UNIVERSIDAD NACIONAL DEL LITORAL

Facultad de Ingeniería y Ciencias Hídricas

Auditoría Informática

Empresa: ICOP Santa Fe S.R.L.

Alumnos: Adjadj, Agustín; Bargas, Santiago.

Profesores: Mollerach, Edgardo Darío; Robledo, Miguel Ángel.

Fecha de Entrega: 24/11/2025

En esta etapa, se buscará conocer la organización donde se realizarán los trabajos de auditoría informática, tener un conocimiento amplio del área de sistemas e infraestructura tecnológica de la misma, identificando los recursos con los cuales se cuenta para llevar adelante sus funciones. Además, se buscará conocer la problemática existente que permita abordar la tarea de auditoría, seleccionando aquellas más relevantes o necesarias.

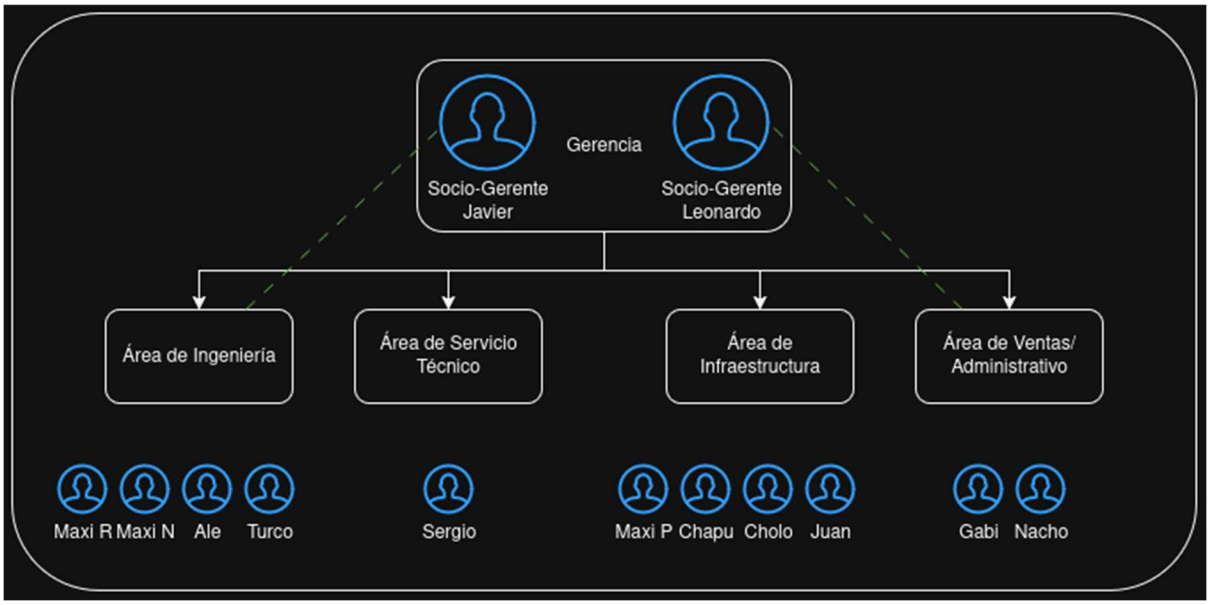
Nuestro punto de inicio será Javier, uno de los socios gerentes de ICOP, que en concordancia con Agustín (quién trabaja en la empresa y también es uno de los hacedores del informe) generarán las respuestas e informes necesarios. También, Alejandro, del área de Ingeniería será un apoyo para algunos relevamientos importantes.

Presentación de la organización

ICOP, fundada en 1974 en Santa Fe, es una de las empresas más antiguas del sector informático de la región. A lo largo de más de 40 años ha evolucionado de ser un proveedor de computadoras e insumos a convertirse en un referente en soluciones integrales de tecnología, conectividad y energía.
La empresa brinda servicios a organismos públicos, empresas y particulares, ofreciendo desde provisión de equipos y servidores, hasta diseño e implementación de proyectos de redes, seguridad informática, virtualización, soluciones en la nube y desarrollo de centros de datos. En los últimos años amplió su alcance al área de Energía, incorporando proyectos eléctricos y obras llave en mano con equipos multidisciplinarios.
El objetivo de la empresa es la de proveer productos y servicios de alta calidad que acompañen el crecimiento de sus clientes, manteniendo independencia de fabricantes y plataformas para ofrecer asesoramiento objetivo y eficiente.
Dentro de sus servicios, podemos encontrar los siguientes como el área de injerencia para los clientes:

- Provisión, instalación y mantenimiento de hardware y software.
- Implementación y administración de servidores, virtualización y servicios en la nube.
- Cableado estructurado, fibra óptica y enlaces de datos.
- Consultoría en redes y seguridad informática.
- Configuración de routers, switches, firewalls y VPNs.
- Diseño y construcción de centros de datos.
- Proyectos eléctricos y de automatización.

A continuación, se presenta un organigrama general de la organización



Si bien se ven los sectores bien definidos, las áreas trabajan de forma general en constante comunicación para las correctas puestas en marcha de algunos servicios.
Javier, uno de los socios gerente, es el encargado del área de Ingeniería. Dicha área de ingeniería trabaja en conjunto con el área de Servicio Técnico en caso de ser requerido. En tanto, el área de infraestructura depende del área de ingeniería para empezar los proyectos de tendido de fibra o cableados, a fin de disponer de los equipos necesarios.
El área de ventas/administrativo, siendo Leonardo el encargado, es primordial para que los proyectos de Ingeniería empiecen.

Presentación y organización del Área IT

El área IT dentro de la empresa, es el Área de Ingeniería y el Área de Servicio Técnico en el organigrama. Internamente no se tiene un sector específico para los equipos informáticos, sino que se asignan recursos cuando surgen necesidades y mejoras en la red interna, ya que el personal está capacitado para realizar estas tareas.
Dicha capacitación del personal tiene en cuenta muchos aspectos, pero a considerar entre ellos son de interés:

- Manejo de equipos de red y seguridad (Switches, Routers, AP’s)
- Conocimiento en manejo de Sistemas Operativos Windows/Linux.
- Administración de servidores y servicios (Web, Correo, etc.)
- Conocimiento de equipos informáticos para resolución de problemas.
- Conocimiento en soporte técnico en equipos informáticos.

Infraestructura y equipamiento

Equipos de seguridad	Fortigate 70F
Equipos de red	2x Switch Administrable HP 24 bocas
	2x FortiAP
Equipos de almacenamiento	NAS Seagate [Backups]
Servidores	Servidor HP [Producción]
	Servidor IBM [Producción]
	Servidor IBM [Terminal Server]
Dispositivos de comunicación	6x Teléfonos Internos + Central Telefónica
	7x Celulares corporativos
Dispositivos de vigilancia	4x Cámaras de seguridad IP
Computadoras	5x Notebooks de empresa + 4x PC's de Escritorio + 3x PC's Personales
UPS	UPS 10KVA + 3x UPS 1000VA [Oficinas]
Otros	2x Impresora [Brother + Epson] IP

Dentro de la infraestructura, ninguna de las PC's correspondientes a la empresa está inventariada con respecto a un ID o sus características.
Sin embargo, se utiliza el software ESET Cloud para ver el inventario de los equipos y su hardware.

Aplicaciones y servicios IT

Los servicios internos están corriendo sobre Proxmox en los servidores de producción, que tienen un esquema de redundancia ante fallos.

Software de documentación	Netbox	Utilizado para documentación a más alto nivel de los equipos y contraseñas, servicios, fotos, esquemas, etc. de los distintos clientes. Se está migrando en la actualidad para deprecar Rattic.
	Rattic	Utilizado para documentación de equipos y contraseñas de los clientes.
	MediaWiki	Utilizado para documentación interna de eventos y procesos especiales a llevar a cabo. También, muy importante para la documentación de los backups.
Correo electrónico	Carbonio	Utilizado como servidor de correos de la empresa. Los DNS están manejados por Cloudflare y publicados.

		Dentro, contiene Fail2Ban y varios plugin de configuraciones.
Servidor Web	WordPress	La empresa cuenta con un servidor web, que no se tiene en mantenimiento ni actualizado bajo WordPress.
Servidor de archivos	Zentyal	Dentro de uno de los servidores, corre el servidor de archivos de la empresa, donde tienen documentos de implementaciones de cada cliente e información de varios tipos, como manuales, cursos, instaladores, etc. Es uno de los servicios más importantes.
Gestión de empresa	Sistema de sueldo	Existe un sistema de sueldos desarrollado en Cobol, en una máquina virtual XP donde se encuentra el sistema de sueldos. El mismo, es un desarrollo hecho a misma por la empresa para su gestión interna.
	Control de horario	Existe un sistema de control de ingreso/egreso a la oficina.
	OpenOrange	Sistema de gestión comercial, de stock, balances e inventario, utilizado en un servidor con una base de datos.

Dentro de los servicios externos, podemos ver varios trabajando en la Nube, entre ellos:

Antivirus	ESET Protect Cloud	Servicio en la nube de protección antivirus, con manejo de los agentes, políticas de seguridad, tareas, etc.
Mesa de ayuda	Invgate	Utilizado por la empresa para el manejo de tickets de los clientes, seguimiento de tareas con horarios, trazabilidad y procedimiento.

Videoconferencia	Zoom	Cuenta de zoom con licencia para videoconferencias y reuniones con clientes.
Servicios de Hosting	DonWeb + Claro Cloud	Servicio de hosting alquilado por la empresa para prestar servicios a terceros a través de las mismas. Dentro de ellas hay servicios propietarios de clientes.
Seguimiento de tareas	Trello	Seguimiento interno de tareas de la empresa a fin de definir roles y procesos a realizar por los recursos.

La documentación de los sistemas será la publicada por los mismos en los entornos de documentación, y se los buscará cada vez que se necesite de ellas. En tanto a los desarrollos internos, que es uno, no se tiene una documentación actualizada.
Los sistemas están en general Open Source y los que son pagos, se tienen todas las documentaciones en internet, por lo que no se guarda una copia física o en algún servidor.
En tanto a los Sistemas Operativos utilizados, se genera la lista:

- 11x Microsoft Windows 10 Pro
- 1x Microsoft Windows 10 Pro for Workstations
- 1x Microsoft Windows 11 Pro
- 1x Microsoft Windows Server 2019 Standard
- 1x Microsoft Windows Server 2022 Standard Evaluation
- 2x Ubuntu

Mapa de comunicaciones

La empresa, gracias a su equipo de seguridad Fortigate, maneja los ruteos y conexiones tanto internas, como con clientes (A través de túneles IPSEC), como los empleados de forma remota (A través de SSL VPN), como los accesos por cualquier persona externa ya sea al servidor de correos, como al servidor web (mediante políticas de acceso).
Internamente, la empresa tiene dividida en 2 la red:

- Un direccionamiento para servicio técnico.
- Un direccionamiento para todas las demás áreas.

Hoy en día, se está planificando migrar a distintos direccionamientos, pero los servicios están en el mismo direccionamiento que el área “general”.
Para poder navegar, se necesita tener un usuario/contraseña dentro de ICOP, a fin de tener posibilidad de tener acceso a servidores, internet, etc.
De forma externa, se tienen políticas de acceso con detección de intrusos gracias a los servicios contratados de Fortigate.
Todos los equipos informáticos tienen antivirus ESET instalados, con políticas de seguridad predefinidas y controladas por ESET Protect Cloud, donde se tiene un dashboard general.
La empresa cuenta con 2 enlaces de internet, con sus respectivas IP públicas y políticas de acceso SD-WAN, tanto para navegar como para ingresar por VPN. Las mismas son Claro y Gigared. También, se tiene un enlace DMZ de Claro para realizar pruebas específicas por si se quieren probar nuevos accesos “fuera” de la empresa.

Seguridad

Actualmente, la organización no cuenta con una política formal de Seguridad de la Información. Los mecanismos de confidencialidad se limitan principalmente al control de accesos a redes y recursos de los sistemas, complementados por el registro de eventos a través de logs.
En cuanto a la capacitación, se realizan cursos de seguridad informática de manera eventual, a través de proveedores como Fortinet (Forti) u otras instancias de formación que resulten de interés para el personal.

Resguardos y plan de continuidad IT

Existe una política de backups en base a los servicios utilizados, servidor de archivos y máquinas virtuales.

Netbox	A diario a las 00:00 se genera un backup de la base de datos. Además, cada 1 semana se genera un dump de la máquina virtual, guardando máximo 2 backups.
Rattic	Una vez a la semana, se genera un backup de la base de datos. Además, cada 1 semana se genera un dump de la máquina virtual, guardando máximo 2 backups.
MediaWiki	Una vez a la semana, se genera un backup de la base de datos. Además, cada 1 semana se genera un dump de la máquina virtual, guardando máximo 2 backups.
FileServer Zentyal	A diario a las 2:00 se genera un cron sin borrado de los archivos modificados en el día. Además, cada 1 semana se genera un dump de la máquina virtual, guardando máximo 2 backups.
OpenOrange	A diario a las 02:00 se genera un backup de la base de datos. Además, cada 1 semana se genera un dump de la máquina virtual, guardando máximo 2 backups.
Servidor de Backups	Además de guardar los backups, una vez a la semana (los domingos) genera un backup del backup de la semana, en otra partición, generando más redundancia de los archivos que resultan clave. En esto están tenidos en cuenta todos los anteriores descriptos.

Todos los días se hace control integral de los backups. En base a esto, no existe documentación interna ante plan de contingencia, ya que, se espera que se sepa realzar un backup de cero.
En tanto, hay otros backups que se hacen manuales según se realicen cambios, o algunos que están en el servidor de archivos, como pueden ser del Fortigate o configuraciones de switches, que no se tendrán en cuenta en este esquema.

Relaciones con terceros

La principal fuente de trabajo de ICOP se basa en la prestación de servicios a terceros. Entre los usuarios de la organización se encuentran diversos entes públicos y privados, tales como: Aire de Santa Fe, ARCORE, Banco Bica, Caja Municipal de Jubilaciones, Centro de Justicia Penal, IAFAS, IAPSER, Municipalidad de Santa Fe, Poder Judicial de la Provincia de Santa Fe, Premoldeados Bertone, Sanatorio Garay y Tresal, entre otros.

En cuanto a proveedores y servicios contratados, la organización mantiene convenios con diferentes terceros, entre los que se destacan: Invgate, Claro Cloud, DonWeb y OpenOrange.

Problemas y Soluciones.

A partir de este momento, se detallarán cada uno de los problemas, junto con un riesgo asociado a la no actuación por parte de la empresa, una o más soluciones propuestas, y el esfuerzo asociado a cada una.

Además, se dejan conclusiones finales para que la organización este enterada de la generalidad.

Ausencia de una política formal de seguridad de la información

Problema

La seguridad de ICOP se basa en herramientas técnicas como el firewall Fortigate y el antivirus ESET, gestionadas por el personal técnico sin un documento que unifique criterios. Los controles se limitan al acceso por contraseña y al registro de logs, mientras que la capacitación del personal es esporádica y no planificada.
Asimismo, tampoco hay una política de seguridad de la información física. Hay varias impresoras y documentos que no siguen una política de eliminación en caso de no utilizarse más.

La seguridad de los datos informatizados está controlada por accesos a las redes, a través de usuario/contraseña, ya sea a navegación como a conexiones a servidores de archivos. No existe un ingreso “guest”. Lo mismo pasa con las conexiones VPN SSL y VPN IPSEC. Los usuarios no están centralizados (por ejemplo, en un LDAP) sino que hay varios accesos con mismos usuarios, pero contraseñas no necesariamente similares.

No existe documentación sobre la seguridad informática tenida en cuenta, tanto informática como física. Todo es por conocimiento de leer reglas o investigar por parte del área de ingeniería.

Riesgo de no actuar

Continuar sin una política formal expone a la empresa a riesgos significativos. La gestión de la seguridad es reactiva y depende del conocimiento del personal técnico. Esto puede llevar a una respuesta lenta y caótica ante un incidente de seguridad, incrementando el tiempo de inactividad.
A nivel legal, la empresa podría estar en incumplimiento de la Ley 25.326 de Protección de Datos Personales, exponiéndose a sanciones por no tomar las medidas de seguridad adecuadas para proteger la información de terceros.

Solución

Desarrollo e Implementación de una Política de Seguridad de la Información (PSI)

- **Paso 1:** La Gerencia debe liderar la iniciativa, asignar formalmente a un responsable del proyecto y comunicar la obligatoriedad de la política a toda la empresa.
- **Paso 2:** El equipo responsable debe definir qué información es la más crítica (datos de clientes, configuraciones de red, datos financieros) y los objetivos de la política (ej. "Proteger la información de los clientes y cumplir con la Ley 25.326").
- **Paso 3:** Basándose en estándares de la industria, redactar la política que establece los principios generales de seguridad.
- **Paso 4:** La Gerencia debe revisar y aprobar formalmente las políticas. Deben publicarse en un lugar accesible para todos, como el MediaWiki interno, o en documentos físicos.
- **Paso 5:** Realizar una capacitación obligatoria para **todo el personal** explicando las nuevas reglas. Cada empleado debe firmar un acuerdo de confidencialidad y adhesión a la política.

Esfuerzo

- **Estimación Económica: Bajo-Medio.**
    - *Opción 1 (Bajo Costo):* Se realiza 100% con recursos internos. El costo principal son las **horas-hombre** del Área de Ingeniería para la redacción y de Gerencia para la revisión.
    - *Opción 2 (Medio Costo)* [Recomendado]*:* Se contrata un **consultor externo** especializado en seguridad y Ley 25.326 para guiar el proceso, asegurar que se cumplan los requisitos legales y acelerar la redacción.

- **Estimación de Tiempos: Mediano Plazo (3-6 meses).** Es un proyecto que requiere análisis, consenso, redacción, aprobación y capacitación.

- **Personal Involucrado: Toda la organización.**
    - Gerencia: Aprobación y asignación de recursos.
    - Área de Ingeniería: Liderazgo, redacción y ejecución técnica.
        - Puede adherirse el consultor externo.
    - Todo el personal: Capacitación y cumplimiento obligatorio.

Inexistencia de un plan de contingencia y continuidad del negocio

La empresa ejecuta y verifica backups diarios de forma rigurosa, estando detallados en una documentación interna los mismos. Sin embargo, no existe ningún documento que detalle los pasos a seguir para recuperar los sistemas en caso de un desastre mayor. El proceso de restauración no está formalizado y depende completamente del conocimiento y la experiencia del personal técnico. Además, estos procedimientos esporádicamente han sido probados, por lo que no hay certeza de que funcionen en una emergencia real en la actualidad.

Ante un incidente grave, la falta de un plan probado podría llevar a una recuperación caótica y fallida, provocando una interrupción prolongada del servicio con pérdida de datos. Además, se presupone que el personal técnico tiene el conocimiento básico para realzar el backup a la producción.

Riesgo de no actuar

Aunque los backups se hacen bien, y la documentación de estos está bastante documentada, la restauración depende de la memoria del personal técnico y no se prueba. Ante una crisis real, ya sea por un ciberataque o pérdida de datos inesperada, la recuperación sería caótica y lenta. Esto es inaceptable para clientes clave y podría causar la pérdida de contratos y un daño grave a la documentación interna.

Solución

Formalizar y Probar un Plan de Recuperación

- **Paso 1:** El Área de Ingeniería debe escribir en el MediaWiki la guía "paso a paso" exacta de cómo restaurar cada servicio crítico (OpenOrange, Zentyal, etc.) desde cero. También, tener en cuenta un plan de cambios y revisiones, adherido a lo ya existente.
- **Paso 2:** Agendar pruebas de restauración bimestrales o semestrales en un entorno aislado (para no afectar la producción) y registrar los tiempos y problemas encontrados. Generar los cambios necesarios, planificados en el paso anterior.
- **Paso 3:** Implementar una copia de seguridad en la nube para proteger los datos contra desastres físicos (incendio, robo) que destruyan el NAS local.

Esfuerzo

- **Estimación Económica: Bajo-Medio.** La documentación y las pruebas son horas-hombre (costo bajo). La copia en la nube (Paso 3) tiene un costo mensual recurrente (costo medio-alto) dependiente de la solución implementada.
- **Estimación de Tiempos: Corto Plazo (1-2 meses)** para documentar y configurar el backup off-site. Las pruebas son un proceso continuo (semestral).
- **Personal Involucrado: Gerencia** (para aprobar el costo del backup off-site) y el Área de Ingeniería (para documentar y ejecutar las pruebas).

Dependencia de sistemas críticos con tecnología obsoleta

El sistema de liquidación de sueldos, una aplicación crítica desarrollada en Cobol, funciona sobre una máquina virtual con Windows XP, un sistema operativo sin soporte ni actualizaciones de seguridad. La plataforma es extremadamente vulnerable a ciberataques modernos y, además, la tecnología obsoleta dificulta enormemente el mantenimiento y la recuperación del sistema en caso de fallo. No existen controles de seguridad particulares para dicha máquina, sin embargo, una persona capacitada en Cobol (quien desarrolló dicho

sistema) es quien eventualmente hace cambios según necesidades correctivas que puedan surgir.

Tampoco existe una documentación del sistema para que, al no estar disponible el recurso humano con conocimiento, lo pueda seguir (sin tener en cuenta, que es un lenguaje de programación robusto y de a poco obsoleto).

Un fallo o ataque a esta máquina virtual podría paralizar la liquidación de sueldos, y una brecha de seguridad podría servir como punto de entrada para comprometer toda la red interna de la empresa. Una falla operativa puede paralizar por completo la liquidación de los sueldos, esencial para la empresa.

Riesgo de no actuar

Es uno de los **mayores riesgos** de la empresa. La VM con Windows XP es una puerta de entrada abierta para un ciberataque (ransomware) que podría paralizar la liquidación de sueldos y expandirse a toda la red. Además, el sistema depende de una sola persona y de un lenguaje (Cobol) del cual no hay documentación, lo que lo hace "inmantenible" a largo plazo.

Soluciones

Propuesta A: Aislamiento

Esto no resuelve el problema de raíz, pero reduce el riesgo inmediato.

- **Paso único:** Usar el firewall Fortigate para crear una VLAN que aísle completamente la VM de Windows XP, bloqueando todo el tráfico de red hacia y desde ésta VM, permitiendo únicamente la comunicación mínima para el funcionamiento (accesos de usuarios).

Propuesta B: Proyecto de Migración [Recomendada]

- **Paso 1:** Documentar, con la persona que lo desarrolló, todas las reglas de negocio del sistema de sueldos. Luego, evaluar la compra de un sistema moderno, ya sea como servicio o enlatado, o pensar en un desarrollarlo de nuevo, propio de la empresa.
- **Paso 2:** Seleccionar una solución, planificar la migración de datos históricos y establecer un cronograma.
- **Paso 3:** Implementar el nuevo sistema y operar ambos (el viejo y el nuevo) en paralelo durante al menos un ciclo de liquidación para validar que los resultados sean idénticos.
- **Paso 4:** Una vez validado, dar de baja y eliminar permanentemente la VM con Windows XP.

Esfuerzo

Propuesta A:

- **Estimación económica: Bajo** solo horas-hombre.
- **Estimación de tiempos: Corto Plazo (1-2 meses)**. Es una regla y pruebas de funcionamiento. Solo debe planificarse con tiempo para los nuevos accesos y permisos.
- **Personal Involucrado:** Involucra solo al **Área de Ingeniería** para la implementación. También, involucra al programador del sistema que ayude a la documentación, y el personal Administrativo para las pruebas de funcionamiento.

Propuesta B:

- **Estimación Económica: Alto.** Este es un proyecto de inversión. Implica el costo de licencias de un nuevo software o las horas de desarrollo (internas o externas), además de la migración de datos.
- **Estimación de Tiempos: Largo Plazo (6-12 meses).** Es un proyecto complejo que debe realizarse con el seguimiento de la empresa, cumpliendo con los funcionamientos.
- **Personal Involucrado: Gerencia** (aprobación de la inversión), **Área de Ingeniería** (liderazgo del proyecto), **Personal Administrativo** (para validación) y el desarrollador original (para la transferencia de conocimiento).

Servidor Web en WordPress sin mantenimiento ni actualizaciones

La empresa cuenta con un servidor web bajo WordPress que no recibe mantenimiento ni se le aplican las actualizaciones de seguridad de forma periódica. Un sitio WordPress desactualizado es un blanco fácil y común para ataques automatizados que explotan vulnerabilidades conocidas en el software, los plugin o los temas.

El ingreso está controlado por políticas de acceso del firewall Fortigate implementado.
Los controles son a nivel de red (bloqueo de IPs, Fail2Ban), pero al no estar actualizado ni en mantenimiento por alguien interno, los riesgos están vigentes.

Tampoco existe una documentación sobre cómo está configurado el mismo, sino que, si alguna vez se le hace mantenimiento, es generando bastante esfuerzo necesario y se hace de forma incompleta o defectuosa. La falta de un ciclo de vida de mantenimiento es visible, pudiendo ser un punto de entrada para ataques sofisticados contra la red interna, al confiar tanto en la seguridad perimetral.

Riesgo de no actuar

Un sitio WordPress desactualizado es un blanco fácil para ataques automatizados. Esto puede llevar a que la página sea intervenida de forma no esperada, que el servidor sea usado para

distribuir malware a los visitantes o, en el peor de los casos, que sea usado como punto de entrada para atacar la red interna de la empresa.

Soluciones

Propuesta A: Implementar un Protocolo de Mantenimiento y Hardening

- **Paso 1:** Realizar un backup completo del sitio, posterior a actualizar el núcleo de WordPress, todos los plugin y todos los temas a sus últimas versiones. Eliminar cualquier plugin o tema que no esté en uso.
- **Paso 2:** Asignar formalmente la tarea al Área de Ingeniería para que, mensualmente, revisen y apliquen todas las actualizaciones de seguridad.
- **Paso 3:** Instalar un plugin de seguridad integral, para implementar un firewall de aplicación web y monitoreo de integridad de archivos.
- **Paso 4:** Registrar los cambios y las credenciales del sitio.

Propuesta B: Plan de Migración [Recomendada]

- **Paso 1**: Quitar el servidor web local y migrar la infraestructura en la nube. Actualmente, sitios como DonWeb, Hostinger proponen gestiones de la web y hosting propios.
- **Paso 2:** Mover los DNS al nuevo servidor, y proponer el mismo seguimiento de mantenimiento del sitio (configuraciones mínimas)
- **Paso 3:** Documentar el mantenimiento, accesos y quitar todos los accesos configurados en Fortigate, dejando fuera las “puertas” de acceso anteriores.

Esfuerzo

Propuesta A:

- **Estimación Económica: Bajo-Medio.** La mayoría de las acciones son horas-hombre (costo bajo). Puede tener un costo medio si se opta por la versión *premium* de un plugin de seguridad (recomendado).
- **Estimación de Tiempos: Corto Plazo.** La limpieza inicial y el fortalecimiento se pueden hacer en **1-2 días**. El mantenimiento es un proceso continuo (pocas horas al mes).
- **Personal Involucrado: Área de Ingeniería** (ejecución y mantenimiento).

Propuesta B:

- **Estimación Económica: Alto.** Este es un proyecto de inversión. Implica el costo de hosting, mantenimiento o las horas de desarrollo (internas o externas), además de la migración de datos.

- **Estimación de Tiempos: Medio Plazo (3-6 meses).** Requiere planificación, configuración de DNS, migración de datos, pruebas, documentación.
- **Personal Involucrado: Área de Ingeniería** (para la arquitectura), **Gerencia** (aprobación de presupuesto).

Incertidumbre en la gestión de accesos y privilegios

Si bien se requiere un usuario/contraseña para acceder a la red, como se comentó con anterioridad, la auditoría reveló una falta de claridad sobre cómo se administran los permisos y privilegios de los usuarios en los distintos sistemas internos. No existe un procedimiento formal para asignar, revisar y revocar accesos, conduciendo a que los empleados acumulen más permisos de los estrictamente necesarios para sus funciones, aumentando significativamente el riesgo de fugas de información y accesos no autorizados a datos sensibles (de la empresa o de clientes), ya sea por un error humano o por el compromiso de una cuenta con privilegios excesivos.

Si bien los accesos están definidos en grupos, no existe una documentación, sino un criterio por parte del jefe de ingeniería para realizarlo, no existiendo el proceso de asignación, modificación y revocación de dichos privilegios. Tampoco existe una revisión periódica de los permisos asignados o procedimientos para baja de usuarios (Se vieron en la auditoría usuarios que no trabajan más y que aún su usuario está habilitado).

Riesgo de no actuar

La falta de un proceso formal ("incertidumbre") lleva a que exempleados mantengan sus accesos y que los empleados actuales acumulen permisos innecesarios. Esto es un riesgo de seguridad interno (errores, fugas de datos) y externo (una cuenta robada con permisos excesivos es muy peligrosa). También incumple principios de seguridad de la Ley 25.326 de Protección de Datos Personales.

Solución

Implementar una Política de Gestión de Identidad y Acceso

- **Paso 1:** Como parte de la política de la seguridad de la información, establecer el "Principio de Mínimo Privilegio" (cada empleado solo tiene el acceso estrictamente necesario para su trabajo) y formalizar que el Área de Ingeniería es la única autorizada para crear o modificar accesos.
- **Paso 2:** Formalizar los accesos, dejando las altas, bajas y modificaciones definidas, definiendo que el Área de Ingeniería lo realice en tiempo y forma.
    - **Altas:** Prohibir las solicitudes verbales. Se debe crear un formulario (digital o papel) que requiera la aprobación de un gerente *antes* de que Ingeniería cree la cuenta.

    - **Bajas:** El área Administrativa/Gerencia debe notificar *inmediatamente* al Área de Ingeniería cuando un empleado se desvincula, para que sus cuentas sean deshabilitadas el mismo día.
- **Paso 3:** Realizar una auditoría de *todas* las cuentas de usuario existentes, deshabilitar las cuentas de exempleados y ajustar los permisos del resto al mínimo privilegio necesario.
- **Paso 4:** Documentar estos procesos a fin de tener una política interna definida.

Esfuerzo

- **Estimación Económica: Bajo.** Esta solución es un proceso. El costo son las horas-hombre para definir la política y realizar la auditoría inicial.
- **Estimación de Tiempos: Corto Plazo (1-2 semanas).** La política y la auditoría inicial son rápidas de implementar. El cumplimiento es un proceso continuo.
- **Personal Involucrado: Gerencia** (para aprobar la política y hacer cumplir los formularios), **Área de Ingeniería** (para ejecutar la auditoría y gestionar las cuentas) y **Área Administrativa** (para notificar las bajas).

Falta de políticas de concientización y entrenamiento continuo en seguridad informática

La capacitación en seguridad para el personal se realiza de manera "eventual" y no como parte de un programa estructurado y continuo. Los empleados no están consistentemente informados sobre las amenazas actuales, ni sobre su rol y responsabilidad en la protección de la información de la empresa y sus clientes. El conocimiento de la seguridad es a través de noticias que se encuentran en páginas de interés para la empresa, y solo en general para los empleados del sector de ingeniería. Esto, aumenta la probabilidad de incidentes de seguridad causados por error humano. Un empleado podría fácilmente ser víctima de un engaño, resultando en una infección por malware, robo de credenciales o una fuga de datos.
No existe evidencia de entrenamientos obligatorios, campañas de simulación de phishing o comunicaciones sobre amenazas actuales.

Riesgo de no actuar

El personal sigue siendo el *eslabón más débil*. La capacitación actual es "eventual" y técnica, no para todos los usuarios. Esto eleva la probabilidad de un incidente por error humano: un empleado que cae en un engaño (phishing) puede resultar en el robo de credenciales, una infección por ransomware o una fuga de datos sensibles.

Solución

Implementar un Programa de Concientización Continua

- **Paso 1:** Realizar una capacitación de seguridad obligatoria para todo el personal (incluyendo Gerencia y Ventas). Esta debe ser no-técnica y cubrir los riesgos reales identificados: cómo detectar un email de phishing, la importancia de no compartir contraseñas y los riesgos del uso de equipos personales.
- **Paso 2:** Contratar un servicio de simulación de phishing. Estos servicios envían emails falsos (pero seguros) a los empleados. Si un empleado "cae" en la trampa, se le presenta una breve lección instantánea.
- **Paso 3:** Enviar un breve boletín de seguridad mensual (o publicarlo en MediaWiki) con consejos prácticos y recordatorios.

Esfuerzo

- **Estimación Económica: Bajo-Medio.** La capacitación inicial puede ser interna (costo bajo, solo horas-hombre). Los servicios de simulación de phishing tienen un costo anual (costo medio), pero son muy efectivos. También, la empresa lo puede utilizar para sus clientes a fin de brindar un servicio.
- **Estimación de Tiempos: Corto Plazo (1 mes)** para la capacitación inicial. El programa de simulación y comunicación es un **proceso continuo** (pocas horas al mes).
- **Personal Involucrado: Área de Ingeniería** (para organizar y gestionar el programa) y **Todo el Personal** (participación obligatoria).

Documentación de sistemas internos desactualizada

Los sistemas desarrollados internamente, como el de sueldos en Cobol, no tienen una documentación actualizada, como se explicó en otro ítem. Además, el conocimiento sobre el funcionamiento, mantenimiento y solución de problemas de estos sistemas críticos reside únicamente en la memoria del personal actual, sin un respaldo escrito que sirva de guía.

Si el personal clave que entiende el sistema se va de la empresa, la empresa enfrentaría una enorme dificultad para mantener o reparar una función crítica, poniendo en riesgo la operatividad de dicho sistema.

Además, otros sistemas (Como Netbox, Wiki Interna) solamente existe la documentación del propio software, pero poca documentación existe acerca de su implementación, cambios, seguimiento de actualizaciones, generando posibles brechas de seguridad o falta de conocimiento para mantenimiento y manejo de ellos.

No existe un procedimiento formal que exija documentar los cambios o las funcionalidades del sistema. La limitación fundamental es la falta de una cultura y un proceso para tratar el conocimiento técnico como un activo de la empresa.

Riesgo de no actuar

La empresa tiene una dependencia crítica del personal que entiende el sistema de sueldos en Cobol. Si esa persona se va, ICOP enfrentaría una enorme dificultad para mantener o reparar una función vital del negocio. Además, esta falta de documentación bloquea cualquier proyecto futuro de migración, ya que nadie sabe cómo funciona el sistema por dentro.

Solución

Proyecto de Transferencia y Centralización de Conocimiento

- **Paso 1:** Asignar a un miembro del Área de Ingeniería para que realice entrevistas formales con el desarrollador de Cobol. El objetivo es documentar todas las reglas de negocio, la arquitectura y los procesos de mantenimiento del sistema de sueldos.
- **Paso 2:** Decretar que MediaWiki es el repositorio oficial único para *toda* la documentación técnica. Cargar allí la documentación del sistema de sueldos y la de otros sistemas (como Netbox, etc.).
- **Paso 3:** Establecer como regla que ningún cambio en un sistema se considera "terminado" hasta que su documentación correspondiente haya sido actualizada en MediaWiki.

Esfuerzo

- **Estimación Económica: Bajo.** El costo es 100% en **horas-hombre** del personal existente (el desarrollador de Cobol y el ingeniero que documenta).
- **Estimación de Tiempos: Mediano Plazo (2-4 meses).** La documentación inicial del sistema Cobol es una tarea considerable. El resto es un proceso continuo.
- **Personal Involucrado:** Gerencia (para exigir la nueva regla), Área de Ingeniería (para documentar) y el desarrollador de Cobol (para transferir el conocimiento).

Escasa segregación de redes internas

La red interna solo tiene dos segmentos: uno para servicio técnico y otro "general" para todas las demás áreas y servidores. La falta de una segmentación adecuada crea una red "plana", donde no hay barreras de seguridad entre los diferentes departamentos o entre las estaciones de trabajo y los servidores críticos. Un incidente de seguridad en un solo equipo (ej. una infección por malware) podría propagarse lateralmente sin control por toda la red, comprometiendo rápidamente otros sistemas y servidores críticos, ya que los mismos están en la misma red actualmente.

El único control de segregación es la división por usuarios de navegación mencionadas anteriormente, pero a nivel lógico, la red está plana en el mismo segmento. Tampoco existe documentación de diagrama de red o documentación formal, sin embargo, la empresa está planificando migrar a distintos direccionamientos y generar la documentación necesaria.

También, es crucial segmentar los sistemas de la red plana (Por ejemplo: una red DMZ interna o segmentación de servidores).

Riesgo de no actuar

La red actual es "plana", con los servidores críticos en el mismo segmento que los usuarios generales. Si una sola PC de un empleado se infecta con ransomware, el malware puede propagarse lateralmente sin ninguna barrera y comprometer todos los servidores de la empresa en cuestión de minutos. La contención de un incidente se vuelve casi imposible.

Solución

Implementar Segmentación de Red con VLANs

El informe indica que la empresa ya está planificando esta migración. Esta solución formaliza ese plan.

- **Paso 1:** Planificar y diseñar segmentos de red lógicos basados en la función y criticidad:
  - VLAN 1: **Servidores** (Crear una DMZ para aislarlos).
  - VLAN 2: **Ingeniería / Servicio Técnico**.
  - VLAN 3: **Administración / Ventas**.
  - VLAN 4: **Infraestructura**.
- **Paso 2:** Implementar estas VLANs en los switches administrables que la empresa ya posee.
- **Paso 3:** Usar el Fortigate para crear reglas de seguridad que controlen el tráfico entre estas nuevas redes. La regla base debe ser "denegar todo" y solo permitir la comunicación estrictamente necesaria (ej. permitir que la VLAN de Administración acceda al servidor de archivos Zentyal, pero bloquear todo lo demás).
- **Paso 4:** Documentar los accesos y permisos necesarios. Definir también las reglas con los accesos de seguridad necesarios, sobre todo en las VLANs de servidores.

Esfuerzo

- **Estimación Económica: Bajo.** La empresa **ya posee el hardware necesario** (switches administrables y un firewall potente). El costo es 100% en **horas-hombre** del personal técnico.
- **Estimación de Tiempos: Corto a Mediano Plazo (1-3 meses).** La planificación es la parte más crítica. La implementación se puede hacer de forma gradual para minimizar la interrupción del servicio, planificando con cada área.
- **Personal Involucrado: Área de Ingeniería** (requiere conocimiento avanzado de redes para planificar y ejecutar la migración de forma segura).

Utilización de computadoras personales para el trabajo

Se permite al personal utilizar sus propios equipos portátiles para realizar tareas laborales. La empresa no tiene control sobre la seguridad de estos dispositivos personales, solamente la instalación del antivirus ESET Endpoints que es gestionado a través del ESET Protect Cloud.

A pesar de esto, existe la probabilidad de fuga o robo de información si un equipo personal se pierde, es robado o compartido. También aumenta el riesgo de que malware ingrese a la red corporativa desde una máquina personal no segura.

El mantenimiento, seguridad, información en cada PC, recae directamente en los empleados (dueños de dichas PCs), sin una supervisión formal por parte de la empresa, y mucho menos, una documentación o seguimiento de esta.

De esto se detecta la falta de visibilidad y configuración de seguridad de los equipos que no le pertenecen. La empresa no garantiza que los dispositivos estén libres de software malicioso, actualizaciones de seguridad e información utilizada.

Riesgo de no actuar

La empresa no tiene control sobre la seguridad de estos equipos personales, más allá del antivirus ESET, y la navegación desde el Firewall propio. Esto crea un riesgo de fuga de información si un equipo se pierde o es robado, y un vector de entrada de malware a la red interna desde un dispositivo no seguro. La mezcla de datos personales y laborales sensibles es una mala práctica de seguridad.

Soluciones

Propuesta A: Implementar una Política de "Trae tu Propio Dispositivo" (BYOD)

Esta política no prohíbe el uso de equipos personales, sino que establece las **reglas mínimas de seguridad obligatorias** para poder conectarlos a la red de la empresa.

- **Paso 1:** Como parte de la Política de Seguridad de la Información, definir que todo equipo personal debe cumplir con lo siguiente:
    - Tener el antivirus corporativo ESET instalado y actualizado (ya se cumple).
    - Tener el cifrado de disco completo habilitado (ej. BitLocker en Windows Pro) para proteger los datos en caso de robo. También ESET tiene provisto un Cifrado de disco, por lo que se puede utilizar eventualmente.
    - Tener el sistema operativo con actualizaciones automáticas habilitadas.
    - Tener una contraseña robusta y un bloqueo de pantalla automático por inactividad.

- **Paso 2:** Cada empleado que use un equipo personal debe firmar un documento aceptando esta política. El Área de Ingeniería debe verificar que el equipo cumple los requisitos antes de darle acceso.
- **Paso 3:** Aplicar reglas de firewall en el Fortigate que limiten el acceso de estos equipos personales solo a los servicios estrictamente necesarios (ya se cumple en gran parte).
- **Paso 4:** Empezar a establecer políticas de “Zero Trust”, aunque tengan un costo adicional si se implementa, para accesos por VPN externos hacia la empresa (con las PCs identificadas u otras).

Propuesta B: Estandarización de Equipos Corporativos (Prohibición de BYOD)

En lugar de gestionar los riesgos de los equipos personales, esta solución los elimina proporcionando a todo el personal un equipo propiedad de la empresa. Esta solución da a la empresa un control total sobre el activo y los datos, elimina la mezcla de información personal/laboral y es mucho más fácil de gestionar y asegurar.

- **Paso 1:** La Gerencia aprueba la compra de los equipos portátiles necesarios para que el 100% del personal tenga un dispositivo corporativo. Esto en parte se cumple, pero algunos equipos empezaron a ser obsoletos y debería tratarse con mayor mantenimiento de los requerimientos y usos.
- **Paso 2:** El Área de Ingeniería prepara todos los equipos (nuevos y existentes) con una "imagen" de software estándar que incluye Windows 10/11 Pro, ESET, cifrado de disco BitLocker y el software de trabajo necesario.
- **Paso 3:** Se establece como política que **solo los equipos propiedad de ICOP** pueden conectarse a la red interna y manejar datos de la empresa. Los dispositivos personales quedan prohibidos para el acceso a recursos corporativos. Esto se puede realizar también en base al acceso de reglas en el Firewall.

Esfuerzo

Propuesta A:

- **Estimación Económica: Bajo.** La solución es principalmente procedural. El costo en horas-hombre es para definir la política y realizar la verificación inicial.
- **Estimación de Tiempos: Corto Plazo (1 mes).** La política se puede definir y comunicar rápidamente.
- **Personal Involucrado: Gerencia** (para hacer cumplir la política), **Área de Ingeniería** (para verificar los equipos) y **Empleados con equipos personales** (para cumplir los requisitos).

Propuesta B [Recomendada]:

- **Estimación Económica: Medio a Alto.** El costo principal es la **inversión de capital (hardware)** para comprar los equipos portátiles faltantes. Aunque es un costo inicial alto, simplifica la gestión y la seguridad a largo plazo.
- **Estimación de Tiempos: Corto Plazo (1 mes).** El tiempo necesario para comprar, configurar y entregar los nuevos equipos.
- **Personal Involucrado: Gerencia** (aprobación de la compra) y **Área de Ingeniería** (configuración y despliegue).

Inventario de equipos informáticos incompleto o no estandarizado

La empresa no cuenta con un inventario formal que identifique cada equipo con un ID o sus características específicas. Se utiliza el software ESET Cloud para visualizar el hardware de los equipos de forma indirecta.

No existe una gestión de activos tecnológicos centralizada. Esto dificulta la planificación de renovaciones, el seguimiento del ciclo de vida del hardware y la administración de licencias de software de manera eficiente.

Si bien existe la documentación de los accesos a los equipos informáticos (servidores, switches, etc.) no están identificados ninguno de los equipos informáticos tipo notebook, pcs de escritorio, impresoras, monitores, etc.

Lo único que tiene seguimiento de licencias y hardware es el dispositivo Fortigate, y el servicio de Invgate y ESET, el pago anual de la licencia.

Riesgo de no actuar

La falta de un inventario centralizado genera el riesgo de "activos fantasma". Además, impide la respuesta eficaz ante incidentes: si aparece una vulnerabilidad crítica para un modelo específico de placa madre o versión de firmware, Ingeniería no tiene forma de saber cuántos y cuáles equipos están afectados sin revisarlos uno por uno, aumentando drásticamente el tiempo de exposición.

Solución

Generar un relevamiento físico y etiquetado con una base de datos simple.

- **Paso 1:** Generar etiqueta de los activos (stickers con código numérico correlativo) y realizar un "barrido" físico oficina por oficina.
- **Paso 2:** Pegar etiqueta en cada gabinete, monitor e impresora. Volcar los datos (ID, Usuario, Modelo, Nro. de Serie, Ubicación) en una planilla compartida (Excel/Google Drive Excel) o una base de datos simple (ej. Access).

- **Paso 3:** Cruzar manualmente los datos relevados con el reporte de "Equipos Vistos" de la consola de ESET para detectar discrepancias.

Esfuerzo

- **Estimación Económica: Bajo.** El costo principal es de las etiquetas que se van a pegar.
- **Estimación de Tiempos: Corto Plazo (1-2 semanas).** Tiempo necesario para ir oficina por oficina y relevar bien cada equipo.
- **Personal Involucrado: Soporte Técnico.** Solo estará el relevamiento físico involucrado y la predisposición del personal para unos minutos prestar su PC al relevamiento.

Falta de seguridad física en la sala de servidores y oficinas

Se ha identificado una vulnerabilidad crítica en el control de acceso a la sala que alberga la infraestructura tecnológica principal de la empresa (servidores, Fortigate, switch de Core, enlaces de internet y UPS). El ingreso a este lugar se realiza a través de una puerta simple, no contiene cerradura o cualquier otro mecanismo de control. A pesar de que la ruta de acceso requiere pasar por las oficinas de Ventas e Infraestructura, no existe un sistema que restrinja o registre el ingreso del personal interno.

Esta falta de control expone los activos críticos a un riesgo elevado de manipulación no autorizada, desconexión accidental o intencionada y daños físicos, lo que podría comprometer la continuidad operativa del negocio.

Las cinco oficinas distribuidas en la instalación permanecen sin llave durante la jornada laboral, y fuera de ella, permitiendo el libre acceso a cualquier persona que se encuentre en el edificio. Sin embargo, las oficinas tienen alarmas centralizadas y las ventanas están aseguradas fuera de horario.
El riesgo se ve incrementado debido a que los equipos utilizados para laboratorios o configuraciones, si bien están inventariados (en el stock de la empresa), suelen encontrarse dispersos y sin aseguramiento físico en estas áreas.

Riesgo de no actuar

El acceso físico no controlado es la vulnerabilidad definitiva: un atacante (o empleado descontento/descuidado) con acceso físico al servidor puede reiniciar equipos, extraer discos rígidos (saltando toda seguridad lógica y firewalls), inyectar malware vía USB o desconectar la infraestructura crítica causando una denegación de servicio inmediata. Además, el incumplimiento de normativas de seguridad física podría invalidar garantías de hardware o seguros contratados.

Soluciones

Propuesta A:

Fortalecimiento de barreras físicas y política de llaves, generando un permiso para ingresar a los equipos y fortaleciendo el problema del fácil acceso.

- **Paso 1:** Instalación inmediata de una cerradura con cerrojo de seguridad en la puerta de la sala de servidores, dejando las llaves bajo custodia exclusiva de la Gerencia de IT.
- **Paso 2:** Crear un "Libro de Guardia" de papel donde cualquier persona ajena a IT que deba ingresar (ej. electricista, limpieza) debe firmar hora de entrada, salida y motivo, siempre acompañado por personal de IT.
- **Paso 3**: Libro de accesos por los empleados, del mismo modo que tiene el de Guardia, pero sin tanto dato y sin acompañamiento, dependiendo de la Gerencia que se completen esos datos.
- **Paso 4:** Definir políticas cuando la gerencia no se encuentre, predisponiendo un “segundo al mando” de las llaves y definir las políticas necesarias.

Propuesta B:

Implementación de un Sistema de Control de Acceso Biométrico y/o Videovigilancia dedicada, reemplazando la cerradura normal.

- **Paso 1**: Definir permisos y softwares para utilizar para el control de acceso. En general, muchas veces, el software a utilizar lo dará el tipo de equipo a implementar.
- **Paso 2:** Reemplazar la cerradura por una cerradura controlada por un lector biométrico (huella) o tarjeta, integrada a la red. Esto permite dar de baja permisos instantáneamente si un empleado se va y deja un registro digital inalterable de quién entró y cuándo.
- **Paso 3:** Instalar una o dos cámaras IP dentro del cuarto de servidores (y en la puerta) con sensor de movimiento, que envíe alertas al celular del responsable de infraestructura si detecta presencia fuera de horario laboral.
- **Paso 4:** Probar el control de acceso y fuera de horario para correcto funcionamiento.

Esfuerzo

Propuesta A:

- **Estimación Económica: Bajo.** El costo principal de la cerradura y/o candados en caso de implementar.
- **Estimación de Tiempos: Corto Plazo (2-3 días).** Tiempo necesario para instalar la cerradura nueva.

- **Personal Involucrado:** Se puede instalar por alguno del personal que tenga conocimiento, o un cerrajero que lo instale, generando un costo.

Propuesta B:

- **Estimación Económica: Medio-Alto.** Requiere compra de hardware: cerraduras biométricas, controladora, cámaras y cableado.
- **Estimación de Tiempos: Corto Plazo (1-2 semanas).** Tiempo necesario para instalación de las cámaras y equipos necesarios, y la configuración del software.
- **Personal Involucrado:** El Área de Infraestructura tiene capacidad para instalar estos equipos. El Área de Ingeniería para la configuración de software.

Conclusiones

En general, las soluciones propuestas han sido seleccionadas priorizando aquellas que sean alcanzables y realistas para la estructura actual de la empresa. Se evita sugerir reingenierías costosas o inversiones desproporcionadas que no se alineen con el interés de la gerencia, salvo en situaciones donde el riesgo crítico lo amerite (como la migración a la nube o el reemplazo de hardware obsoleto).

A pesar de contar con un área de Ingeniería y Servicio Técnico, existe una marcada ausencia de políticas formales, procedimientos documentados y planes de contingencia. La seguridad se gestiona actualmente de manera reactiva y basada en la confianza en el personal, más que en procesos estandarizados.

Se detectaron puntos únicos de fallo que amenazan la continuidad del negocio. La dependencia del sistema de sueldos en Cobol sobre Windows XP y la falta de documentación actualizada de los desarrollos internos representan los riesgos técnicos más elevados. La empresa depende excesivamente del conocimiento tácito de recursos humanos específicos, lo cual dificulta la recuperación ante desastres o la rotación de personal.

Si bien la empresa invierte en seguridad (Firewall Fortigate con servicios, Antivirus ESET), se ha descuidado la seguridad física (acceso libre al Datacenter) y la segmentación interna de la red (red plana).

Por último, La falta de un inventario centralizado y estandarizado de hardware impide una correcta evaluación, dificultando la planificación de renovaciones y el control de seguridad sobre los dispositivos que se conectan a la red corporativa.

Auditores

Adjadj, Agustín

Bargas, Santiago