PLAN DE ACCIÓN ESTRATÉGICO DE CIBERSEGURIDAD

EMPRESA DE ENERGÍA DEL QUINDÍO

28 DE JUNIO DE 2023

OBJETIVOS

- Actualizar los análisis de riesgos de seguridad de la información y ciberseguridad de EDEQ
- Definición y aplicación de líneas base de seguridad para redes, servidores e ICS
- Desarrollo del plan de sensibilización y capacitación 2023
- Implementación del centro de operaciones de seguridad - SOC
- Afinamiento de la plataforma de IDS y análisis de vulnerabilidades de OT - Claroty
- Implementación y prueba del plan de respuesta a incidentes
- Certificación del sistema de gestión de seguridad de la información

Cronograma de actividades - Plan de Ciberseguridad

Actividad	2023	2024	2025
Actualizar los análisis de riesgos de seguridad de la información y ciberseguridad de EDEQ	9 meses		
Definición y aplicación de líneas base de seguridad para redes, servidores e ICS	1 año		
Desarrollo de planes anuales de sensibilización y capacitación	1 año	1 año	1 año
Implementación del centro de operaciones de seguridad - SOC	18 meses		
Afinamiento de la plataforma de IDS y análisis de vulnerabilidades de OT - Claroty	9 meses		
Implementación y prueba del plan de respuesta a incidentes	1 año		
Certificación del sistema de gestión de seguridad de la información	1 año		

PASOS

- Elaboración de propuesta de plan estratégico de ciberseguridad con solicitud de recursos puntuales para los directivos de la empresa
- Investigación de mercados para cotizar los servicios y tecnologías requeridas
- Gestión de presupuestos necesarios para el desarrollo del plan
- Formulación y aprobación de proyecto de ciberseguridad con metodologías ágiles
- Asignación de equipo de trabajo
- Asignación de tareas al equipo de trabajo definido
- Seguimiento y evaluación de las tareas
- Entrega de resultados al proceso de seguridad digital

RECURSOS

Recursos humanos

- Ingeniero de Operación + Ingeniero de Ciberseguridad + Ingeniero de Telco
- Asesor en ISO 27001:2022
- Comunicador social

Recursos Tecnológicos

- Herramientas del SOC (SIEM, escaner de vulnerabilidades, análitica avanzada)
- 2 Equipos de cómputo dotados para trabajo ofimático
- 12 IDS + Plataforma Claroty

Recursos financieros

- USD $ 285.000 aprox