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

PLAN DE TRATAMIENTO DE RIESGOS

EMPRESA DE SERVICIOS PÚBLICOS DE CAJICÁ SA ESP

VIGENCIA 2025 - 2027

Actualizado 2025.
Profesional Universitario Sistemas

Contenido

1. RESUMEN EJECUTIVO

Mediante la definición del Plan de Tratamiento de Riesgos se busca establecer medidas para mitigar los riesgos presentes en su análisis (perdida de confidencialidad, perdida de integridad y perdida de disponibilidad de los activos de información), lo que permite evitar situaciones que generen incertidumbre en el cumplimiento de los objetivos de la Empresa de Servicios Públicos de Cajicá S.A. E.S.P.

El Plan de Tratamiento de Riesgo se define con el fin de evaluar las posibles acciones que se deben tomar para mitigar los riesgos identificados en los procesos de la entidad, estas acciones son organizadas en actividades, definiendo para cada una de ellas las tareas, el responsable y sus fechas de ejecución que serán aplicadas durante la vigencia del plan.

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 basa en una orientación estratégica que requiere el desarrollo de una cultura de carácter preventivo, de manera que, al comprender el concepto de riesgo, así como el contexto del proceso, se planean acciones que reduzcan la afectación a la entidad en caso de materialización, adicionalmente busca desarrollar estrategias para la identificación, análisis, tratamiento, evaluación y monitoreo de dichos riesgos con mayor objetividad, dando a conocer aquellas situaciones que pueden comprometer el cumplimiento de los objetivos trazados en el Entorno TIC para el Desarrollo Digital.

Lo anterior dando seguimiento a lo recomendado por el Documento CONPES 3995 de 2020 y el Decreto Único Reglamentario del Sector TIC, Decreto 1078 de 2015, que señala la el habilitador de seguridad y privacidad de la Información, reglamentado por la Resolución 500 de 2021, por la cual se establecen los lineamientos y estándares para la estrategia de seguridad digital y se adopta el modelo de seguridad y privacidad, acogiendo las buenas prácticas y los lineamientos de los estándares ISO 27001, ISO 31000:2018 y la guía para la administración del riesgo y el diseño de controles en entidades públicas establecidos en el Modelo Integrado de Planeación y Gestión.
Teniendo en cuenta lo anterior, se procede a crear el documento dando cumplimiento a lo establecido en el Decreto 612 de 2018, implementación del Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información de la Empresa de Servicios Públicos de Cajicá S.A. E.S.P..

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

Efectuar una eficiente gestión de riesgos de Seguridad y Privacidad de la información, Seguridad Digital y Continuidad de la Operación de los servicios (riesgos de interrupción), que permita

integrar en los procesos y procedimientos de la entidad, buenas prácticas que contribuyan a la toma de decisiones y prevenir incidentes que puedan afectar el logro de los objetivos y la Misión de la Entidad.

Adicionalmente dar los lineamientos para poder identificar, analizar, tratar, evaluar y monitorear los riesgos de seguridad y privacidad de la información en la Empresa de Servicios Públicos de Cajicá S.A. E.S.P.
El Plan de Tratamiento de Riesgo tendrá en cuenta todos los riesgos en especial los que se encuentren en los niveles Moderado, Alto y Extremo acorde con los lineamientos definidos por el Ministerio de TIC, teniendo en cuenta que los riesgos que se encuentren en niveles inferiores serán aceptados por la Entidad.

6. MARCO REFERENCIAL

6.1. 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 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 debe tener en cuenta diferentes aspectos como infraestructura física, áreas de trabajo, entorno y ambiente en general, para lo cual se hace indispensable que cada uno de los procesos tenga identificado los activos información, y reconocer las situaciones potenciales que causarían daño a la entidad poniendo en riesgo el logro de los objetivos establecidos.
La falta de apropiación en temas referentes a la seguridad de la información o la ausencia de controles (vulnerabilidades) puede ser aprovechadas por una amenaza causando la materialización de un riesgo (Incidente), por lo que es preciso identificar en el formato del mapa de riesgos: El atributo de la triada de la información afectado (Confidencialidad, Integridad, Disponibilidad), dueño del riesgo (líder del proceso), activo de información afectado, amenazas, vulnerabilidades y consecuencias.
En determinar los activos afectados es necesario validarlos dentro del inventario de activos de información del proceso en donde en su valoración se estableció la criticidad, la clasificación de la información y otros atributos importantes a tener en cuenta en el análisis del posible riesgo.

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 acorde a la metodología para la administración de riesgos mencionada 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.
Es así como en mesas de trabajo con los procesos se analizará el contexto, se identifican los riesgos y se realiza el análisis de la probabilidad e impacto como valoración preliminar para identificar el nivel del riesgo inherente, asociando sus amenazas, vulnerabilidades y consecuencias e identificando los controles establecidos en la Norma ISO 27001 para mitigarlas. A estos controles se le identifican las variables a evaluar para su adecuado diseño como son: la asignación de un responsable, segregación y autoridad del responsable, tipo de control (preventivo, detectivo o correctivo), implementación (manual o automático), periodicidad, propósito, cómo se realiza la actividad de control, qué pasa con las observaciones o desviaciones y la evidencia de la ejecución del control. Adicionalmente se evalúa que cada control se ejecute

de manera consistente, de tal forma que pueda mitigar el riesgo. Esta valoración se realiza de acuerdo con las tablas y metodología establecida y mencionada en la Guía para la administración del riesgo y el diseño de controles en entidades públicas del DAFP.
En los riesgos de interrupción, se indica que los controles identificados pueden ser transversales, partiendo del criterio denominado custodio del activo, puesto que cuando dicho custodio es un proceso diferente al proceso que identifica el riesgo o es un tercero, estos controles y planes de tratamiento deben establecerse de manera conjunta. El proceso donde se identifica el riesgo aporta los niveles de probabilidad, impacto y riesgo inherente que genera la posible indisponibilidad del activo

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.

<table>
<tr><td>RECURSOS</td><td>VARIABLE</td></tr>
<tr><td>HUMANO</td><td>• Director Administrativo
• Profesional Universitario de Calidad
• Profesional Universitario de Sistemas
• Lideres de Procesos</td></tr>
<tr><td>TECNICOS</td><td>• 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)</td></tr>
<tr><td>LOGISTICOS</td><td>Gestión de recursos para realizar socializaciones, transferencia de conocimientos y seguimiento a la gestión de riesgos.</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><td>Iniciativa</td><td>Proyecto</td><td>Presupuesto</td></tr>
<tr><td>Fortalecimiento de las herramientas tecnológicas y de comunicación</td><td>Actualización de las herramientas tecnológicas y de comunicación.</td><td>$ 140.000.000</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>$ 96.000.000</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.

NOTA: El Plan de Tratamiento a los Riesgos de Seguridad y Privacidad de la Información para la vigencia 2025, se aprobó por Comité Institucional de Gestión y Desempeño realizado el 20 de diciembre de 2024 mediante el acta número 05 de 2024.