1. Objetivos y Alcance de los lineamientos de Ciberseguridad.

Implementar normas, acuerdos y medidas organizacionales, técnicas y físicas orientadas a la identificación, aseguramiento, recuperación y respuesta ante incidente en los activos y ciber activos críticos que pertenecen a la compañía, así como las prácticas de gobierno de personal, control de acceso y gestión en la cadena de suministro, que permitan mitigar los efectos de acciones como: accesos no autorizados tanto electrónicos como físicos, indisponibilidad del suministro de energía eléctrica y uso no adecuado tanto de la información como de los equipos que permiten operar el sistema eléctrico, que tengan origen intencional o accidental.

Con este documento se presentan los objetivos que permitan alcanzar un nivel de riesgo no crítico en la operación de los sistemas de tecnología de la información y del sistema eléctrico, los cuales establezcan las políticas de ciberseguridad reconociendo y documentando los riesgos reales y potenciales en el sistema eléctrico que opera la Empresa de Energía de Pereira, para disminuir y gestionar ciberataques implementando la prevención de accesos no autorizados a la tecnología de la información (TI) y la tecnología operativa (OT) y relacionar los activos y ciber activos críticos manteniendo la lista actualizada de los activos de TI y OT, con el fin de garantizar la segmentación de cada ambiente en la prevención y durante ciberataques si estos se presentan.

El área de infraestructura junto con los comités de ciberseguridad y supervisión serán los encargados de la implementación, sensibilización y divulgación diferencial a todos los usuarios finales de la compañía en lo relacionado con: listado de activos y ciber activos críticos, perímetros de seguridad (electrónicos y físicos), procedimientos y formatos de registro, identificación y análisis de vulnerabilidades.

2. DESARROLLO:

Lineamientos para la ciberseguridad.

La política expuesta en este documento define algunas funcionalidades alrededor del cumplimiento de los acuerdos expuestos por el CNO en temas relacionados con ciberseguridad.

- **Identificación de activos y ciber activos críticos:** Tanto los activos y ciber activos críticos domo los ciber activos identificados y clasificados por el comité de ciberseguridad de listan y actualizan en un inventario con el fin de mitigar riesgos contra actos de terceros que acceden a estos y que pueden causar una operación inadecuada o inestabilidad en el suministro de energía eléctrica.

- **Gobierno y gestión de personal:** La política de ciberseguridad planteada en este documento mitiga el efecto de los vectores de ciberataques, reduce los riesgos y costos en la recuperación de activos y ciber activos, y protege la información junto con la política de seguridad de la información ADMTIOT05. Además, de mantener una lista actualizada y verificada de las personas tanto pertenecientes a la empresa como terceras partes que tengan acceso a los activos críticos donde residen ciber activos críticos.

- **Seguridad de los perímetros físicos y lógicos:** Prevenir acceso no autorizado a información de los ciber activos asociados a los activos críticos, especificando procedimientos de protección de la información para evitar eventos que puedan conducir a operación inadecuada o inestabilidad.

- **Plan de recuperación:** Los comités de ciberseguridad y supervisión junto con el área de operaciones deben implementar los procedimientos de recuperación de funciones en los ciber activos críticos asociados en la operación de activos críticos con el fin de conservar la continuidad del suministro de energía eléctrica.

- **Plan de respuesta:** Mitigar los efectos y riesgos en la operación en estado seguro y confiable de los ciber activos críticos asociados a los activos críticos bajo incidentes de ciber seguridad, especificando requerimientos de respuesta a incidentes.

- **Gestión del riesgo en la cadena de suministro:** Mantener un listado detallado de terceros o contratistas que cuenten con acceso a dispositivos clasificados como ciber activos críticos, que residan dentro de los perímetros físicos y lógicos de un activo crítico para reducir riesgos de ciber seguridad identificando y evaluando los tipos de riesgos de ciber seguridad en ciber activos, para la gestión en la cadena de suministros y así garantizar una operación confiable y segura en el suministro de energía eléctrica.

3. Estructura Organizacional para la ciberseguridad.

A continuación, se presentan las partes involucradas, funciones y responsabilidades con el objetivo de implementar y cumplir con la política descrita.

- **Comité de Ciberseguridad.**

El comité de ciberseguridad debe analizar y socializar las normas que en materia de ciberseguridad se expidan por parte de diferentes autoridades, para consulta o en firme, de tal manera que se garantice la operación del sistema eléctrico de forma confiable y segura cumpliendo los criterios de eficiencia económica, e identificar las necesidades y hacer las recomendaciones al CNO sobre aspectos tecnológicos relacionados con la ciberseguridad y en coordinación con el comité de supervisión.

Integrante	Habilidades
Líder de infraestructura	Tecnología de la información
Ingeniero de control	Control de sistemas eléctricos
Líder de plantas y subestaciones	Ingeniero eléctrico, gestión de sistemas

Cuadro 1: **Comité de Ciberseguridad.**

- **Comité de supervisión.**

Las funciones que desempeña este comité permiten comunicar la detección de eventos por medio de mecanismos (alerta de antivirus,

alertas de inicio de sesión) que son controlados y administrados para alertar potenciales eventos. Este comité debe realizar el proceso para que el personal encargado pueda analizar y responder a un incidente. De acuerdo con el nivel de criticidad y el impacto potencial en las funciones de la Empresa de Energía de Pereira se han establecido criterios para escalar dichos eventos al comité de ciberseguridad.

Integrante	Habilidades
TI especialista en redes	Tecnología de información
Auxiliar de ciberseguridad	Ingeniero electricista

Cuadro 2: **Comité de supervisión.**

Definiciones.

- **Activo crítico:** Instalaciones, sistemas o equipos eléctricos que, de ser destruidos, degradados o puestos indisponibles, afecten la confiabilidad (suficiencia y seguridad), operatividad, o que comprometan la seguridad de la operación del SIN.

- **Ciber activo crítico:** Dispositivo para la operación confiable de activos críticos que cumple alguno de los atributos descritos:

  - El ciber activo usa un protocolo enrutable para comunicarse afuera del perímetro de seguridad electrónica, o
  - El ciber activo usa un protocolo enrutable con un centro de control, o
  - El ciber activo es accesible por marcación.

- **Ciber activo:** Dispositivo electrónico programable y elementos de las redes de comunicaciones incluyendo hardware, software, datos e información. Así como aquellos elementos con protocolos de comunicación enrutables, que permitan el acceso al mismo de forma local o remota.

- **Ciber activo transitorio:** Puede ser uno de los muchos tipos de dispositivos que son especialmente diseñados para dar soporte o mantenimiento a los ciber activos críticos existentes, que puede ejecutarse desde un computador portátil o una tableta y que además puede interactuar o ejecutar aplicaciones compatibles con los ciber

activos críticos existentes o con la red en donde éstos se encuentran conectados.

- **CNO (Consejo Nacional de Operación):** En el sector eléctrico, es un organismo que tiene como función principal acordar los aspectos técnicos para garantizar que la operación del Sistema Interconectado Nacional (SIN) sea segura, confiable y económica y ser el ejecutor del Reglamento de Operación

- **Evento:** Un suceso que potencialmente pone en peligro, la confidencialidad, integridad o disponibilidad de un sistema de información o un sistema de procesa información, almacena, transmite o constituye en la violación o amenaza las políticas se seguridad de la información.

- **Incidente de Ciberseguridad:** Cualquier acto malicioso que compromete o intenta comprometer, la seguridad física o electrónica de un ciber activo crítico o su perímetro.

- **OT (*Operational Technology*):** Mientras TI o tecnología de información se encarga del almacenamiento, procesos y comunicación de datos, OT o tecnología operativa es acerca del control, seguridad y disponibilidad de los procesos en activos eléctricos.

- **Perímetro de Seguridad Electrónica:** Es la frontera lógica, con acceso controlado, que rodea una red aislada o con conectividad enrutable a otras redes dentro de la cual están conectados los ciber activos críticos.

- **Perímetro de Seguridad Física:** Es la frontera física, con acceso controlado, completamente contenida ("seis paredes") que rodea cuartos de control, cuartos de comunicaciones, centros de operación y otros sitios que alojan ciber activos críticos.

- **Programa:** Es un conjunto de iniciativas, planes o proyectos desarrollados para el logro de objetivos comunes y concretos.

- **Puntos de acceso al (los) Perímetro(s) de Seguridad Electrónica:** Primera capa de defensa que controla el tráfico de red entrante y saliente de un perímetro de seguridad electrónica y entre otras zonas externas.

- **Responsable de Ciberseguridad:** Persona con la autoridad para dirigir la implementación de la guía de ciberseguridad.

- **Riesgo:** Amenaza evaluada en términos de impacto y probabilidad, conforme a la política de riesgos de cada entidad, con el fin de minimizar posibles impactos en la operación confiable (suficiencia y seguridad) del SIN.

- **Seguridad de la información:** Consiste en la preservación de las siguientes características:

  - **Confidencialidad:** Se garantiza que la información sea accesible sólo a aquellas personas autorizadas a tener acceso a ella.

  - **Disponibilidad:** Se garantiza que los usuarios autorizados tengan acceso y puedan usar la información y los recursos relacionados con ella cada vez que se requiera.

  - **Integridad:** Se salvaguarda la exactitud y completitud de la información y los métodos de procesamiento.

  - **No-repudio:** Se previene la negación de la autoría de una acción que tuvo lugar o reclamar la autoría de una acción que no se llevó a cabo.

- **TI (Tecnología de la información):** Área encargada de mantener la infraestructura de las comunicaciones garantizando un modelo de continuidad de negocio.