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

Vigencia 2026

Calle 24 #51-40, Bogotá
Capital Tower- Piso 7 y 11
Tel: **601 580 16 72** - Código Postal: 111321
Contactenos@epc.com.co
www.epc.com.co
@EPCUNDI

TABLA DE CONTENIDO

1. Introducción

El Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información de Empresas Públicas de Cundinamarca S.A. E.S.P. se constituye como un instrumento técnico y operativo del Modelo de Seguridad y Privacidad de la Información (MSPI), orientado a definir, implementar y hacer seguimiento a las acciones necesarias para el tratamiento de los riesgos que puedan afectar la confidencialidad, integridad, disponibilidad y autenticidad de la información institucional.

Este plan adopta un enfoque preventivo, sistemático y basado en riesgos, en coherencia con el Modelo Integrado de Planeación y Gestión (MIPG), los lineamientos de Gobierno Digital, y las disposiciones del Decreto 612 de 2018, integrándose de manera transversal a los procesos institucionales y apoyando la toma de decisiones estratégicas de la entidad.

El documento se articula con los instrumentos de planeación y gestión de Tecnologías de la Información de la entidad, en particular con el Plan Estratégico de Tecnologías de la Información (PETI), el Plan Estratégico de Seguridad y Privacidad de la Información (PESI) y el Sistema Integrado de Gestión (SIG), asegurando coherencia documental, trazabilidad y consistencia metodológica.

El Proceso de Tecnologías de la Información, adscrito a la Dirección de Planeación, actúa como habilitador estratégico del tratamiento de los riesgos de seguridad y privacidad de la información, en coordinación con las dependencias responsables y en articulación permanente con la Gerencia General, las Subgerencias y las Direcciones vigentes de la entidad, sin perjuicio de las funciones propias de control y seguimiento ejercidas por la Dirección de Control Interno.

La implementación y seguimiento de este plan permite a la entidad:

- Reducir la probabilidad y el impacto de la materialización de riesgos asociados a la información.
- Fortalecer la cultura institucional de seguridad y privacidad de la información.
- Contar con evidencias verificables para auditorías internas y externas.
- Facilitar la mejora continua del MSPI y el cumplimiento de los requisitos normativos aplicables.

El presente Plan de Tratamiento tiene vigencia 2026 y será objeto de seguimiento, evaluación y actualización conforme a los resultados obtenidos, los cambios en el contexto institucional, tecnológico y normativo, y las directrices definidas por la alta dirección de la entidad.

2. Marco Estratégico e Institucional

El Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información se enmarca dentro del sistema de planeación, gestión y control de Empresas Públicas de Cundinamarca S.A. E.S.P., y constituye un instrumento operativo que materializa el enfoque de gestión del riesgo definido por la entidad, en coherencia con el Modelo Integrado de Planeación y Gestión (MIPG) y los lineamientos de Gobierno Digital.

Desde la perspectiva estratégica, el tratamiento de los riesgos de seguridad y privacidad de la información contribuye de manera directa al cumplimiento de los objetivos institucionales, en tanto protege los activos de información que soportan la gestión misional, administrativa, financiera, contractual y técnica de la entidad, así como la toma de decisiones por parte de la alta dirección.

El Proceso de Tecnologías de la Información, adscrito a la Dirección de Planeación, actúa como proceso de apoyo estratégico y transversal, responsable de habilitar los mecanismos técnicos y de gestión necesarios para la identificación, análisis, tratamiento y seguimiento de los riesgos asociados a la información y a los servicios tecnológicos que la soportan. En este sentido, el plan se integra de forma armónica con los instrumentos de planeación institucional y sectorial, evitando duplicidades y garantizando consistencia metodológica.

El presente documento se articula de manera directa con:

- El Plan Estratégico de Tecnologías de la Información (PETI), como instrumento rector de la planeación TI.
- El Plan Estratégico de Seguridad y Privacidad de la Información (PESI), como marco de implementación del MSPI.
- El Modelo de Seguridad y Privacidad de la Información (MSPI), como referente normativo y metodológico para la gestión de la seguridad digital.
- El Sistema Integrado de Gestión (SIG), en lo relacionado con gestión del riesgo, control interno y mejora continua.

Adicionalmente, el plan reconoce la responsabilidad de las diferentes dependencias institucionales en la gestión del riesgo, bajo un esquema de corresponsabilidad, en el cual la Gerencia General, las Subgerencias y las Direcciones vigentes participan activamente en la identificación de riesgos, la definición de acciones de tratamiento y el suministro de evidencias, de acuerdo con sus competencias funcionales.

El marco estratégico e institucional definido en este documento garantiza que el tratamiento de los riesgos de seguridad y privacidad de la información no se gestione

de manera aislada, sino como parte integral del modelo de gobierno, planeación y control de la entidad, asegurando su alineación con los principios de eficiencia, transparencia, legalidad y mejora continua que rigen la gestión pública.

3. Objetivos del Plan de Tratamiento

Objetivo General

Definir, implementar y hacer seguimiento a las acciones de tratamiento de los riesgos de Seguridad y Privacidad de la Información de Empresas Públicas de Cundinamarca S.A. E.S.P., con el fin de reducir su probabilidad de ocurrencia y/o impacto, protegiendo los activos de información institucionales y garantizando la confidencialidad, integridad, disponibilidad y autenticidad de la información, en coherencia con el Modelo de Seguridad y Privacidad de la Información (MSPI), el Modelo Integrado de Planeación y Gestión (MIPG) y los lineamientos de Gobierno Digital.

Objetivos Específicos

- Identificar y analizar los riesgos de seguridad y privacidad de la información asociados a los procesos, activos de información y servicios tecnológicos de la entidad, conforme a la metodología institucional de gestión del riesgo.
- Definir y priorizar acciones de tratamiento de riesgos alineadas con el nivel de riesgo identificado, considerando controles preventivos, predictivos y correctivos, de acuerdo con las buenas prácticas y estándares aplicables.
- Asignar responsables, plazos y entregables para cada acción de tratamiento, garantizando la corresponsabilidad de las dependencias involucradas y la articulación con el Proceso de Tecnologías de la Información.
- Realizar el seguimiento, control y monitoreo de la ejecución de las acciones de tratamiento, generando evidencias verificables que soporten la toma de decisiones y el ejercicio de control interno.
- Gestionar de manera controlada los riesgos residuales, asegurando que su aceptación se realice bajo criterios institucionales definidos y con el debido respaldo de la alta dirección, cuando aplique.
- Fortalecer la mejora continua del Modelo de Seguridad y Privacidad de la Información, mediante la retroalimentación derivada del tratamiento de riesgos, auditorías y evaluaciones internas y externas.

4. Marco Normativo y de Referencia

El Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información de Empresas Públicas de Cundinamarca S.A. E.S.P. se formula y ejecuta en cumplimiento del marco normativo, técnico y metodológico vigente aplicable a las entidades públicas colombianas, así como de los estándares internacionales adoptados como buenas prácticas para la gestión del riesgo y la seguridad de la información.

El presente plan se alinea con las disposiciones legales y lineamientos institucionales que regulan la planeación, la gestión del riesgo, la seguridad digital, la protección de datos personales, la transparencia y la gestión documental, garantizando coherencia con el Modelo Integrado de Planeación y Gestión (MIPG) y con los instrumentos internos del Sistema Integrado de Gestión (SIG).

Marco normativo aplicable

- Decreto 612 de 2018, por el cual se establecen las directrices para la integración de los planes institucionales y estratégicos al Plan de Acción de las entidades del Estado.
- Decreto 338 de 2022, por el cual se modifican disposiciones relacionadas con la Política de Gobierno Digital.
- Decreto 1078 de 2015, Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones, y sus modificaciones.
- Documento CONPES 3854 de 2017, Política Nacional de Seguridad Digital.
- Ley 1581 de 2012, por la cual se dictan disposiciones generales para la protección de datos personales.
- Ley 1712 de 2014, Ley de Transparencia y del Derecho de Acceso a la Información Pública Nacional.
- Ley 594 de 2000, Ley General de Archivos.
- Decreto 2157 de 2017, por el cual se establecen directrices generales para la gestión del riesgo en las entidades públicas.
- Lineamientos vigentes de Gobierno Digital emitidos por el Ministerio de Tecnologías de la Información y las Comunicaciones.
- Lineamientos y guías del Modelo Integrado de Planeación y Gestión (MIPG).
- Tablas de Retención Documental (TRD) y procedimientos del Sistema Integrado de Gestión (SIG) de la entidad.

Marco técnico y de referencia

- ISO/IEC 27001:2022, Sistemas de Gestión de Seguridad de la Información.

- ISO/IEC 27005, Gestión de riesgos de seguridad de la información.
- ISO/IEC 27031, Directrices para la preparación de las tecnologías de la información y la comunicación para la continuidad del negocio.
- ISO 22301:2019, Sistemas de gestión de la continuidad del negocio.
- ISO 31000, Gestión del riesgo – Principios y directrices.
- Guía para la administración del riesgo y el diseño de controles en entidades públicas, versión vigente, del Departamento Administrativo de la Función Pública.

Guía del Modelo de Seguridad y Privacidad de la Información (MSPI) del Ministerio de Tecnologías de la Información y las Comunicaciones, versión vigente.

Las normas, lineamientos y estándares aquí relacionados se aplican de manera articulada, permitiendo que el tratamiento de los riesgos de seguridad y privacidad de la información se realice bajo criterios homogéneos, verificables y auditables, y se actualice de forma permanente ante cambios normativos, institucionales o tecnológicos.

5. Glosario de Términos y Acrónimos

Con el fin de unificar criterios, facilitar la comprensión del documento y evitar interpretaciones ambiguas, se definen a continuación los principales términos técnicos y acrónimos utilizados en el Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información de Empresas Públicas de Cundinamarca S.A. E.S.P.

Acrónimos

- EPC: Empresas Públicas de Cundinamarca S.A. E.S.P.
- TI: Tecnologías de la Información.
- MSPI: Modelo de Seguridad y Privacidad de la Información.
- PESI: Plan Estratégico de Seguridad y Privacidad de la Información.
- PETI: Plan Estratégico de Tecnologías de la Información.
- MIPG: Modelo Integrado de Planeación y Gestión.
- SIG: Sistema Integrado de Gestión.
- TRD: Tablas de Retención Documental.
- MDA: Mesa de Ayuda.

Términos técnicos

Activo de información: Información, datos o conjuntos de datos, en cualquier formato o soporte, que tienen valor para la entidad y cuya confidencialidad, integridad y disponibilidad deben ser protegidas.

Riesgo: Posibilidad de que una amenaza explote una vulnerabilidad y genere un impacto negativo sobre los activos de información y los objetivos institucionales.

Riesgo de seguridad y privacidad de la información: Riesgo asociado a la pérdida de confidencialidad, integridad, disponibilidad o autenticidad de la información institucional.

Tratamiento del riesgo: Proceso mediante el cual se definen e implementan acciones para modificar el nivel de riesgo, incluyendo su mitigación, aceptación, transferencia o eliminación.

Riesgo residual: Nivel de riesgo que permanece después de aplicar las acciones de tratamiento definidas.

Aceptación del riesgo: Decisión institucional mediante la cual se asume un riesgo residual, bajo criterios definidos, cuando su nivel se encuentra dentro de los rangos de tolerancia establecidos.

Incidente de seguridad de la información: Evento o conjunto de eventos no deseados que pueden comprometer la seguridad o privacidad de la información institucional.

Evidencia: Registro verificable que demuestra la ejecución de una acción, control o actividad definida en el Plan de Tratamiento.

Seguimiento y monitoreo: Actividades orientadas a verificar el estado, avance y efectividad de las acciones de tratamiento de riesgos.

Glosario MinTIC: https://www.mintic.gov.co/portal/inicio/Glosario/

6. Alcance del Plan

El Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información tiene como alcance la definición, ejecución y seguimiento de las acciones orientadas a tratar los riesgos que puedan afectar los activos de información, los servicios

tecnológicos y los procesos institucionales de Empresas Públicas de Cundinamarca S.A. E.S.P., en el marco de la vigencia 2026.

Alcance institucional: El presente plan aplica de manera transversal a toda la entidad, involucrando a la Gerencia General, las Subgerencias y las Direcciones vigentes, en concordancia con el principio de corresponsabilidad en la gestión del riesgo establecido por el Modelo Integrado de Planeación y Gestión (MIPG), cada dependencia es responsable de identificar, reportar y apoyar el tratamiento de los riesgos asociados a los activos de información bajo su custodia o administración.

Alcance por procesos: El plan cubre los riesgos de seguridad y privacidad de la información asociados a los procesos estratégicos, misionales, de apoyo y de evaluación de la entidad, conforme a la caracterización de procesos definida en el Sistema Integrado de Gestión (SIG), el Proceso de Tecnologías de la Información, adscrito a la Dirección de Planeación, actúa como facilitador y articulador del tratamiento de los riesgos, sin asumir de manera exclusiva la responsabilidad sobre los riesgos propios de cada proceso.

Alcance sobre activos de información y servicios TI, el plan aplica a:

- Los activos de información identificados y clasificados en el inventario institucional, independientemente de su formato (físico, digital o mixto).
- La infraestructura tecnológica, los sistemas de información, aplicaciones, plataformas y servicios TI que soportan la operación institucional.
- Los servicios tecnológicos provistos por terceros, en la medida en que estos soporten procesos o manejen información institucional, de acuerdo con las condiciones contractuales y los controles definidos.

Exclusiones y consideraciones:

- No sustituye ni reemplaza la gestión integral del riesgo institucional, sino que se articula como un componente especializado del MSPI.
- No desarrolla en detalle planes específicos como el Plan de Continuidad del Negocio o el Plan de Recuperación Tecnológica, los cuales se abordan en documentos independientes, aunque se coordina con ellos cuando los riesgos identificados así lo requieran.
- Se limita a la vigencia definida, sin perjuicio de que pueda ser ajustado o actualizado ante cambios relevantes en el contexto normativo, organizacional o tecnológico.

El alcance definido garantiza que el Plan de Tratamiento sea realista, aplicable y verificable, permitiendo su evaluación por parte de los órganos de control y su integración efectiva al modelo de gestión institucional.

7. Articulación

El Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información se articula de manera directa y obligatoria con el Modelo de Seguridad y Privacidad de la Información (MSPI) de Empresas Públicas de Cundinamarca S.A. E.S.P., constituyéndose como uno de sus instrumentos operativos para la gestión efectiva del riesgo.

El MSPI define los lineamientos, principios, roles y controles generales para la seguridad y privacidad de la información en la entidad, mientras que el presente plan operacionaliza dichos lineamientos mediante la identificación de riesgos específicos, la definición de acciones de tratamiento y el seguimiento a su implementación, asegurando coherencia metodológica y consistencia documental.

Relación del plan con los componentes del MSPI

El Plan de Tratamiento se integra con los componentes del MSPI de la siguiente manera:

- Gestión del riesgo: el plan materializa el componente de gestión del riesgo del MSPI, aplicando la metodología institucional para identificar, analizar, evaluar y tratar los riesgos de seguridad y privacidad de la información.
- Controles de seguridad: las acciones de tratamiento definidas se alinean con los controles establecidos en el MSPI y con las buenas prácticas de los estándares adoptados por la entidad, evitando la definición de controles aislados o no armonizados.
- Gobierno y mejora continua: el seguimiento y evaluación del plan alimentan los procesos de mejora continua del MSPI, permitiendo ajustar controles, priorizar acciones y fortalecer la madurez del modelo.
- Conciencia y corresponsabilidad: el plan promueve la participación activa de las dependencias institucionales en la gestión del riesgo, en coherencia con los roles y responsabilidades definidos en el MSPI, fortaleciendo la cultura de seguridad y privacidad de la información.

Articulación con otros instrumentos de gestión TI

El Plan de Tratamiento se articula, además, con los siguientes instrumentos institucionales:

- El Plan Estratégico de Seguridad y Privacidad de la Información (PESI), del cual deriva como instrumento de ejecución anual.
- El Plan Estratégico de Tecnologías de la Información (PETI), garantizando que las acciones de tratamiento sean coherentes con la planeación TI.
- El Sistema Integrado de Gestión (SIG), en lo relacionado con gestión del riesgo, control interno y mejora continua.

Esta articulación garantiza que el tratamiento de los riesgos de seguridad y privacidad de la información no se gestione de manera fragmentada, sino como parte integral del sistema de gobierno, planeación y control de la entidad, facilitando la trazabilidad, la generación de evidencias y la rendición de cuentas ante los órganos de control.

8. Roles y Responsabilidades

El tratamiento de los riesgos de Seguridad y Privacidad de la Información en Empresas Públicas de Cundinamarca S.A. E.S.P. se fundamenta en el principio de corresponsabilidad institucional, en el cual cada dependencia participa de acuerdo con sus funciones, competencias y nivel de exposición al riesgo, en coherencia con el Modelo de Seguridad y Privacidad de la Información (MSPI) y el Modelo Integrado de Planeación y Gestión (MIPG).

Los roles y responsabilidades definidos a continuación se circunscriben exclusivamente al tratamiento de los riesgos de seguridad y privacidad de la información y no sustituyen ni duplican las funciones establecidas en otros instrumentos institucionales.

Gerencia General

- Orientar las decisiones estratégicas relacionadas con la gestión del riesgo de seguridad y privacidad de la información.
- Garantizar el respaldo institucional para la ejecución de las acciones de tratamiento priorizadas.

Dirección de Planeación

- Articular el Plan de Tratamiento con los instrumentos de planeación institucional.
- Garantizar la coherencia del plan con el MIPG, el SIG y los planes estratégicos vigentes.

- Consolidar y hacer seguimiento a los resultados del tratamiento de riesgos en el marco de la gestión institucional.
- Aprobar, cuando aplique, la aceptación de riesgos residuales que superen los niveles de tolerancia definidos institucionalmente.

Proceso de Tecnologías de la Información: Adscrito a la Dirección de Planeación, es responsable de coordinar técnica y metodológicamente el tratamiento de los riesgos de seguridad y privacidad de la información.

Coordinador de Tecnologías de la Información

- Liderar la formulación, actualización y ejecución del Plan de Tratamiento de Riesgos.
- Coordinar la identificación, análisis y priorización de los riesgos de seguridad y privacidad de la información.
- Definir, en articulación con las dependencias responsables, las acciones de tratamiento, responsables, plazos y entregables.
- Realizar el seguimiento técnico a la ejecución de las acciones de tratamiento.
- Presentar los resultados del seguimiento a la Dirección de Planeación y a las instancias que correspondan.
- Coordinar la gestión de riesgos relacionados con infraestructura, servicios tecnológicos y proveedores TIC.
- Articular el tratamiento de riesgos con los planes de continuidad y recuperación tecnológica, cuando aplique.

Mesa de Ayuda (MDA)

- Ejecutar las acciones técnicas de tratamiento de riesgos que le sean asignadas.
- Registrar incidentes, eventos, cambios y evidencias relacionadas con la seguridad y privacidad de la información.
- Apoyar la implementación de controles técnicos y operativos definidos en el plan.
- Suministrar información y soportes para el seguimiento y la auditoría del plan.

Dependencias responsables de procesos

- Identificar y reportar los riesgos de seguridad y privacidad de la información asociados a sus procesos y activos de información.
- Participar en la definición de acciones de tratamiento y en la priorización de riesgos.

- Ejecutar las acciones de tratamiento que les correspondan y suministrar las evidencias requeridas.
- Informar oportunamente sobre cambios en los procesos que puedan afectar el nivel de riesgo.

Dirección de Control Interno

- Verificar la adecuada implementación y seguimiento del Plan de Tratamiento.
- Evaluar la efectividad de las acciones de tratamiento desde la perspectiva de control interno.
- Formular recomendaciones de mejora, sin asumir funciones de ejecución.

La definición clara de roles y responsabilidades permite asegurar que el tratamiento de los riesgos de seguridad y privacidad de la información se realice de manera coordinada, controlada y verificable, evitando vacíos de responsabilidad y fortaleciendo el sistema de control institucional.

9. Metodología

La metodología para el tratamiento de los riesgos de Seguridad y Privacidad de la Información adoptada por Empresas Públicas de Cundinamarca S.A. E.S.P. se fundamenta en el enfoque de gestión integral del riesgo, en coherencia con el Modelo Integrado de Planeación y Gestión (MIPG), la Guía para la Administración del Riesgo y el Diseño de Controles en Entidades Públicas del Departamento Administrativo de la Función Pública, y las buenas prácticas establecidas en los estándares ISO 31000 e ISO/IEC 27005.

Esta metodología se aplica de manera sistemática y documentada, garantizando la trazabilidad de las decisiones adoptadas y la generación de evidencias verificables para efectos de seguimiento, control interno y auditoría.

1 Enfoque metodológico, el tratamiento de riesgos se desarrolla bajo un enfoque preventivo y basado en riesgo, que considera:

- El contexto institucional, estratégico y operativo de la entidad.
- La criticidad de los activos de información y de los servicios tecnológicos.
- El impacto potencial sobre los objetivos institucionales.
- La probabilidad de ocurrencia de eventos que afecten la seguridad y privacidad de la información.

Las acciones de tratamiento se definen priorizando los riesgos con mayor nivel de exposición, de acuerdo con los criterios de evaluación establecidos institucionalmente.

2 Etapas de la metodología, la metodología comprende las siguientes etapas:

Análisis de la información: Consiste en la revisión y análisis de la información suministrada por los procesos, incluyendo:

- Identificación de activos de información.
- Identificación de amenazas y vulnerabilidades.
- Revisión de riesgos previamente identificados.
- Actualización de la valoración del riesgo, cuando aplique.

Evaluación del riesgo: En esta etapa se determina el nivel de riesgo, considerando la probabilidad y el impacto, y se establece su priorización conforme a los criterios institucionales definidos en el marco del MIPG y del MSPI.

Definición de acciones de tratamiento: Para cada riesgo priorizado se definen acciones de tratamiento, las cuales pueden incluir:

- Evitar el riesgo.
- Reducir el riesgo mediante la implementación o fortalecimiento de controles.
- Compartir el riesgo, cuando aplique.
- Aceptar el riesgo residual, bajo los criterios institucionales establecidos.

Cada acción de tratamiento debe contar con un responsable, un plazo de ejecución y un entregable claramente definido.

Implementación del tratamiento: Las acciones definidas son ejecutadas por los responsables designados, con el acompañamiento técnico del Proceso de Tecnologías de la Información, cuando corresponda, y con el registro de las evidencias que soporten su ejecución.

Seguimiento y revisión: Se realiza el seguimiento periódico al estado de las acciones de tratamiento, verificando su avance y efectividad, y ajustando el plan cuando se presenten cambios en el contexto institucional, tecnológico o normativo.

3 Criterios para la aceptación del riesgo residual: Cuando, luego de la aplicación de las acciones de tratamiento, persista un nivel de riesgo residual, este será evaluado conforme a los criterios institucionales de tolerancia al riesgo. La Dirección de

Planeación es la responsable de aprobar la aceptación del riesgo residual, cuando aplique, dejando constancia documentada de la decisión y de las condiciones bajo las cuales se acepta el riesgo, la aceptación del riesgo residual no exime a la entidad de realizar seguimiento continuo ni de implementar acciones de mejora cuando el contexto así lo requiera.

10. Plan de Tratamiento de Riesgos

El Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información establece el conjunto de acciones definidas para reducir, controlar o gestionar los riesgos identificados, en coherencia con la metodología institucional y los lineamientos del Modelo de Seguridad y Privacidad de la Información (MSPI).

Este plan se formula a partir de la matriz de riesgos de seguridad y privacidad de la información, priorizando aquellos riesgos cuyo nivel de exposición pueda afectar de manera significativa el cumplimiento de los objetivos institucionales y la prestación de los servicios a cargo de la entidad.

1 Resumen de Riesgos Prioritarios y Acciones de Tratamiento

El presente apartado consolida los riesgos prioritarios de seguridad y privacidad de la información identificados por la entidad, considerando el análisis institucional realizado, los insumos del PETI, el MSPI, los ejercicios de seguimiento previos y las observaciones derivadas de auditorías y procesos de control.

Este resumen tiene como finalidad:

- Facilitar la toma de decisiones por parte de la alta dirección.
- Evidenciar la coherencia entre los riesgos críticos y las acciones definidas.
- Permitir el seguimiento ejecutivo al tratamiento de los riesgos más relevantes.

La matriz completa de riesgos se gestiona como un documento técnico y se referencia como insumo del presente plan.

ID	Riesgo prioritario	Descripción del riesgo	Acción de tratamiento principal	Responsable

1	Gestión incompleta de activos de información	Inconsistencias en la identificación, clasificación y responsable de los activos de información institucionales	Actualizar y validar el inventario de activos de información, articulado con procesos y responsables	Coordinador TIC
2	Debilidades en el registro y gestión de incidentes	Incidentes de seguridad no registrados oportunamente o sin trazabilidad completa	Fortalecer el registro, análisis y seguimiento de incidentes a través de la Mesa de Ayuda	Coordinador TIC / MDA
3	Falta de seguimiento estructurado a acciones de tratamiento	Acciones de tratamiento sin evidencia clara de ejecución o cierre	Implementar esquema de seguimiento y monitoreo periódico con evidencias verificables	Coordinador TIC
4	Dependencia de conocimiento operativo no documentado	Riesgo de indisponibilidad o pérdida de información por ausencia de documentación técnica	Documentar procedimientos clave y respaldar la operación TI	Coordinador TIC
5	Debilidades en la generación y custodia de evidencias	Evidencias dispersas o no alineadas con TRD y SIG	Definir tipos de evidencia, responsables de generación y custodia	Coordinador TIC
6	Riesgos asociados a cambios tecnológicos no controlados	Implementación de cambios sin análisis de impacto en seguridad y privacidad	Articular la gestión de cambios con el tratamiento de riesgos y el MSPI	Coordinador TIC

2 Estructura del Plan de Tratamiento

El Plan de Tratamiento se documenta y gestiona mediante una matriz que, como mínimo, contempla los siguientes elementos:

- Identificación del riesgo.
- Proceso y activo de información asociado.
- Nivel de riesgo inicial.
- Tipo de tratamiento definido (evitar, reducir, compartir o aceptar).
- Acción(es) de tratamiento.
- Responsable de la acción.
- Fecha de inicio y fecha de finalización.
- Entregables y evidencias asociadas.
- Nivel de riesgo residual esperado.

Esta estructura permite asegurar la trazabilidad entre el riesgo identificado, la acción definida y el resultado esperado, facilitando el seguimiento y la evaluación de la efectividad del tratamiento.

3 Definición de acciones de tratamiento

Las acciones de tratamiento se definen considerando, entre otros aspectos:

- La criticidad del activo de información.
- La viabilidad técnica, operativa y financiera de la acción.
- El impacto sobre los procesos institucionales.
- La articulación con controles existentes en el MSPI, el PESI y el SIG.

Las acciones pueden corresponder a la implementación de controles técnicos, administrativos u operativos, así como al fortalecimiento de procedimientos, capacidades o prácticas institucionales.

4 Responsables y plazos: Cada acción de tratamiento cuenta con un responsable claramente identificado, perteneciente al proceso o dependencia que gestiona el riesgo, con el acompañamiento del Proceso de Tecnologías de la Información, cuando aplique, los plazos de ejecución se definen de acuerdo con la prioridad del riesgo y la capacidad institucional, garantizando su cumplimiento dentro de la vigencia del plan.

5 Articulación con otros planes y proyectos: El Plan de Tratamiento se articula con otros planes y proyectos institucionales, tales como el Plan Estratégico de Tecnologías de la Información, el Plan Estratégico de Seguridad y Privacidad de la

Información, los planes de continuidad y recuperación, y los planes de mejoramiento derivados de auditorías, con el fin de evitar duplicidades y optimizar el uso de los recursos disponibles.

El Plan de Tratamiento de Riesgos constituye un instrumento dinámico, susceptible de actualización cuando se presenten cambios relevantes en los riesgos, en el contexto institucional o en el entorno tecnológico.

11. Gestión de Riesgos Residuales y Aceptación del Riesgo

La gestión de los riesgos residuales forma parte integral del Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información y permite a Empresas Públicas de Cundinamarca S.A. E.S.P. tomar decisiones informadas y documentadas frente a aquellos riesgos que, aun después de aplicar las acciones de tratamiento definidas, mantienen un nivel de exposición residual.

1 Definición de riesgo residual

Se entiende por riesgo residual el nivel de riesgo que permanece una vez implementadas y verificadas las acciones de tratamiento establecidas en el plan, este riesgo puede persistir debido a limitaciones técnicas, operativas, presupuestales o por la naturaleza misma del proceso o del activo de información.

La existencia de un riesgo residual no implica una falla en la gestión del riesgo, sino la necesidad de evaluar su aceptación o la definición de acciones adicionales de mejora.

2 Criterios para la gestión del riesgo residual

La gestión de los riesgos residuales se realiza considerando, como mínimo, los siguientes criterios:

- Nivel de riesgo residual resultante frente a los umbrales de tolerancia definidos institucionalmente.
- Impacto potencial sobre los objetivos estratégicos, misionales y de apoyo de la entidad.
- Capacidad institucional para implementar controles adicionales.
- Relación costo–beneficio de nuevas acciones de tratamiento.
- Articulación con otros riesgos institucionales y planes de mejoramiento.

Estos criterios permiten priorizar la atención de los riesgos residuales y asegurar decisiones coherentes con el contexto institucional y el enfoque del MIPG.

3 Aceptación del riesgo residual

Cuando el riesgo residual se ubica dentro de los niveles de tolerancia definidos institucionalmente, o cuando no es viable técnica u operativamente implementar acciones adicionales de tratamiento, la Dirección de Planeación es la instancia responsable de evaluar y aprobar la aceptación del riesgo residual, dejando constancia documentada de dicha decisión.

La aceptación del riesgo residual debe:

- Estar debidamente justificada.
- Contar con el análisis de impacto correspondiente.
- Identificar las condiciones bajo las cuales se acepta el riesgo.
- Definir, cuando aplique, medidas de seguimiento o mitigación complementarias.

4 Seguimiento a los riesgos residuales

Los riesgos residuales aceptados son objeto de seguimiento periódico, con el fin de verificar que las condiciones bajo las cuales fueron aceptados se mantienen y que no se presentan cambios en el contexto que incrementen su nivel de exposición.

En caso de presentarse variaciones significativas en el riesgo residual, este deberá ser reevaluado y, de ser necesario, incorporado nuevamente al Plan de Tratamiento para la definición de nuevas acciones.

La gestión adecuada de los riesgos residuales contribuye a una administración responsable del riesgo y fortalece la toma de decisiones basada en evidencia dentro de la entidad.

12. Seguimiento, Control y Monitoreo

El seguimiento, control y monitoreo del Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información tiene como propósito verificar el cumplimiento, la oportunidad y la efectividad de las acciones definidas, así como identificar de manera temprana desviaciones, brechas o necesidades de ajuste, en coherencia con el Modelo Integrado de Planeación y Gestión (MIPG) y el Sistema Integrado de Gestión (SIG).

1 Seguimiento a las acciones de tratamiento

El seguimiento a las acciones de tratamiento se realiza de forma trimestral, con base en los plazos, responsables y entregables definidos en la matriz del plan. Este seguimiento permite:

- Verificar el estado de avance de cada acción.
- Validar la ejecución de los controles definidos.
- Identificar retrasos, incumplimientos o dificultades en la implementación.
- Solicitar ajustes cuando se presenten cambios en el contexto institucional o tecnológico.

El Proceso de Tecnologías de la Información, adscrito a la Dirección de Planeación, consolida la información del seguimiento y apoya técnicamente la validación de los avances reportados por las dependencias responsables.

2 Control y verificación

El control del Plan de Tratamiento se orienta a verificar que las acciones implementadas correspondan efectivamente a los riesgos identificados y que contribuyan a la reducción del nivel de riesgo. Para ello se tienen en cuenta, entre otros, los siguientes aspectos:

- Coherencia entre el riesgo, la acción de tratamiento y el entregable definido.
- Existencia y calidad de las evidencias generadas.
- Alineación con los controles establecidos en el MSPI y el PESI.
- Cumplimiento de los procedimientos definidos en el SIG.

La Dirección de Control Interno ejerce labores de verificación y evaluación independiente sobre la ejecución y efectividad del plan, formulando observaciones y recomendaciones de mejora, sin asumir funciones operativas.

3 Monitoreo y actualización del plan

El monitoreo del Plan de Tratamiento permite evaluar su vigencia y pertinencia frente a cambios en:

- El contexto normativo.
- La estructura organizacional.
- Los procesos institucionales.
- La infraestructura tecnológica y los servicios TI.

- El perfil de riesgo de la entidad.

Cuando se identifiquen cambios relevantes, el plan podrá ser ajustado o actualizado, garantizando la debida trazabilidad y la aprobación correspondiente, de acuerdo con los lineamientos institucionales de planeación y control.

El seguimiento y monitoreo sistemático del Plan de Tratamiento es realizado de forma trimestral por la Dirección de Planeación, fortaleciendo la gestión del riesgo, facilitando la rendición de cuentas y aportando insumos para la mejora continua del Modelo de Seguridad y Privacidad de la Información.

13. Recursos

La ejecución del Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información se realizará utilizando los recursos humanos, técnicos y administrativos existentes en Empresas Públicas de Cundinamarca S.A. E.S.P., en coherencia con el principio de eficiencia en el uso de los recursos públicos y con la planeación institucional vigente.

1 Recursos humanos: Las acciones de tratamiento de riesgos serán desarrolladas por los servidores y contratistas que integran las dependencias responsables de los procesos y activos de información, con el acompañamiento y coordinación del Proceso de Tecnologías de la Información, adscrito a la Dirección de Planeación.

En particular:

- El Coordinador de Tecnologías de la Información lidera y articula la ejecución del plan desde el punto de vista técnico y metodológico.
- La Mesa de Ayuda (MDA) ejecuta las acciones técnicas y operativas que le sean asignadas.
- Las demás dependencias aportan los recursos humanos necesarios para la ejecución de las acciones bajo su responsabilidad.

2 Recursos técnicos: Para la implementación de las acciones de tratamiento se utilizarán los recursos tecnológicos institucionales disponibles, tales como infraestructura, sistemas de información, herramientas de soporte y mecanismos de control existentes, de acuerdo con el nivel de madurez tecnológica de la entidad y sin comprometer la operación normal de los servicios, no se contempla la incorporación de plataformas o herramientas no existentes, salvo que estas se encuentren debidamente justificadas y articuladas con los instrumentos de planeación y contratación institucional.

3 Recursos financieros: La ejecución del Plan de Tratamiento no implica, de manera general, la asignación de recursos financieros adicionales a los ya previstos en la planeación institucional. En caso de requerirse recursos específicos para la implementación de acciones de tratamiento, estos deberán ser gestionados a través de los mecanismos institucionales correspondientes y priorizados conforme al nivel de riesgo identificado.

La definición de los recursos garantiza que el Plan de Tratamiento sea realista, viable y sostenible, y que su ejecución pueda ser evaluada y auditada conforme a los principios de la gestión pública.

14. Medición y Mejora Continua

La medición y la mejora continua del Modelo de Seguridad y Privacidad de la Información constituyen un componente esencial para evaluar la efectividad del Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información y asegurar su alineación permanente con los objetivos institucionales de Empresas Públicas de Cundinamarca S.A. E.S.P.

1 Indicadores, Metas Cuantitativas y Responsables de Reporte

Con el fin de medir la efectividad del Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información, se definen indicadores cuantitativos que permiten evaluar el avance, cumplimiento y resultado de las acciones de tratamiento, en coherencia con el Modelo Integrado de Planeación y Gestión (MIPG), el MSPI y los lineamientos de Gobierno Digital.

Los indicadores establecidos son realistas, medibles y auditables, y se alinean con el nivel de madurez actual de la entidad.

ID	Indicador	Descripción	Fórmula de medición	Meta	Periodicidad	Responsable de reporte
1	Ejecución de acciones de tratamiento	Mide el porcentaje de acciones de tratamiento ejecutadas	(Acciones ejecutadas / Acciones programadas) × 100	≥ 90 %	Trimestral	Coordinador TIC

		frente a las programadas				
2	Registro de incidentes de seguridad	Mide el porcentaje de incidentes de seguridad y privacidad registrados frente a los incidentes identificados	(Incidentes registrados / Incidentes identificados) × 100	100%	Permanente	Mesa de Ayuda (MDA)
3	Acciones con evidencia válida	Mide el porcentaje de acciones que cuentan con evidencia verificable conforme a TRD y SIG	(Acciones con evidencia / Acciones ejecutadas) × 100	≥ 85 %	Trimestral	Coordinador TIC
4	Seguimiento a riesgos prioritarios	Mide el porcentaje de riesgos prioritarios con seguimiento documentado	(Riesgos con seguimiento / Riesgos prioritarios) × 100	100%	Trimestral	Coordinador TIC
5	Oportunidad en el cierre de acciones	Mide el porcentaje de acciones cerradas dentro del plazo definido	(Acciones cerradas a tiempo / Acciones cerradas) × 100	≥ 80 %	Semestral	Coordinador TIC

2 Lecciones Aprendidas de Ciclos Anteriores y Auditorías

El análisis de los ciclos anteriores de planeación, seguimiento y auditoría relacionados con la gestión de la seguridad y privacidad de la información, permitió identificar un conjunto de lecciones aprendidas que sirven como insumo para el fortalecimiento del Plan de Tratamiento de Riesgos.

Las lecciones aprendidas aquí consignadas se derivan de:

- Seguimientos institucionales previos.
- Ejercicios de control interno.
- Observaciones recurrentes en procesos de auditoría.
- Insumos considerados en la actualización del PETI y del MSPI.

Lecciones aprendidas identificadas

- Necesidad de mayor consistencia en la identificación de activos de información: Se evidenció la importancia de mantener actualizado y alineado el inventario de activos de información con los procesos institucionales y los responsables definidos, para evitar inconsistencias en la gestión del riesgo.
- Fortalecimiento del registro y trazabilidad de incidentes: La falta de registros oportunos y completos de incidentes limitó el análisis de causas y la toma de acciones correctivas, lo que resalta la necesidad de un registro sistemático y centralizado.
- Importancia del seguimiento documentado a las acciones de tratamiento: Se identificaron acciones ejecutadas sin evidencia suficiente, lo que afectó su validación en auditorías, destacando la necesidad de fortalecer el seguimiento y la gestión de evidencias.
- Relevancia de la articulación entre planeación y operación: La gestión del riesgo requiere una coordinación permanente entre el Proceso de Tecnologías de la Información, la Dirección de Planeación y las dependencias responsables de los procesos, evitando enfoques aislados.
- Necesidad de formalizar criterios para la aceptación del riesgo residual: La ausencia de criterios documentados para la aceptación del riesgo residual generó observaciones, lo que motivó su formalización en el presente plan.

Aplicación de las lecciones aprendidas en la vigencia: Las lecciones aprendidas identificadas se reflejan en la vigencia mediante:

- El fortalecimiento del Plan de Tratamiento de Riesgos y su alineación con el MSPI.
- La definición de indicadores con metas cuantitativas y responsables claros.
- La formalización de los criterios de aceptación del riesgo residual.

- La incorporación de lineamientos claros sobre evidencias y custodia documental.

3 Medición del tratamiento de riesgos: La medición se orienta a verificar el grado de cumplimiento y efectividad de las acciones de tratamiento definidas, mediante indicadores que permitan evaluar, entre otros aspectos:

- Nivel de avance en la ejecución de las acciones de tratamiento.
- Reducción del nivel de riesgo frente a la línea base.
- Cumplimiento de plazos y responsables definidos.
- Calidad y suficiencia de las evidencias generadas.

Los indicadores utilizados se articulan con los definidos en el MSPI, el PESI y el SIG, evitando la duplicación de mediciones y garantizando coherencia con los requerimientos de seguimiento institucional y de reporte a instancias de control.

4 Fuentes de información para la medición: La información para la medición del plan se obtiene, entre otras, de las siguientes fuentes:

- Matriz de riesgos de seguridad y privacidad de la información.
- Informes de seguimiento al Plan de Tratamiento.
- Registros de incidentes y eventos de seguridad.
- Resultados de auditorías internas y externas.
- Informes de Control Interno y evaluaciones del MIPG.

Estas fuentes permiten contar con información objetiva y verificable para la toma de decisiones y la rendición de cuentas.

5 Mejora continua: Los resultados de la medición constituyen insumo para la mejora continua del Modelo de Seguridad y Privacidad de la Información, permitiendo:

- Ajustar o redefinir acciones de tratamiento.
- Fortalecer controles existentes.
- Priorizar nuevos riesgos o escenarios emergentes.
- Formular planes de mejoramiento cuando se identifiquen brechas o debilidades.

La mejora continua se desarrolla en el marco del ciclo Planear – Hacer – Verificar – Actuar (PHVA), en coherencia con el Sistema Integrado de Gestión y los estándares adoptados por la entidad.

La aplicación sistemática de la medición y la mejora continua contribuye al fortalecimiento progresivo de la madurez institucional en materia de seguridad y privacidad de la información.

15. Gestión Documental, Evidencias y Conservación de Registros

La gestión documental asociada al Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información garantiza la trazabilidad, disponibilidad, integridad y conservación de la información y de las evidencias generadas durante su formulación, ejecución y seguimiento, en cumplimiento de la Ley 594 de 2000, las Tablas de Retención Documental (TRD) y los procedimientos del Sistema Integrado de Gestión (SIG) de Empresas Públicas de Cundinamarca S.A. E.S.P.

1 Tipos de Evidencia, Responsable de Generación y Custodia

Con el propósito de garantizar la trazabilidad, verificabilidad y disponibilidad de la información asociada a la ejecución del Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información, se definen los tipos de evidencia requeridos, así como los responsables de su generación y custodia, en coherencia con el Sistema Integrado de Gestión (SIG) de Empresas Públicas de Cundinamarca S.A. E.S.P.

Las evidencias aquí definidas permiten demostrar de manera objetiva el cumplimiento de las acciones de tratamiento, el seguimiento realizado y la toma de decisiones asociadas al riesgo.

ID	Tipo de evidencia	Descripción	Responsable de generación
1	Matriz de riesgos de seguridad y privacidad de la información	Documento que consolida los riesgos identificados, su valoración y acciones de tratamiento	Coordinador TIC
2	Plan de Tratamiento de Riesgos	Documento aprobado que define las acciones, responsables y plazos	Coordinador TIC
3	Registros de incidentes de seguridad	Registros de incidentes, eventos y acciones correctivas asociadas	Mesa de Ayuda (MDA)

4	Informes de seguimiento y monitoreo	Reportes periódicos sobre el avance y estado de las acciones de tratamiento	Coordinador TIC
5	Evidencias de ejecución de acciones	Soportes que demuestran la implementación de las acciones de tratamiento (actas, registros, configuraciones, procedimientos)	Dependencias responsables / Coordinador TIC
6	Evidencias de socialización	Correos, actas o comunicaciones que acreditan la socialización del documento	Coordinador TIC
7	Evidencias de aceptación del riesgo residual	Registros documentados de la decisión de aceptación del riesgo residual	Coordinador TIC

2 Gestión y custodia documental: Los documentos y registros derivados del Plan de Tratamiento serán gestionados conforme a los lineamientos institucionales de gestión documental, asegurando:

- Clasificación y organización de la información según las TRD vigentes.
- Custodia por parte de las dependencias responsables del proceso o actividad.
- Acceso controlado a la información, de acuerdo con los niveles de confidencialidad definidos.
- Disponibilidad oportuna para fines de seguimiento, control interno, auditoría y rendición de cuentas.

El Proceso de Tecnologías de la Información, en articulación con la Dirección de Planeación, apoyará la correcta gestión de los registros técnicos asociados al tratamiento de riesgos.

3 Evidencias del Plan de Tratamiento

Constituyen evidencias del Plan de Tratamiento, entre otras:

- Matriz de riesgos de seguridad y privacidad de la información.
- Planes y matrices de tratamiento de riesgos.
- Informes de seguimiento y monitoreo.

- Actas, comunicaciones y soportes de aprobación cuando aplique.
- Registros de incidentes, eventos y acciones correctivas.
- Resultados de auditorías y evaluaciones internas o externas.

Las evidencias deberán ser completas, verificables y consistentes con las acciones reportadas, permitiendo demostrar la correcta ejecución del plan ante los órganos de control.

4 Conservación y disposición final: La conservación y disposición final de los documentos y registros asociados al Plan de Tratamiento se realizará conforme a los tiempos y criterios establecidos en las TRD institucionales, garantizando el cumplimiento de la normativa archivística y la preservación de la memoria institucional.

La adecuada gestión documental y de evidencias fortalece la transparencia, la rendición de cuentas y la capacidad de la entidad para atender requerimientos de control y auditoría.

16. Matriz de Roles y Responsabilidades

Con el fin de fortalecer la claridad organizacional, la trazabilidad y la rendición de cuentas en la ejecución del Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información, se establece la siguiente matriz de roles y responsabilidades, en coherencia con el Modelo Integrado de Planeación y Gestión (MIPG), el Modelo de Seguridad y Privacidad de la Información (MSPI) y la estructura organizacional vigente de Empresas Públicas de Cundinamarca S.A. E.S.P.

La presente matriz no crea cargos ni instancias adicionales, sino que consolida las responsabilidades asociadas al tratamiento de riesgos de seguridad y privacidad de la información.

ID	Rol / Dependencia	Responsabilidades en el Plan de Tratamiento
1	Dirección de Planeación	Aprobar la aceptación del riesgo residual; articular el Plan de Tratamiento con la planeación institucional y el MIPG; custodiar documentos estratégicos asociados al tratamiento de riesgos.

2	Coordinador de Tecnologías de la Información	Liderar la formulación, actualización y ejecución del Plan de Tratamiento; coordinar la identificación y tratamiento de riesgos; realizar seguimiento y reporte de indicadores; generar y consolidar evidencias.
3	Proceso de Tecnologías de la Información	Apoyar la implementación de controles técnicos y administrativos; gestionar evidencias técnicas; articular la operación TI con el tratamiento de riesgos.
4	Mesa de Ayuda (MDA)	Registrar y gestionar incidentes de seguridad y privacidad de la información; apoyar la ejecución de acciones técnicas; suministrar evidencias operativas.
5	Dependencias responsables de procesos	Identificar riesgos asociados a sus procesos y activos de información; ejecutar acciones de tratamiento asignadas; generar evidencias y apoyar el seguimiento.
6	Dirección de Control Interno	Verificar la implementación y efectividad del Plan de Tratamiento; realizar evaluaciones independientes; formular recomendaciones de mejora.

17. Mecanismos de seguimiento, revisión y actualización

El Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información contará con mecanismos formales de seguimiento, revisión y actualización, orientados a garantizar su vigencia, efectividad y alineación con la planeación institucional.

1 Seguimiento: El seguimiento al Plan se realizará de manera sistemática, con el propósito de verificar el avance y cumplimiento de las acciones de tratamiento definidas, así como la efectividad de los controles implementados.

- El seguimiento será liderado por el Coordinador de Tecnologías de la Información.
- Se realizará con base en los indicadores definidos, los informes de avance y las evidencias documentadas.
- Los resultados del seguimiento servirán como insumo para la toma de decisiones, la gestión de riesgos residuales y los procesos de control interno.

2 Revisión: El Plan será objeto de revisión periódica con el fin de evaluar su pertinencia y coherencia frente al contexto institucional.

La revisión se realizará:

- De manera anual, en el marco del ciclo de planeación institucional.
- Cuando se presenten cambios normativos, organizacionales o tecnológicos relevantes.
- Como resultado de auditorías, evaluaciones de control interno o incidentes significativos de seguridad y privacidad de la información.

La revisión podrá generar recomendaciones de ajuste, las cuales serán documentadas y evaluadas para su incorporación.

3 Actualización: La actualización del Plan se efectuará cuando los resultados del seguimiento o la revisión así lo requieran.

- Las actualizaciones serán coordinadas por el Coordinador de Tecnologías de la Información, en articulación con la Dirección de Planeación.
- Toda actualización deberá quedar registrada en el Control de Cambios, garantizando la trazabilidad documental.
- Las versiones actualizadas serán socializadas con las dependencias con injerencia, conforme a los lineamientos institucionales.

18. Documentos relacionados

El Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información se articula con los siguientes documentos institucionales, los cuales constituyen insumos, referentes o instrumentos complementarios para su formulación, ejecución, seguimiento y mejora continua.

La relación de estos documentos evita duplicidades, garantiza coherencia institucional y facilita los procesos de control y auditoría.

Documentos estratégicos y de planeación

- Plan Estratégico de Tecnologías de la Información (PETI).
- Plan Estratégico de Seguridad y Privacidad de la Información (PESI).
- Modelo de Seguridad y Privacidad de la Información (MSPI).
- Plan de Acción institucional (cuando aplique).

- Instrumentos de planeación asociados al MIPG.

Documentos de gestión del riesgo y control
- Matriz de riesgos de seguridad y privacidad de la información.
- Informes de seguimiento y monitoreo del Plan de Tratamiento.
- Informes de Control Interno y auditorías relacionadas.
- Registros de incidentes de seguridad y privacidad de la información.

Documentos del Sistema Integrado de Gestión
- Procedimientos del Proceso de Tecnologías de la Información.
- Lineamientos de Gestión Documental.
- Registros y formatos definidos en el SIG para seguimiento y control.

Otros documentos relacionados
- Normativa y lineamientos de Gobierno Digital.
- Políticas y directrices internas aplicables a la seguridad y privacidad de la información.

19. Disposiciones finales

El Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información de Empresas Públicas de Cundinamarca S.A. E.S.P. constituye un instrumento institucional de carácter obligatorio, orientado a la gestión sistemática de los riesgos que puedan afectar la confidencialidad, integridad y disponibilidad de la información.

Vigencia: El presente Plan rige a partir de su aprobación y adopción institucional y tendrá vigencia para la anualidad correspondiente, sin perjuicio de las revisiones y actualizaciones que se realicen conforme a lo establecido.

Obligatoriedad: Las disposiciones contenidas en el Plan son de obligatorio cumplimiento para las dependencias y servidores que participen en la gestión, tratamiento y uso de la información institucional, en el marco de sus funciones y responsabilidades.

Aplicación institucional: La aplicación del Plan se realizará de manera articulada con:
- El Modelo Integrado de Planeación y Gestión (MIPG).
- Los procesos y procedimientos definidos en el Sistema Integrado de Gestión (SIG).

Difusión: El Plan será socializado con las dependencias con injerencia institucional y estará disponible en los repositorios definidos por la entidad, conforme a los lineamientos de gestión documental y transparencia aplicables.

Casos no previstos: Los aspectos no contemplados expresamente en el presente Plan serán resueltos conforme a la normatividad vigente y los lineamientos institucionales, dejando la correspondiente trazabilidad documental.

20. Control de Cambios

CONTROL DE CAMBIOS				
VERSIÓN	**FECHA**	**DESCRIPCIÓN DEL CAMBIO**	**RESPONSABLE**	**CARGO**
0	28/01/2026	Versión inicial	Diego Ernesto Guevara	Director de Planeación

PROYECTÓ	**REVISÓ**	**APROBÓ**
Nombre: Héctor Gil	Nombre: Carlos Garavito	Nombre: Diego Guevara
Cargo: Coordinador TI – Planeación	Cargo: Contratista-Planeación	Cargo: Director de Planeación
Dirección: Planeación	Subgerencia y/o Dirección: Planeación	Dirección: Planeación
Fecha: 28/01/2026	Fecha: 28/01/2026	Fecha: 28/01/2026

PLAN DE TRABAJO
Plan de tratamiento de riesgos de seguridad y privacidad de la información

OBJETIVO	Validar, ajustar y formalizar el Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información – Vigencia 2026, garantizando su coherencia institucional.
JUSTIFICACIÓN	El Plan de Mejoramiento se formula en cumplimiento del Decreto 612 de 2018 y del Modelo Integrado de Planeación y Gestión (MIPG), con el fin de consolidar un documento técnico que requiere validación interdependencial, ajustes de forma y control documental, y formalización institucional para su correcta aplicación, seguimiento y evaluación por parte de Control Interno y demás instancias de control.
LIDER	Coordinador TIC
EQUIPO	Dirección de Planeación

Item	Acción	Responsable	Producto	Fecha inicio	Fecha Fin	DIAS PARA EL CUMPLIMIENTO (28/1/2026)
1	Alistamiento normativo, metodológico y documental	Coordinador TIC	Insumos normativos y diagnóstico documental	1/02/2026	31/03/2026	62
2	Actualización de documentos relacionados con el Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información	Coordinador TIC	Plan de Tratamiento de Riesgos actualizado y articulado	1/02/2026	31/05/2026	123
3	Registro y gestión de incidentes de seguridad y privacidad de la información	Coordinador TIC Mesa de Ayuda (MDA)	Registros de incidentes, eventos y acciones correctivas documentadas conforme al MSPI	1/02/2026	30/11/2026	306
4	Definición de alcance y actores institucionales del Plan	Coordinador TIC	Alcance definido y listado de dependencias con injerencia	1/03/2026	31/03/2026	62
5	Elaboración y actualización integral del Plan de Tratamiento de Riesgos	Coordinador TIC	Documento preliminar del Plan y matriz de tratamiento de riesgos	1/03/2026	31/05/2026	123
6	Definición y documentación de la gestión de riesgos residuales y aceptación del riesgo	Coordinador TIC	Sección documentada y validada de riesgos residuales	1/05/2026	30/06/2026	153
7	Definición de componentes de soporte del Plan	Coordinador TIC	Lineamientos de seguimiento, recursos, indicadores y mejora continua	1/06/2026	31/08/2026	215
8	Monitoreo y seguimiento al Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información	Coordinador TIC	Informes de seguimiento, control y evidencias de monitoreo del Plan	1/06/2026	30/11/2026	306
9	Gestión documental, evidencias y conservación de registros	Coordinador TIC	Lineamientos documentales conforme TRD y SIG	1/08/2026	30/09/2026	245

10	Socialización institucional del Plan de Tratamiento de Riesgos	Coordinador TIC	Evidencias de socialización con dependencias	1/09/2026	30/09/2026	245
11	Incorporación de observaciones y ajustes finales al documento	Coordinador TIC	Documento ajustado con observaciones incorporadas, cuando aplique	1/10/2026	31/10/2026	276
12	Formalización, cierre y aceptación tácita del Plan	Coordinador TIC	Plan de Tratamiento de Riesgos	1/11/2026	30/11/2026	306