EMPRESA DE ACUEDUCTO Y ALCANTARILLADO DE CÚCUTA SA E.S.P.

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

**2025**

# Tabla de contenido

## Tablas

## INTRODUCCIÓN

La Empresa de Acueducto y Alcantarillado SA E.S.P, ha implementado las tecnologías de la información y la comunicación cómo eje fundamental en la administración, uso y respaldo de los datos proporcionados por los usuarios de la entidad. Permitiendo el fácil acceso y manejo de la información de una forma más organizada, no sólo por los funcionarios que la administran sino también por aquellos que la mantienen bajo su custodia.

El subproceso de Gestión de soporte y apoyo informático 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 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, los cuales son integrados en el mapa de riesgos institucional el cual sigue “Guía para la Administración del Riesgo y el diseño de controles en entidades públicas Versión 6”

El propósito del plan es, por lo tanto, garantizar que los riesgos de seguridad de la información en la Empresa de Acueducto y Alcantarillado SA E.S.P, sean definidos, divulgados y mitigados de manera clara y eficaz.

# 1. OBJETIVOS

## 1.1. Objetivo general

Establecer los conceptos básicos y metodológicos para una adecuada administración de riesgos a partir de su identificación, manejo y seguimiento, para mitigar, aceptar, transferir o evitar el riesgo los activos de información de los procesos con el fin de preservar confidencialidad, integridad, disponibilidad de la información.

## 1.2. Objetivos específicos

- Identificar riesgos
- Establecer soluciones para minimizar los riesgos que están expuestos cada activa
- Involucrar y comprometer a todos en la formulación e implementación de controles y acciones encaminadas a prevenir y administrar los riesgos.

# 2. Alcance

Este plan nos brindara técnicas para emprender la implementación del plan de gestión del riesgo en la seguridad de la información en la entidad.

Este plan hace parte integral del desarrollo gradual del mapa de riesgos institucional donde se integran todos los riesgos de la empresa a través de la guía de la función pública versión 6.

# 3. Definiciones

Para la administración del riesgo, se tendrán en cuenta los siguientes términos y definiciones:

- **Administración de riesgos:** conjunto de etapas secuenciales que se deben desarrollar para el adecuado tratamiento de los riesgos.
- **Amenaza:** situación externa que no controla la entidad y que puede afectar su operación
- **Análisis del riesgo:** etapa de la administración del riesgo, donde se establece la probabilidad de ocurrencia y el impacto del riesgo antes de determinar los controles (análisis del riesgo inherente).
- **Causa:** medios, circunstancias y/o agentes que generan riesgos.
- **Calificación del riesgo:** estimación de la probabilidad de ocurrencia del riesgo y el impacto que puede causar su materialización.

- **Consecuencia:** efectos que se pueden presentar cuando un riesgo se materializa.
- **Control:** acción o conjunto de acciones que minimiza la probabilidad de ocurrencia de un riesgo o el impacto producido ante su materialización.
- **Control preventivo:** acción o conjunto de acciones que eliminan o mitigan las causas del riesgo; está orientado a disminuir la probabilidad de ocurrencia del riesgo.
- **Control correctivo:** acción o conjunto de acciones que eliminan o mitigan las consecuencias del riesgo; está orientado a disminuir el nivel de impacto del riesgo.
- **Debilidad:** situación interna que la entidad puede controlar y que puede afectar su operación.
- **Evaluación del riesgo:** resultado del cruce cuantitativo de las calificaciones de probabilidad e impacto, para establecer la zona donde se ubicará el riesgo.
- **Evitar el riesgo:** opción de manejo que determina la formulación de acciones donde se prevenga la materialización del riesgo mediante el fortalecimiento de controles identificado.
- **Frecuencia:** ocurrencia de un evento expresado como la cantidad de veces que ha ocurrido un evento en un tiempo dado.
- **Identificación del riesgo:** etapa de la administración del riesgo donde se establece el riesgo con sus causas (asociadas a factores externos e internos de riesgo), consecuencias y se clasifica de acuerdo con los tipos de riesgo definidos
- **Impacto:** medida para estimar cuantitativa y cualitativamente el posible efecto de la materialización del riesgo.
- **Materialización del riesgo:** ocurrencia del riesgo identificado
- **Opciones de manejo:** posibilidades disponibles para administrar el riesgo posterior a la valoración de los controles definidos (asumir, reducir, evitar compartir o transferir el riesgo residual).
- **Plan de contingencia:** conjunto de acciones inmediatas, recursos, responsables y tiempos establecidos para hacer frente a la materialización del riesgo y garantizar la continuidad del servicio
- **Procedimiento:** conjunto de especificaciones, relaciones, responsabilidades, controles y ordenamiento de las actividades y tareas requeridas para cumplir con el proceso.

- **Riesgo:** eventualidad que tendrá un impacto negativo sobre los objetivos institucionales o del proceso.
- **Riesgo inherente:** es aquel al que se enfrenta una entidad o proceso en ausencia de controles y/o acciones para modificar su probabilidad o impacto.
- **Valoración del riesgo:** establece la identificación y evaluación de los controles para prevenir la ocurrencia del riesgo o reducir los efectos de su materialización. En la etapa de valoración del riesgo se determina el riesgo residual, la opción de manejo a seguir, y si es necesita.

## 4. Roles Y Responsabilidades Frente A La Administración Del Riesgo

El éxito de la administración del riesgo depende de la decidida participación de los directivos, servidores públicos y contratistas; por esto, es preciso identificar los actores que intervienen:

| Rol | Responsabilidad |
|---|---|
| Comité de Desempeño | Aprueban las directrices para la administración del riesgo en la Entidad. La Alta Dirección es la responsable del fortalecimiento de la política de administración del riesgo |
| Proceso Administración del Sistema Integrado de Gestión | Genera la metodología para la administración del riesgo de la Empresa, coordina, lidera, capacita y asesora en su aplicación. |
| Gestión de Soporte y Apoyo Informático | Identificar controles para mitigar los riesgos. |
| Servidores y/o contratistas | Ejecutar los controles y acciones definidas para la administración de los riesgos definidos, aportar en la identificación de posibles riesgos que puedan afectar la gestión de los procesos y/o de la entidad. |
| Evaluación y Control | Debe realizar evaluación y seguimiento a la política, los procedimientos y los controles propios de la administración de riesgos |

*Tabla 1.Roles y Responsabilidad*

## 5. Política De Administración Del Riesgo

La Empresa de Acueducto y Alcantarillado SA E.S.P, a través de su Modelo Integrado de Gestión, se compromete a mantener una cultura de la gestión del riesgo asociados con la

responsabilidad de diseñar, adoptar y promover las políticas, planes, programas del sector TIC.

La política identifica las opciones para tratar y manejar los riesgos basados en su valoración, permiten tomar decisiones adecuadas y fijar los lineamientos para administración de los mismos; a su vez, transmiten la posición de la dirección y establecen las guías de acción necesarias a todos los colaboradores De la EIS CUCUTA A E.S.P,

- Mantener un control permanente sobre los cambios en la calificación de los riesgos para realizar oportunamente los ajustes pertinentes.
- Reportar los eventos de riesgo que se materialicen, utilizando los procedimientos e instrumentos establecidos para el efecto.

- Desarrollar e implementar planes de contingencia para asegurar la continuidad de los procesos, en los eventos de materialización de los riesgos que afecten a los objetivos institucionales previstos y los intereses de los usuarios y partes interesadas.

## 7. Cronograma General Para La Administración De Riesgos De Seguridad Y Privacidad De La Información

| No. | ACTIVIDAD | FECHA INICIO | FECHA FINAL | RESPONSABLE |
|---|---|---|---|---|
| 1 | Establecer y o desarrollar el Plan tratamiento de Riesgos de Seguridad y Privacidad de la Información. | 30/01/2025 | 30/01/2025 | Gestión de Soporte y Apoyo Informático (Sistemas) Comité Institucional de Gestión y Desempeño. |
| 2 | Realizar verificación de software no autorizado dentro de las actividades programadas en el mantenimiento. | 01/02/2025 | 30/07/2025 | Gestión de Soporte y Apoyo Informático (Sistemas) |
| 3 | Desarrollar y/o actualizar el inventario de activos de información. | 01/02/2025 | 30/06/2025 | Gestión de Soporte y Apoyo Informático (Sistemas) Técnico Administrativo (Archivo) y líderes de proceso. |
| 4 | Revisión de la instalación del antivirus | 01/05/2025 | 31/12/2025 | Gestión de Soporte y Apoyo Informático (Sistemas) |
| 5 | Envió de Tips de Seguridad(mensual) | 01/03/2025 | 31/12/2025 | Gestión de Soporte y Apoyo Informático (Sistemas). |

| | | | | |
|---|---|---|---|---|
| 6 | Reporte de ataques de malware al firewall (Semestral) | 01/03/2025 | 31/12/2025 | Gestión de Soporte y Apoyo Informático (Sistemas) |
| 7 | Pruebas de Vulnerabilidad | 01/02/2025 | 31/12/2025 | Gestión de Soporte y Apoyo Informático (Sistemas)<br><br>Proveedor |
| 8 | Realizar seguimiento a la Declaración de Aplicabilidad para seguridad de la información a fin de evidenciar el tratamiento de los controles de acuerdo con la norma ISO:27001-2013 Anexo A | 01/01/2025 | 31/12/2025 | Gestión de Soporte y Apoyo Informático (Sistemas) y líderes de proceso. |
| 9 | Informe de seguimiento por parte del grupo TI(Controles establecidos en el mapa de Riesgos institucional)(semestral) | 01/01/2025 | 31/12/2025 | Gestión de Soporte y Apoyo Informático (Sistemas) y líderes de proceso. |

*Tabla 2.Cronograma de Actividades*

## 8. Indicador

| Código | Nombre | Objetivo | Frecuencia de medición |
|---|---|---|---|
| IND.01 | Indicador de Riesgo TI. | La medición se realiza con un indicador de gestión que está orientada principalmente determinar el porcentaje de ejecución de actividades definidas en el plan de tratamiento de riesgos de seguridad y privacidad de la información. | Cuatrimestral |

| Variables y formulación |
|---|
| #TotalR = Número total de riesgos incluidos en la evaluación de riesgos de la entidad.<br>#RiesgosTI = Número total de riesgos de TI o relacionados con TI, incluidos en la evaluación de riesgos de la entidad.<br>Indicador de seguimiento a riesgos de TI = #Riesgos TI / #TotalR * 100.<br>Indicador de seguimiento = #Actividades / #Actividades Programadas * 100. |

| Rangos | | | | |
|---|---|---|---|---|
| Bueno | De | 90% | A | 100% |
| Intermedio | De | 60% | A | 89% |
| Malo | De | 0% | A | 59% |

*Tabla 3.Indicador*

**9.** Seguimiento Y Control

semestralmente Evaluación y control realizará seguimiento a todo el componente de administración de riesgos (mapa de Riesgos institucional) y plan de Acción donde se integran los planes y actividades adicionales que puedan contribuir a la verificación detección y mitigación del riesgo

CONTROL DE CAMBIOS DEL DOCUMENTO

| **CONTROL DE CAMBIOS** | | |
|---|---|---|
| **VERSION** | **FECHA** | **DESCRIPCION DEL CAMBIO** |
| 01 | 30/01/2024 | Creación De Plan Vigencia 2024 |
| 01 | 30/01/2025 | Creación De Plan Vigencia 2025 |