PLAN DE MITIGACION DE RIESGO

EMPRESA DE SERVICIOS PÚBLICOS DE CAJICÁ SA ESP

VIGENCIA 2026

Actualizado 2026

Profesional Universitario Sistemas

Empresa de Servicios Públicos de Cajicá S.A. E.S.P.

Contenido

1. RESUMEN EJECUTIVO

El Plan de Tratamiento de Riesgos tiene como finalidad establecer las directrices, lineamientos y controles necesarios para mitigar los riesgos asociados a la pérdida de confidencialidad, integridad y disponibilidad de los activos de información de la Empresa de Servicios Públicos de Cajicá S.A. E.S.P.

Este plan se formula a partir de los resultados del análisis de riesgos y tiene como objetivo prevenir eventos que puedan generar incertidumbre o afectar el cumplimiento de los objetivos estratégicos, misionales y operativos de la entidad.

El Plan de Tratamiento de Riesgos contempla la identificación y evaluación de las acciones requeridas para tratar los riesgos identificados en los diferentes procesos institucionales. Dichas acciones se estructuran en actividades específicas, para las cuales se definen tareas, responsables y cronogramas de ejecución, los cuales serán implementados, monitoreados y evaluados durante la vigencia del plan.

El cumplimiento de las disposiciones establecidas en el presente plan es de carácter obligatorio para todas las áreas y funcionarios de la entidad, en el marco del Sistema de Gestión de Seguridad de la Información y de las políticas institucionales vigentes.

2. INTRODUCCIÓN

El Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información, Seguridad Digital y Continuidad de la Operación de los servicios (riesgos de interrupción) de la Empresa de Servicios Públicos de Cajicá S.A. E.S.P. se formula en el marco del Modelo Integrado de Planeación y Gestión (MIPG), específicamente en la **Dimensión de Gobierno Digital**, como parte del **Habilitador de Seguridad Digital y Seguridad y Privacidad de la Información**.

Este Plan se fundamenta en una orientación estratégica que promueve el fortalecimiento de una cultura institucional de carácter preventivo, orientada a la gestión integral del riesgo. En este sentido, a partir de la comprensión del concepto de riesgo y del contexto de los procesos institucionales, la entidad planifica e implementa acciones que permitan reducir la probabilidad de ocurrencia y el impacto de los riesgos asociados a la pérdida de confidencialidad, integridad y disponibilidad de los activos de información, así como aquellos relacionados con la interrupción de la operación de los servicios.

El Plan tiene como objetivo contribuir al cumplimiento de los objetivos estratégicos, misionales y operativos de la entidad, mediante el desarrollo de estrategias sistemáticas para la identificación, análisis, tratamiento, evaluación y monitoreo de los riesgos de Seguridad y Privacidad de la Información y Seguridad Digital, permitiendo anticipar y gestionar de manera oportuna aquellas situaciones que puedan afectar el logro de los resultados definidos en el Entorno TIC para el Desarrollo Digital.

La formulación e implementación del presente Plan se realiza en concordancia con los lineamientos establecidos en el Documento CONPES 3995 de 2020, el Decreto Único Reglamentario del Sector TIC – Decreto 1078 de 2015, y la Resolución 500 de 2021, por la cual se establecen los lineamientos y estándares de la Estrategia de Seguridad Digital y se adopta el Modelo de Seguridad y Privacidad de la Información en las entidades públicas. Asimismo, el Plan adopta las buenas prácticas y lineamientos de los estándares internacionales ISO/IEC 27001 e ISO 31000:2018, así como la Guía para la Administración del Riesgo y el Diseño de Controles en Entidades Públicas definida en el marco del MIPG.

En cumplimiento de lo dispuesto en el Decreto 612 de 2018, la Empresa de Servicios Públicos de Cajicá S.A. E.S.P. establece el presente documento como un instrumento de planeación institucional, articulado con los planes, programas y proyectos de la entidad, y como un mecanismo de control y seguimiento permanente a la gestión de los riesgos de Seguridad y Privacidad de la Información, Seguridad Digital y Continuidad de la Operación.

El presente Plan es de obligatorio cumplimiento para todas las dependencias, procesos, servidores públicos, contratistas y terceros que tengan acceso a los activos de información de la entidad, y su implementación será objeto de seguimiento, evaluación y mejora continua, conforme a los principios y lineamientos del MIPG.

3. TERMINOLOGIA

En la Empresa de Servicios Públicos de Cajicá S.A. E.S.P., define los siguientes términos a utilizar en el Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información.

- **Riesgo**: Efecto que se causa sobre los objetivos de las entidades, debido a eventos potenciales.
- **Riesgo de Seguridad de la Información:** Posibilidad de que una amenaza concreta pueda explotar una vulnerabilidad para causar una pérdida o daño en un activo de información. Suele considerarse como una combinación de la probabilidad de un evento y sus consecuencias. (ISO/IEC 27000).
- **Amenaza:** es un ente o escenario interno o externo que puede hacer uso de una vulnerabilidad para generar un perjuicio o impacto negativo en la institución (materializar el riesgo).
- **Vulnerabilidad:** es una falencia o debilidad que puede estar presente en la tecnología, las personas o en las políticas y procedimientos.
- **Probabilidad:** se entiende la posibilidad de ocurrencia del riesgo. Estará asociada a la exposición al riesgo del proceso o actividad que se esté analizando.
- **Impacto:** consecuencias que puede ocasionar a la organización la materialización del riesgo.
- **Control o Medida**: Medida que permite reducir o mitigar un riesgo.

4. OBJETIVOS

- Definir y aplicar los lineamientos para tratar de manera integral los riesgos de Seguridad y Privacidad de la Información, Seguridad Digital y Continuidad de la Operación de los servicios (riesgos de interrupción) a los que pueda estar expuesto, la Empresa de Servicios Públicos de Cajicá S.A. E.S.P., y de esta manera alcanzar los objetivos, la misión y la visión institucional, protegiendo y preservando la integridad, confidencialidad, disponibilidad, privacidad y autenticidad de la información.

- Cumplir con los requisitos legales, reglamentarios, regulatorios y de las normas técnicas colombianas en materia de seguridad y privacidad de la información, seguridad digital y protección de la información personal.

- Gestionar los riesgos de Seguridad y Privacidad de la información, Seguridad Digital y Continuidad de la Operación de los servicios (riesgos de interrupción), de acuerdo con los contextos establecidos en los procesos y procedimientos de la Entidad.

- Fortalecer y apropiar conocimiento referente a la gestión de riesgos de Seguridad y Privacidad de la información, Seguridad Digital y Continuidad de la Operación de los servicios (riesgos de interrupción) de la Empresa de Servicios Públicos de Cajicá S.A. E.S.P..

5. ALCANCE

El Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información, Seguridad Digital y Continuidad de la Operación de los servicios (riesgos de interrupción) aplica a todos los procesos estratégicos, misionales, de apoyo y de evaluación de la Empresa de Servicios Públicos de Cajicá S.A. E.S.P., así como a los activos de información asociados, independientemente de su formato, medio de almacenamiento, procesamiento o transmisión.

El presente Plan comprende la gestión de los riesgos que puedan afectar la confidencialidad, integridad y disponibilidad de la información, así como aquellos riesgos que puedan generar interrupciones en la prestación de los servicios, impactando la continuidad de la operación institucional.

El alcance del Plan incluye a todas las dependencias, servidores públicos, contratistas, proveedores y terceros que, en el ejercicio de sus funciones o actividades, tengan acceso, administren, procesen o custodien activos de información de la entidad, así como a las infraestructuras tecnológicas, sistemas de información, servicios digitales y recursos asociados al Entorno TIC de la Empresa.

El Plan de Tratamiento de Riesgos se aplica durante la vigencia establecida para su implementación y seguimiento, y se articula con los instrumentos de planeación institucional, el Sistema de Gestión de Seguridad de la Información (SGSI), la Estrategia de Gobierno Digital y los lineamientos del Modelo Integrado de Planeación y Gestión (MIPG).

Asimismo, el alcance contempla la identificación, análisis, tratamiento, evaluación y monitoreo de los riesgos, priorizando aquellos clasificados en niveles Moderado, Alto y Extremo, de conformidad con los lineamientos definidos por el Ministerio de Tecnologías de la Información y las Comunicaciones – MinTIC, sin perjuicio de la gestión y control de los demás riesgos identificados.

6. MARCO REFERENCIAL

POLÍTICA DE ADMINISTRACION DE RIESGOS

La Empresa de Servicios Públicos de Cajicá S.A. E.S.P., a través de su Modelo de Gestión de Calidad, se compromete a mantener una cultura de la gestión del riesgo que permita fortalecer las medidas de prevención, monitoreo y seguimiento al control para mitigar la posible ocurrencia de riesgos, en las actividades desarrolladas por la Entidad asociadas con la responsabilidad de diseñar, adoptar, ejecutar y promover las políticas, planes, programas, iniciativas y proyectos del sector TIC, mediante mecanismos, sistemas y controles que detecten hechos asociados, de manera Integral, con la estrategia, la gestión la transparencia y la ética, seguridad y privacidad de la información, seguridad digital y continuidad de la operación, riesgo fiscal, aspectos ambientales y de seguridad y salud en el trabajo, que puedan afectar el cumplimento de los objetivos institucionales, el aprovechamiento al máximo los recursos destinados y la atención a nuestros grupos de interés.

El objetivo de la política es establecer los parámetros necesarios para una adecuada gestión de los Riesgos de Seguridad y Privacidad de la información, Seguridad Digital y Continuidad de los servicios (riesgos de interrupción) en la Empresa de Servicios Públicos de Cajicá S.A. E.S.P., procurando que no se materialicen, atendiendo los lineamientos establecidos en la Guía para la administración del riesgo y el diseño de controles en entidades públicas del DAFP, orientando a la toma de decisiones oportunas y minimizando efectos adversos al interior de la Entidad, con el fin de dar continuidad a la gestión institucional y asegurar el cumplimiento de los compromisos con los Grupos de interés.

El tratamiento de riesgos es la respuesta establecida por la primera línea de defensa, es decir, el líder o responsable del proceso junto con su equipo de trabajo para la mitigación de los diferentes riesgos. El tratamiento o respuesta dada al riesgo, se enmarca en las siguientes categorías:

- **Aceptar el riesgo:** No se adopta ninguna medida que afecte la probabilidad o el impacto del riesgo. (Ningún riesgo de corrupción es aceptado). La aceptación del riesgo puede ser una opción viable en la entidad, para los riesgos bajos, pero también pueden existir

escenarios de riesgos a los que no se les puedan aplicar controles y, por ende, se acepta el riesgo. En ambos escenarios debe existir un seguimiento continuo del riesgo.

- **Reducir el riesgo:** Se adoptan medidas para reducir la probabilidad o el impacto del riesgo, o ambos; por lo general conlleva a la implementación de controles. Deben seleccionarse controles apropiados y con una adecuada segregación de funciones, de manera que el tratamiento al riesgo adoptado logre la reducción prevista sobre este.

- **Evitar el riesgo:** Se abandonan las actividades que dan lugar al riesgo, es decir, no iniciar o no continuar con la actividad que lo provoca.

- **Compartir el riesgo:** Se reduce la probabilidad o el impacto del riesgo transfiriendo o compartiendo una parte de este. Los riesgos de corrupción se pueden compartir, pero no se puede transferir su responsabilidad. Los dos principales métodos de compartir o transferir parte del riesgo son: seguros y tercerización.

La gestión de riesgos de Seguridad y privacidad de la Información, seguridad digital y continuidad de la operación de los servicios (riesgos de interrupción) le permite que la Empresa de Servicios Públicos de Cajicá S.A. E.S.P., realice una identificación, análisis y tratamiento de los riesgos que puedan generar afectación al cumplimiento de los objetivos de sus procesos, contribuyendo en la toma de decisiones, y en la prevención de la materialización de estos. La administración de riesgos de Seguridad y Privacidad de la Información, Seguridad Digital y Continuidad de la Operación de los servicios (riesgos de interrupción) se encuentra enfocada en identificar, analizar, valorar y tratar las amenazas y vulnerabilidades de los activos de información de la entidad, teniendo presente su criticidad y protección. Las etapas presentes en la gestión de riesgos permiten alinearlas con los objetivos, estrategias y políticas de la entidad, logrando un nivel de riesgo que pueda aceptar o asumir la Alta Gerencia.

7. MAPA DE RIESGOS DE CORRUPCIÓN

Se establecen los riesgos asociados a los procesos de TI y el plan de Mitigación de los mismos.

- Mejorar Continuamente la eficiencia, eficacia y efectividad de la Empresa de Servicios Públicos de Cajicá S.A. E.S.P.
- Contar con el recurso humano competente, en el manejo de la infraestructura tecnologías que sea suficiente para el cumplimiento de los objetivos misiónales de la Entidad.
- Garantizar el cumplimiento de las actividades según las leyes y políticas del Estado.
- Generar mecanismos para la Transparencia y Acceso a la Información.

7.1. GESTIÓN DEL RIESGO DE CORRUPCIÓN

La gestión de riesgo de corrupción de la Empresa de Servicios Públicos de Cajicá S.A. E.S.P., se proyecta inmersamente en el mapa de riesgos de corrupción que funciona como instrumento que permite a la Entidad identificar, analizar y controlar los posibles hechos generadores de corrupción, tanto internos como externos. Este mecanismo tiene como fin identificar y prevenir los riesgos de corrupción el cual busca obtener como resultado la generación de alarmas que funcionan como el insumo para la elaboración de mecanismos focalizados en pro de prevenirlos y evitarlos.

7.2. IDENTIFICACIÓN DEL RIESGO

Para la identificación de los riesgos de Seguridad y Privacidad de la Información, Seguridad Digital y Continuidad de la Operación de los servicios (riesgos de interrupción) de la Empresa de Servicios Públicos de Cajicá S.A. E.S.P., se deberán considerar, entre otros, los aspectos relacionados con la infraestructura física, las áreas de trabajo, el entorno tecnológico y el ambiente organizacional en general.

Para tal efecto, es indispensable que cada proceso tenga debidamente identificados y actualizados sus activos de información, a fin de reconocer las situaciones potenciales que puedan causar daño a la entidad y poner en riesgo el cumplimiento de los objetivos estratégicos, misionales y operativos establecidos.

La ausencia de controles o la falta de apropiación de prácticas relacionadas con la Seguridad y Privacidad de la Información (vulnerabilidades) pueden ser aprovechadas por amenazas internas o externas, dando lugar a la materialización de un riesgo, entendido como un incidente de seguridad de la información. En consecuencia, durante el ejercicio de identificación de riesgos, se deberá diligenciar el formato institucional del mapa de riesgos, registrando como mínimo los siguientes elementos:

- El atributo de la tríada de la información afectado (Confidencialidad, Integridad y/o Disponibilidad).
- El dueño del riesgo, correspondiente al líder del proceso.
- El activo de información afectado.
- Las amenazas identificadas.
- Las vulnerabilidades asociadas.
- Las posibles consecuencias o impactos para la entidad.

Para la determinación de los activos de información afectados, será obligatorio validar dicha información frente al **Inventario de Activos de Información** del proceso correspondiente, en el cual se encuentran definidos atributos como la criticidad, la clasificación de la información y otros elementos relevantes que deben ser considerados en el análisis del riesgo y en la definición de las acciones de tratamiento.

7.3. VALORACIÓN DEL RIESGO

La valoración de los riesgos de Seguridad y Privacidad de la Información, Seguridad Digital y Continuidad de la Operación de los servicios (riesgos de interrupción) de la Empresa de

Servicios Públicos de Cajicá S.A. E.S.P. se realizará de conformidad con la metodología para la administración de riesgos definida en la **Guía para la Administración del Riesgo y el Diseño de Controles en Entidades Públicas**, emitida por el Departamento Administrativo de la Función Pública (DAFP), en articulación con los lineamientos del Modelo Integrado de Planeación y Gestión (MIPG).

Para tal efecto, se llevarán a cabo mesas de trabajo con los líderes de los procesos, en las cuales se analizará el contexto interno y externo, se identificarán los riesgos y se realizará el análisis de la probabilidad y el impacto como valoración preliminar, con el fin de determinar el nivel de riesgo inherente. En este proceso se asociarán las amenazas, vulnerabilidades y consecuencias, así como los activos de información afectados, y se identificarán los controles existentes definidos en la Norma ISO/IEC 27001 orientados a su mitigación.

A cada control identificado se le evaluará su diseño y efectividad, considerando, como mínimo, las siguientes variables: asignación de un responsable, segregación de funciones y nivel de autoridad, tipo de control (preventivo, detectivo o correctivo), forma de implementación (manual o automática), periodicidad, propósito del control, descripción de la actividad de control, tratamiento de las observaciones o desviaciones identificadas y evidencia de su ejecución. Adicionalmente, se verificará que los controles se ejecuten de manera consistente y adecuada, de tal forma que contribuyan efectivamente a la mitigación del riesgo identificado.

La valoración de los riesgos y de la efectividad de los controles se realizará conforme a las tablas de probabilidad, impacto y niveles de riesgo establecidas en la metodología definida en la Guía para la Administración del Riesgo y el Diseño de Controles en Entidades Públicas del DAFP, lo cual permitirá determinar el nivel de riesgo residual y definir las acciones de tratamiento correspondientes.

En el caso de los riesgos de interrupción de la operación, los controles identificados podrán ser de carácter transversal, considerando el criterio del **custodio del activo de información**. Cuando dicho custodio corresponda a un proceso diferente al que identifica el riesgo o a un tercero, los controles y planes de tratamiento deberán establecerse de manera conjunta y coordinada entre las partes involucradas. El proceso que identifica el riesgo será responsable de aportar la valoración de la probabilidad, el impacto y el nivel de riesgo inherente asociado a la posible indisponibilidad del activo, en articulación con el custodio correspondiente.

7.4. DEFINICIÓN Y APROBACIÓN DE MAPAS DE RIESGOS Y PLANES DE TRATAMIENTO.

Una vez se obtenga la valoración de los riesgos de Seguridad y Privacidad de la Información, Seguridad Digital y Continuidad de la Operación de los Servicios (riesgos de interrupción) de la Empresa de Servicios Públicos de Cajicá S.A. E.S.P., los líderes de los procesos deberán justificar la aprobación de los mapas de riesgos y de los planes de tratamiento con las actividades requeridas que permitan mitigar aquellos riesgos cuyo nivel residual este en zona Moderada, Alta o Extrema.

7.5. MATERIALIZACIÓN

En la materialización de un riesgo, se debe ser reportado de acuerdo con el procedimiento de gestión de incidentes de seguridad y privacidad de la información. Así mismo se deberá analizar el riesgo y validar en qué nivel queda posterior a la materialización, registrando los cambios respectivos en el mapa de riesgos.
En caso de que se materialice un riesgo que no esté identificado, deberá ser reportado para que se inicie su correspondiente identificación en el mapa de riesgos.

8. Oportunidad de Mejora

La Empresa de Servicios Públicos de Cajicá S.A. E.S.P., no sólo deberá centrarse en los riesgos identificados, sino que este análisis o apreciación del riesgo debe ser la base para identificar oportunidades. Por lo anterior la oportunidad deberá entenderse como la consecuencia positiva frente al resultado del tratamiento del Riesgo.

9. RECURSOS

La Empresa de Servicios Públicos de Cajicá S.A. E.S.P., en el marco de la gestión de riesgos de Seguridad y Privacidad de la información, Seguridad Digital y Continuidad de la Operación de los servicios (riesgos de interrupción), dispone de los siguientes recursos.

RECURSOS	VARIABLE
HUMANO	• Director Administrativo • Profesional Universitario de Calidad • Profesional Universitario de Sistemas • Lideres de Procesos
TECNICOS	• Guía para la administración del riesgo y el diseño de controles en entidades públicas - Riesgos de gestión, corrupción y seguridad digital del DAFP. • Herramienta para la gestión de riesgos (Matriz de Riesgos)
LOGISTICOS	Gestión de recursos para realizar socializaciones, transferencia de conocimientos y seguimiento a la gestión de riesgos.

<table>
<tr><td></td><td></td></tr>
<tr><td>FINANCIEROS</td><td>Recursos para la adquisición de conocimiento, recursos humanos, técnicos, y desarrollo de auditorías en Sistema de Seguridad y Privacidad de la Información
<table>
<tr><th>Iniciativa</th><th>Proyecto</th><th>Presupuesto</th></tr>
<tr><td>Fortalecimiento de las herramientas tecnológicas y de comunicación</td><td>Actualización de las herramientas tecnológicas y de comunicación.</td><td>$ 450.000.000</td></tr>
<tr><td>Fortalecimiento del personal profesional de sistemas</td><td>Contratar personal profesional de sistemas para la implementación de las herramientas tecnológicas y de comunicación.</td><td>$ 101.200.000</td></tr>
</table></td></tr>
</table>

10. PRESUPUESTO PARA LA IMPLEMENTACIÓN DE CONTROLES

Para la estimación y asignación del presupuesto para el plan de tratamiento de riesgos de Seguridad y Privacidad de la Información, Seguridad Digital y Continuidad de la Operación de los servicios (riesgos de interrupción) identificados en la entidad, corresponderá al dueño del riesgo (líder del proceso), quien es el responsable de contribuir con el seguimiento y control de la gestión, además de la implementación de los controles definidos y del plan de tratamiento.

Este Plan Tratamiento a los riesgos de Seguridad Privacidad de la Información para la vigencia 2026 se aprobó por Comité Institucional de Gestión y Desempeño realizado el 29 de Enero de 2026 mediante el acta número 001.

Proyectó: Oscar López – Profesional Universitario Sistemas
Revisó y Aprobó: Comité Institucional de Gestión y Desempeño (CIGD)