Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información 2023

ENELAR
Empresa de Energía de Arauca
ESP

icontec
ISO 9001
SC-CER546783

CERTIFIED
IQNet
MANAGEMENT SYSTEM

mipg
modelo integrado de planeación y gestión

TABLA DE CONTENIDO

1. INTRODUCCIÓN

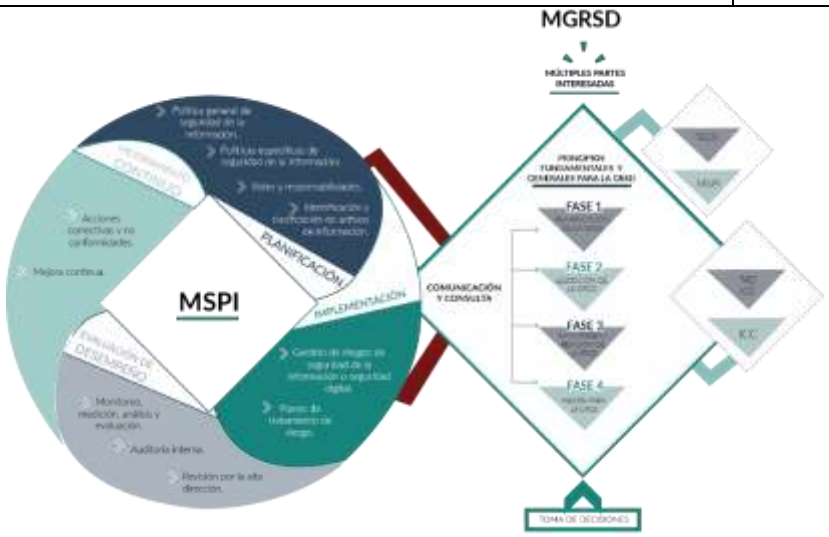
La Gerencia de La Empresa de Energía de Arauca – ENELAR E.S.P, ha establecido una política clara de apoyo y compromiso frente a los temas relacionados con la Seguridad de la Información, que se ve reflejada en Resoluciones N. 367 de 2018 y ajustado mediante resolución 233 de 2019. "Por la cual se establecen los responsables de la Política de Gobierno Digital" y demás instrumentos que reglamentan esta política.

De igual forma, teniendo en cuenta el nuevo concepto de Gobierno Digital y la alineación de la Política de Gobierno Digital como una de las dimensiones del Modelo Integrado de Planeación y Gestión – MIPG, la implementación del Modelo de Seguridad y Privacidad de la Información – MSPI, se constituye en el instrumento que soportará el habilitador transversal de la Seguridad de la Información de La Empresa de Energía de Arauca – ENELAR E.S.P; dentro de los instrumentos que apoyan la implementación del MSPI de la Entidad, en la Fase 3 – Implementación, se encuentra la necesidad de definir el Plan de Tratamiento de Riesgos de Información que permitirá la identificación, análisis, valoración y tratamiento de riesgos relacionados con la información institucional ya sea física o digital, en cada uno de sus procesos, con el fin de garantizar la seguridad en términos de integridad, confiabilidad y disponibilidad

De acuerdo con lo indicado en el ámbito de aplicación del Decreto 1078 de 2015, respecto a la política de Gobierno Digital, las entidades públicas deben realizar la implementación del Modelo de seguridad y privacidad de la información (MSPI) con el objetivo de conformar un Sistema de Gestión de Seguridad de la Información (SGSI) al interior de la entidad.

En el MSPI se incorpora un componente de gestión de riesgos en las etapas de planificación, implementación, evaluación y mejora. Este modelo es adoptado por ENELAR E.S.P. en la ejecución del SGSI.

De acuerdo con lo anterior, la relación e interacción entre la gestión de seguridad de la información con el Modelo Nacional de Gestión de Riesgos de Seguridad Digital (MNGRSD) se visualiza y se describe de la siguiente manera:



Interacción entre el MSPI y el MGRSD. Fuente: MinTIC.

En esencia, la interacción entre ambos modelos puede resumirse de la siguiente manera:

- Las actividades de identificación de activos, análisis, evaluación y tratamiento de riesgos se alinean con la fase de planificación del MSPI.
- Las actividades de implementación de los planes de tratamiento de riesgos se alinean con la fase de implementación del MSPI.
- Las actividades de monitoreo y revisión, revisión de los riesgos residuales, efectividad de los planes de tratamiento o los controles implementados y auditorias se alinean con la fase de medición del desempeño del MSPI.
- Las actividades de mejoramiento continuo en ambos modelos son similares y trabajan simultáneamente ya que dependen de las fases de medición de desempeño para identificar aspectos a mejorar en la aplicación de ambos modelos.

2. OBJETIVO

Generar el Plan de Tratamiento de Riesgos de Seguridad de Información como una guía metodológica alineada a la Política de Administración del Riesgo, que permita a los responsables de los procesos de La Empresa de Energía de Arauca – ENELAR E.S.P gestionar los riesgos que en materia de seguridad y privacidad de la información sea necesario sobre los activos de información que hacen parte del Registro de Activos de Información de la Empresa de Energía de Arauca – ENELAR E.S.P y que sean identificados con una criticidad alta por sus dueños según la valoración dada a su **confidencialidad, integridad y su disponibilidad**.

3. ALCANCE

La gestión de riesgos de seguridad de la información, incluido su tratamiento será aplicado sobre todos los activos de información de La Empresa de Energía de Arauca identificados por cada uno de los procesos y que hacen parte del Registro de Activos de Información de la la Empresa de Energía de Arauca – ENELAR E.S.P; con base en las normas vigentes, la metodología definida por la entidad para la gestión del riesgo definida, las pautas y recomendaciones previstas en la ISO/IEC 27001:2013 para su seguimiento, monitoreo y evaluación enfocado al cumplimiento y mejoramiento continuo.

4. PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACION FRENTE A LOS ACTIVOS DE INFORMACION REGISTRADOS

Como actividad fundamental para el tratamiento de los riesgos de seguridad y privacidad de la información, esta el mantener identificados y documentados los activos de información, los cuales son el objeto de análisis de riesgos para así mismo dar el tratamiento correspondiente.

Para el año 2023 la subdirección de sistemas, informática y telecomunicaciones, con el fin de mitigar la materialización de riesgos de seguridad y privacidad de la información contempla desarrollar las siguientes actividades:

N.	Descripción de actividades	Responsable	Tiempo
1	Sensibilización, socialización a las personas que desarrollan actividades en el proceso de Gestión TI sobre el proceso de valoración, tratamiento y gestión de riesgos frente a ciber amenazas.	Daniel Orlando Suarez Ruiz – Coordinador de Sistemas y Telecomunicaciones	01/05/2023 31/12/2023
2	Actualización del inventario de activos de información en el formato ITT-FO-11	Daniel Orlando Suarez Ruiz – Coordinador de Sistemas y Telecomunicaciones	01/05/2023 31/05/2023
3	Identificación y valoración de riesgos de seguridad informática frente a ciber amenazas.	Aníbal Fuentes Galvis – Subdir de Sistemas y Telecomunicaciones	01/06/2023 31/12/2023
4	Evaluación de los controles de seguridad de la información implementados frente a ciberamenazas.	Aníbal Fuentes Galvis – Subdir de Sistemas y Telecomunicaciones	01/08/2023 31/10/2023
5	Actualización del plan de tratamiento de riesgos frente a ciberamenzas	Aníbal Fuentes Galvis – Subdir. de Sistemas y Telecomunicaciones	01/01/2023 31/12/2023