



Tecnológico de Monterrey - Campus Monterrey

Escuela de Ingeniería y Ciencias

Ingeniería en Tecnologías Computacionales

Interconexión de Dispositivos

## **Reto - Fase 1: Descripción del escenario**

Group #304

Santiago Quintana Moreno A01571222

Ian Fernando León Hernández A01785078

Santiago Borbolla Regato A01660035

Miguel Ángel Gavito González A00839096

Manuel Arias Alcocer A01571655

Ing. Joel Hiram Chávez Verástegui

Ing. Mario Jesús Gárate Vélez

Monterrey, Nuevo León a 18 de mayo del 2025

## INTRODUCCIÓN:

- **Empresa:** AztechTech S.A. de C.V.
- **Matriz / Oficina Central:** San Pedro Garza García, Nuevo León.
- **Oficina Secundaria:** Polanco, Ciudad de México.
- **POS / Tiendas:** 30 en la República Mexicana.
- **Empleados:** 250 totales
  - 35, San Pedro Garza García, Nuevo León.
  - 35, Polanco, Ciudad de México.
  - 6, en cada sucursal / POS.
- AztechTech S.A. de C.V., con su sede principal en San Pedro Garza García y una oficina secundaria en Polanco, opera una red de 30 puntos de venta a lo largo de la República Mexicana. Se estima que sus ventas mensuales, impulsadas por su presencia a nivel nacional, rondan los \$5 millones de pesos, acumulados en línea y en storefront. Una posible fortaleza radica en su extensa red de puntos de venta, facilitando el acceso a sus productos o servicios. Sin embargo, una debilidad podría ser la gestión y coordinación de un equipo distribuido en tantas ubicaciones, lo que podría impactar en la eficiencia operativa.
- Gracias al aumento de sus ventas a nivel nacional, tanto en línea como físicamente en sus sucursales, la empresa ha evolucionado de sus servicios básicos de comunicación y de tecnología contratados reactivamente, a necesitar de una renovación de dichos servicios para una operación continua y eficiente con mínimo tiempo de baja.
- Por otra parte, las tendencias del mercado mexicano refuerzan la urgencia de actualizar la infraestructura. El consumo de productos tecnológicos y electrónicos sigue en auge: en 2024 el comercio electrónico minorista creció un 20% hasta alcanzar los \$789,700 millones de pesos (Rodríguez, 2025), representando ya cerca del 16% de las ventas minoristas del país (Rodríguez, 2025). Se estima que un 84% de los internautas en México ya realizan compras en línea (Ortega, 2024), reflejo de nuevos hábitos de compra más digitalizados y de la preferencia por experiencias omnicanal por parte de los clientes (Ortega, 2024). En este contexto, expertos advierten que alrededor del 90% de las PyMEs que no adopten la digitalización podrían fracasar en los próximos años (Storecheck & Storecheck, 2025b). Por ello, adoptar una infraestructura de red de última generación no es solo una mejora técnica, sino una necesidad estratégica para asegurar la competitividad y la continuidad del negocio.

**ANTECEDENTES:**

AztechTech S.A. de C.V. se encuentra actualmente operando bajo una infraestructura de red y conectividad ampliamente superada por las demandas actuales del negocio. Esta infraestructura presenta una serie de deficiencias críticas tanto a nivel físico; hardware, lógico; software y servicios como de conectividad externa; servicios de Internet, lo que ha afectado directamente la continuidad operativa, la seguridad de la información y la eficiencia de los procesos internos.

En primer lugar, los equipos de red en uso, principalmente switches no administrables, routers básicos y cableado desorganizado o de categorías antiguas no ofrecen ningún nivel de segmentación, monitoreo ni control de tráfico. La inexistencia de VLANs o políticas de calidad de servicio (QoS) impide la separación lógica entre áreas sensibles como punto de venta (POS), administración, cámaras de vigilancia e inventario, lo que facilita la propagación de amenazas internas y genera competencia innecesaria por ancho de banda. Esta arquitectura de red “plana” no cumple con estándares modernos de seguridad ni escalabilidad. Las latencias elevadas, las caídas recurrentes en el servicio y la imposibilidad de priorizar tráfico crítico se han vuelto síntomas frecuentes que impactan directamente la experiencia del cliente, las transacciones en caja y la coordinación logística entre sedes.

Por otra parte, en el plano del software, se detectó una convivencia de múltiples versiones obsoletas del sistema operativo en servidores dentro de cada oficina central como en los POS, muchas de ellas fuera de soporte oficial y sin actualizaciones de seguridad. Esta diversidad impide aplicar políticas centralizadas de gestión, control de parches y seguridad, además de representar un riesgo elevado de vulnerabilidades conocidas y explotables. Tampoco existe una estructura de dominio con Active Directory, lo cual obliga a una administración manual y descentralizada de usuarios, accesos, y dispositivos en cada punto de venta o sede. Los servicios críticos como ERP, nómina, inventario y CRM residen en servidores locales sin virtualización, sin respaldo en la nube, y sin replicación entre sedes, lo cual reduce considerablemente la disponibilidad y confiabilidad del sistema.

Finalmente, desde la perspectiva de conectividad externa (capa 3), se observó que la empresa depende en gran medida de servicios residenciales o comerciales básicos contratados con ISPs sin garantías empresariales (SLA), ni enlaces dedicados. Las conexiones entre sedes se realizan mediante túneles VPN sobre enlaces asimétricos sin redundancia ni respaldo físico, lo cual genera una alta tasa de pérdida de paquetes, desconexiones frecuentes y problemas serios de sincronización entre los servicios centrales y los puntos de venta. La ausencia de enlaces MPLS o fibra óptica dedicada ha creado un escenario de único punto de fallo (SPOF), donde cualquier falla en la conexión principal puede paralizar operaciones completas. Este esquema, si bien aparentemente más económico en corto plazo, ha generado mayores pérdidas operativas, aumento de incidencias, y un costo oculto por improductividad y atención a contingencias.

En resumen, la empresa opera actualmente con una arquitectura tecnológica reactiva, no estandarizada, vulnerable y carente de escalabilidad. Esta situación no solo frena el crecimiento operativo y la expansión comercial de la empresa, sino que expone sus activos informáticos a riesgos significativos de seguridad y pérdida de información. Estos antecedentes justifican una intervención integral orientada a modernizar la infraestructura de red, implementar controles unificados de software, estandarizar el entorno operativo y profesionalizar la conectividad entre sedes, todo con el objetivo de garantizar continuidad, eficiencia y seguridad en la operación.

#### DIAGNÓSTICO Y DICTAMEN:

| CAUSA RAÍZ  | EFEECTO VISIBLE  | SOLUCIÓN PROPUESTA   |
|---|--|--|
| Uso de switches no administrables, hubs o routers obsoletos.              | Alta latencia, interrupciones frecuentes, cuellos de botella.                  | Reemplazo por switches administrables capa 3, implementación de topología jerárquica, cableado estructurado Cat 6A.                                |
| Equipos de red sin segmentación (red plana sin VLANs).                    | Riesgo de propagación de malware, tráfico no controlado, fallos generalizados. | Creación de VLANs por función (POS, administración, cámaras, visitantes), políticas de QoS, enrutamiento con OSPF.                                 |
| Diversidad de versiones de sistema operativo obsoletas.                   | Incompatibilidades, brechas de seguridad, dificultad en administración.        | Estandarización a Windows 11 Enterprise o server edition, dominio con Active Directory, políticas de grupo y control de parches con WSUS o Intune. |
| Conectividad entre sedes por VPNs residenciales o enlaces asimétricos.    | Caídas frecuentes, pérdida de sincronización entre ERP, nómina e inventario.   | Migración a fibra óptica dedicada (DIA), enlaces MPLS con SLA empresarial, redundancia de ISP y balanceo de carga.                                 |
| Ausencia de firewalls de nueva generación.                                | Exposición a amenazas externas, falta de control sobre el tráfico.             | Implementación de NGFW con IDS/IPS, VPN IPsec, filtrado web y segmentación perimetral  |
| Gestión manual de inventario y falta de visibilidad en tiempo real.       | Errores en stock, desabasto en sucursales, decisiones lentas.                  | Implementación de sensores RFID e integración con Azure IoT Hub y Power BI para visibilidad en tiempo real y análisis predictivo                   |
| Ausencia de redundancia de conectividad e infraestructura crítica (SPOF). | Interrupciones operativas completas ante fallos ISP o de energía.              | Dual WAN con failover, energía redundante (UPS) y enlaces duales en sitios críticos.   |
| Mala gestión de IPs, sin subredes claras ni escalabilidad                 | Conflictos de red, dificultad de administración, límites de crecimiento.       | Planificación con subredes /24 por función o ubicación, integración de DHCP centralizado y DNS empresarial.  |

Durante la intervención técnica realizada en la empresa de retail tecnológico con sede en Monterrey, se identificó una serie de deficiencias estructurales y operativas en la infraestructura de red que justifican una intervención urgente y profunda. El ecosistema tecnológico de la organización muestra síntomas severos de obsolescencia: equipos de red sin capacidad de administración, una red plana sin segmentación funcional, sistemas operativos desactualizados y sin parches, así como enlaces a internet residenciales sin respaldo ni contratos empresariales con SLA.

Esta falta de planeación ha traído como consecuencias interrupciones constantes en los servicios críticos como el ERP, las aplicaciones de nómina e inventario, además de vulnerabilidades de seguridad generalizadas que podrían facilitar desde ataques internos hasta ransomware. La conexión entre sedes se encuentra sustentada en túneles VPN poco confiables, sin enlaces dedicados ni mecanismos de failover, haciendo que cualquier falla en la conectividad provoque pérdida de sincronización de datos entre puntos de venta y oficinas principales.

Además, se observó una dependencia de procesos manuales en áreas clave como inventarios y POS, lo cual genera errores humanos, falta de visibilidad operativa y baja capacidad de reacción ante fluctuaciones de demanda. En consecuencia, se propone una modernización integral, que abarca desde la capa física (cableado, switching, enlaces dedicados) hasta la capa lógica (sistemas operativos, políticas de red, servicios cloud e IoT). Esta transformación no solo resolverá los problemas actuales, sino que dotará a la organización de una plataforma tecnológica moderna, segura, escalable y preparada para competir a nivel nacional e internacional en el sector de retail tecnológico.

## REFERENCIAS:

Ortega, R. (2024, November 28). *La Digitalización del Retail: Un Mercado de Crecimiento para los Canales en México*. eSemanal - Noticias Del Canal.

<https://esemanal.mx/2024/11/la-digitalizacion-del-retail-un-mercado-de-crecimiento-para-los-canales-en-mexico/>

Rodríguez, E. M. (2025, March 14). Comercio electrónico en México creció 20% en 2024, alcanzó un valor de 789,000 millones de pesos. *El Economista*.

<https://www.eleconomista.com.mx/el-empresario/comercio-electronico-mexico-crecio-20-2024-alcanzo-valor-789-000-millones-pesos-20250312-750213.html>

Storecheck, R., & Storecheck, R. (2025, January 22). *Recap del Retail 2024 en México: Adaptación y nuevas oportunidades*. Blog Storecheck.

<https://blog.storecheck.com.mx/retail-2024-en-mexico-adaptacion-y-nuevas-oportunidades/>