Auditoría Informática

ICOP Santa Fe S.R.L.

Adjadj, Agustín | Bargas, Santiago

Presentación de la Organización

Historia y Misión

Fundada en 1974, **ICOP** es un referente en tecnología, conectividad y energía en Santa Fe. Con más de 40 años de trayectoria, evolucionó de proveedor de insumos a integrador de soluciones completas.

Su objetivo es proveer productos de alta calidad manteniendo independencia de marcas para ofrecer asesoramiento objetivo.

Servicios Principales

- Provisión e instalación de Hardware y Software.
- Virtualización y Servicios en la Nube.
- Seguridad Informática y Consultoría de Redes.
- Centros de Datos y Cableado Estructurado.
- Proyectos Eléctricos y Energía.

Estructura Organizacional

Infraestructura y Servicios IT

Hardware

Seguridad: Fortigate 70F

Red: Switches HP, FortiAP

Servidores: HP & IBM (Proxmox + ESXi), NAS Seagate

Usuarios: 11x PCs/Notebooks (Win 10/11) + Celulares empresariales

Software Interno

Gestión: OpenOrange, Sistema de Sueldos (Cobol)

Documentación: Netbox, Rattic, MediaWiki

Archivos: Zentyal

Correo: Carbonio

Web: WordPress

Servicios Nube

Seguridad: ESET Protect Cloud

Mesa de Ayuda: Invgate

Hosting: DonWeb + Claro Cloud

Colaboración: Zoom, Trello

Problemas y soluciones

SE DETALLAN

PROBLEMA → Riesgo

SOLUCIÓN → Pasos a seguir

ESFUERZO → Económico / Tiempo / Personal

1. Ausencia de política de Seguridad de la Información

⚠ PROBLEMA

La seguridad se basa en herramientas técnicas (Fortigate, ESET) y gestión reactiva. **No existe un documento formal** que unifique criterios, roles y responsabilidades.

Riesgo: Gestión caótica ante incidentes, incumplimiento legal (Ley 25.326) y dependencia exclusiva del conocimiento tácito de los técnicos.

SOLUCIÓN

Paso 1: Gerencia debe asignar responsable y comunicar obligatoriedad.

Paso 2: Identificar activos críticos y redactar principios generales basados en estándares.

Paso 3: Aprobar formalmente y publicar en MediaWiki.

Paso 4: Capacitación obligatoria y firma de acuerdo de confidencialidad por todo el personal.

ESFUERZO

Economico: Bajo - Medio

- Recursos Internos
- Consultor Externo

Tiempo: Mediano plazo

- 3 a 6 meses.

Personal: Toda la Organización

- Gerencia.
- Área de Ingeniería
- Todo el Personal

2. Inexistencia de plan de Contingencia y Continuidad

⚠ PROBLEMA

Se realizan backups diarios correctamente, pero **no existe un plan documentado de restauración** ante desastres mayores. El proceso depende 100% de la memoria del personal técnico y no se realizan pruebas de recuperación.

Riesgo: Recuperación lenta y fallida ante un desastre real (Ransomware, incendio), posible pérdida de datos críticos.

SOLUCIÓN

Paso 1: Crear guías "paso a paso" en MediaWiki para restaurar cada servicio crítico (OpenOrange, Zentyal) desde cero.

Paso 2: Agendar simulacros de restauración semestrales en entornos aislados.

Paso 3: Implementar copia de seguridad en la nube para protección contra desastres físicos locales.

ESFUERZO

Economico: Bajo - Medio

- Recursos Internos
- Copia en Nube

Tiempo: Corto plazo

- 1 a 2 meses.

Personal:

- Gerencia.
- Área de Ingeniería

3. Dependencia de sistemas críticos con tecnología obsoleta

PROBLEMA

El sistema crítico de sueldos corre en una VM con **Windows XP** (sin soporte) y desarrollado en **Cobol**. Mantenido por una sola persona.

Riesgo: Alta vulnerabilidad a ataques, dificultad extrema de mantenimiento y riesgo operativo total si el desarrollador no está disponible.

SOLUCIÓN

Corto Plazo: Aislar la VM en una VLAN sin acceso a internet, permitiendo solo tráfico esencial.

Largo Plazo: Documentar reglas de negocio con el desarrollador actual y migrar a un software moderno de liquidación de sueldos. Validar en paralelo antes de eliminar el sistema original.

ESFUERZO

Economico: Bajo - Alto

- Horas hombre [Bajo]
- Proyecto nuevo (licencias y desarrollo)

Tiempo: Corto plazo - Largo plazo

- 1 a 2 meses [Corto]
- 6 a 12 meses [Largo]

Personal:

- Área de Ingenieria [Corto]
- Gerencia [Alto]

4. Servidor Web WordPress sin mantenimiento ni actualizaciones

⚠ PROBLEMA

Servidor web propio con WordPress que **no recibe actualizaciones** de seguridad ni mantenimiento periódico. Solo tiene políticas de acceso por firewall y a nivel de red (Fail2Ban, IP Blocks).

Riesgo: Blanco fácil para ataques automatizados, inyección de malware y posible vector de entrada a la red interna.

SOLUCIÓN

Plan de migración: Mover el sitio a un hosting gestionado en la nube (ej. DonWeb, Hostinger) para delegar la seguridad de infraestructura.

Mantenimiento y Hardening: Si se mantiene local, establecer protocolo mensual de actualizaciones de core/plugins y registrar accesos y configuraciones DNS.

ESFUERZO

Economico: Bajo/Medio - Alto

- Horas hombre + Plugins [Bajo]
- Proyecto nuevo (hosting y mantenimiento)

Tiempo: Corto plazo - Medio plazo

- 1 a 2 días [Corto]
- 3 a 6 meses [Medio]

Personal:

- Área de Ingenieria [Corto]
- Gerencia + Área de Ingeniería [Medio]

5. Incertidumbre en la gestión de accesos y privilegios

PROBLEMA

Falta de claridad en permisos. Usuarios acumulan privilegios innecesarios y **cuentas de ex-empleados siguen activas**. No hay proceso formal de altas/bajas.

Riesgo: Fuga de información, acceso no autorizado por cuentas zombies o compromiso de credenciales con altos privilegios.

SOLUCIÓN

Paso 1: Revisar y ajustar permisos al mínimo necesario para cada rol (Mínimo privilegio)

Paso 2: Crear formularios de Alta/Baja obligatorios. RRHH debe notificar desvinculaciones inmediatamente.

Paso 3: Realizar limpieza inmediata de usuarios inactivos y ex-empleados.

Paso 4: Documentación de procesos a fin y una política interna definida.

ESFUERZO

Economico: Bajo

- Horas hombre

Tiempo: Corto plazo

- 1 a 2 semanas

Personal:

- Área de Ingenieria
- Gerencia
- Área Administrativa

6. Falta de políticas de concientización y entrenamiento continuo en Seguridad Informática

⚠ PROBLEMA

Existe una capacitación eventual y técnica. **No existe un programa continuo** para empleados generales sobre amenazas actuales (Phishing, Ingeniería Social).

Riesgo: El factor humano es el eslabón más débil. Alto riesgo de infección por malware o robo de credenciales vía engaño.

SOLUCIÓN

Paso 1: Charlas obligatorias no técnicas sobre riesgos reales.

Paso 2: Contratar campañas de Phishing simulado para entrenar en la detección práctica.

Paso 3: Boletines mensuales breves con consejos de seguridad y recordatorios.

ESFUERZO

Economico: Bajo - Medio

- Horas hombre
- Servicios simulación phishing

Tiempo: Corto plazo

- 1 mes

Personal:

- Área de Ingenieria
- Resto del personal

7. Documentación de sistemas internos desactualizada

PROBLEMA

Sistemas internos (Cobol) y configuraciones críticas residen en la "memoria" del personal. Documentación existente dispersa o desactualizada.

Riesgo: Punto único de fallo si el personal clave se retira. Bloquea proyectos de migración y dificulta la resolución de problemas.

SOLUCIÓN

Paso 1: Realizar entrevistas formales con el desarrollador y quienes implementaron los sistemas internos.

Paso 2: Establecer MediaWiki como fuente oficial de verdad. Documentación oficial para seguimiento.

Paso 3: Establecer regla de "Cambio no documentado = Cambio no terminado".

ESFUERZO

Economico: Bajo

- Horas hombre

Tiempo: Mediano plazo

- 2 a 4 meses

Personal:

- Área de Ingenieria
- Gerencia

8. Escasa Segregación de red interna

PROBLEMA

Red dividida solo en 2 segmentos básicos. Servidores críticos conviven en la misma red lógica que usuarios generales.

Riesgo: Movimiento lateral de amenazas. Una infección en una PC de usuario puede comprometer todos los servidores rápidamente.

SOLUCIÓN

Paso 1: Segmentar. Crear VLANs por función: Servidores (DMZ), Ingeniería, Administración, Infraestructura.

Paso 2: Implementar VLANs en switches administrables.

Paso 3: Configurar reglas estrictas en Fortigate entre VLANs (Deny All por defecto).

Paso 4: Diagramar y documentar la nueva topología lógica.

ESFUERZO

Economico: Bajo

- Horas hombre

Tiempo: Corto a Medio plazo

- 1 a 3 meses

Personal:

- Área de Ingenieria

9. Utilización de computadoras personales para el trabajo

⚠ PROBLEMA

Uso permitido de notebooks personales sin control exhaustivo más allá del antivirus. Mezcla de datos personales y laborales.

Riesgo: Fuga de información por robo/pérdida de equipo personal. Vector de entrada de malware desde entornos no seguros.

SOLUCIÓN

Opción 1: Exigir cifrado de disco (Bitlocker), Sistemas Operativos actualizados y contraseña robusta para conectar a la red.

Opción 2: Prohibir Dispositivos Personales. Proveer equipos corporativos a todo el personal con imagen estándar segura y contol total.

ESFUERZO

Economico: Bajo - Medio/Alto

- Horas hombre [Bajo]
- Inversión [Medio/Alto]

Tiempo: Corto Plazo

- 1 mes

Personal:

- Gerencia
- Area de Ingenieria
- Empleados [Bajo → Con equipos personales]

10. Inventario de equipos informáticos incompleto o no estandarizado

PROBLEMA

Equipos no inventariados físicamente (sin ID/Etiqueta). Gestión parcial vía software ESET.

Riesgo: Activos fantasma, dificultad para planificar renovaciones y rastrear hardware afectado por vulnerabilidades específicas.

SOLUCIÓN

Paso 1: Generar etiquetas para los activos y realizar un relevamiento físico oficina por oficina

Paso 2: Pegar la etiqueta en cada equipo y volcar los datos en una planilla o base de datos simple

Paso 3: Cruzar manualmente los datos del relevamiento físico con el reporte de "Equipos Vistos" de la consola de ESET para detectar diferencias.

ESFUERZO

Economico: Bajo

- Horas hombre

Tiempo: **Corto Plazo**

- 1 a 2 Semanas

Personal:

- Soporte Tecnico

11. Falta de seguridad física en la sala de servidores y oficinas

PROBLEMA

Sala de servidores y equipos críticos con acceso mediante puerta simple sin llave. Oficinas abiertas en horario laboral.

Riesgo: Manipulación no autorizada, robo, desconexión accidental o intencional de infraestructura crítica (saltando toda seguridad lógica).

SOLUCIÓN

Opción 1: Instalación de una cerradura con llave bajo custodia de Gerencia. Libro de guardias para visitas.

Opción 2: Implementar cerradura biométrica/tarjera para registro digital de los accesos.

ESFUERZO

Economico: Bajo - Medio/Alto

- Costo de cerradura y/o candados
- Cerraduras biométricas y cámaras

Tiempo: **Corto Plazo**

- 2 a 3 días
- 1 a 2 Semanas

Personal:

- Personal con conocimiento (interno) o Cerrajero.

Conclusiones Finales

DIAGNÓSTICO GENERAL

GESTION REACTIVA

ICOP tiene una base sólida de infraestructura (Fortigate, ESET), pero la gestión de seguridad es reactiva y no preventiva.

CONFIANZA VS PROCESOS

La operación depende excesivamente del conocimiento "tácito" del personal, sin políticas formales ni documentación actualizada.

PUNTOS DE FALLOS CRITICOS

Existen riesgos altos en sistemas obsoletos (Cobol/XP) y una seguridad desbalanceada: fuerte en el perímetro pero débil internamente (red plana, acceso físico libre).

EL CAMINO A SEGUIR

ENFOQUE REALISTA

Las soluciones propuestas priorizan acciones alcanzables para la estructura actual, evitando inversiones desproporcionadas.

FORMALIZAR LA GESTIÓN

Es necesario transformar la "confianza" en procesos documentados, políticas claras e inventarios estandarizados.

PROTEGER Y MODERNIZAR

El objetivo inmediato es mitigar riesgos físicos y lógicos (Segmentación, Accesos), para luego planificar la modernización tecnológica.