



DOCUMENTO TÉCNICO INSTITUCIONAL

Diagnóstico y Propuesta de Topología de Red Segura

SUPERINTENDENCIA DE TRANSPORTE

Documento de referencia arquitectónica y de ciberseguridad

Fecha	18 de marzo de 2026
Alcance	Topología lógica segura con enfoque de defensa en profundidad
Base de entrada	Diagrama compartido por el solicitante

Resumen Ejecutivo

El diagrama actual evidencia, a nivel conceptual, una base tecnológica importante: firewalls, switch core de capa 3, switching de borde, puntos de acceso, servidores, FortiWeb, FortiAnalyzer, FortiAuthenticator, FortiNAC y solución de backup. Sin embargo, en el diagrama compartido no se observan con suficiente detalle la segmentación lógica, la existencia de una DMZ formal, la separación del plano de administración, el aislamiento de invitados, ni el dominio independiente de respaldo.

Este documento propone una topología segura, controles recomendados, prácticas obligatorias y errores a evitar para reducir la superficie de ataque y aumentar la resiliencia operativa.



Nota: Este documento es una guía arquitectónica de alto nivel; no reemplaza un assessment técnico de configuración ni una auditoría formal de cumplimiento.

1. Introducción

A partir del diagrama de red suministrado, se aprecia una arquitectura que combina conectividad a Internet, firewalls perimetrales, switching core y de borde, puntos de acceso inalámbricos, servidores, controles Fortinet de seguridad perimetral e identidad, y una plataforma de respaldo. Esta base es adecuada para evolucionar hacia una arquitectura segura, pero requiere formalizar zonas de confianza, reglas de tránsito, controles de identidad, monitoreo y recuperación.

El propósito de este documento es definir cómo debería verse una topología lógica segura usando los componentes observados, bajo el principio de **defensa en profundidad**. La propuesta busca disminuir el riesgo de movimiento lateral, exposición innecesaria de servicios internos, accesos no autorizados, abuso de privilegios, pérdida de trazabilidad y afectación del servicio por ransomware o incidentes operativos.

La recomendación aquí consignada está alineada con buenas prácticas de seguridad de la información, gestión del riesgo digital y continuidad operativa aplicables a entidades públicas y organizaciones con exposición de servicios críticos.

2. Objetivos

2.1 Objetivo General

Definir una topología de red segura para la Superintendencia de Transporte, basada en segmentación lógica, control de acceso por identidad, protección perimetral, monitoreo centralizado y recuperación resiliente, aprovechando los componentes tecnológicos reflejados en el diagrama compartido.

2.2 Objetivos Específicos

- Establecer zonas de seguridad con límites de confianza claros entre Internet, DMZ, acceso de usuarios, WiFi, servidores internos, gestión y backup.
- Reducir el riesgo de compromiso transversal de la red mediante VLAN, ACL, políticas entre zonas, NAC y autenticación fuerte.
- Proteger los servicios expuestos a Internet usando una DMZ formal y un WAF delante de los portales públicos.
- Separar el tráfico corporativo, administrativo, invitado y de administración técnica para evitar mezclas de confianza.
- Garantizar trazabilidad, capacidad de investigación y respuesta con centralización de logs y correlación de eventos.
- Fortalecer la continuidad del negocio con backups aislados, copias inmutables y pruebas periódicas de restauración.

3. Metodología Propuesta

La definición de una topología segura no debe empezar por equipos aislados sino por funciones, riesgos y flujos autorizados. La metodología recomendada para esta arquitectura es la siguiente:

#	Fase	Propósito	Resultado esperado
1	Inventario y clasificación	Identificar activos, servicios críticos, datos, dependencias y responsables.	Mapa de activos y criticidad.
2	Delimitación de zonas	Separar entornos con distinto nivel de confianza: Internet, DMZ, usuarios, WiFi, servidores, gestión y backup.	Modelo de segmentación lógica.
3	Análisis de flujos	Definir qué tráfico sí debe existir, en qué puertos, sentidos y horarios.	Matriz de flujos autorizados.
4	Mapeo de controles	Asignar WAF, NAC, MFA, ACL, VPN, logging, hardening y respaldo según la zona.	Controles técnicos por segmento.
5	Priorización	Cerrar primero los riesgos de mayor impacto: exposición externa, acceso privilegiado, lateralidad y respaldo.	Hoja de ruta por fases.

- ❗ Esta metodología evita uno de los errores más comunes: construir la red alrededor de la conveniencia operativa y no alrededor del riesgo. En entornos institucionales, el diseño debe partir de la protección del servicio, los datos y la capacidad de recuperación.

4. Marco Normativo y de Referencia

Para entidades públicas en Colombia, el diseño de una topología de red segura debe articularse con la Política de Gobierno Digital, la gobernanza de seguridad digital, la protección de datos personales y los lineamientos del Modelo de Seguridad y Privacidad de la Información – MSPI. A esto se suman estándares internacionales de buenas prácticas que sirven como referencia técnica.

Instrumento	Enfoque	Implicación para la topología
Decreto 1078 de 2015 y Decreto 767 de 2022	Gobierno Digital	Exigen estructurar capacidades TIC y de seguridad digital como parte del modelo institucional, con responsables y mejora continua.
Decreto 338 de 2022	Gobernanza de seguridad digital	Obliga a gestionar riesgo digital y fortalecer la gobernanza, lo que impacta segmentación, monitoreo y respuesta.
Resolución 500 de 2021	Lineamientos de seguridad digital	Formaliza lineamientos sobre MSPI, gestión del riesgo e incidentes.
Resolución 2277 de 2025	Actualización del MSPI	Actualiza el MSPI y lo alinea con ISO/IEC 27001:2022, elevando el estándar esperado para la gestión de seguridad.
Ley 1581 de 2012, Decreto 1377 de 2013 y Decreto 886 de 2014	Protección de datos personales	Exigen proteger la confidencialidad y el tratamiento de datos; la red debe separar, registrar y controlar accesos.
Ley 1273 de 2009	Delitos informáticos	Refuerza la necesidad de prevenir acceso abusivo, interceptación, daño informático y otros delitos.
ISO/IEC 27001, 27002, 27005 y 22301	Buenas prácticas	Sirven como referencia para SGSI, controles, gestión de riesgo y continuidad.

5. Vista Actual y Propuesta de Arquitectura

A continuación se presenta, de forma comparativa, el diagrama base compartido y la topología lógica segura propuesta.

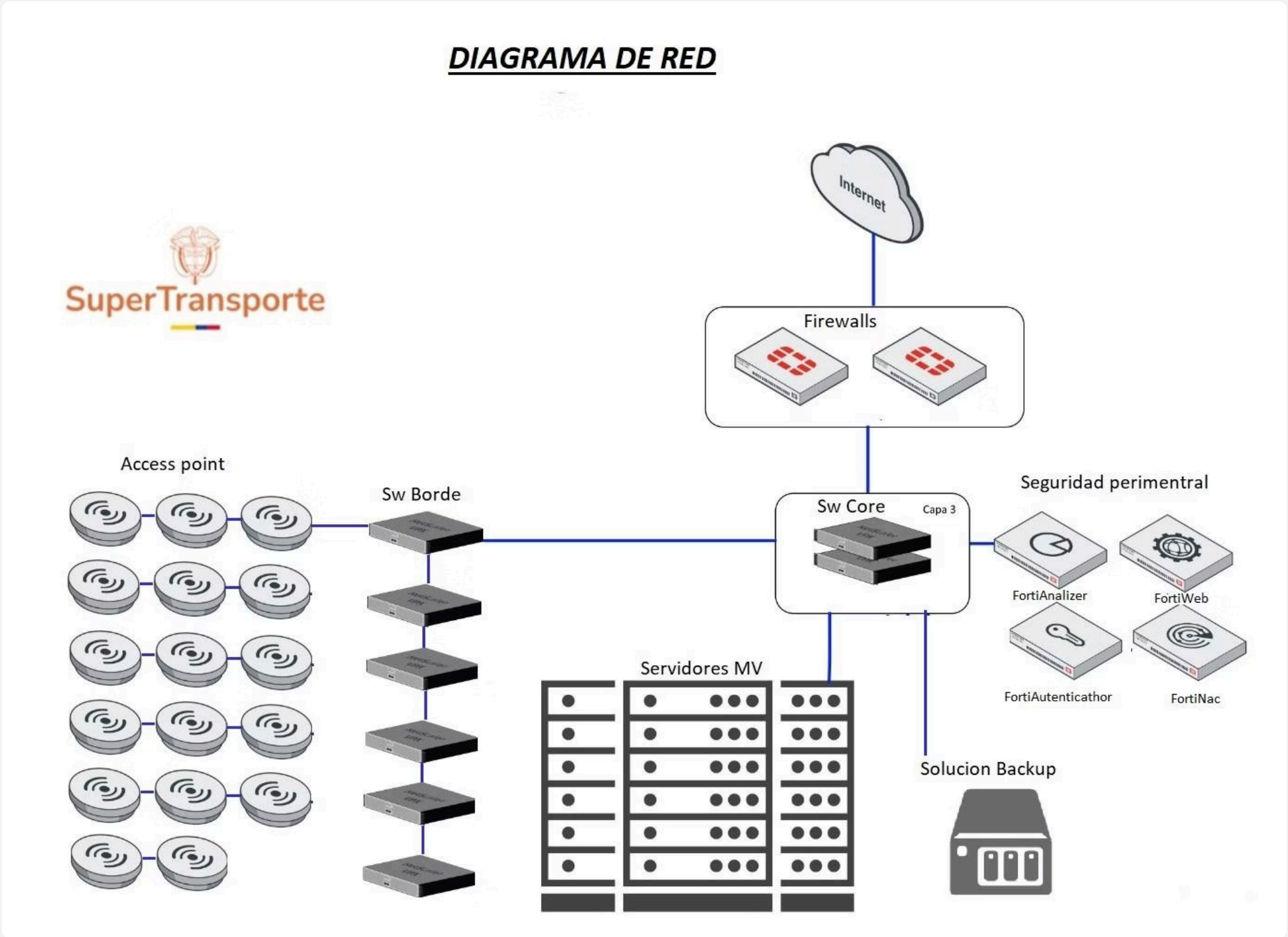


Figura 1. Diagrama base compartido por el solicitante.

- 1

1. Falta de segmentación visible

No se observan zonas separadas como DMZ, usuarios, servidores, administración, WiFi o backups. Esto facilita el movimiento lateral si un equipo se compromete.
- 2

2. Red demasiado centralizada en el Core

El Switch Core capa 3 concentra firewalls, servidores, seguridad y backup. Esto crea un single point of failure con impacto potencialmente total.
- 3

3. Sin DMZ para servicios expuestos

Los servidores MV podrían estar publicados sin una zona desmilitarizada separada. Una intrusión podría habilitar pivoting hacia sistemas internos.
- 4

4. Seguridad perimetral sin ubicación lógica clara

FortiAnalyzer, FortiWeb, FortiAuthenticator y FortiNAC no muestran una integración clara en el flujo de tráfico. Si no operan en línea, las herramientas no protegen efectivamente.
- 5

5. Riesgo en la red inalámbrica

Hay muchos access points, pero no se aprecia separación lógica ni controles WiFi específicos. Esto aumenta el riesgo de acceso no autorizado, movimiento lateral y suplantación de dispositivos.
- 6

6. Backups en la misma red productiva

La solución de backup parece conectada directamente al entorno principal. Si entra ransomware, podría cifrar o borrar los respaldos.
- 7

7. Sin red de administración separada

No se ve una red dedicada para gestionar firewalls, switches, servidores y consolas. Un atacante interno podría intentar comprometer la infraestructura directamente.
- 8

8. Falta de inspección interna

El diagrama muestra controles perimetrales, pero no inspección del tráfico este-oeste. Esto permite desplazamiento libre entre usuarios, APs y servidores.
- 9

9. Alta dependencia del perímetro

La arquitectura se concentra en el borde: Internet → firewalls → core. Eso la hace más débil frente a credenciales robadas, phishing o malware en endpoints.
- 10

10. Redundancia incompleta

Se observan dos firewalls, pero no hay HA clara en core, switches, enlaces, backup o autenticación. Puede existir indisponibilidad ante fallas de hardware, energía o configuración.

Principales brechas de diseño: ausencia de microsegmentación, falta de DMZ definida, backup no aislado, falta de red de administración separada, controles insuficientes sobre WiFi, poca visibilidad del tráfico interno, dependencia excesiva de la seguridad perimetral y posibles puntos únicos de falla.

TOPOLOGÍA SEGURA PROPUESTA - SUPERTRANSPORTE

Diseño lógico recomendado con los componentes observados: firewalls, core, switches de borde, AP, FortiAnalyzer, FortiWeb, FortiAuthenticator, FortiNAC y backup

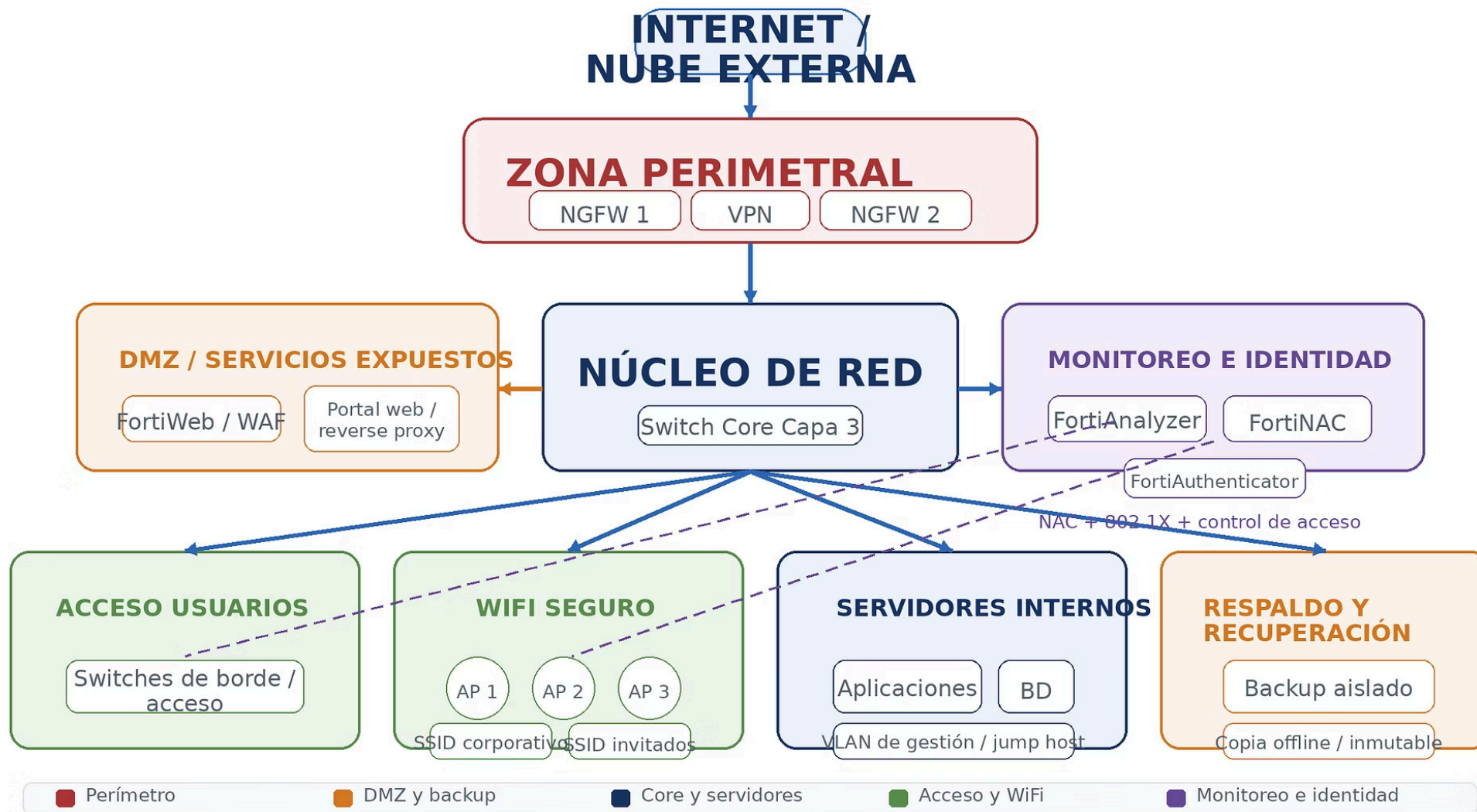


Figura 2. Topología lógica segura propuesta.

6. Topología Segura Recomendada

La topología objetivo debe separar la red por zonas y no por conveniencia de cableado. El principio es simple: **todo lo que no comparta el mismo nivel de confianza no debe convivir en el mismo segmento.**

Zona	Activos / función	Controles clave	Regla principal
Perímetro	Firewalls HA y VPN	IPS, filtrado entrante/saliente, MFA para acceso remoto	Nada entra a la red interna sin pasar por política.
DMZ	FortiWeb y portales públicos	Publicación controlada, hardening, logs, reverse proxy	Nunca publicar servidores internos directamente.
Core	Switch capa 3	ACL entre VLAN, rutas controladas, listas de administración	El core enruta, pero no debe convertirse en red plana.
Acceso usuarios	Switches de borde	VLAN por rol, puertos seguros, NAC	Usuarios no deben alcanzar redes administrativas.
WiFi	AP corporativos e invitados	802.1X, SSID separado, aislamiento invitado	Invitados solo a Internet; nunca a servidores.
Servidores	Aplicaciones y BD	Microsegmentación, acceso admin por VLAN dedicada	Las aplicaciones no deben hablar libremente entre sí.
Monitoreo e identidad	FortiAnalyzer, FortiNAC, FortiAuthenticator	Logs centralizados, NAC, control de postura e identidad	Toda decisión crítica debe dejar trazabilidad.
Backup	Plataforma de respaldo	Aislamiento, copia offline/inmutable, restore test	El backup no debe compartir dominio de riesgo.

6.1 Principios Técnicos que Deben Cumplirse

Segmentación por rol

Segmentación por VLAN y por rol, no solo por edificio o piso.

Mínimo privilegio

Principio de mínimo privilegio entre zonas: denegar por defecto y permitir por excepción.

Separación estricta

Separación estricta entre red corporativa, red de invitados, servidores, administración y respaldo.

Autenticación por identidad

Autenticación basada en identidad para acceso cableado, WiFi y remoto; de preferencia con MFA.

Registro centralizado

Registro centralizado de eventos de seguridad, administración y autenticación.

Protección WAF y DMZ

Protección de servicios expuestos con WAF y publicación controlada en DMZ.

Acceso administrativo controlado

Acceso administrativo únicamente desde una VLAN o jump host de gestión.

Backups aislados

Backups aislados, con copia inmutable u offline y pruebas reales de restauración.

7. Qué Hacer

Prácticas Recomendadas Y Acciones de Alto Impacto Inmediato

Prácticas Recomendadas

- Crear una DMZ formal para portales y aplicaciones expuestas.
- Separar SSID corporativo y SSID de invitados en VLAN diferentes.
- Aplicar 802.1X y políticas de NAC para acceso a la red.
- Centralizar logs de firewall, NAC, WAF, autenticación y servidores.
- Usar MFA en VPN, consolas y cuentas privilegiadas.
- Definir matriz de flujos autorizados y cerrar todo lo no documentado..

Acciones de Alto Impacto Inmediato

- Aislar inmediatamente la plataforma de backup del dominio productivo.
- Revisar y endurecer reglas Any-Any o accesos excesivos entre VLAN.
- Restringir la administración de switches, AP y firewalls a una red de gestión.
- Verificar que ningún servidor interno esté publicado de forma directa
- Habilitar retención y sincronización horaria consistente para logs.
- Probar restauración de copias y acceso alternativo ante caída del servicio.

8. Qué No Hacer

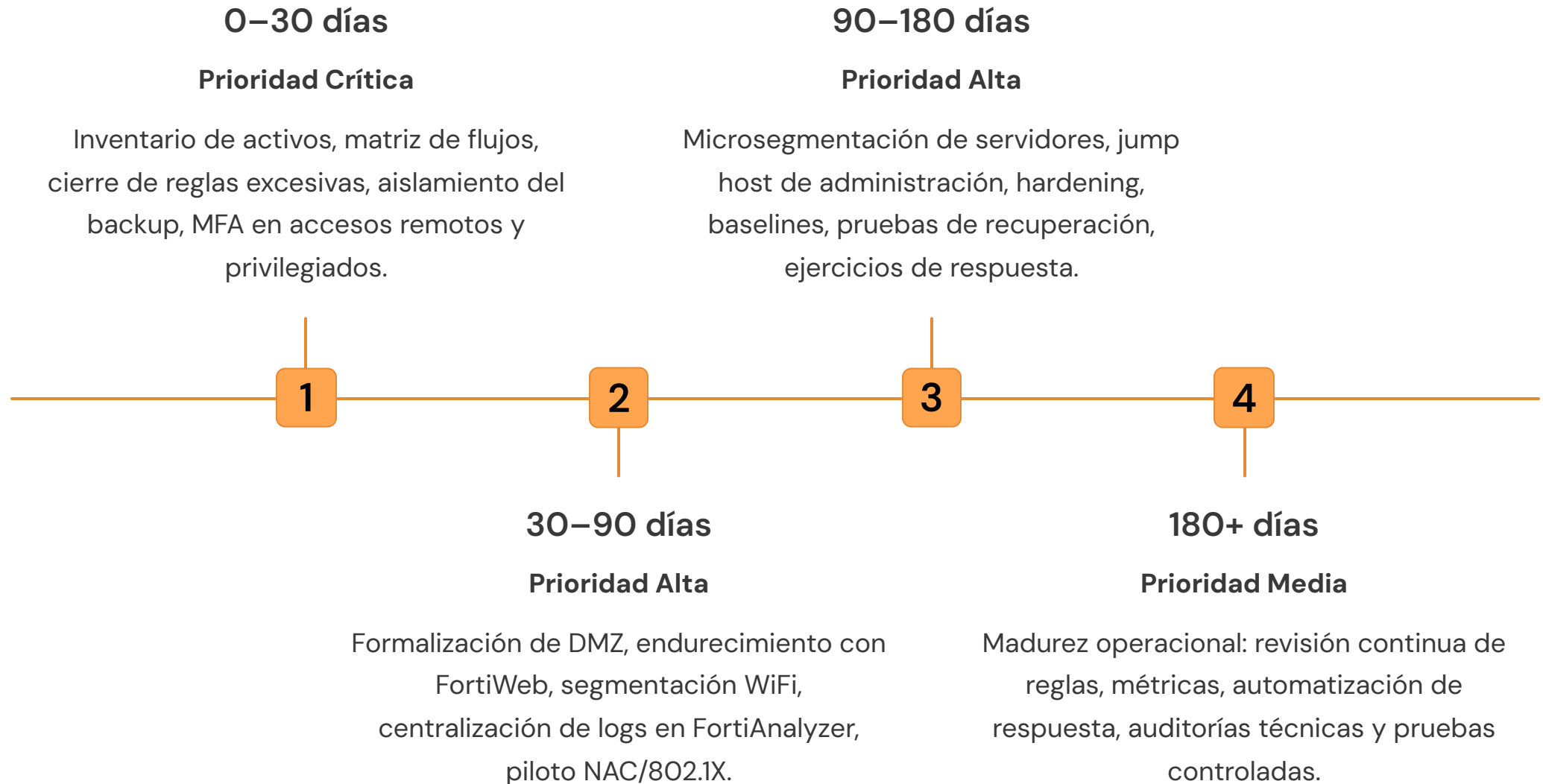
- No dejar la red interna plana ni permitir tránsito libre entre usuarios y servidores.
- No administrar firewalls, switches o AP desde la misma red de usuarios.
- No mezclar WiFi corporativo y WiFi de invitados en el mismo segmento o gateway lógico.
- No exponer servidores internos directamente a Internet sin DMZ, WAF y reglas específicas.
- No confiar únicamente en el firewall perimetral; la protección debe continuar dentro de la red.
- No unir el backup al mismo dominio de riesgo del entorno productivo.
- No dejar cuentas privilegiadas sin MFA, sin trazabilidad o compartidas entre varias personas.
- No conservar reglas antiguas, objetos huérfanos o excepciones temporales convertidas en permanentes.
- No depender de logs locales dispersos; sin centralización no hay investigación confiable.
- No implementar cambios de red sin gestión de cambios, pruebas y rollback.

9. Hoja de Ruta Sugerida de Implementación

A continuación se presenta la hoja de ruta de implementación organizada por horizontes temporales y nivel de prioridad:

Horizonte	Prioridad	Acciones sugeridas
0–30 días	Crítica	Inventario de activos; matriz de flujos; cierre de reglas excesivas; aislamiento del backup; restricción del plano de administración; MFA en accesos remotos y privilegiados.
30–90 días	Alta	Formalización de DMZ; endurecimiento de publicación web con FortiWeb; segmentación WiFi corporativo/invitados; centralización completa de logs en FortiAnalyzer; piloto de NAC/802.1X.
90–180 días	Alta	Microsegmentación de servidores; jump host de administración; revisión de hardening; baselines de configuración; pruebas de recuperación; ejercicios de respuesta a incidentes.
180+ días	Media	Madurez operacional: revisión continua de reglas, métricas, automatización de respuesta, auditorías técnicas y pruebas controladas de seguridad.

9. Hoja de Ruta – Visualización por Fases



10. Conclusión

La Superintendencia de Transporte ya cuenta, según el diagrama observado, con varios componentes valiosos para construir una arquitectura robusta. El reto no está solamente en poseer herramientas, sino en integrarlas dentro de una topología segura y gobernada: perímetro con política estricta, DMZ formal, control por identidad, segmentación interna, monitoreo centralizado y recuperación aislada.

La topología propuesta permite evolucionar desde una representación funcional de red hacia una arquitectura de confianza controlada. Su implementación no requiere desechar lo existente; exige reorganizar, endurecer y gobernar mejor los mismos activos para reducir la exposición, aumentar la trazabilidad y mejorar la continuidad del servicio.

Como siguiente paso práctico, se recomienda validar esta propuesta contra la arquitectura real, levantar inventario técnico, revisar reglas actuales de tránsito entre segmentos y construir una matriz formal de accesos autorizados.

Síntesis de Componentes Clave de la Arquitectura Propuesta

Perímetro con política estricta

Firewalls HA, IPS, filtrado entrante/saliente y MFA para acceso remoto.

DMZ formal

FortiWeb, portales públicos, publicación controlada y reverse proxy.

Control por identidad

FortiAuthenticator, FortiNAC, 802.1X, MFA y control de postura.

Segmentación interna

VLAN por rol, ACL entre zonas, microsegmentación de servidores.

Monitoreo centralizado

FortiAnalyzer, logs centralizados, correlación de eventos y trazabilidad.

Recuperación aislada

Backup con dominio independiente, copia inmutable/offline y pruebas de restauración.

SECCIÓN 11

11. Fuentes Normativas y Técnicas Consultadas

Marco Normativo Nacional

Ministerio TIC Resolución 500 de 2021

Lineamientos y estándares para la estrategia de seguridad digital y adopción del MSPI.

Ministerio TIC Resolución 2277 de 2025

Actualización del Anexo 1 del MSPI y alineación con ISO/IEC 27001:2022.

Función Pública Decreto 1078 de 2015

Decreto Único Reglamentario del Sector TIC.

Función Pública Decreto 767 de 2022

Lineamientos generales de la Política de Gobierno Digital.

Función Pública Decreto 338 de 2022

Gobernanza de seguridad digital.

11. Fuentes Normativas y Técnicas Consultadas
Protección de Datos y Delitos Informáticos

SUIN-Juriscol — Ley 1581 de 2012 Protección de datos personales.	SUIN-Juriscol — Decreto 1377 de 2013 y Decreto 886 de 2014 Reglamentación complementaria en materia de protección de datos personales.	SUIN-Juriscol — Ley 1273 de 2009 Delitos informáticos.
--	--	--

Estándares Internacionales

ISO/IEC 27001:2022 Sistema de Gestión de Seguridad de la Información (SGSI).	ISO/IEC 27002:2022 Controles de seguridad de la información.
ISO/IEC 27005 Gestión del riesgo de seguridad de la información.	ISO 22301 Continuidad del negocio.

Resumen de Zonas de Seguridad y Controles

Zona Perímetro

Firewalls HA y VPN — IPS, filtrado entrante/saliente, MFA para acceso remoto. **Regla:** Nada entra a la red interna sin pasar por política.

Zona Core

Switch capa 3 — ACL entre VLAN, rutas controladas, listas de administración. **Regla:** El core enruta, pero no debe convertirse en red plana.

Zona WiFi

AP corporativos e invitados — 802.1X, SSID separado, aislamiento invitado. **Regla:** Invitados solo a Internet; nunca a servidores.

Zona Monitoreo e Identidad

FortiAnalyzer, FortiNAC, FortiAuthenticator — Logs centralizados, NAC, control de postura e identidad. **Regla:** Toda decisión crítica debe dejar trazabilidad.

Zona DMZ

FortiWeb y portales públicos — Publicación controlada, hardening, logs, reverse proxy. **Regla:** Nunca publicar servidores internos directamente.

Zona Acceso Usuarios

Switches de borde — VLAN por rol, puertos seguros, NAC. **Regla:** Usuarios no deben alcanzar redes administrativas.

Zona Servidores

Aplicaciones y BD — Microsegmentación, acceso admin por VLAN dedicada. **Regla:** Las aplicaciones no deben hablar libremente entre sí.

Zona Backup

Plataforma de respaldo — Aislamiento, copia offline/inmutable, restore test. **Regla:** El backup no debe compartir dominio de riesgo.

Cierre del Documento

Datos del Documento

Título: Diagnóstico y Propuesta de Topología de Red Segura

Entidad: Superintendencia de Transporte

Fecha: 18 de marzo de 2026

Alcance: Topología lógica segura con enfoque de defensa en profundidad

Base de entrada: Diagrama compartido por el solicitante

Advertencia de Alcance

Este documento es una guía arquitectónica de alto nivel; no reemplaza un assessment técnico de configuración ni una auditoría formal de cumplimiento.

Próximos Pasos

- Validar esta propuesta contra la arquitectura real.
- Levantar inventario técnico detallado.
- Revisar reglas actuales de tránsito entre segmentos.
- Construir una matriz formal de accesos autorizados.



Marco de referencia: ISO/IEC 27001:2022 · ISO/IEC 27002:2022 · ISO/IEC 27005 · ISO 22301 · Decreto 338 de 2022 · Resolución 2277 de 2025 · MSPI Colombia