



TDXSECURE

2025

NET RESILIENCE



NUESTRA SOLUCIÓN

El servicio NetResilience de TxDxSecure ofrece un análisis integral de la red para evaluar y mejorar su resiliencia, seguridad y disponibilidad. A través de un estudio detallado de la infraestructura física y lógica, se identifican puntos vulnerables y se proponen optimizaciones estratégicas en las configuraciones, con el fin de asegurar una alta disponibilidad y una rápida recuperación ante fallos.

DURACIÓN:
4 semanas

BENEFICIOS DEL SERVICIO

Mejora en la Disponibilidad y Resiliencia:

Se identifican oportunidades para optimizar la red mediante configuraciones más robustas, mejorando la capacidad de recuperación ante fallos..



Fortalecimiento de la Seguridad

Se realiza un hardening básico de los dispositivos clave y se proporcionan recomendaciones para proteger la red contra ataques.



Recomendaciones de Alta Disponibilidad (HA)

Se analizan las configuraciones actuales y se entregan recomendaciones para implementar alta disponibilidad, incluyendo redundancia lógica y física, sin realizar las implementaciones complejas.



ACCIONES DE IMPLEMENTACIÓN



1. ESTUDIO Y ANÁLISIS DE LA RED



Análisis de Topología

Revisión de la topología de la red para identificar puntos únicos de fallo y mejorar la redundancia y disponibilidad.



Análisis del Equipo Core

Evaluación de los dispositivos principales (routers, switches, firewalls) para identificar mejoras en términos de redundancia.



Auditoría de Configuraciones Actuales

Verificación de que las configuraciones sigan buenas prácticas de seguridad y disponibilidad.



Análisis de los Nodos de Red

Revisión de las facilidades, como ubicación, suministro eléctrico, sistema de enfriamiento, monitoreo, y cableado.



2. OPTIMIZACIÓN Y CONFIGURACIÓN



Protocolos de Alta Disponibilidad

Configuración de protocolos como MSTP, HSRP, VRRP, y OSPF/BGP para mejorar la redundancia y reducir el tiempo de recuperación en caso de fallos.



Redundancia de Enlaces y Agregación

Optimización mediante EtherChannel, agregación de enlaces y balanceo de carga para aumentar la disponibilidad y resiliencia.



Hardening

Aplicación de medidas de seguridad en dispositivos core, como CoPP, Rate Limiting, ACLs y SSH, para minimizar riesgos de ataques.



3. RECOMENDACIÓN DE IMPLEMENTACIÓN DE ALTA DISPONIBILIDAD

Si se detectan puntos críticos que requieran mayor redundancia, se realizará una recomendación de un esquema de Alta Disponibilidad, que puede incluir:

- **Enlaces redundantes de fibra óptica** para garantizar la conectividad en caso de fallos físicos.
- **Instalación de equipos adicionales** para asegurar la redundancia de los dispositivos principales para asegurar la continuidad del servicio.
- **Implementación física de equipos de backup** que se activen automáticamente en caso de caídas del equipo principal.



4. PRUEBAS DE RESILIENCIA Y DISPONIBILIDAD

Una vez implementadas las configuraciones y de ser el caso los equipos de alta disponibilidad, se llevarán a cabo pruebas de resiliencia. Estas pruebas incluirán:



Simulación de fallos

Probar cómo la red responde a la caída de enlaces y dispositivos críticos.

Evaluación de tiempos de conmutación

Verificar el tiempo de failover y el comportamiento de los sistemas ante un fallo, asegurando una rápida recuperación.

Validación de estabilidad y rendimiento

Evaluar la estabilidad de la red bajo diferentes condiciones, asegurando que las configuraciones optimizadas no afecten el rendimiento general.



ENTREGABLES

- ❖ **Presentación Kick Off "Análisis de Gobernanza" (PAG):** Documento inicial con el análisis de la situación actual de la red y los objetivos del servicio.
- ❖ **Documento de Relevamiento de Información (SRD):** Informe detallado de la topología actual de la red, los dispositivos evaluados y sus configuraciones.
- ❖ **Documento de Diseño de Alto Nivel (HLD):** Propuesta de las configuraciones y cambios a realizar para optimizar la resiliencia y la alta disponibilidad.
- ❖ **Documento de Pruebas Operacionales Simplificadas (Test Plan):** Plan detallado para la ejecución de pruebas de resiliencia y alta disponibilidad en la red.
- ❖ **Documento de Plan de Implementación (NIP):** Cronograma y pasos a seguir para la implementación de las configuraciones y los equipos necesarios.
- ❖ **Presentación de Transferencia Operacional (PTO):** Capacitación al equipo de operación sobre las configuraciones implementadas y el uso de los nuevos equipos y protocolos.
- ❖ **Documento de Informe Final (DIF):** Informe que recoge los resultados de las pruebas, las configuraciones implementadas y las recomendaciones futuras para la continuidad operativa.



TXDXSECURE S.A.C.

RUC: 20607043427

Contáctanos: +51 942 325 448; +51 999 379 845

Correo: administracion@txdxsecure.com

Calle las Gorsellas No 167 Naranjal
San Martín de Porres
Lima, Perú

www.txdxsecure.com



2025