UNL • FACULTAD DE INGENIERÍA Y CIENCIAS HÍDRICAS

UNIVERSIDAD NACIONAL DEL LITORAL

Facultad de Ingeniería y Ciencias Hídricas

Auditoría Informática

Etapa 1 – Entrega 1

Empresa: ICOP Santa Fe S.R.L.

Alumnos: Adjadj, Agustín; Bargas, Santiago.

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

Fecha de Entrega: 18/10/2025

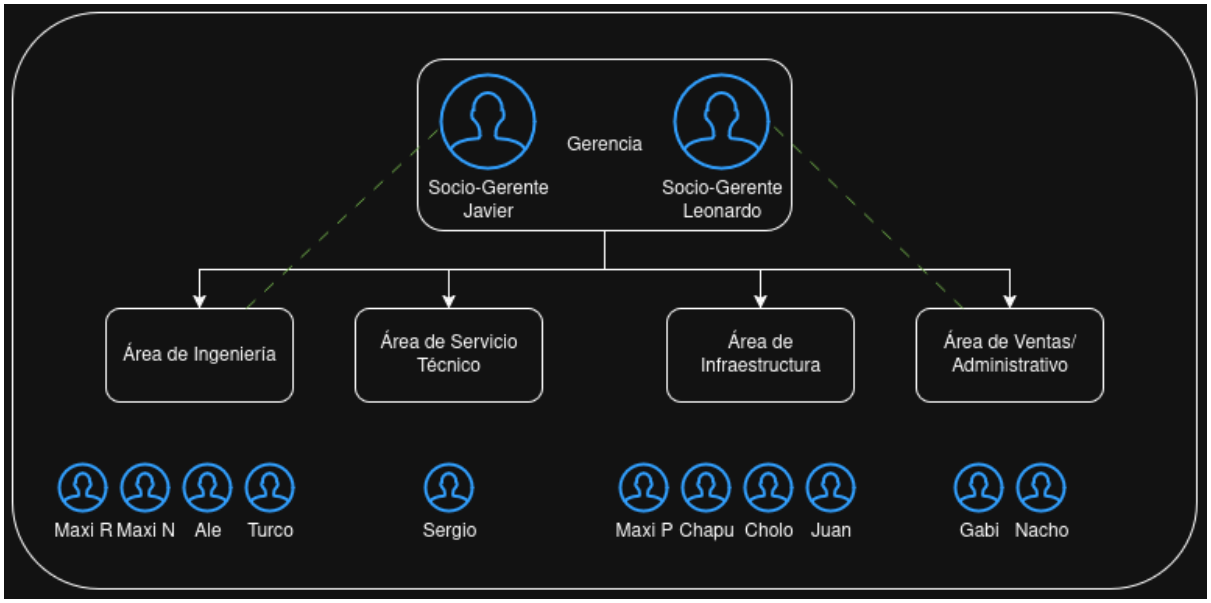
En esta etapa, se buscará conocer la organización donde se realizarán los trabajos de auditoría informática, tener un conocimiento amplio del área de sistemas e infraestructura tecnológica de la misma, identificando los recursos con los cuales se cuenta para llevar adelante sus funciones. Además, se 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 Administrables 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 plugins 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.

Identificación de problemas, necesidades e incertidumbres

PROBLEMA / NECESIDAD / INCERTIDUMBRE	***CATEGORIA***	***RIESGO ASOCIADO***
Ausencia de una política formal de seguridad de la información	*Seguridad*	*Alto*
Falta de políticas de concientización y entrenamiento continuo en seguridad informática	*Seguridad*	*Medio*
Inexistencia de un plan de contingencia y continuidad del negocio	*Continuidad operativa*	*Alto*
Inventario de equipos informáticas incompleto o no estandarizado	*Gestión de archivos*	*Medio*
Documentación de sistemas internos desactualizada	*Documentación / Gestión*	*Medio*
Dependencia de sistemas críticos con tecnología obsoleta	*Infraestructura*	*Alto*
Servidor Web en WordPress sin mantenimiento ni actualizaciones	*Seguridad*	*Alto*
Escasa segregación de redes internas	*Infraestructura / seguridad*	*Medio*
Incertidumbre respecto a la gestión de accesos y privilegios	*Seguridad*	*Alto*
Necesidad de evaluar periódicamente a los proveedores de servicios críticos	*Relaciones con terceros*	*Medio*
Utilización de computadoras personales para el trabajo	*Seguridad*	*Medio*
Falta de seguridad física en la sala de servidores	*Infraestructura / Seguridad*	*Medio*

Etapa 2

En esta segunda etapa del informe, nos enfocaremos en desarrollar en profundidad los problemas, necesidades e incertidumbres identificados en la fase inicial. Para ello, se realizará una clasificación de estos según su nivel de criticidad y se describirá detalladamente el contexto, las causas y las consecuencias de cada uno, utilizando la evidencia recolectada para comprender su impacto real en la organización ICOP.

Descripción Detallada de los Problemas

Ausencia de una política formal de seguridad de la información

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.

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.

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.

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 plugins 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 como 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.

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).

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.

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 item. 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.

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).

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 Endpoint 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 seguiradd 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.

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.

Necesidad de evaluar periódicamente a los proveedores de servicios críticos

ICOP depende de varios proveedores para servicios clave (Invgate, DonWeb, Claro Cloud, OpenOrange); No existe un proceso formal para reevaluar periódicamente si estos proveedores siguen cumpliendo con los requisitos de rendimiento y seguridad, por lo que no hay una política o procedimiento para evaluación de proveedores. La relación con los proveedores es estática, y no se verifica si su nivel de servicio se mantiene, si su seguridad es adecuada o si existen mejores alternativas en el mercado

La empresa podría estar "atada" a un proveedor cuyo servicio ha decaído o presenta vulnerabilidades de seguridad. Si bien la empresa intenta mantenerse actualizada en esto, no hay una documentación o planificación para realizarlo, y se toman decisiones muchas veces poco óptimas, produciendo estancamientos en tecnologías.

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.