PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN
2025

EMPRESA DE SERVICIOS PÚBLICOS DE SANTA FE DE ANTIOQUIA S.A.S E.S.P

1. OBJETIVO

Brindar a la Empresa de Servicios Públicos de Santa Fe de Antioquia s.a.s. E.S.P. una herramienta que proporcione las pautas necesarias para el adecuado tratamiento de los riesgos a los que está expuesta la entidad, que permitan una adecuada toma de decisiones para disminuir la probabilidad de materialización de amenaza o para reducir la vulnerabilidad del sistema o el posible impacto en la Entidad.

1.1. Objetivos Específicos

• Proteger los activos de información de acuerdo con su clasificación y criterios de confidencialidad, Integridad y Disponibilidad.
• Garantizar el manejo correcto de los riesgos para disminuir su probabilidad e impacto.
• Generar conciencia institucional de la importancia del tratamiento de riesgos.

2. ALCANCE

La gestión de riesgos de seguridad de la información y su tratamiento, podrá ser aplicada sobre cualquier proceso de la Empresa de Servicios Públicos de Santa Fe de Antioquia s.a.s. E.S.P, a través de los principios básicos y metodológicos para la administración de los riesgos de seguridad de la información, así como las estrategias para la identificación de los riesgos de seguridad de la información , análisis y evaluación, opciones de tratamiento o manejo del riesgo según la zona de riesgo; incluye además pautas y recomendaciones para su seguimiento, monitoreo y evaluación.

3. MARCO CONCEPTUAL

3.1. Factores Externos e Internos de Riesgo

Los factores de riesgo son aquellos que afectan a la entidad en mayor o menor grado de impacto.

CONTEXTO FACTORES EXTERNOS E INTERNOS DE RIESGO	
FACTORES EXTERNOS	**FACTORES INTERNOS**
Económicos: disponibilidad de capital, emisión de deuda o no pago de la misma, liquidez, mercados financieros, desempleo, competencia.	**Procesos:** Eventos Relacionados con errores en la actividades que deben realizar los servidores de la organización.
Medioambientales: emisiones y residuos, energía, catástrofes naturales, desarrollo sostenible.	**Talento Humano:** Incluye SST , Se analiza posible dolo e intención frente a la corrupción.
Políticos: cambios de gobierno, legislación, políticas públicas, regulación.	**Infraestructura:** Eventos relacionados con la infraestructura fisica de la entidad.
Sociales: demografía, responsabilidad social, terrorismo.	**Tecnología:** Eventos relacionados con la infraestructura tecnológica de la entidad
Tecnológicos: interrupciones, comercio electrónico, datos externos, tecnología emergente.	

3.2. Riesgos

3.2.1. Clases de Riesgos

En el desarrollo de las actividades de la entidad, esta se enfrenta a diversos riegos que pueden afectar de diferentes maneras el correcto funcionamiento y seguridad de los datos. Para conocer el contexto, la Empresa de Servicios Públicos de Santa Fe de Antioquia s.a.s. E.S.P, ha definido aquellos riesgos a los cuales se enfrenta para poder generar las diferentes estrategias y mitigar los efectos negativos de estos.

CLASES DE RIESGO	
CLASE	**DESCRIPCIÓN**
ESTRATEGICO	Se asocia con la forma en que se administra la Entidad. Se enfoca a asuntos globales relacionados con la misión y el cumplimiento de los objetivos estratégicos, la clara definición de políticas, diseño y conceptualización de la entidad por parte de la alta gerencia.
IMAGEN	Están relacionados con la percepción y la confianza por parte de la ciudadanía hacia la institución.
OPERATIVOS	Comprenden riesgos provenientes del funcionamiento y operatividad de los sistemas de información institucional, de la definición de los procesos, de la estructura de la entidad, de la articulación entre dependencias.

FINANCIEROS	Se relacionan con el manejo de los recursos de la entidad que incluyen: la ejecución presupuestal, la elaboración de los estados financieros, los pagos, manejos de excedentes de tesorería y el manejo sobre los bienes.
DE CUMPLIMIENTO	Se asocian con la capacidad de la entidad para cumplir con los requisitos legales, contractuales, de ética pública y en general con su compromiso ante la comunidad.
DE TECNOLOGÍA	Están relacionados con la capacidad tecnológica de la Entidad para satisfacer sus necesidades actuales y futuras y el cumplimiento de la misión.
DE CORRUPCIÓN	Están relacionados con el uso indebido del poder, de los recursos o de la información, para la obtención de un beneficio particular.
AMBIENTALES	Están relacionados con las Perdidas por contaminación de recursos naturales; Pérdidas generadas por situaciones de emergencia ambiental, pagos de sanciones de la autoridad ambiental o resarcimiento de daños a partes interesadas afectadas; Perdidas por fallas en la continuidad de la operación generadas por dificultad para el acceso a los componentes del ecosistema (Agua, Aire, Suelo, Fauna, Flora, Personas).
POLITICO	Está relacionado con Pérdidas por decisiones políticas que afectan a la organización.
COMERCIAL	Está relacionado con las Pérdida de clientes o mercados; Pérdidas económicas por pérdida de clientes; Perdidas por reclamaciones y atención de garantías.
DE ORDEN PUBLICO	Están Relacionados con la Pérdida derivada del conflicto armado; Pérdidas por afectación de la seguridad.
DEL RECURSO HUMANO	Pérdida por indisponibilidad del recurso humano con el conocimiento y la competencia requerida para cumplir con los resultados previstos.
FENOMENOS NATURALES	Pérdidas por manifestaciones de la naturaleza que puedan afectar los recursos de la organización y la continuidad del negocio.

3.2.2. Clasificación del Riesgo

De acuerdo con las clases de riesgo, se ha establecido un valor para la probabilidad de la ocurrencia del riesgo teniendo en cuenta la descripción y frecuencia, de la siguiente manera:

MATRIZ DE CALIFICACIÓN DEL RIESGO			
PROBABILIDAD	**VALOR**	**FRECUENCIA DE LA ACTIVIDAD**	**PROBABILIDAD**
Muy Baja	1	La actividad que conlleva el riesgo se ejecuta como máximo 2 veces por año.	20%
Baja	2	La actividad que conlleva el riesgo se ejecuta de 3 a 24 veces por año.	40%
Media	3	La actividad que conlleva el riesgo se ejecuta de 24 a 500 veces por año.	60%
Alta	4	La actividad que conlleva el riesgo se ejecuta mínimo 500 veces al año y máximo 5000 veces por año.	80%
Muy Alta	5	La actividad que conlleva el riesgo se ejecuta más de 5000 veces al año.	100%

4. METODOLOGIA

El plan de tratamiento de riesgos permitirá hacer énfasis de cómo se enfrentarán los riesgos en la entidad.
Para ello se establecen las siguientes actividades:

Actividad	Tarea	Responsable	Fecha inicio	Fecha fin
Implementación	Implementar nuevos controles establecidos en la matriz de riesgos.	Gestión de las Tics	Febrero de 2025	Febrero de 2025
Informe	Realizar un informe de las actividades realizadas para controlar y mejorar los seguimientos.	Gestión de las Tics	Junio de 2025	Junio de 2025
Seguimiento	Realizar seguimiento de funcionamiento a los controles implementados especialmente aquellos a mitigar los riesgos.	Gestión de las Tics	Junio de 2025	Junio de 2025

Implementación	Implementar nuevos controles establecidos en la matriz de riesgos.	Gestión de las Tics	Julio de 2025	Julio de 2025
Seguimiento	Realizar seguimiento de funcionamiento a los controles implementados por el área de sistemas	Gestión de las Tics	Julio de 2025	Julio de 2025
Capacitación	Realizar una capacitación de la policía Nacional para el manejo de los ciberataques.	Gestión de las Tics	Septiembre 2025	Septiembre 2025
Informe	Realizar un informe de las actividades realizadas para controlar y mejorar los seguimientos.	Gestión de las Tics	Noviembre de 2024	Diciembre de 2024
Revisar y Actualizar los lineamientos de los riesgos	Revisar y actualizar la matriz de riesgos de TIC (De acuerdo con el informe de hacking ético)	Gestión de las Tics	Diciembre de 2025	Diciembre de 2025