Plan de Seguridad y Privacidad de la Información 2026

Introducción

En un entorno cada vez más digitalizado y alineado con los procesos de modernización institucional definidos en el Plan Estratégico de la corporación, la seguridad y la privacidad de la información se consolidan como ejes transversales para el fortalecimiento de la gobernanza, la innovación organizacional y la generación de confianza en los grupos de interés. La Corporación reconoce que la protección de la información es un habilitador clave para la transformación digital, la eficiencia operativa y la sostenibilidad institucional.

En este contexto estratégico, la corporación asume el manejo adecuado de los datos y de los activos de información como un compromiso ético, legal y corporativo, estrechamente vinculado a los objetivos estratégicos de gestión del riesgo, transparencia, control interno y mejora continua. La adecuada administración de la información contribuye de manera directa al cumplimiento de la misión institucional, a la toma de decisiones basadas en datos confiables y a la protección de los derechos de clientes, colaboradores, aliados y demás partes interesadas.

El Plan de Seguridad y Privacidad de la Información se articula con las líneas estratégicas institucionales orientadas al fortalecimiento del ecosistema digital, la adopción de buenas prácticas de gobierno y gestión, y la consolidación de una cultura organizacional basada en la responsabilidad y el autocontrol. Su objetivo es establecer directrices claras para la protección, gestión, uso, almacenamiento y transmisión segura de la información en todos los niveles de la organización, minimizando los riesgos asociados a la pérdida, alteración, acceso no

autorizado, divulgación indebida o uso inapropiado de la información confidencial.

De igual forma, este plan se integra con los componentes estratégicos de gestión del riesgo institucional y continuidad del negocio, promoviendo la identificación, evaluación y tratamiento de los riesgos de seguridad y privacidad de la información, así como la implementación de controles preventivos, detectivos y correctivos. Estas acciones contribuyen al logro de los objetivos estratégicos relacionados con la resiliencia organizacional, la protección de los procesos críticos y la prestación confiable de los servicios institucionales.

Finalmente, en coherencia con el enfoque estratégico de innovación y mejora continua, la corporación se compromete a implementar medidas de seguridad proactivas, procesos de monitoreo permanente y esquemas de revisión y actualización periódica del plan, que permitan adaptarse oportunamente a los cambios normativos, tecnológicos y a las amenazas emergentes. De esta manera, el Plan de Seguridad y Privacidad de la Información se consolida como un instrumento estratégico que respalda la transformación digital, el fortalecimiento institucional y la confianza sostenida de los grupos de interés durante la vigencia 2026.

Objetivo General

Fortalecer la seguridad y la privacidad de la información de la Corporación Rotorr durante la vigencia 2026, mediante la

implementación de lineamientos, controles y buenas prácticas que permitan proteger los activos de información, gestionar de manera integral los riesgos asociados y garantizar la confidencialidad, integridad y disponibilidad de los datos, en coherencia con el Plan Estratégico institucional, la gestión del riesgo, la transformación digital y la normativa vigente.

Objetivos Específicos

- Establecer y actualizar políticas, lineamientos y procedimientos de seguridad y privacidad de la información, alineados con el Plan Estratégico Institucional y los planes operativos, asegurando su incorporación en la planeación, ejecución y evaluación de los procesos institucionales.

- Promover una cultura organizacional basada en la responsabilidad, la ética, la transparencia y el autocontrol, mediante acciones de sensibilización y capacitación en seguridad y privacidad de la información para servidores, contratistas y colaboradores.

- Fortalecer las competencias del talento humano en materia de protección de la información y datos personales, asegurando que los roles y responsabilidades en seguridad de la información sean comprendidos y aplicados en el desarrollo de las funciones institucionales.

- Definir e implementar indicadores y mecanismos de seguimiento que permitan evaluar la efectividad de los controles de seguridad y

privacidad de la información, así como el nivel de cumplimiento de los objetivos del plan durante la vigencia 2026.

- Garantizar la gestión adecuada, segura y confiable de la información institucional, asegurando la protección de los datos personales y sensibles, y fortaleciendo los canales de comunicación interna y externa conforme a los principios de integridad, confidencialidad y oportunidad.

- Incorporar buenas prácticas, lecciones aprendidas y mejoras continuas en seguridad y privacidad de la información, aprovechando la innovación tecnológica y el aprendizaje organizacional para responder de manera efectiva a los riesgos y amenazas emergentes.

- Articular la gestión de la seguridad y privacidad de la información con el Sistema de Control Interno y la gestión del riesgo institucional, mediante la identificación, evaluación y tratamiento de riesgos, así como la implementación de controles preventivos, detectivos y correctivos.

Alcance

El Plan de Seguridad y Privacidad de la Información de la corporación para la vigencia 2026 aplica de manera transversal a todos los procesos estratégicos, misionales, de apoyo y de evaluación de la entidad, de conformidad con el Modelo Integrado de Planeación y Gestión – MIPG. Su alcance comprende la gestión integral de la seguridad y la privacidad de la información en todas las dependencias, niveles jerárquicos y modalidades de vinculación.

El plan cobija a todos los contratistas, colaboradores, aliados estratégicos y terceros que, en el ejercicio de sus funciones o actividades, accedan, administren, procesen, almacenen, transmitan o custodien información y activos de información de la Corporación Rotorr, independientemente del medio o formato en que esta se encuentre (físico, digital, electrónico o verbal).

Asimismo, el alcance incluye todos los activos de información institucionales, tales como bases de datos, sistemas de información, aplicaciones, infraestructuras tecnológicas, documentos físicos y digitales, plataformas de comunicación, servicios en la nube y demás recursos tecnológicos que soportan los procesos institucionales y la prestación de servicios.

El Plan de Seguridad y Privacidad de la Información se articula con la gestión del riesgo institucional, el Sistema de Control Interno, el Gobierno Digital y los planes de continuidad del negocio, abarcando la identificación, evaluación, tratamiento y monitoreo de los riesgos asociados a la seguridad y privacidad de la información. Igualmente, contempla la implementación de controles preventivos, detectivos y correctivos, así como acciones de sensibilización, capacitación, seguimiento y mejora continua.

Finalmente, el alcance del plan se extiende al cumplimiento de la normativa vigente en materia de protección de datos personales, seguridad de la información y transparencia, así como a la revisión y actualización periódica de los lineamientos establecidos, permitiendo a la Corporación Rotorr responder de manera oportuna a los cambios normativos, tecnológicos y a las amenazas emergentes durante la vigencia 2026.

Marco legal

- Ley 1581 de 2012 del Congreso de la República, "Por la cual se dictan disposiciones generales para la protección de datos personales".

- Decreto 2609 de 2012 de la Presidencia de la República, "Por el cual se reglamenta el Título V de la Ley 594 de 2000, parcialmente los artículos 58 y 59 de la Ley 1437 de 2011 y se dictan otras disposiciones en materia de Gestión Documental para todas las Entidades del Estado".

- Decreto 1377 de 2013 del Ministerio de Comercio, Industria y Turismo, "Por el cual se reglamenta parcialmente la Ley 1581 de 2012".

- Decreto 612 de 2018 de la Presidencia de la República, "Por el cual se fijan directrices para la integración de los planes institucionales y estratégicos al Plan de Acción por parte de las entidades del Estado".

- Decreto 886 de 2014 del Ministerio de Comercio, Industria y Turismo, "Por el cual se reglamenta el artículo 25 de la Ley 1581 de 2012, relativo al Registro Nacional de Bases de Datos".

- Ley 1712 de 2014 del Congreso de la República, "Por medio de la cual se crea la Ley de Transparencia y del Derecho de Acceso a la Información Pública Nacional y se dictan otras disposiciones".

- NTC-ISO/IEC 27001:2013, Tecnología de la información. Técnicas de seguridad. Sistemas de Gestión de la seguridad de la información (SGSI). Requisitos (ISO/IEC 27001:2013 – Information technology – Security techniques – Information security management systems – Requirements).

- Decreto 103 de 2015 de la Presidencia de la República, "Por medio del cual se reglamenta parcialmente la Ley 1712 de 2014 y se dictan otras disposiciones".

- Decreto 1008 de 2018 del Ministerio de Tecnologías de la Información y las Comunicaciones, "Por el cual se establecen los lineamientos generales de la política de Gobierno Digital y se subroga el capítulo 1 del título 9 de la parte 2 del libro 2 del Decreto 1078 de 2015, Decreto Único Reglamentario del sector de Tecnologías de la Información y las Comunicaciones".

- Decreto 1083 de 2015 del Departamento Administrativo de la Función Pública, "Por medio del cual se expide el Decreto Único Reglamentario del Sector de Función Pública", el cual establece las políticas de Gestión y Desempeño Institucional, entre las que se

encuentran las de "11. Gobierno Digital, antes Gobierno en Línea" y "12. Seguridad Digital".

- Modelo Integrado de Planeación y Gestión – MIPG versión 4, marzo de 2021.

- Decreto 2106 de 2019 del Departamento Administrativo de la Función Pública, "Por el cual se dictan normas para simplificar, suprimir y reformar trámites, procesos y procedimientos innecesarios existentes en la administración pública", en el cual se establece que las autoridades que realicen trámites, procesos y procedimientos por medios digitales, deberán disponer de una estrategia de seguridad digital siguiendo los lineamientos que emita el Ministerio de Tecnologías de la Información y las Comunicaciones.

- Resolución 0500 de 2021 del Ministerio de Tecnologías de la Información y las Comunicaciones, "Por la cual se establecen los lineamientos y estándares para la estrategia de seguridad digital y se adopta el modelo de seguridad y privacidad como habilitador de la política de Gobierno Digital".

- Modelo de Seguridad y Privacidad de la Información (MSPI), Política de Gobierno Digital Ministerio de Tecnologías de la Información y las Comunicaciones – versión 4. 2021.

- CONPES 3995 de 2020 - Política Nacional de Confianza y Seguridad Digital.

- Política de Seguridad y Privacidad de la Información.

Definiciones

- **Seguridad de la Información**: Conjunto de medidas, políticas y procedimientos diseñados para proteger la información de accesos no autorizados, modificaciones no deseadas o destrucción accidental. Este concepto incluye:
    - Confidencialidad: Solo las personas autorizadas pueden acceder a la información.
    - Integridad: La información es precisa, completa y está protegida contra modificaciones no autorizadas.
    - Disponibilidad: La información está accesible para los usuarios autorizados cuando la necesiten.
- Privacidad de la Información: Se refiere al derecho y las prácticas que aseguran el manejo adecuado de los datos personales y sensibles, protegiendo la identidad y la intimidad de las personas relacionadas con la organización. En Colombia, esto está regulado por la Ley 1581 de 2012.
- Plan: Es un documento estructurado que establece objetivos, estrategias, roles, recursos y cronogramas para implementar y mantener medidas de seguridad y privacidad.

Componentes

Para llevar a cabo el proyecto de diseño, implementación y documentación del sistema gestión de seguridad y privacidad de la información de la corporación, tomamos como referencia la Planeación Estratégica.

Configuración del Ecosistema ITEM

Estrategia	Componente	Objetivo del Componente	Actividades Clave 2026	Indicador	Meta 2026
Fortalecer la gobernanza del Ecosistema ITEM	Gobernanza y Gestión Integral de la Información	Consolidar un modelo institucional de seguridad y privacidad de la información que soporte la articulación del Ecosistema ITEM	• Actualizar políticas de seguridad y privacidad • Definir roles y responsabilidades • Integrar el MSPI a la planeación institucional	Políticas y lineamientos actualizados	100% políticas actualizadas e implementadas
			• Identificar y clasificar activos de información	Inventario de activos de información	100% de activos identificados

Innovaciones

Estrategia	Componente	Objetivo del Componente	Actividades Clave 2026	Indicador	Meta 2026
Impulsar procesos de	Seguridad de la Información para la Innovación y la	Integrar la seguridad y la privacidad desde el diseño en	• Aplicar principios de security y privacy by design	Proyectos innovadores evaluados en seguridad	100% de proyectos evaluados

innovación seguros	Transformación Digital	iniciativas innovadoras	• Evaluar riesgos tecnológicos de nuevos proyectos		
			• Definir lineamientos de seguridad para nuevas tecnologías	Lineamientos adoptados	1 documento institucional aprobado

Transferencia de Conocimiento

Estrategia	Componente	Objetivo del Componente	Actividades Clave 2026	Indicador	Meta 2026
Fortalecer capacidades institucionales	Cultura, Capacitación y Gestión del Conocimiento en Seguridad de la Información	Desarrollar una cultura organizacional orientada a la protección de la información	• Diseñar e implementar plan de capacitación • Jornadas de sensibilización	Porcentaje de servidores capacitados	≥ 60% del personal
			• Documentar buenas prácticas y lecciones aprendidas	Documentos de conocimiento generados	Mínimo 3 documentos

Emprendimientos de Base Tecnológica

Estrategia	Componente	Objetivo del Componente	Actividades Clave 2026	Indicador	Meta 2026
Proteger la información en alianzas estratégicas	Protección de la Información en Alianzas y Emprendimientos Tecnológicos	Garantizar el intercambio seguro de información con terceros y emprendedores	• Definir cláusulas de seguridad y privacidad • Evaluar riesgos de terceros	Convenios con cláusulas de seguridad	Proteger la información en alianzas estratégicas

			Lineamientos para protección de propiedad intelectual	Lineamientos adoptados	Lineamientos para protección de propiedad intelectual

Desarrollo de Tecnologías Profundas

Estrategia	Componente	Objetivo del Componente	Actividades Clave 2026	Indicador	Meta 2026
Gestionar riesgos de tecnologías emergentes	Gestión Avanzada de Riesgos y Seguridad de Tecnologías Emergentes	Mitigar riesgos asociados al uso de deep tech y tecnologías de alto impacto	• Identificar riesgos de IA, analítica, automatización • Definir controles de seguridad	Riesgos tecnológicos gestionados	100% de riesgos identificados
			• Monitorear cumplimiento ético y normativo	Reportes de seguimiento	2 reportes anuales

Desarrollo Organizacional Líquido, Ubicuo y Fluido

Estrategia	Componente	Objetivo del Componente	Actividades Clave 2026	Indicador	Meta 2026
Fortalecer la resiliencia institucional	Resiliencia, Continuidad y Seguridad Operacional	Asegurar la continuidad y resiliencia de los procesos institucionales	• Actualizar plan de continuidad • Gestión de incidentes de seguridad	Plan de continuidad actualizado	100% actualizado
			• Realizar pruebas de respaldo y recuperación		

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 Seguridad y Privacidad de la Información.

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