Plan de acción estratégico de ciberseguridad para Empresa de Energía del Quindío EDEQ S.A. E.S.P.

Responsable:
Mario Alberto Martínez Martínez

Colaboradores:
Diego Fernando Jiménez Mendoza
Andrés Felipe Gómez Barbosa
Cristian Camilo Ospina Alzate
Darwin Andrés Molina Osorio
Juan David Restrepo Cardona

Organización: Empresa de Energía del Quindío EDEQ S.A. E.S.P.

Departamento: Tecnología de Información y Operación Integrada

Fecha: 26/06/2023

1) Resumen ejecutivo

Recomendaciones y acciones clave para implementar prácticas de ciberseguridad.

La Empresa de Energía del Quindío ha desarrollado una historia de maduración de la seguridad de la información y la ciberseguridad que empezó en el año 2013 con acciones aisladas y descoordinadas, las cuales se consolidaron con la ejecución de un proyecto de ciberseguridad que impactó toda la organización durante los años 2020 y 2021. Este proyecto produjo resultados puntuales como la implementación de un sistema de gestión de seguridad de la información ajustado a la norma ISO 27001:2013, que es operado por un proceso organizacional de seguridad digital y continuidad de servicios de tecnología. A partir del año 2022 inició la gestión continua del proceso y el SGSI como parte de la gestión del macroproceso de Tecnología de Información. Adicionalmente se viene trabajando en el cumplimiento de la Guía de Ciberseguridad del sector Eléctrico (Acuerdo del Concejo Nacional de Operación de Colombia 1502), el cual se fundamenta en el estándar NERC-CIP.

A partir de los avances logrados con las acciones descritas anteriormente, se define el siguiente plan estratégico orientado principalmente a:

- Consolidar un equipo de profesionales contratados directamente por la empresa y capacitados constantemente, que se dediquen a la gestión de seguridad de la información y ciberseguridad en las TI y TO
- Finalizar la implementación de la guía de ciberseguridad del CNO 1502 que debe alcanzar el 100% en el cumplimiento de sus requisitos el octubre 3 de 2024
- Planear y ejecutar las acciones para la certificación del Sistema de Gestión de Seguridad de la Información que se encuentra establecido
- Realizar la planeación presupuestal y la gestión para la aprobación de dichos recursos ante la alta dirección de la compañía

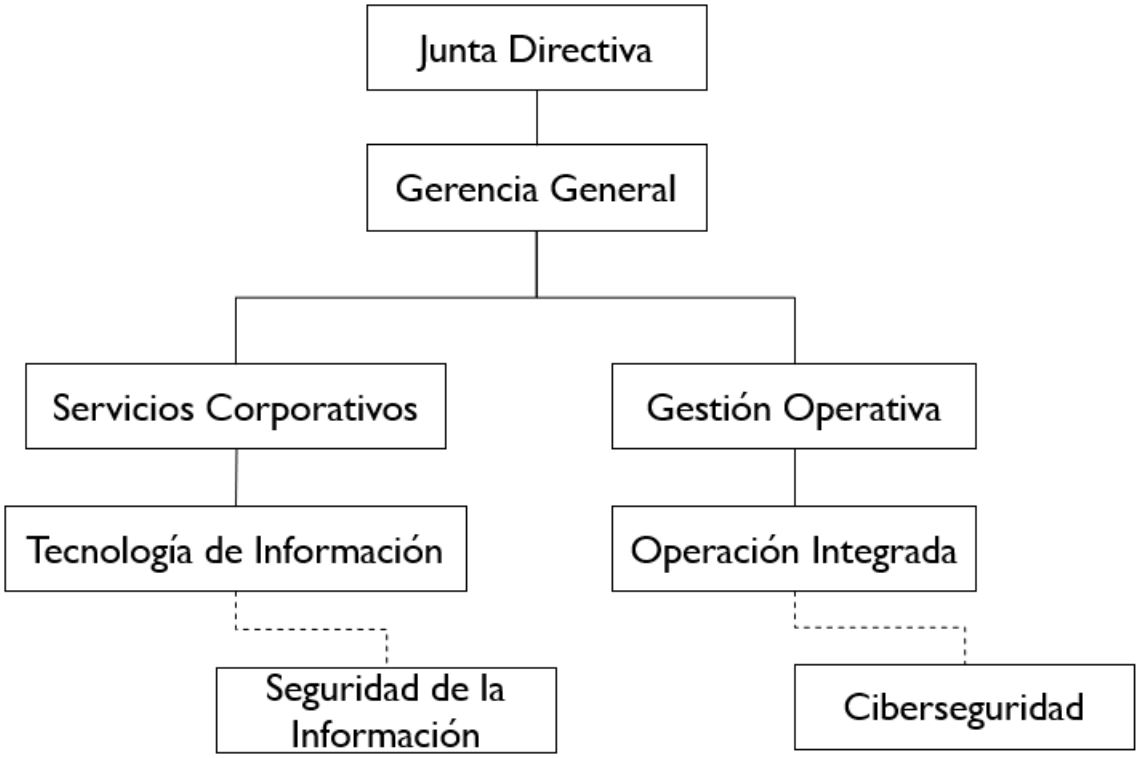
2) Introducción

Descripción general de la organización, estructura y prácticas actuales de TI / cibernética

La Empresa de Energía del Quindío se creó en 1988 para atender la prestación del servicio de energía eléctrica en 12 municipios del departamento del Quindío, ubicado en la región del eje cafetero, zona centro occidental de Colombia. Es una empresa de economía mixta que pertenece en un 99.2% al Grupo EPM desde el 2009. Cuenta con 5.300 Km de red instalados, 8.354 transformadores, 13 subestaciones de energía en los niveles de tensión I, II y III, 17 puntos de Atención al cliente

EDEQ se dedica a la comercialización y distribución de energía eléctrica para 213.000 clientes, 89% en el sector residencial y 11% en el sector industrial

El equipo de seguridad digital está conformado por personas que se dedican a la seguridad de la información en las TI y otras que trabajan en la TO. Todos están coordinados bajo un plan de trabajo único y supervisados por la líder de Tecnología de Información (TI) y el líder de Operación Integrada (TO). Estos dos equipos hacen parte de las áreas de Servicios Corporativos y Gestión Operativa respectivamente, éstos últimos a su vez dependen de la gerencia general y la junta directiva de la empresa.



La compañía ha venido adoptando prácticas diversas para la gestión de tecnologías de información y los sistemas de control industrial entre las cuales se destacan:

- Adopción del estándar ITIL para la gestión de los procesos de tecnologías de información, enfocando esfuerzos principalmente en la arquitectura de tecnología, la gestión de la disponibilidad del servicio, la gestión de las solicitudes de usuario y los incidentes, la gestión de cambios, la gestión de problemas y la implementación de la mesa de ayuda
- Planificación anual del presupuesto de tecnología que incluye el soporte administración y mantenimiento de aplicaciones, la compra de servicios especializados como los de seguridad digital, la adquisición de tecnologías nuevas o la renovación de las obsoletas.
- Construcción y mantenimiento de las redes de fibra óptica en toda su área de cobertura para los servicios tecnológicos de los ICS y los servicios comerciales de la empresa
- Implementación de subestaciones digitales migrando las existentes y construyendo las nuevas bajo este nuevo modelo tecnológico

- En las prácticas de ciberseguridad se han implementado firewalls en todas las instalaciones de ICS, sistemas de detección de intrusos IDS y un sistema para el control de acceso a los ciberactivos
- Se cuenta con una plataforma de servicios de centro de operaciones de seguridad - SOC que realiza recolección, almacenamiento y correlación de eventos, análisis de vulnerabilidades, analítica avanzada de red y analítica del comportamiento de usuarios.
- Se han desarrollado procedimientos para la gestión de incidentes, la gestión de cambios y la gestión de configuración en los ICS, segregación de funciones y mínimo privilegio.

Lista de desafíos/problemas de ciberseguridad

- Maduración de las prácticas de Ciberseguridad en el personal responsable de las TI y TO a nivel de proceso, personas y tecnologías.
- Automatización de tareas de monitoreo de eventos y contención de amenazas
- Desarrollo de un equipo de respuesta a incidentes en la empresa - CSIRT
- Integración de las soluciones de seguridad física con las prácticas de Ciberseguridad empresariales
- Gestión de riesgos a nivel de activos de información y ciberactivos críticos
- Fortalecimiento de los planes de recuperación de ciberactivos críticos y articulación con el plan de recuperación ante desastres

Lecciones aprendidas del curso

- La ciberseguridad de los ICS es un proceso evolutivo que requiere trabajo, constancia, conocimiento y recursos para alcanzar un nivel de madurez apropiado.
- Se debe identificar y analizar los riesgos de los activos que se gestionan, para concentrar los esfuerzos y los recursos en aquellos más críticos, sin descuidar los de menor impacto.
- Elaborar y probar un plan de respuesta a incidentes es una obligación prioritaria.
- Se debe identificar los activos que se quiere proteger porque no es posible cuidar lo que no se conoce.
- Wiper es una amenaza superior al ransomware porque no intenta robar los datos, sino borrarlos definitivamente. Se debe contar con una estrategia de copias de respaldo eficaz para este tipo de ataques.
- La cultura organizacional y la ciberhigiene son claves para evitar que los ataques de ingeniería social tengan éxito.
- El programa de ciberseguridad de una compañía debe abordar controles para la gestión de la cadena de suministro

3) Metodología para el Plan de Acción

a) Prioridades y alcance

- **Actualizar los análisis de riesgos de seguridad de la información y ciberseguridad de EDEQ**: a partir de lecciones aprendidas en ciberataques se debe profundizar la identificación de riesgos de seguridad digital en las tecnologías de información y las tecnologías de operación.
- **Definición y aplicación de líneas base de seguridad para redes, servidores e ICS**: ya se cuenta con los documentos de líneas base de seguridad, pero deben ser aplicados en los diferentes dispositivos con la gestión de cambios y permisos en los entes reguladores para las indisponibilidades de servicio
- **Desarrollo del plan de sensibilización y capacitación 2023**: cada año se planea, ejecuta y evalúa actividades de sensibilización y entrenamiento en seguridad de la información que incluyen

presentaciones, videos, material impreso, pruebas de ingeniería social, pruebas de ethical hacking, ejercicios CTF, etc.

- **Implementación del centro de operaciones de seguridad – SOC**: contratación con empresa especializada en ciberseguridad para obtener los servicios de recolección, almacenamiento y correlación de eventos de la infraestructura de TI y TO, analítica avanzada de red y usuarios, análisis de vulnerabilidades y ciberinteligencia de amenazas.
- **Afinamiento de la plataforma de IDS y análisis de vulnerabilidades de OT – Claroty**: esta plataforma supone un reto importante para la compañía porque debe ser configurada y ajustada a medida que descubre nuevos equipos en la redes de TO, esta configuración se hará siguiendo el modelo Purdue para el nombramiento y zonificación de los servicios y creando escenarios de alertamiento de los tráficos y comportamientos que no son reconocidos.
- **Implementación y prueba del plan de respuesta a incidentes**: es la tarea que más esfuerzo requiere porque debemos empezar por la creación de los playbooks para los escenarios de ataque o incidentes frecuentes en el sector eléctrico. A medida que se avance en esta tarea se requiere realizar la pruebas correspondientes con la ayuda del servicio SOC.
- **Certificación del sistema de gestión de seguridad de la información**: en la legislación colombiana existe la resolución CREG 101 001 que en su artículo 21 nos obliga a certificar un SGSI para la implementación de la infraestructura de medición avanzada AMI.

b) Evaluaciones

El plan de acción descrito anteriormente es evaluado cada mes en reuniones de seguimiento con los jefes responsables de la seguridad de la información y la ciberseguridad de la compañía, por medio de indicadores que miden:

- Cantidad de actividades realizadas frente a las planeadas en la vigencia
- Cantidad de trabajadores impactados con los entrenamientos y nivel de aprendizaje
- Cantidad de vulnerabilidades mitigadas frente a vulnerabilidades identificadas
- Cantidad de incidentes atendidos frente a incidentes declarados
- Índice del nivel de riesgo de ciberseguridad

Adicionalmente el área de auditoría interna realiza auditorías de seguridad digital anualmente para verificar que las acciones emprendidas si están aportando a la reducción del riesgo cibernético.

4) Plan de acción priorizado

A partir de los conocimientos adquiridos en el curso de Ciberseguridad y Digitalización para el sector eléctrico y la planeación interna de la compañía, se han priorizado las siguientes actividades:

a) **Actualizar los análisis de riesgos de seguridad de la información y ciberseguridad de EDEQ**: la infraestructura de TI y TO ha aumentado en la compañía y los riesgos de seguridad de la información y ciberseguridad no han sido actualizados en los últimos 2 años, razón por la cual se ha decidido priorizar esta actividad en 2023 dedicando a ella 3 ingenieros expertos en ciberseguridad durante 3 meses. El objetivo principal es mejorar el nivel de detalle en los riesgos identificados a nivel de tecnologías, procesos y personas involucradas en la cadena de valor del servicio público que prestamos y obtener un índice de riesgo cibernético actualizado.

b) **Definición y aplicación de líneas base de seguridad para redes, servidores e ICS**: se ha identificado un gran número de dispositivos instalados en la red de TI / TO con configuraciones de fábrica que deben ser fortalecidos y actualizados en su firmware y configuraciones para evitar ataques comunes como accesos no autorizados, robo de datos o control remoto no supervisado.

c) **Desarrollo del plan de sensibilización y capacitación 2023**: en este aspecto serán tomadas en cuenta las recomendaciones de SEL con afiches que sensibilicen a los trabajadores en las pequeñas e importantes acciones que contribuyen a mejorar la ciberseguridad. Este mismo plan llevará a los procesos de la cadena de suministro una presentación masiva para que todas las partes involucradas sepan que EDEQ está comprometida con la seguridad de la información incluidos sus proveedores.
d) **Implementación del centro de operaciones de seguridad – SOC**: la implementación del SOC es muy urgente porque la capacidad de monitoreo es muy limitada con todas las tareas de ciberseguridad que debe desarrollar el equipo. Este servicio con la ayuda de la inteligencia artificial y herramientas modernas como Tenable.io, Darktrace y Exabeam se convierten en un apoyo fundamental para prever y anticipar e identificar comportamientos que puedan conducir a la materialización de un incidente de ciberseguridad.

5) Conclusión

Se espera que el desarrollo de este plan de acción ayude a madurar las prácticas de seguridad de la información de EDEQ por medio de la identificación temprana de vulnerabilidades, riesgos y brechas de seguridad. Con esta información se pretende identificar acciones de bajo costo y alto impacto que puedan ser atendidas en el corto plazo. Paralelamente se quiere aumentar la conciencia situacional de los trabajadores porque cada uno de ellos se debe convertir en un defensor activo de la información y servicios de la compañía.

En el mediano plazo se espera certificar el sistema de gestión de seguridad de la información tomando los estándares ISO 27001:2022 y NERC-CIP para el cumplimiento de normas y leyes colombianas, así como mejorar la integración de TI y TO frente a la ciberseguridad.