DEPARTAMENTO DE TECNOLOGIA Y ADMINISTRACION
CARRERA

INGENIERIA EN INFORMATICA

ASIGNATURA: SEGURIDAD DE LOS SISTEMAS INFORMATICOS

COMISIÓN: 0A TURNO NOCHE

Docente: Daniel Benítez – Marcelo Bugallo

Estudiante/s: Alex Urquiza


TeleComNet
Conectando el Futuro

Índice

Empresa de telecomunicaciones TeleComNet S.A

Resumen

El proyecto es un relevamiento dirigido a la empresa de **telecomunicaciones TeleComNet S.A**, la cual es un operador de servicios de telefonía que provee conectividad empresarial, enlaces MPLS/SD-WAN, servicios VoIP/SIP y conexiones a plataformas en la nube, sobre los riesgos de seguridad de la compañía, la cual nos contrató como auditoría externa. Exponiendo las debilidades de la organización de la red empresarial implementando metodologías, estándares de seguridad y calidad que mitiguen la actual necesidad de mejorar y restructurar los procesos que se llevan a cabo en el área de mesa de ayuda. Aplicando los estándares de la ISO 27001 y las prácticas de la ISO 27002 en el dominio de las telecomunicaciones.

Ubicada en [redacted], [redacted], [redacted]. (oficinas corporativas principales en [redacted]). Hacen una solicitud el día 2 de noviembre del 2025 por parte la Ing. [redacted] CEO de la organización, presentando detalles como antecedentes, contexto,

alcance del relevamiento y objetivos concretos de este relevamiento.

Organización

Dada la criticidad de la disponibilidad, confidencialidad e integridad de los enlaces de comunicaciones y el inminente crecimiento de la red, el Directorio ha decidido realizar un relevamiento técnico alineado con ISO 27001/2 (Dominio 13). Actualmente se nos pide revisar las siguientes áreas de la empresa:

- Seguridad de redes y comunicaciones entre sedes principales.
- NOC.
- Enlaces a clientes críticos y proveedores.
- Evaluar seguridad de equipos de red (routers, switches, firewalls, SBC/VoIP), enlaces de transmisión (fibra, MPLS, enlaces Internet), servicios de túneles remotos (VPN/SSL), acceso de terceros y conexión a la nube.

Para ello debemos analizar políticas/procedimientos de transferencia de información, segregación de redes y gestión de servicios de red. Revisar acuerdos de nivel de servicio (SLA) y contratos con proveedores de conectividad en aspectos de

seguridad y continuidad. Todo esto, en un intervalo de un año para empezar a aplicar las primeras medidas del proyecto para mitigar la incertidumbre y error.

Permiso de acceso a datos

Inicialmente la empresa nos otorga acceso a los siguientes datos: Diagramas de red, inventario de equipos de red, exports de configuración de routers/firewalls y contratos SLA con proveedores. Se coordinará acceso al NOC y a responsables técnicos para entrevistas. Se nos autoriza el análisis de configuración, revisión de logs y escaneos pasivos. Pruebas activas (escaneo de puertos/penetración) deberán coordinarse y autorizarse por separado. Todo bajo el contacto y coordinación principal del CEO, Ing. [redacted] — CTO.

Datos extras

Actualmente la empresa cuenta con aproximadamente 14–15 mil empleados a escala global. En el ultimo año (2024) tuvieron un ingreso de $5.68 mil millones de dólares. La cantidad de usuarios que se verían afectados por alguna falla ronda entre los 147 millones (EE.UU, Canadá, Reino Unido).

La empresa cuenta con una mesa directiva y comités de auditoría/seguridad. Tiene dependencias de proveedores cloud,

partners de integración, proveedores de servicios gestionados y subcontratistas de datos/hosting. Las auditorias regulatorias han señalado problemas de supervisión y control sobre datos tercerizados (afectando así al intercambio de información y acuerdos).

Objetivo general

El objetivo principal es la relevación de los distintos riesgos que puedan afectar a la empresa, tanto de manera interna como externa. Esto, para luego establecer planes de contingencia y a futuro que puedan contener estas vulnerabilidades.

Objetivos específicos

1. Identificar y clasificar amenazas y fallas relacionadas con comunicaciones.
2. Evaluar riesgo (probabilidad × impacto) y priorizar hallazgos.
3. Proponer controles técnicos, procedimentales y contractuales.
4. Entregar un plan de implementación con estimación de costos y cronograma por fases.
5. Definir controles de seguimiento para garantizar que las medidas no se revieran con el tiempo.

Riesgos relevados

Riesgos por causas técnicas

Detallamos riesgos basados en fallas internas o amenazas externas que puedan afectar negativamente a la empresa.

Categoria	Riesgo	Probabilidad (%)	Impacto	Descripción corta	Costo de daño causado (USD)
Controles de red	Acceso no autorizado a redes/enlaces	30–35%	Alto	Acceso lateral, exfiltración, interrupción de servicios críticos.	$4.88M
	Configuraciones inseguras (routers/switches/firewalls/SBC)	32%	Alto	Acceso no autorizado y exposición masiva por servicios mal configurados.	$4.24M – $4.88M
	Ausencia de monitoreo centralizado (NOC insuficiente)	67% detección tardía	Alto	Mayor tiempo de compromiso y daño reputacional.	$4.88M (+$1M detección tardía)
	Ataques DDoS a servicios VoIP/enlaces	25–30%	Alto	Interrupción de servicios críticos y sobrecarga operativa.	$4–9M
	Falta de parches/firmware en equipos de red	26–30%	Alto	Explotación remota y persistencia en red.	$4.88M (hasta $10M en infra
	Uso de protocolos inseguros (Telnet, HTTP, SNMPv1)	30%	Moderado–Alto	Intercepción de credenciales y acceso no autorizado.	$4–5M
Mecanismos de seguridad asociados a servicios en red	Falta de cifrado/autenticación en VPN/Túneles/SIP	30–35%	Alto	Interceptación de tráfico y espionaje de comunicaciones.	$4–5M
	Exposición de VoIP a Internet sin SBC/firewall	30%	Alto	Fraude telefónico y denegación de servicio.	$4–9M
	Intercepción/manipulación de datos en tránsito	30–35%	Alto	Modificación o robo de datos sensibles.	$4.88M
	Dependencia de proveedores sin SLA de seguridad	20–30%	Alto	Compromisos de cadena de suministro y multas regulatorias.	$4.9M
Segregación de redes	Ausencia de separación entre redes (corp/NOC/clientes)	80%	Muy Alto	Movimiento lateral y exposición a gran escala.	$5.9–6.8M
	Tráfico VoIP/administrativo compartido sin controles	25–35%	Alto	Exfiltración de datos y caídas de servicio.	$4–9M
Intercambio de información con partes externas	Transmisión de información sensible sin cifrado/trazabilidad	50–72%	Muy Alto	Exposición de PII y sanciones regulatorias.	$4.88M
	Ausencia de políticas claras de intercambio (SFTP/NDA)	20–30%	Alto	Errores en manejo de datos y riesgo por proveedores.	$4.9M
	Mensajería electrónica — Phishing/spoofing	50–60%	Muy Alto	Robo de credenciales y ransomware por ingeniería social.	$4.88M
	Ausencia de NDAs/confidencialidad con proveedores/NOC	20–30%	Alto	Fuga de información técnica o comercial.	$4.9M
Total		35%-41%			$74.12-87.86M

- **Probabilidad**: Datos estadísticos del último año (2024) de empresas que sufrieron estos ataques, que determinan la probabilidad de que ocurra este riesgo si no aplicamos los controles requeridos.
    - **Total**: Promedio de que ocurran todas.
- **Costo de daño causado**: Cual es el costo estimado, basándonos en los datos obtenidos del último año (2024) por sufrir este tipo de ataque.

- **+$1M detección tardía**: Si una brecha no se detecta internamente (por ejemplo, se descubre por un tercero o después de mucho tiempo), el costo promedio del incidente aumenta aproximadamente un millón de dólares**.**
- **Hasta $10M en infra crítica**: En infraestructuras críticas o de telecomunicaciones, los ataques por vulnerabilidades sin parchear (por ejemplo, routers/firewalls comprometidos) pueden tener un impacto mucho mayor que el promedio global. Los informes de 2024–2025 citan costes superiores a $10 millones en sectores críticos (energía, [redacted], salud, financiero).
- El $4.88 millones (USD) es el promedio global del costo total por brecha de datos en 2024, reportado por IBM y citado por Secureframe, Varonis y AIMultiple**.** Es una referencia base para medir el impacto general de una violación de seguridad en cualquier organización, no solo en telecomunicaciones. Se usa cuando las fuentes no desglosan el costo por tipo de ataque, y se toma

como valor medio de referencia (un benchmark global).

Riesgos por causas legales

Detallamos las multas que pueden recibirse debido a no implementar los controles requeridos provocando fallos y afectando a terceros. Se divide en tres escenarios distintos**:**

Severa (alta), moderada (media) y contenida (baja).

Causas	Brecha severa	Brecha Moderada	Contenido (pero con impacto)
Multas regulatorias federales (FTC/CFPB)	$200M – $350M		
Demandas corporativas / acuerdos judiciales	$150M – $300M	$30M–$80M	
Pagos de devoluciones a clientes comerciales & SLA rotos	$50M – $150M	$15M–$50M	$1M - 15M
Costes legales + auditorías forenses	$25M – $60M		
Remediación técnica / infraestructura	$50M – $120M	$30M–$60M	$3M - 15M
Pérdida operacional + reputacional	$25M – $60M		
Multas regulatorias modestas		$20M–$60M	$5 - 20M
Honorarios legales		$10M–$20M	
Forense/Legal			$2 - 10M
Inversión total	**$500M - $1.040M**	**$105M-$270M**	**$11M y $60M**

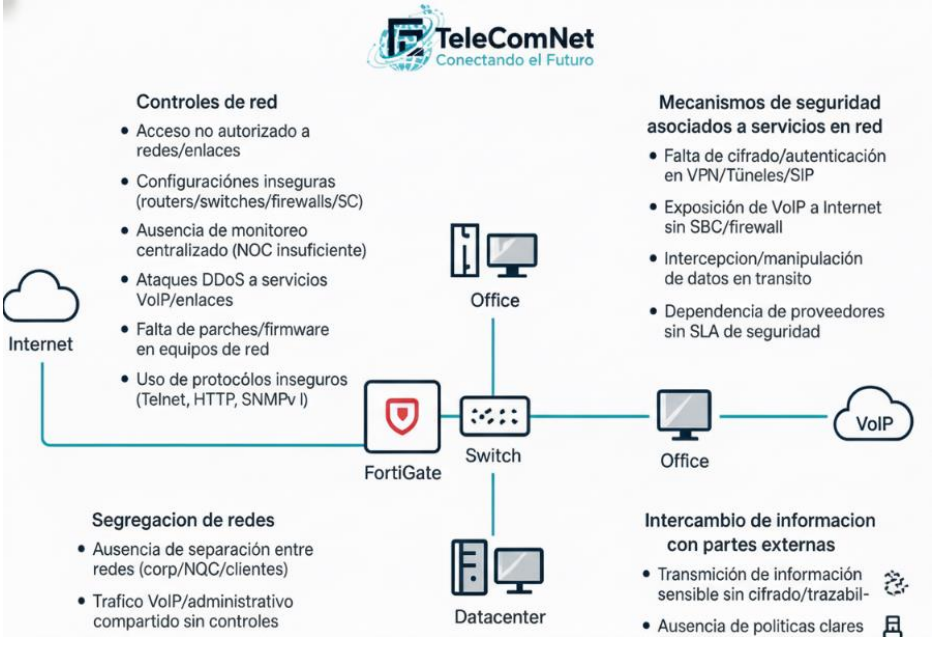
- Se considera como **brecha severa** cuando hay:
    - Exfiltración masiva de datos sensibles (clientes empresariales).
    - Fallas de parcheo.
    - Segmentación inadecuada.
    - Servicios expuestos.
    - Mala detección.

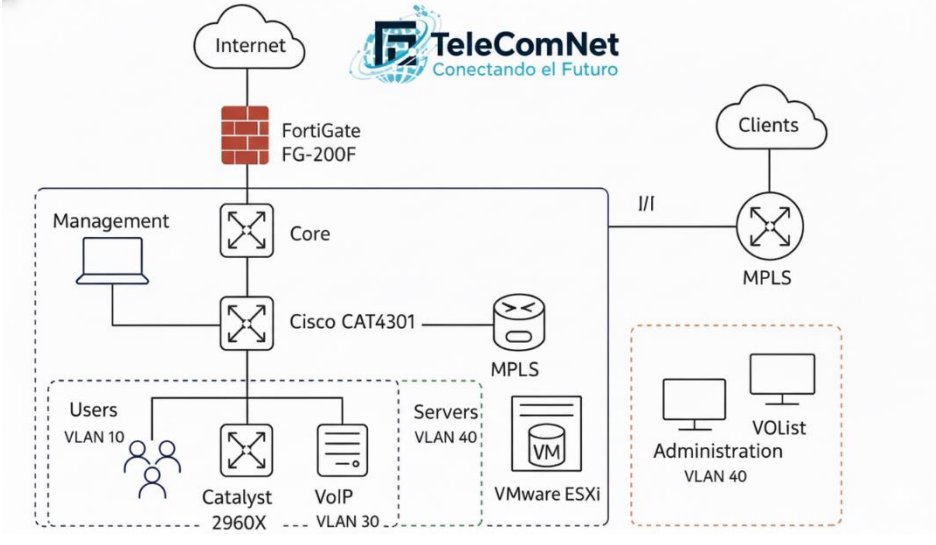
- Compromiso de proveedor.

- Se considera como **brecha moderada** cuando hay:
  - Perdiste registros empresariales, pero no **PII** (dato que puede identificar directa o indirectamente a una persona) masiva individual.
- Se considera como **brecha contenida** cuando hay:
  - Brecha en una sola sede, impacto reducido por controles rápidos.

Recursos, herramientas y permisos disponibles

Diagrama de red





Inventario de activos

Activo	Riesgos Aplicables	Plan de Mitigación
Firewall FortiGate FG-200F (Cluster HA)	42 reglas *any-to-any* antiguas. Certificado SSL Deep Inspection vencido. IPS no aplicado en muchas reglas. Firmware potencialmente desactualizado.	NGFW interno / segmentación. Administración segura + hardening. SIEM/SOC para monitoreo continuo. Plan de parches del firewall.
Routers Cisco ISR4431	ACLs viejas no utilizadas. Contraseñas MD5 (inseguras). SNMPv2c habilitado sin restricciones. BGP sin seguridad adicional.	Administración segura (SSH, HTTPS, SNMPv3). Hardening automatizado (Ansible). Segmentación por ACLs/VRFs.
Switch core Cisco CAT4301 (Núcleo de conmutadores)	VLANs definidas pero no implementadas. Red de gestión sin aislamiento. Trunks sin seguridad (sin BPDU Guard, Root Guard).	VLANs + ACLs (segmentación lógica). NAC (control de acceso por puerto). Segregación de red.
tches de Acceso Catalyst 2960X (Interruptores de acce	Usuarios y VoIP compartiendo la misma VLAN. Red administrativa dentro de la misma capa 2.	VLAN por rol (usuarios/VoIP/gestión). NAC.
Servidores VoIP (VLAN 30)	Exposición a ataques SIP. VoIP mezclado con tráfico de usuarios. Sin análisis profundo en SBCs.	Segmentación de VoIP. SIP/TLS y SRTP. IDS/IPS o perfiles VoIP del FortiGate. SIEM para señales de fraude VoIP.
Servidores VMware ESXI y Servidores (VLAN 40)	Movimientos laterales posibles por falta de segmentación. Gestión sin aislamiento.	Mover servidores a VLAN propia protegida por NGFW. Cifrado + administración segura. Plan de parches.
Túneles VPN / Acceso Remoto	Falta de MFA. Métodos inseguros de autenticación. Métodos inseguros de autenticación.	MFA (acceso remoto). Cifrado IPSec/TLS 1.3. Política de Criptografía formal.
Servicio de Correo Electrónico (Email)	Riesgos de phishing que afectan reputación. Falta de controles DMARC/SPF/DKIM. Riesgo regulatorio si se compromete correo.	DMARC/SPF/DKIM. Antiphishing avanzado. Capacitación de usuarios.
Contratos SLA con Proveedores	No hay cláusulas de auditoría. No se definen controles de seguridad. AWS sin GuardDuty/Shield/WAF.	Auditorías de SLA. Renegociación contractual. Métricas de seguridad obligatorias.
Información Sensible (Clientes/Técnicos)	Exfiltración sin trazabilidad. Transmisión sin cifrado. Falta de NDAs con terceros.	MFT/SFTP seguro. NDA + confidencialidad. Registro y auditoría.

Exports de configuración de routers/firewalls

1) Routers

a) Configuración completa de 8 de los 12 Cisco ISR4431.

b) Contiene:

i) BGP con AS interno (AS65010).

ii) Listas de acceso antiguas no utilizadas (ACL 101, 102, 105).

iii) Contraseñas de consola encriptadas con MD5 (weak).

iv) SNMP habilitado en versión v2c (sin comunidades restringidas).

2) Firewalls

a) Backup del FortiGate cluster (firmware v7.2.4).

b) Reglas principales:

i) 157 reglas en política WAN→LAN.

ii) 42 reglas “any-to-any temporary” creadas hace más de 3 años.

iii) No se aplican perfiles IPS en muchas reglas.

iv) Certificado SSL Deep Inspection vencido hace 3 meses.

3) Switches core

a) Configs muestran:

i) VLANs definidas, pero no implementadas.

ii) Red de gestión no aislada.

iii) Puertos troncales sin seguridad (sin BPDU Guard / Root Guard).

Contratos SLA con proveedores

Se entregan copias PDF de los contratos con:

1) **ISP principal (AT&T Business Fiber)**
    a) Uptime: 99.5% mensual.
    b) Soporte 24/7.
    c) Sin cláusulas de auditoría de seguridad.
    d) No se menciona cifrado “in-flight”, solo aislamiento L2.
2) **Proveedor MPLS**
    a) Garantizan 99.9% en enlaces troncales.
    b) No define controles de seguridad del plano de control.
    c) No obliga a uso de BGP TTL Security ni MD5.
3) **Proveedor Cloud (AWS)**
    a) Cuenta empresarial estándar.
    b) Sin habilitar AWS GuardDuty, Shield ni WAF en varios servicios.

Acceso al NOC

1) **Acceso físico**

a) Ingreso a la sala NOC (cuarto [redacted]).

b) Horario: [redacted].

2) Personal disponible para entrevistas

a) [redacted] — Jefe de NOC.

b) [redacted] — Administradora de redes.

c) [redacted] — Especialista VoIP/SIP.

d) [redacted] — Administrador de firewalls.

3) Información adicional

a) El NOC no documenta incidentes menores.

b) SolarWinds muestra alertas duplicadas desde hace 7 meses.

c) No existe matriz RACI formal.

Autorizaciones a análisis técnicos

1) Análisis permitido

a) Revisión completa de configuraciones.

b) Revisión de logs de: FortiGate, switches, routers, servidores DC, softswitch VoIP

c) Escaneos pasivos: ARP scanning, LLDP Discovery, Traffic sniffing (solo SPAN port preparado por el NOC).

2) **Analisis restringido:**

a) No se permiten escaneos activos (como Nmap full-scan, TCP/UDP exhaustive).

b) No se permite explotación de vulnerabilidades sin aprobación adicional.

c) No se permiten pruebas de estrés (DoS, SIP flooding, fuzzing).

3) **Pruebas activas (bajo aprobación):**

a) Escaneo de puertos controlado (solo ventanas autorizadas).

b) Escaneo de vulnerabilidades con OpenVAS.

c) Test de credenciales SSH/WinRM.

Plan de Mitigación de Riesgos (controles de activos)

Riesgo	Control	Tipo	Prioridad	Dominio ISO 27001	CAPEX mínimo	CAPEX máximo	OPEX mínimo	OPEX máximo	HH mínimo	HH máximo
Falta de segmentación y protección	VLANs + ACLs	Técnico	Alta	13.1.1 / 13.1.3	0	0	0	2000	40	80
	NGFW de segmentación	Técnico	Alta	13.1.3	2000	7000	500	1500	40	40
	NAC (RBAC)	Técnico	Alta	13.1.1	0	0	240	480	80	120
	Matriz de Flujo de Red	Procedimental	Alta	13.1.1	0	0	0	0	20	30
Configuración insegura	Administración Segura	Técnico	Alta	13.1.1	0	0	0	0	30	50
	Hardening Automatizado	Técnico	Media	13.1.1	0	5000	5000	15000	60	100
	SIEM/SOC	Técnico	Alta	13.1.1	0	0	18000	60000	0	0
	Plan de Parches	Procedimental	Alta	13.1.1	0	0	0	0	10	20
Falta de cifrado robusto	Cifrado E2E IPSec/TLS1.3	Técnico	Alta	13.1.2	0	0	0	5000	40	60
	MFA Acceso Remoto	Técnico	Alta	13.1.2	0	0	24	48	0	0
	MFT/SFTP Seguro	Técnico	Media	13.2.1	0	0	500	2000	10	10
	Política de Criptografía	Procedimental	Alta	13.2.1	0	0	0	0	15	15
Intercambio seguro y confidencialidad	DMARC/SPF/DKIM	Técnico	Alta	13.2.3	0	0	600	1800	10	20
	Antiphishing Avanzado	Técnico	Alta	13.2.3	0	0	24	60	0	0
	Capacitación/Conciencia	Procedimental	Alta	13.2.3	0	0	20	50	10	10

- **Control técnico**: Son controles implementados mediante tecnología: hardware, software, configuraciones, herramientas de seguridad. Protegen a red, los sistemas o datos reduciendo el riesgo directamente. **Los técnicos bloquean el ataque**.
- **Control procedimental**: Son procesos, normas o políticas que definen como se debe actuar para asegurar la información. Establecen pasos, roles, instrucciones y responsabilidades asegurando tareas. No requieren equipos o licencias, sino tiempo del personal. **Evita errores humanos**.

Para cada activo, se define (en la mayor medida de lo posible), los dos tipos de control juntos para que la combinación pueda crear un sistema completo de defensa en profundidad.

Controles activos

Inicialmente nos enfocaremos en los siguientes activos, siendo un total de seis. Estos son:

1. Firewall FortiGate FG-200F (Cluster HA).
2. Routers Cisco ISR4431.
3. Switch core Cisco CAT4301 (Núcleo de conmutadores).

4. Switches de Acceso Catalyst 2960X (Interruptores de acceso).
5. Túneles VPN / Acceso Remoto.
6. Servicio de Correo Electrónico (Email).

Activo(s): Perímetro (FortiGate) y Correo Electrónico

- **Control: Matriz de Flujo de Red**.
    - **Acción:** Definir y documentar qué zonas pueden hablar con qué zonas. Esto es un requisito antes de implementar VLAN. Es un prerrequisito para segmentar.
- **Control: Plan de Parches**.
    - **Acción:** Actualizar el firmware de FortiGate, aplicar parches críticos a enrutadores y conmutadores. Cierra riesgos inmediatos
- **Control: DMARC/SPF/DKIM**.
    - **Acción:** Configurar los registros DNS para proteger el dominio de correo de TeleComNet contra la suplantación de identidad. Asegura el intercambio de información.
- **Control: Capacitación/Conciencia**.

- **Acción:** Lanzar la primera campaña de simulación de phishing y concientización para todos los empleados.

- **Control: NGFW de Segmentación**.
  - **Acción:** Una vez que las VLAN estén activadas, se crean políticas granulares en el FortiGate (usando la capacidad de NGFW) para que actúe como el firewall interno entre zonas (Ej.: Los usuarios no pueden iniciar conexiones a servidores, solo al revés).

Activo: Red Interna (Switches Core y Acceso)

- **Control: VLAN + ACL**.
  - **Acción:** Implementar básicamente las VLAN definidas (Ej.: VLAN 10 Usuarios, VLAN 30 VoIP, VLAN 40 Servidores) y aplicar ACL en los conmutadores para controlar el tráfico entre VLAN. La red de gestión debe moverse a VLAN.

Activo: Acceso Remoto (VPN)

- **Control: MFA Acceso Remoto**.
  - **Acción:** Desplegar una solución de Multi-Factor Authentication (MFA) para todas las conexiones VPN de empleados y administración. Autentificación robusta.

- **Control: Política de Criptografía**.

- **Acción:** Formalizar y publicar la política que exige cifrado robusto (TLS 1.3, IPSec) para todos los servicios nuevos.

Activo: Equipos de Red (Routers)

- **Control: Administración Segura**.
  - **Acción:** Deshabilitar protocolos inseguros y forzar el uso de SSH, HTTPS y SNMPv3 en todos los enrutadores y conmutadores para la gestión.

Activo: Equipos de Red (Routers) y Perímetro (FortiGate)

- **Control: Endurecimiento Automatizado**.
  - **Acción:** Comenzar el desarrollo de playbooks (Ej.: Ansible) para estandarizar las configuraciones seguras y asegurar que no se reviertan.

Activo(s): Los cinco activos iniciales

- **Control: SIEM/SOC**.
  - **Acción:** Iniciar la ingesta de logs de los 5 activos priorizados (FortiGate, Routers, Switches, VPN, Email) en la solución SIEM/SOC para monitoreo 24/7. Ya viene incluido en el servicio gestionado contratado, solo

hay que habilitar el envío de logs. No tiene costo propio.

- **Control: Antiphishing Avanzado**.
    - **Acción:** Desplegar la solución técnica (filtro/sandbox) para el correo.

Plan de continuidad de los controles

Objetivo

El objetivo del plan de continuidad es asegurar que los controles implementados en el proyecto mantengan su eficacia a lo largo del tiempo mediante actividades operativas recurrentes. Esto para poder garantizar:

- Que los controles no se degraden.
- Que la operación de seguridad sea constante y medible.
- Que el equipo de TI ejecute las tareas correspondientes sin depender de nuevas inversiones.
- Que los riesgos tratados no vuelvan a niveles altos.

Alcance del plan de continuidad

Este plan cubre los controles implementados en:

1. Firewall FortiGate FG-200F (Cluster HA).
2. Routers Cisco ISR4431.
3. Switch core Cisco CAT4301 (Núcleo de conmutadores).
4. Switches de Acceso Catalyst 2960X (Interruptores de acceso).
5. Túneles VPN / Acceso Remoto.
6. Servicio de Correo Electrónico (Email).

Controles recurrentes

1) **Plan de Gestión de Parches**
    a. Frecuencia: Mensual.
    b. Responsable/s: Equipo de Redes + Seguridad.
    c. Objetivo: Asegurar que todos los activos se mantengan actualizados.
    d. Riesgo controlado: Exposición por software sin parche.
2) **Matriz de Flujo de Red (Actualización)**
    a. Frecuencia: Anual o ante cambios significativos.
    b. Protección: Mantiene la segmentación correcta.
    c. Riesgo controlado: Movimientos laterales y reglas innecesarias.
3) **Política de Gestión de Excepciones**
    a. Frecuencia: Continua.
    b. Objetivo: Evitar que cambios ad-hoc rompan los controles.
    c. Ejemplo: Reglas temporales en firewall con fecha de expiración.
4) **Política de Criptografía**
    a. Frecuencia: Anual.
    b. Obliga al uso de: TLS 1.3, IPSec, AES-256, SSHv2.

5) **Política de Capacitación**
    a. Frecuencia: Trimestral.
    b. KPI: Reducción de clics en phishing.
6) **Política de Privilegios y Gestión de Accesos**
    a. Frecuencia: Mensual + trimestral.
    b. Actividades:
        i. Revisión de accesos.
        ii. Baja de usuarios inactivos.
        iii. Validación MFA.

Inversiones

División de tareas

Vamos a dividir nuestras prioridades (los controles de activos del plan de mitigación) en tres fases para iniciar el proyecto con una estimación total de 9 meses.

Fase 1

El objetivo de esta fase es cerrar las brechas más obvias y de mayor riesgo que no requieren una reingeniería completa de la red.

- Matriz de flujo de red.
- Plan de parches.
- DMARC/SPF/DKIM.
- Capacitación/Conciencia.
- MFA Acceso Remoto.

Diagrama de actividades (Fase 1)

		Semanas											
Actividad	Duración (semanas)	1	2	3	4	5	6	7	8	9	10	11	12
Matriz de flujo de red	1												
Plan de parches	0,2												
DMARC/SPF/DKIM	0,5												
Activación OPEX (suscripción)	0,2												
MFA Acceso Remoto	0,2												
Capacitación/Conciencia	0,25												
Activación OPEX	0,2												
Validación y pruebas	1												
Buffer/Correciones	1												

Como podemos ver, hay un par de puntos importantes a destacar:

1) La activación OPEX son servicios, suscripciones anuales o una simple activación que deben iniciarse durante cada fase. Dependen de un servicio contratado del CAPAX especifico. Lleva un solo día (menos realmente).
2) Como medimos en semanas, las actividades que sean fraccionarios los redondeamos a 1 directamente.
3) Destaquemos, que agregaremos dos semanas extras. Uno para pruebas del sistema y otro para realizar correcciones de lo hallado en el periodo de pruebas.

Como podemos ver, ahorramos 5 semanas de trabajo, pasando de 12 semanas teóricas (3 meses para la primer fase) a tan solo 7 semanas de trabajo total.

Fase 2

Esta es la fase de trabajo pesado. Usando la Matriz de Flujo de la fase anterior, se implementa la segmentación real.

- VLAN + ACL.
- NGFW de Segmentación.
- Cifrado E2E (IPSec / TLS 1.3).
- Administración Segura.

Diagrama de actividades (Fase 2)

		Semanas											
Actividad	Duración (semanas)	1	2	3	4	5	6	7	8	9	10	11	12
VLAN + ACL	3												
Activación OPEX (FWaaS/SASE)	1												
	0,2												
Cifrado E2E (IPSec / TLS 1.3)	2												
Administración Segura	1,25												
Validación y pruebas	1												
Buffer/Correciones	1												

De esta forma, como podemos observar, estamos ahorrando un total de 2 semanas de las 12 semanas (3 meses) esperadas del total.

Fase 3

Con la red segmentada y endurecida, el foco pasa a ser la detección y la automatización.

- NAC (RBAC básico).
- SIEM/SOC.
- Antiphishing Avanzado.
- Endurecimiento Automatizado.
- Política de Criptografía.
- MFT / SFTP (Configuración).

Diagrama de actividades (Fase 3)

		Semanas											
Actividad	Duración (semanas)	1	2	3	4	5	6	7	8	9	10	11	12
NAC (RBAC básico)	3												
SIEM/SOC	0,2												
Antiphishing Avanzado	0,2												
Endurecimiento Automatizado	2,5												
Activación OPEX (SW SaaS)	0,2												
Política de Criptografía	0,4 a 0,6												
MFT / SFTP (Configuración)	0,2 a 0,4												
Validación y pruebas	1												
Buffer/Correciones	1												

Siendo la única fase en la que se completan las 12 semanas (3 meses) para realizar en su totalidad esta última etapa.

Diagrama de actividades – Total

Ahora podemos resumir las tres fases de la siguiente manera:

		Meses								
Actividad	Duración (meses)	1	2	3	4	5	6	7	8	9
Fase 1	3									
Fase 2	3									
Fase 3	3									

Aunque cabe aclarar, que considerando que las dos primeras fases nos ahorran un total de 7 semanas, estamos hablando de que el proyecto equivaldria a un total de 8 meses (de 7,25 que redondeamos para arriba). Siendo asi, que completariamos tal proyecto un mes antes de lo planeado. De esta forma, nuestro diagrama final quedaria de la siguiente manera:

		Meses								
Actividad	Duración (meses)	1	2	3	4	5	6	7	8	9
Fase 1	3									
Fase 2	3									
Fase 3	3									

Estimación de inversión

Inversión CAPEX

Son inversiones en bienes o infraestructura física que tienen una vida útil prolongada. Ej.: Comprar un firewall nuevo, adquirir un switch core, un SBC, construir una sala de comunicaciones o actualizar cableado estructurado. Se paga una sola vez, se capitaliza y se amortiza a lo largo de varios años. Todo gasto vinculado a infraestructura o equipamiento duradero.

Fase (Duración)	Controles Implementados (H/H del Plan)	Costo de mano de obra (CAPEX)
Fase 1 (Meses 1-3)	Matriz de Flujo (30)	$9,000
	DMARC/SPF/DKIM (20)	(60 H/H x $150/hora)
	Capacitación (Configuración) (10)	
Fase 2 (Meses 4-6)	VLAN + ACL (80)	$34,500
	Cifrado E2E (IPSec/TLS) (60)	(230 H/H x $150/hora)
	Administración Segura (50)	
	NGFW de Segmentación (40)	
Fase 3 (Meses 7-9)	NAC (RBAC) (120)	$36,750
	Endurecimiento Automatizado (100)	(245 H/H x $150/hora)
	Política de Criptografía (15)	
	MFT/SFTP (Configuración) (10)	
Subinversión total	Total 535 H/H	$80,250

Inversión OPEX

Son los costos recurrentes necesarios para operar, mantener o licenciar los sistemas y servicios. Ej.: Licencias anuales de firewall o antivirus, pago mensual de enlaces MPLS/internet, soporte técnico contratado, servicios de monitoreo o cloud. Se paga cada mes o año y se registra como gasto operativo en el mismo periodo. Todo gasto periódico para mantener la operación y seguridad.

Fase (Inicio)	Servicios OPEX (Suscripción Anual)	Costo anual mínimo (USD)	Costo anual máximo (USD)
Fase 1 (Meses 1-3)	Labor Recurrente (Plan de Parches)	$18,000	$36,000
	MFA (Acceso Remoto)	$7,200	$7,200
	Capacitación (Conciencia)	$7,000	$7,000
	DMARC / SPF / DKIM	$600	$1,800
Fase 2 (Meses 4-6)	NGFW (FWaaS / SASE)	$10,000	$15,000
Fase 3 (Meses 7-9)	SIEM / SOC	$18,000	$60,000
	Endurecimiento de SW (SaaS)	$5,000	$15,000
	Antiphishing Avanzado	$8,400	$8,400
Subinversión total		$74,200	$150,400

Inversión de continuidad

Control	Costo Anual (USD)	HH/año	Descripción de la Actividad de Continuidad
Plan de Parches	$18,000 – $36,000	120–240 HH	Aplicación mensual de parches en Firewalls, Switches, Routers, VPN y Email. Validación y rollback.
SIEM/SOC	$18,000 – $60,000	96 HH	Revisión semanal de alertas, reunión mensual con SOC, ajuste de casos de uso.
Auditorías SLA / Revisión de Controles	$14,400	96 HH	Auditorías trimestrales de cumplimiento, revisión de reglas, controles y evidencias.
NGFW (FWaaS)	$10,000 – $15,000	48 HH	Revisión de políticas, reglas, logs, perfiles IPS/AV, validación de segmentación.
Endurecimiento Automático (SaaS)	$5,000 – $15,000	48 HH	Validación de configuraciones estándar, detección de desviaciones, corrección.
Antiphishing Avanzado	$8,400	24 HH	Gestión mensual de reportes, análisis de intentos, ajustes de políticas.
MFA Acceso Remoto	$7,200	24 HH	Altas/bajas de usuarios, revisión de fallas de autenticación, tokens.
Capacitación (Conciencia)	$7,000	16 HH	4 campañas anuales de phishing, reportes y retroalimentación.
DMARC / SPF / DKIM	$600 – $1,800	24 HH	Revisión de informes DMARC, monitoreo de intentos de spoofing.
Monitoreo de Software / SLA Secundario	$0 – $500	24 HH	Verificación mensual de vigencia y configuración de software crítico.

De esta manera, tendríamos:

- **Costo anual mínimo**: $88,600.
- **Costo anual máximo**: $165,300.
- **Tiempo interno requerido**: 520 – 640 HH/año equivalente a 30% del tiempo de un empleado full-time (1 FTE de jornada).

Inversión total

Componente de Inversión	Costo mínimo (USD)	Costo máximo (USD)
Subinversión total CAPEX	$80,250	$80,250
Subinversión total OPEX	$74,200	$150,400
Subinversión plan continuidad	$88,600	$165,300
Inversión total	$243,050	$395,950

Así, tenemos la inversión total que debemos realizar en estos primero nueve meses del primer año para asegurar estos cinco

primer activos. Además, considerando la continuidad de estos programas para evitar futuros sucesos no deseados.

¿Por qué deberían invertir?

La inversión no busca solamente implementar mejoras para que haya una funcionalidad del sistema. Si no, buscamos asegurar la continuidad del negocio y proteger sus ingresos.
Hoy TeleComNet pierde competitividad porque no cumple con varios requisitos mínimos exigidos por clientes, auditorias, contratos SLA y practicas de seguridad en la empresa.
Generando desconfianza en sus clientes y perdiendo credibilidad en cuanto asegurar la protección y transmisión de sus datos.
Aplicar estos controles no solo asegura una mayor confianza en quienes buscan solicitar sus servicios, si no, que es un seguro de vida en caso de que algo salga mal.

Inversión total por perdidas por no invertir

Debemos tener en cuenta que el costo total, según la variación de las brechas aplicables por no aplicar estos controles,

conllevaría una inversión total de $11M a $1.04B de dólares, como lo indica la siguiente tabla:

Tipo de Brecha	Inversión Técnica (USD)	Inversión en legales (USD)	Inversión totales (USD)
Brecha Contenida	$4.88M – $9M	$7M – $51M	$11M – $60M
Brecha Moderada	$4.24M – $9M	$100M – $261M	$105M – $270M
Brecha Severa	$4.24M – $10M	$495M – $1.03B	$500M – $1.04B

Pudiendo ahorrar esto con un pequeño costo de $243,050 a $395,950 dólares. Y esto es solo para los primeros 5 activos que estamos controlando. Aun faltarían los otros 5 para mitigar el resto de los errores que se llevarían a cabo en una segunda parte, si se llegase a continuar el proyecto.

Podemos compararlo con el caso de [redacted], que, si bien el área de esta empresa era el sector financiero, compartía casi la mayoría de estos riesgos (solo que en nuestro caso sobrepasamos estos), teniendo que pagar casi más de miles de millones por perdida de datos, mala seguridad y multas corporativas debido a la ineficiencia de sus sistemas de seguridad. Y hablando esto en 2017.

Retorno de la inversión

Además, considerando el **retorno de inversión (ROI)** podemos hablar de una recuperación importante de:

Escenario	ROI (inversión mínima)	ROI (inversión máxima)
Brecha contenida (11M)	4.425% – 24.583%	2.678% – 15.053%
Brecha moderada (105M–270M)	43.100% – 110.975%	26.419% – 68.088%
Brecha severa (500M–1.04B)	205.658% – 427.801%	126.173% – 262.551%

Por lo que, la inversión total por implementar los controles de mitigación sobre los activos a tratar es demasiado mínima comparado con la perdida tras sufrir alguna de estas brechas legales (y esto incluye los riesgos técnicos según la brecha correspondiente, puede verse esto en la tabla anterior). Es por ello, que ya el invertir en estos planes de mitigación no es solo por un simple control, es una obligación para poder proteger la continuidad de la organización.

Conclusión

Aunque tal vez en un inicio no lo parezca, hay muchas áreas que debemos de cubrir, cada sector y cada pequeña segmento de una red corporativa puede conllevar a una gran pérdida económica e incluso a una bancarrota superando las expectativas. Es inmediatamente necesario empezar a aplicar estos controles para poder evitar consecuencias masivas, más allá de lo económico, también los datos sensibles que quedarían expuestos si alguien decidiera provocar un ataque. Tenemos muchos casos similares como [redacted], que, por no asegurar sus defensas, perdieron tanto en lo económico como en la confianza de sus clientes. Como dije anteriormente, esto no es solo una inversión para asegurar el momento, es un seguro de vida que evitara que todo finalicé en el momento.

Bibliografía

1. **Riesgos, probabilidades, costos**:
    a. https://www.varonis.com/blog/cybersecurity-statistics
    b. https://aimultiple.com/network-security-statistics
    c. https://secureframe.com/blog/data-breach-statistics
    d. https://spacelift.io/blog/cloud-security-statistics
2. **Multas**:
    a. ftc.gov/enforcement
    b. consumerfinance.gov/enforcement
    c. sec.gov/litigation
    d. gao.gov/reports-testimonies
    e. enforcementtracker.com
    f. ibm.com/reports/data-breach
3. [redacted]:
    a. https://www.breachsense.com/blog/[redacted]/
    b. https://archive.epic.org/privacy/data-breach/[redacted]/
    c. https://www.mozilla.org/en-US/products/monitor/[redacted]/