Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la información 2026

Introducción

En el contexto actual y prospectivo de la vigencia 2026, caracterizado por una acelerada transformación digital, la adopción de nuevas tecnologías y el incremento sostenido de las amenazas cibernéticas, la gestión integral de los riesgos asociados a la seguridad y privacidad de la información se consolida como un eje estratégico para la sostenibilidad, la confianza institucional y la continuidad operativa. Las crecientes exigencias normativas, junto con la evolución constante de los riesgos tecnológicos, demandan un enfoque sistemático, preventivo y dinámico en la protección de los activos de información.

En este marco, la corporación Rotorr-Motor de Innovación reconoce que la seguridad de la información y la protección de los datos personales de clientes, colaboradores, aliados estratégicos y demás partes interesadas constituyen una prioridad institucional y un compromiso permanente. Por ello, se fortalece la implementación de medidas técnicas, administrativas y organizacionales orientadas a identificar, evaluar, tratar y monitorear de manera efectiva los riesgos que puedan afectar la confidencialidad, integridad y disponibilidad de la información.

El Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información para la vigencia 2026 ha sido diseñado como un instrumento integral de gestión, alineado con los principios de mejora continua, gestión del riesgo y cumplimiento normativo, con el propósito de consolidar un marco robusto que permita anticipar amenazas, reducir vulnerabilidades y responder oportunamente ante incidentes de seguridad. Este plan articula acciones preventivas y correctivas, basadas en el análisis sistemático de riesgos y en la adopción de controles de

seguridad acordes con estándares y buenas prácticas reconocidas a nivel nacional e internacional.

La corporación Rotorr-Motor de Innovación opera en un entorno cada vez más interconectado, donde la digitalización de procesos, el uso intensivo de plataformas tecnológicas y el intercambio de información incrementan la exposición a riesgos de seguridad y privacidad. En este sentido, el plan trasciende la protección frente a ataques cibernéticos, incorporando una visión integral orientada a garantizar el tratamiento responsable, ético y transparente de la información, fortaleciendo la confianza de los grupos de interés y la reputación institucional.

El Plan de Tratamiento de Riesgos establece de manera clara las estrategias, políticas, roles y controles necesarios para abordar de forma proactiva las amenazas y vulnerabilidades identificadas, e incluye procedimientos definidos de monitoreo permanente, gestión de incidentes, respuesta oportuna y recuperación, asegurando la resiliencia operativa de la organización. Asimismo, reconoce que la seguridad de la información es una responsabilidad compartida, por lo que promueve el fortalecimiento de una cultura organizacional basada en la concienciación, la capacitación continua y el cumplimiento de las directrices institucionales en materia de seguridad y privacidad.

En conclusión, el Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información de la corporación para 2026 se consolida como un documento estratégico y orientador que respalda la toma de decisiones, garantiza un manejo seguro y responsable de la información y contribuye al logro de los objetivos institucionales, asegurando la operación de la Corporación bajo criterios de integridad, confianza,

transparencia y alineación con los más altos estándares de protección de datos y gobierno de la información.

Objetivo General

Fortalecer, para la vigencia 2026, la gestión integral de los riesgos de seguridad y privacidad de la información en la corporación, mediante la identificación, análisis, tratamiento y monitoreo sistemático de las amenazas y vulnerabilidades que puedan afectar la confidencialidad, integridad y disponibilidad de la información, garantizando la continuidad operativa, el cumplimiento normativo y la confianza de las partes interesadas.

Objetivos Específicos

- Identificar y actualizar los riesgos de seguridad y privacidad de la información asociados a los procesos, activos de información y sistemas tecnológicos de la Corporación Rotorr, considerando el contexto organizacional y los cambios derivados de la transformación digital para la vigencia 2026.

- Evaluar y priorizar los riesgos identificados, mediante metodologías de análisis que permitan determinar su impacto y probabilidad, con el fin de definir acciones de tratamiento acordes con el nivel de riesgo aceptable por la organización.

- Diseñar e implementar controles técnicos, administrativos y organizacionales orientados a prevenir, mitigar o corregir los riesgos de seguridad y privacidad de la información, en coherencia con la normatividad vigente y estándares de buenas prácticas.

- Fortalecer los mecanismos de monitoreo y seguimiento, asegurando la revisión periódica de los riesgos, la efectividad de los controles implementados y la actualización continua del Plan de Tratamiento de Riesgos.

- Establecer y aplicar procedimientos de gestión de incidentes de seguridad de la información, que permitan una respuesta oportuna, la contención de impactos y la recuperación de los servicios y activos de información afectados.

- Promover una cultura organizacional de seguridad y privacidad de la información, mediante estrategias de sensibilización, capacitación y apropiación de responsabilidades por parte de todos los servidores, contratistas y colaboradores de la Corporación Rotorr.

- Asegurar el cumplimiento de la normatividad aplicable en materia de protección de datos personales y seguridad de la información, así como de las directrices institucionales y compromisos adquiridos con clientes, aliados y demás partes interesadas.

Alcance

El Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información de la corporación para la vigencia 2026 aplica a todos los

procesos estratégicos, misionales, de apoyo y de evaluación de la entidad, así como a los activos de información, sistemas de información, infraestructuras tecnológicas y recursos asociados que soportan el cumplimiento de los objetivos institucionales.

El alcance del plan comprende la identificación, análisis, evaluación, tratamiento y monitoreo de los riesgos de seguridad y privacidad de la información que puedan afectar la confidencialidad, integridad y disponibilidad de los datos, independientemente de su formato, medio o soporte, incluyendo información física, digital y verbal, gestionada o custodiada por la Corporación Rotorr.

Este plan es de obligatorio cumplimiento para todos los servidores, contratistas, proveedores, aliados estratégicos y terceros que tengan acceso, gestionen o administren información de la Corporación Rotorr, así como para quienes utilicen sus sistemas de información y plataformas tecnológicas, en concordancia con los roles y responsabilidades definidos institucionalmente.

Asimismo, el alcance incluye la implementación de controles técnicos, administrativos y organizacionales; el fortalecimiento de los mecanismos de prevención y detección de incidentes; la definición de procedimientos de respuesta, continuidad y recuperación; y la ejecución de acciones de sensibilización y capacitación orientadas a consolidar una cultura de seguridad y privacidad de la información.

El Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información se articula con el Sistema de Control Interno, el Modelo

Integrado de Planeación y Gestión – MIPG, la gestión institucional del riesgo y los planes estratégicos y operativos de la corporación, garantizando su coherencia con la normatividad vigente en materia de protección de datos personales, seguridad de la información y gobierno digital.

Marco legal

- Circular Externa 004 de 2015 de la Superintendencia de Industria y Comercio (SIC): Esta circular establece las directrices de la Superintendencia de Industria y Comercio sobre la protección de datos personales en Colombia, haciendo hincapié en la necesidad de adoptar medidas de seguridad, realizar un análisis de riesgos, y notificar incidentes de seguridad que comprometan los datos personales.

- Decreto 1074 de 2015 (Régimen de Protección de Datos Personales): Regula la implementación de la Ley 1581 de 2012, estableciendo directrices para la recolección, almacenamiento, uso y transferencia de datos personales en el país. Incluye disposiciones sobre el tratamiento de datos personales sensibles, y establece la necesidad de adoptar medidas de seguridad para proteger dicha información.

- Decreto 1083 de 2015: Esta versión incorpora las modificaciones introducidas al Decreto Único Reglamentario del Sector de Función Pública a partir de la fecha de su expedición.

- Decreto 648 de 2017: en lo que respecta a la aprobación de la política de administración del riesgo y el "artículo 2.2.21.5.4 Administración de riesgos".

- Decreto 1499 de 2017, que establece el Modelo Integrado de Planeación y Gestión (MIPG).

- Ley 1273 de 2009 (Delitos Informáticos): Esta ley establece medidas relacionadas con la protección de la información, el acceso no autorizado a sistemas informáticos, y la protección frente a amenazas informáticas. Trata de la seguridad en la gestión de información en medios digitales, incluyendo la protección contra el robo de información, la manipulación ilegal de datos y la ciberdelincuencia.

- Ley 1581 de 2012 (Protección de Datos Personales: Regula la protección de los datos personales en Colombia, estableciendo los derechos de los titulares de los datos y las obligaciones de las entidades que los manejan. El tratamiento de datos personales debe hacerse de acuerdo con principios de legalidad, necesidad, calidad, transparencia, acceso y circulación restringida, seguridad, y confidencialidad. Las empresas deben realizar un análisis de riesgos y establecer medidas adecuadas para proteger los datos personales de accesos no autorizados y otros riesgos de seguridad.

- Norma NTC-ISO/IEC 27001 (Sistema de Gestión de Seguridad de la Información): La norma ISO/IEC 27001 es un estándar internacional que establece los requisitos para un sistema de gestión de seguridad de la información (SGSI). En Colombia, muchas organizaciones implementan este estándar como parte de su estrategia de protección de la información y gestión de riesgos.

- Norma NTC 5050 (Gestión de riesgos de TI): Esta norma colombiana se centra en la gestión de riesgos en tecnologías de la información, incluyendo la identificación, evaluación y mitigación de riesgos asociados con los sistemas informáticos y el tratamiento de la información.

Definiciones

- **Riesgo:** Efecto que se causa sobre los objetivos de las entidades, debido a eventos potenciales.
- **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 corporación la materialización del riesgo.
- **Control:** Medida que permite reducir o mitigar un riesgo.
- **Riesgo de Seguridad de la Información:** Es la probabilidad de que se produzca una amenaza o vulnerabilidad que afecte negativamente la confidencialidad, integridad o disponibilidad de la información. Este riesgo puede resultar en un daño directo a los activos de información de la organización, como pérdida, robo o alteración de datos.

- **Riesgo de Privacidad de la Información:** Es el riesgo asociado a la posibilidad de que se revele, utilice o acceda de manera inapropiada a la información personal o sensible, violando los derechos de privacidad de individuos, usuarios o clientes.

- **Amenaza:** Es cualquier circunstancia o evento con el potencial de causar daño a los sistemas de información, ya sea por acción humana, natural o tecnológica. Las amenazas pueden incluir ciberataques, errores humanos, fallos de hardware, desastres naturales, entre otros.

- **Vulnerabilidad:** Se refiere a una debilidad o deficiencia en un sistema, proceso o control de seguridad que puede ser aprovechada por una amenaza para causar daño. Las vulnerabilidades pueden ser técnicas, organizativas o humanas.

- **Impacto:** Es la consecuencia o daño potencial que puede resultar de la materialización de un riesgo. El impacto puede variar en gravedad, afectando aspectos como la reputación, las operaciones, la confianza de los clientes, el cumplimiento de normativas o la estabilidad financiera de la organización.

- **Probabilidad:** Es la medida de la posibilidad de que ocurra un evento de riesgo. Se evalúa en función de la frecuencia con la que una amenaza específica puede explotar una vulnerabilidad.

- **Tratamiento de Riesgos:** Es el proceso mediante el cual se toman decisiones para mitigar, transferir, aceptar o evitar un riesgo. Esto incluye la implementación de controles, la mejora de procesos o la adopción de estrategias que reduzcan el impacto o la probabilidad de ocurrencia de los riesgos.

- **Controles de Seguridad:** Son medidas, políticas, procedimientos o tecnologías implementadas para reducir los riesgos a niveles aceptables. Los controles pueden ser preventivos, detectivos o correctivos, y están diseñados para proteger la información contra accesos no autorizados, alteraciones o destrucción.

- **Confidencialidad:** Es el principio que asegura que la información solo sea accesible a las personas o entidades autorizadas para verla o utilizarla. La confidencialidad es clave en la protección de la información sensible.

- **Integridad:** Se refiere a la exactitud, consistencia y confiabilidad de la información a lo largo de su ciclo de vida. La integridad asegura que los datos no sean alterados de manera no autorizada o accidental.

- **Disponibilidad:** Es la propiedad de que los datos e información sean accesibles y utilizables cuando se necesiten, garantizando la continuidad de las operaciones de la organización.

- **Plan de Continuidad de Negocio (BCP, por sus siglas en inglés):** Es un conjunto de estrategias y procedimientos destinados a garantizar que la organización pueda seguir funcionando después de un evento disruptivo. Incluye la protección y restauración de la información crítica en caso de incidentes como desastres naturales o fallos de infraestructura.

- **Incidente de Seguridad de la Información:** Es cualquier evento que afecte la seguridad de la información, como un ataque cibernético, una fuga de datos, una violación de políticas o un error humano que

comprometa la confidencialidad, integridad o disponibilidad de la información.

- **Análisis de Riesgos:** Es el proceso sistemático para identificar, evaluar y priorizar los riesgos. Implica examinar las amenazas, vulnerabilidades y el impacto potencial que podrían tener sobre los activos de información.

- **Evaluación de Impacto en la Privacidad (PIA, por sus siglas en inglés):** Es un proceso utilizado para identificar y mitigar los riesgos que un proyecto, actividad o sistema puede representar para la privacidad de la información personal, asegurando el cumplimiento con las normativas de protección de datos y la minimización de los riesgos asociados.

- **Cumplimiento Normativo:** Se refiere a la conformidad con las leyes, regulaciones y estándares aplicables a la seguridad y privacidad de la información. En muchos casos, esto incluye normativas internacionales como el Reglamento General de Protección de Datos (GDPR) o la Ley de Protección de la Privacidad de los Consumidores de California (CCPA).

- **Gestión de Incidentes:** Es el proceso de identificar, responder y resolver incidentes de seguridad de manera eficaz y eficiente. La gestión de incidentes busca mitigar los daños, restaurar los servicios lo más rápido posible y aprender de los incidentes para prevenir futuros eventos.

- **Autenticación Multifactor (MFA):** Es un proceso de seguridad que requiere que los usuarios presenten dos o más factores de

autenticación (algo que saben, algo que tienen o algo que son) para acceder a un sistema o servicio.

- **Cifrado de Datos:** Es una técnica de protección que convierte la información legible en un formato ilegible mediante un algoritmo, de modo que solo las partes autorizadas, con la clave adecuada, puedan acceder a la información en su forma original.

- **Evaluación de Riesgos Continuos:** Es el proceso de monitorear y evaluar continuamente los riesgos a medida que evolucionan las amenazas, vulnerabilidades y controles. Este proceso es esencial para mantener la efectividad de las estrategias de tratamiento de riesgos a lo largo del tiempo.

Componentes

El Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información de la corporación para la vigencia 2026 define los componentes, actividades y controles orientados a prevenir, mitigar, tratar y monitorear los riesgos que puedan afectar los activos de información de la entidad, en coherencia con los lineamientos establecidos en la Guía para la Gestión del Riesgo de Seguridad Digital del Ministerio de Tecnologías de la Información y las Comunicaciones – MinTIC, así como con el Modelo Integrado de Planeación y Gestión – MIPG.

Este plan adopta un enfoque integral y preventivo, basado en la gestión del riesgo, que permite anticipar amenazas, reducir vulnerabilidades y fortalecer la capacidad institucional de respuesta ante incidentes de seguridad y privacidad de la información, garantizando la continuidad de los servicios, el cumplimiento normativo y la protección de los datos personales y estratégicos de la Corporación.

Identificación del Riesgo

Para la identificación de los riesgos de Seguridad y Privacidad de la Información, cada una de las áreas y procesos de la corporación deberá identificar y mantener actualizados sus activos de información, incluyendo, entre otros, datos personales, financieros, administrativos, contractuales, operativos y de propiedad intelectual, así como los sistemas de información y recursos tecnológicos que los soportan.

La identificación de riesgos se realizará considerando las situaciones internas y externas que puedan generar impactos negativos sobre los activos de información, afectando el cumplimiento de los objetivos institucionales, la prestación de los servicios y la confianza de las partes interesadas.

Como parte de este proceso, se fortalecerá la clasificación de la información, actividad orientada a categorizar los activos de información de acuerdo con su nivel de sensibilidad (información pública, de uso

interno, confidencial y restringida), con el fin de definir e implementar medidas de seguridad proporcionales al nivel de riesgo identificado.

El resultado de este ejercicio se consolidará en la Matriz de Riesgos de Seguridad y Privacidad de la Información, la cual será objeto de revisión y actualización periódica durante la vigencia 2026.

Matriz de Riesgos

Impacto / Probabilidad	*Bajo*	*Medio*	*Alto*
Alto	**Riesgo 1:** Exposición a amenazas internas no detectadas.	**Riesgo 2:** Pérdida de datos por errores de configuración en sistemas.	**Riesgo 3:** Violación de la privacidad de datos de clientes por ataques externos.
Medio	**Riesgo 4:** Accesos no autorizados por debilidades en la gestión de credenciales.	**Riesgo 5:** Filtración accidental de información mediante canales no seguros.	**Riesgo 6:** Robo o pérdida de dispositivos físicos con información confidencial.
Bajo	**Riesgo 7:** Pérdida de información por eventos naturales o contingencias físicas	**Riesgo 8:** Infección por software malicioso debido a sistemas no actualizados.	**Riesgo 9:** Errores humanos en el tratamiento de datos sensibles.

Descripción de los Riesgos

- Exposición a amenazas internas no detectadas: Riesgo asociado a acciones intencionales o no intencionales de servidores, contratistas o terceros con acceso a sistemas y activos de información, que puedan afectar la confidencialidad, integridad o disponibilidad de la información sin ser detectadas oportunamente.

- Pérdida de datos por errores de configuración en sistemas: Riesgo derivado de configuraciones inadecuadas en plataformas tecnológicas, aplicaciones o infraestructuras de TI, que pueden generar vulnerabilidades, fallas de seguridad o exposición no autorizada de la información.

- Violación de la privacidad de datos de clientes por ataques externos: Riesgo relacionado con ciberataques, accesos no autorizados o incidentes de seguridad que puedan ocasionar la divulgación, alteración o pérdida de datos personales, afectando la confianza y la reputación institucional.

- Accesos no autorizados por debilidades en la gestión de credenciales: Riesgo generado por el uso de contraseñas débiles, reutilización de credenciales o ausencia de mecanismos de autenticación robustos, que faciliten el acceso indebido a información crítica.

- Filtración accidental de información mediante canales no seguros: Riesgo asociado al envío, intercambio o almacenamiento de información confidencial a través de medios no autorizados o no seguros, como correos electrónicos personales o aplicaciones no institucionales.

- Robo o pérdida de dispositivos físicos con información confidencial: Riesgo relacionado con la pérdida, hurto o uso indebido de equipos portátiles, dispositivos móviles o medios de almacenamiento que contengan información sensible de la corporación.

- Pérdida de información por eventos naturales o contingencias físicas: Riesgo asociado a desastres naturales, fallas eléctricas, incendios u otros eventos que puedan afectar la infraestructura tecnológica y ocasionar la pérdida de información, en ausencia de planes de respaldo y recuperación.

- Infección por software malicioso debido a sistemas no actualizados: Riesgo derivado del uso de software obsoleto o sin parches de seguridad, que puede facilitar la propagación de malware y comprometer la seguridad de los sistemas y la información.

- Errores humanos en el tratamiento de datos sensibles: Riesgo generado por fallas involuntarias del personal, como el incumplimiento de protocolos, la falta de conocimiento o la manipulación inadecuada de la información, que puede ocasionar incidentes de seguridad o privacidad.

Plan de Tratamiento de Riesgos

Para la vigencia 2026, el Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información define las medidas de control necesarias para reducir la probabilidad de ocurrencia y/o el impacto de los riesgos identificados, de acuerdo con su nivel de criticidad y con el apetito de riesgo definido por la corporación Rotorr.

Las acciones de tratamiento se estructuran mediante controles técnicos, administrativos y organizacionales, orientados a la prevención, detección y corrección de incidentes de seguridad y privacidad de la información, garantizando la protección de los activos de información y la continuidad operativa.

Las medidas de tratamiento definidas para cada riesgo son las siguientes:

- Riesgo 1 (Alto impacto – Baja probabilidad): Implementación de controles estrictos de acceso lógico y físico, segregación de funciones, monitoreo continuo de actividades internas, revisión de registros (logs) y fortalecimiento de los programas de sensibilización y capacitación en seguridad de la información.

- Riesgo 2 (Impacto medio – Probabilidad media): Ejecución de revisiones periódicas de configuraciones de sistemas y aplicaciones, adopción de herramientas automatizadas para la detección de configuraciones inseguras y aplicación de estándares de configuración segura.

- Riesgo 3 (Alto impacto – Alta probabilidad): Fortalecimiento de la infraestructura de seguridad perimetral, implementación de mecanismos de cifrado de la información en tránsito y en reposo, pruebas periódicas de vulnerabilidades y establecimiento de procedimientos de respuesta y gestión de incidentes.

- Riesgo 4 (Bajo impacto – Probabilidad media): Definición y aplicación de políticas robustas de gestión de credenciales, uso de contraseñas

seguras, implementación de autenticación multifactor y revisiones periódicas de accesos.

- Riesgo 5 (Impacto medio – Alta probabilidad): Uso obligatorio de canales seguros de comunicación, definición de lineamientos para el intercambio de información sensible y fortalecimiento de la formación del personal en buenas prácticas de seguridad de la información.

- Riesgo 6 (Bajo impacto – Probabilidad media): Implementación de políticas de seguridad para dispositivos móviles y portátiles, uso de cifrado en equipos y medios de almacenamiento, y procedimientos para la gestión de pérdidas o robos de dispositivos.

- Riesgo 7 (Bajo impacto – Baja probabilidad): Implementación y actualización del Plan de Continuidad del Negocio y del Plan de Recuperación ante Desastres, incluyendo esquemas de respaldo periódico y pruebas de restauración de la información.

- Riesgo 8 (Impacto medio – Alta probabilidad): Gestión continua de actualizaciones, parches de seguridad y mantenimiento de software, así como monitoreo permanente de amenazas de software malicioso.

- Riesgo 9 (Bajo impacto – Probabilidad media): Capacitación permanente en el manejo seguro de la información, fortalecimiento de procedimientos operativos y control del cumplimiento de los protocolos establecidos.

Valoración del Riesgo

La valoración de los riesgos de Seguridad y Privacidad de la Información para la vigencia 2026 se realizará de conformidad con la metodología institucional de administración de riesgos y los lineamientos establecidos por el MinTIC y el Modelo Integrado de Planeación y Gestión – MIPG.

A través de mesas de trabajo con las áreas responsables, se analizará el contexto interno y externo, se identificarán los riesgos y se evaluará su probabilidad e impacto, con el fin de determinar el nivel de riesgo inherente. En este proceso se identificarán las amenazas, vulnerabilidades y consecuencias, así como los controles existentes, tomando como referencia el Anexo A de la Norma ISO/IEC 27001.

Para cada control se evaluarán, como mínimo, las siguientes variables: responsable asignado, nivel de autoridad y segregación de funciones, tipo de control (preventivo, detectivo o correctivo), forma de implementación (manual o automatizada), periodicidad, propósito, procedimiento de ejecución, tratamiento de desviaciones u observaciones y evidencias del control.

Adicionalmente, se verificará que los controles se ejecuten de manera consistente y efectiva, de tal forma que contribuyan a la reducción del nivel de riesgo y permitan establecer el riesgo residual.

Materialización

En caso de materialización de un riesgo de Seguridad y Privacidad de la Información, este deberá ser gestionado conforme a los procedimientos establecidos para la gestión de incidentes, activando las acciones de mitigación definidas en la Matriz de Riesgos.

Posteriormente, se realizará el análisis del riesgo materializado para determinar su nuevo nivel y se actualizará el mapa de riesgos con los ajustes correspondientes. Si se presenta un riesgo no identificado previamente, este deberá ser reportado para iniciar su identificación, análisis y valoración formal.

Medición y Seguimiento

El monitoreo y seguimiento de los riesgos, controles y planes de tratamiento será responsabilidad de los líderes de proceso, de acuerdo con la periodicidad definida, validando el cumplimiento de las actividades y el cargue de los soportes que evidencien la ejecución de los controles.

La información reportada será revisada y validada para consolidar la medición de la gestión del riesgo mediante un indicador institucional, orientado a medir el nivel de implementación de los controles de los riesgos de Seguridad y Privacidad de la Información.

El indicador de medición estará enfocado en determinar el porcentaje de ejecución de los controles definidos, como insumo para la toma de decisiones y la mejora continua.

Oportunidad de Mejora

El Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información se concibe como un documento dinámico y en permanente actualización, que deberá ajustarse a los cambios del entorno normativo, tecnológico y organizacional.

Las oportunidades de mejora identificadas a partir del seguimiento, auditorías, incidentes o cambios contextuales serán incorporadas de manera oportuna, fortaleciendo la madurez institucional en la gestión de la seguridad de la información y la confianza de los grupos de interés.

Hoja de Ruta

Actividades	Responsable	Fecha Inicial	Fecha Final
Socializar lineamientos y herramientas para la Gestión de Riesgos de Seguridad y Privacidad de la Información	Líder del Proceso	Enero 2026	Diciembre 2026
Identificar, analizar y evaluar los riesgos de Seguridad y Privacidad de la Información	Líder del Proceso	Enero 2026	Diciembre 2026
Ajustar y actualizar los riesgos identificados	Líder del Proceso	Enero 2026	Diciembre 2026
Aprobar riesgos y planes de tratamiento	Líder del Proceso	Enero 2026	Diciembre 2026
Publicar mapas de riesgos de los procesos	Líder del Proceso	Enero 2026	Diciembre 2026

Realizar seguimiento a la implementación de controles y planes de tratamiento	Líder del Proceso	Enero 2026	Diciembre 2026
Identificar oportunidades de mejora derivadas del seguimiento	Líder del Proceso	Enero 2026	Diciembre 2026
Revisar y actualizar lineamientos de Seguridad y Privacidad de la Información	Líder del Proceso	Enero 2026	Diciembre 2026
Medir, presentar y reportar indicadores de gestión del riesgo	Líder del Proceso	Enero 2026	Diciembre 2026

Recursos financieros

La Gerencia Financiera y Administrativa de la corporación destinará anualmente, en su respectivo presupuesto, los recursos necesarios para el efectivo cumplimiento de las obligaciones emanadas del Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la información.

Los recursos presupuestales se ejecutarán de conformidad con los programas y proyectos diseñados.