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: 01/10/2025

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.

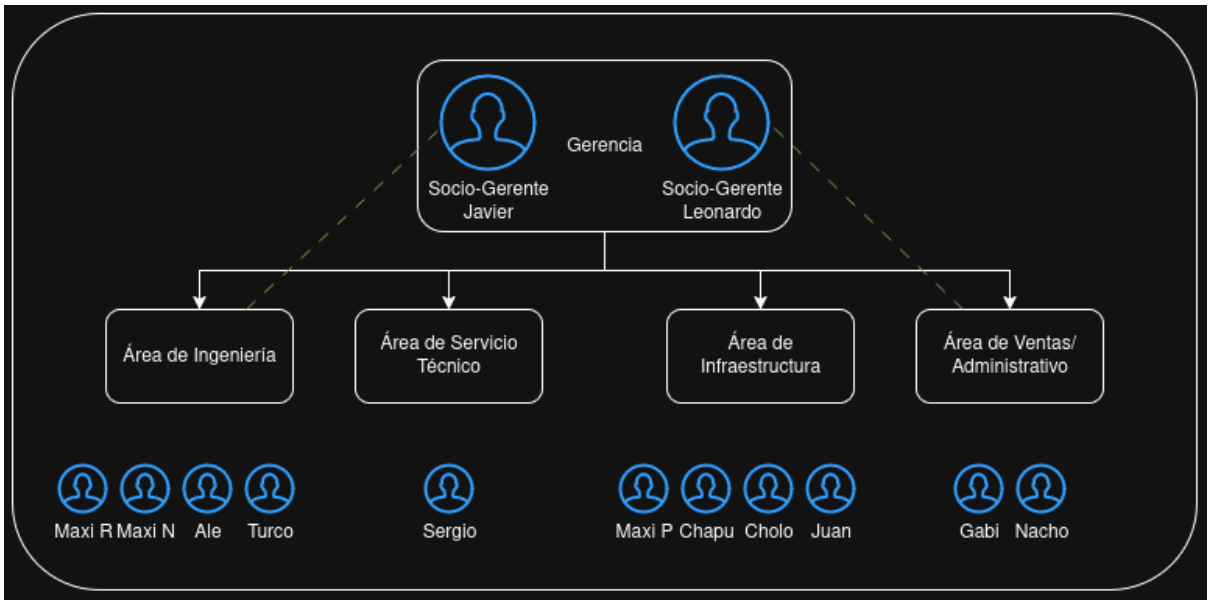
La empresa brinda servicios a organismos públicos, empresas y particulares, ofreciendo desde provisión de equipos y servidores, hasta diseño e implementación de proyectos de redes, seguridad informática, virtualización, soluciones en la nube y desarrollo de centros de datos. En los últimos años amplió 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 documentado y probado	*Continuidad operativa*	*Alto*
Inventario de equipos informáticas incompleto o no estandarizado	*Gestión de archivos*	*Medio*
Documentación de sistemas internos desactualizada (ej. Sistema de sueldos en cobol)	*Documentación / Gestión*	*Medio*
Dependencia de sistemas críticos con tecnología obsoleta (máquina virtual con Windows XP)	*Infraestructura*	*Alto*
Servidor Web en WordPress sin mantenimiento ni actualizaciones	*Seguridad*	*Alto*
Falta de documentación centralizada y actualizada para desarrollos propios	*Documentación*	*Medio*
Dependencia de terceros (Claro Cloud, DonWeb, Invgate, OpenOrange) sin información sobre cláusulas de seguridad ni SLA	*Relaciones con terceros*	*Alto*
Escasa segregación de redes internas (solo división básica entre servicio técnico y general)	*Infraestructura / seguridad*	*Medio*
Necesidad de formalizar procedimientos de backup y restauración ante incidentes	*Continuidad operativa*	*Medio*
Incertidumbre respecto a la gestión de accesos y privilegios en los sistemas internos	*Seguridad*	*Alto*
Necesidad de evaluar periódicamente a los proveedores de servicios críticos	*Relaciones con terceros*	*Medio*