimado**: El servidor principal y el switch principal tienen un consumo total estimado de 600W, por lo que se optará por una UPS con capacidad de al menos **2000 VA** para asegurar un margen adecuado de autonomía.
- **Autonomía recomendada**: La UPS debe proporcionar al menos **20 minutos de autonomía** para cubrir cualquier interrupción breve y permitir un apagado controlado de los equipos.
- **Redundancia y escalabilidad**: En caso de que se añadan más equipos o si se prevé una mayor carga, se evaluará la posibilidad de **adquirir una UPS adicional** o un modelo con mayor capacidad de carga, así como la **instalación de un sistema de monitoreo remoto** para supervisar el estado de la UPS y la salud de la red eléctrica.

Corrección: Verificar la capacidad de la UPS para soportar la carga en caso de añadir equipos adicionales o expansión, y considerar una segunda UPS en caso de una mayor carga o redundancia.

3ra Entrega

7. Contratación de Servicio de Internet

Para asegurar una conexión de alta calidad que satisfaga las necesidades operativas de la empresa, se ha decidido contratar el servicio de ANTEL, una de las principales empresas de telecomunicaciones en la región. A continuación, se detalla el proceso de contratación y configuración del servicio de Internet:

• Proveedor de Servicio: ANTEL

ANTEL es reconocido por su infraestructura robusta y su amplia cobertura de servicios de fibra óptica, lo que lo posiciona como una opción ideal para empresas que requieren conexiones confiables y de alta velocidad. La elección de ANTEL se fundamenta en:

- **Infraestructura de Fibra Óptica:** La fibra óptica de ANTEL garantiza una transmisión de datos rápida y estable, esencial para mantener operaciones fluidas.
- **Cobertura Regional:** Su presencia amplia asegura que la conexión sea accesible y consistente en diferentes ubicaciones de la empresa.
- **Soporte Técnico:** ANTEL ofrece un servicio de atención al cliente eficiente y soporte técnico especializado, lo que minimiza el tiempo de inactividad en caso de incidencias.

El servicio contratado proporciona una velocidad mínima garantizada de 100 Mbps, lo que es adecuado para manejar tareas intensivas en datos como videoconferencias, transferencia de archivos grandes y múltiples dispositivos conectados simultáneamente sin pérdida de rendimiento.

• Tipo de Conexión: Fibra Óptica Dedicada

La elección de una conexión de fibra óptica dedicada se basa en varias ventajas clave:

- **Alta Capacidad de Transmisión de Datos:** Permite manejar grandes volúmenes de tráfico de datos sin congestiones.
- **Baja Latencia:** Esencial para aplicaciones en tiempo real como videollamadas y transacciones en línea.
- **Alta Fiabilidad:** Menor probabilidad de interrupciones, lo que garantiza una conexión estable y continua.
- **Escalabilidad:** Fácil de actualizar conforme crezcan las necesidades de la empresa sin cambios significativos en la infraestructura.

Esta conexión es ideal tanto para las operaciones internas como para la comunicación eficiente con clientes, proveedores y otras filiales, asegurando que todas las partes puedan interactuar sin retrasos ni interrupciones.

• Proceso de Contratación

El proceso de contratación del servicio con ANTEL se llevó a cabo siguiendo una serie de pasos estructurados para asegurar que se cumplieran todas las necesidades de la empresa:

1. **Solicitud de Presupuesto:**

- Se realizó una solicitud detallada a ANTEL, especificando los requisitos mínimos de velocidad, la necesidad de redundancia para asegurar la continuidad del servicio y las características adicionales de seguridad necesarias.
- Incluyó detalles sobre el volumen de tráfico esperado, número de dispositivos conectados y aplicaciones críticas que dependerían de la conexión a Internet.

2. **Revisión de Opciones:**
    - Se analizaron las diferentes ofertas y paquetes disponibles, comparando aspectos como costos, beneficios, tiempos de instalación y soporte técnico.
    - Se evaluaron las opciones en función de la infraestructura existente de la empresa, asegurando compatibilidad y facilidad de integración.
3. **Firma del Contrato:**
    - Tras la aprobación del presupuesto más adecuado, se procedió a la firma del contrato de prestación de servicios.
    - El contrato incluye términos específicos sobre la velocidad de conexión garantizada, los niveles de servicio (SLA), tiempos de respuesta ante fallas y penalizaciones en caso de incumplimiento.
4. **Instalación del Servicio:**
    - ANTEL coordinó la instalación física de la fibra óptica en las instalaciones de la empresa, asegurando una conexión directa al punto de acceso principal.
    - Se realizó la configuración inicial de la red, incluyendo la optimización de parámetros para maximizar el rendimiento y la seguridad de la conexión.

• Redundancia

Para minimizar el riesgo de interrupciones en el servicio de Internet, se ha implementado una solución de redundancia:

- **Conexión Secundaria:** Además de la conexión principal de fibra óptica, se contrató un servicio de conexión secundaria con ANTEL. Esta segunda línea actúa como respaldo automático en caso de fallas en la conexión principal.
- **Alta Disponibilidad:** La redundancia garantiza que las operaciones de la empresa continúen sin interrupciones, incluso ante incidentes técnicos o fallas de infraestructura.
- **Balanceo de Carga:** En algunos casos, la conexión secundaria puede utilizarse para distribuir el tráfico de datos, mejorando la eficiencia y el rendimiento general de la red.

• Configuración del Router

La configuración del router principal es crucial para la seguridad y el rendimiento de la red empresarial:

- **Configuración Profesional:** Técnicos especializados de ANTEL realizaron la configuración inicial del router, asegurando que todos los parámetros estuvieran optimizados para las necesidades específicas de la empresa.
- **Características de Seguridad Avanzadas:**

    - **Firewall Integrado:** Protege la red interna filtrando tráfico malicioso y bloqueando accesos no autorizados.
    - **VPN (Red Privada Virtual):** Permite conexiones seguras para empleados remotos, asegurando que la transmisión de datos sensibles esté cifrada y protegida contra interceptaciones.
- **Segmentación de la Red:**
    - **División por Áreas Funcionales:** Se separaron las redes para las áreas de Desarrollo, Soporte e Infraestructura, lo que mejora la gestión del tráfico y aumenta la seguridad al limitar el acceso entre diferentes segmentos.
    - **Control de Acceso:** Cada segmento de la red tiene políticas de acceso específicas, garantizando que solo el personal autorizado pueda acceder a determinadas áreas y recursos.
- **Optimización del Rendimiento:**
    - **QoS (Quality of Service):** Prioriza el tráfico crítico para asegurar que aplicaciones esenciales, como videoconferencias y transferencias de archivos, reciban el ancho de banda necesario.
    - **Monitoreo Continuo:** Se implementaron herramientas para monitorear el rendimiento del router en tiempo real, permitiendo detectar y resolver rápidamente cualquier anomalía.

8. Detalle y Fundamentación de la Implementación de Seguridad Informática

Para proteger la infraestructura de red, los dispositivos y la información sensible de la empresa, se han implementado diversas medidas de seguridad informática. A continuación, se detallan cada una de ellas:

• Firewall de Última Generación

Un firewall de última generación (NGFW) es esencial para proteger la red empresarial contra amenazas externas e internas:

- **Inspección Profunda de Paquetes (DPI):** Analiza el tráfico a nivel de aplicación, detectando y bloqueando amenazas avanzadas que podrían pasar desapercibidas en firewalls tradicionales.
- **Prevención de Intrusiones (IPS):** Identifica y previene intentos de intrusión mediante la detección de patrones de ataque conocidos.
- **Control de Aplicaciones:** Permite definir políticas específicas para el uso de aplicaciones, limitando o bloqueando aquellas que no sean necesarias para las operaciones empresariales.
- **Protección contra DDoS:** Implementa mecanismos para detectar y mitigar ataques de Denegación de Servicio Distribuida, asegurando la disponibilidad de los servicios críticos.

• VPN (Red Privada Virtual)

La implementación de una VPN es fundamental para asegurar las conexiones remotas de los empleados y sucursales:

- **Cifrado de Datos:** Todos los datos transmitidos a través de la VPN están cifrados, protegiendo la información contra interceptaciones y accesos no autorizados.
- **Autenticación Segura:** Utiliza métodos de autenticación robustos para verificar la identidad de los usuarios antes de permitir el acceso a la red empresarial.
- **Acceso Controlado:** Permite definir qué recursos de la red están disponibles para los usuarios remotos, asegurando que solo accedan a la información necesaria para sus funciones.

• Antivirus y Antimalware

Para proteger todos los dispositivos conectados a la red, se ha implementado una estrategia integral de antivirus y antimalware:

- **Software de Protección Actualizado:** Se instalan soluciones de seguridad que se actualizan automáticamente para detectar y neutralizar las amenazas más recientes.
- **Escaneos Periódicos:** Realizan análisis regulares de todos los dispositivos para identificar y eliminar cualquier software malicioso.
- **Protección en Tiempo Real:** Monitorean continuamente las actividades del sistema para prevenir infecciones antes de que puedan causar daño.

• Control de Accesos

Un sistema robusto de control de accesos es vital para proteger los sistemas críticos de la empresa:

- **Autenticación Fuerte:** Se requiere el uso de contraseñas complejas que combinan letras, números y caracteres especiales para dificultar su adivinación o fuerza bruta.
- **Autenticación de Dos Factores (2FA):** Cuando es posible, se implementa 2FA, añadiendo una capa adicional de seguridad mediante un segundo método de verificación, como un código enviado al teléfono móvil.
- **Gestión de Privilegios:** Se asignan permisos específicos según las responsabilidades de cada empleado, asegurando que solo tengan acceso a la información y herramientas necesarias para su trabajo.

• Seguridad en el Cableado

La protección física de la infraestructura de red es tan importante como la seguridad lógica:

- **Cableado Estructurado:** Se siguen normativas estrictas para el cableado, asegurando una instalación organizada y fácil de gestionar.
- **Dispositivos de Protección:** Se instalan estabilizadores de voltaje y sistemas de protección contra sobrecargas para prevenir daños a los equipos debido a fluctuaciones eléctricas.
- **Acceso Controlado a Infraestructura:** Se restringe el acceso a las áreas donde se encuentran los cables y equipos de red, evitando manipulaciones no autorizadas.

• Backup y Recuperación de Datos

La estrategia de respaldo y recuperación de datos garantiza la continuidad del negocio ante pérdidas de información:

- **Backups Periódicos:** Se realizan copias de seguridad de manera regular, abarcando tanto los servidores como los equipos de trabajo individuales.
- **Almacenamiento Redundante:** Los datos se almacenan en servidores de backup locales y en servicios de almacenamiento en la nube, proporcionando múltiples capas de protección.
- **Planes de Recuperación:** Se establecen procedimientos claros para la restauración rápida de datos en caso de incidentes, minimizando el tiempo de inactividad y la pérdida de información crítica.

• Monitoreo y Auditoría de Seguridad

El monitoreo constante y las auditorías periódicas son esenciales para mantener la integridad de la seguridad informática:

- **Sistemas de Monitoreo:** Herramientas que supervisan el tráfico de la red en tiempo real, detectando actividades sospechosas o anómalas que puedan indicar intentos de ataque.
- **Alertas Automatizadas:** Configuración de alertas que notifican al equipo de seguridad sobre posibles incidentes, permitiendo una respuesta rápida y efectiva.
- **Auditorías Regulares:** Revisiones sistemáticas de las políticas de seguridad, configuraciones de sistemas y prácticas operativas para identificar y corregir vulnerabilidades.
- **Evaluación de Vulnerabilidades:** Uso de herramientas y técnicas para identificar debilidades en la infraestructura de TI antes de que puedan ser explotadas por atacantes.

• Educación y Concientización

La capacitación continua del personal es fundamental para mantener una postura de seguridad sólida:

- **Entrenamientos Regulares:** Sesiones educativas sobre buenas prácticas de seguridad informática, incluyendo la identificación y prevención de ataques de phishing, el uso adecuado de contraseñas y la gestión segura de la información.
- **Simulacros de Seguridad:** Ejercicios prácticos que simulan situaciones de riesgo para preparar al personal a reaccionar adecuadamente ante incidentes de seguridad.
- **Políticas de Seguridad Claras:** Documentación accesible que define las expectativas y responsabilidades de cada empleado en relación con la seguridad de la información.
- **Cultura de Seguridad:** Fomento de un ambiente donde la seguridad es una prioridad compartida, incentivando a los empleados a reportar cualquier actividad sospechosa o incidentes de seguridad.