Plan de Seguridad y Privacidad de la Información

PL-GTI-003 V1

Introducción

En un entorno cada vez más digitalizado, la seguridad y la privacidad de la información se han convertido en pilares fundamentales para garantizar la confianza de nuestros grupos de interés. En la corporación Rotorr-Motor de Innovación, entendemos que el manejo adecuado de los datos sensibles no solo es un compromiso ético, sino también una obligación legal y corporativa que protege tanto a la organización como a los individuos que confían en nuestros servicios.

Este Plan de Seguridad y Privacidad de la Información tiene como objetivo establecer directrices claras para la protección, gestión y almacenamiento de la información en todos los niveles de la organización. Busca minimizar los riesgos asociados con la pérdida, el acceso no autorizado, la divulgación o el uso indebido de la información confidencial y garantizar que la privacidad de nuestros clientes, empleados y otras partes interesadas se respete en todo momento.

Nuestro compromiso es implementar medidas de seguridad proactivas y procesos de monitoreo continuo, adaptados a las mejores prácticas de la industria y cumpliendo con las normativas vigentes de protección de datos. Este plan es un documento vivo que será revisado y actualizado periódicamente para mantenerse al día con los avances tecnológicos y las amenazas emergentes, asegurando así una protección constante de la información que gestionamos.

Objetivo General

Garantizar la gestión adecuada de los riesgos asociados con la información corporativa y los datos personales, estableciendo las actividades necesarias para el fortalecimiento del sistema de gestión de Seguridad y Privacidad de la Información implementando medidas preventivas, correctivas y de recuperación para proteger los activos informativos.

Esta política está alineada con la NTC/IEC ISO 27001:2013, la Política de Gobierno Digital del Ministerio de Tecnologías de la Información y las Comunicaciones, la Política de Seguridad y Privacidad de la Información y Seguridad Digital de Rotorr-Motor de Innovación y el Modelo Integrado de Planeación y Gestión - MIPG.

Objetivos Específicos

- Definir las actividades que darán cumplimiento a las fases del Modelo de Seguridad y Privacidad de la Información tales como: Diagnóstico, Planificación, Operación, Evaluación de desempeño y Mejoramiento continuo.

- Dar cumplimiento a los requisitos legales y normativos en materia de seguridad y privacidad de la información, seguridad digital y protección de la información personal.

- Dar garantías a los grupos de interés de la Custodia de la información que reposa en la corporación a través de la implementación de

controles de seguridad de la información soportados en la confidencialidad, integridad y disponibilidad.

- Incrementar el nivel de madurez del Modelo de Seguridad y Privacidad de la Información en corporación.
- Fomentar una cultura institucional en donde se sensibilice a los colaboradores y contratistas de la corporación acerca del Sistema de Gestión de Seguridad de la Información y el modelo de Privacidad de la información.
- Orientar en la adopción y aplicación de la legislación relacionada con la protección de datos personales.

Alcance

El Plan de Seguridad y Privacidad de la Información aplica para todos los sistemas, bases de datos, procesos, colaboradores, contratistas y terceros que mantengan vínculos laborales o contractuales con la corporación. Este plan cubre a quienes, en el cumplimiento de sus funciones, compartan, utilicen, recolecten, procesen, intercambien o consulten información corporativa, ya sea de manera interna o externa, sin importar su ubicación. Asimismo, la política abarca toda la información creada, procesada o utilizada por la corporación, independientemente del medio, formato, presentación o lugar donde se encuentre, incluyendo datos personales de clientes, empleados y proveedores.

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, se deben ejecutar las siguientes fases:

Planificación

De acuerdo con el resultado de la fase de diagnóstico, se definen las necesidades y objetivos de seguridad y privacidad de la información basados en el contexto estratégico, el modelo de operación de Rotorr-Motor de Innovación, los recursos disponibles y su articulación con el Plan Estratégico Institucional, entre otros, los cuales permiten definir los

lineamientos para asegurar el cumplimiento de los requisitos de Modelo de Seguridad y Privacidad de la Información.

Operación

Es necesario desarrollar la implementación de la Política General de Seguridad y Privacidad de la Información a través de la estructuración y puesta en marcha de los controles de seguridad de la información que ayudan a mitigar el impacto de los riesgos definidos en la etapa de Planificación que hacen parte del Modelo de Seguridad y Privacidad de la Información.

Evaluación de Desempeño

La evaluación del desempeño del Modelo de Seguridad y Privacidad de la información, se realiza a través de la medición y monitoreo de los indicadores de gestión, el seguimiento de la eficacia de los controles para determinar su efectividad, la revisión por la Alta Dirección de la corporación para determinar las acciones necesarias que permitan mejorar la implementación su implementación y finalmente las auditorías internas. Con la revisión periódica se debe asegurar que las mejoras realizadas cumplan con los objetivos dispuestos en la Política de Seguridad y Privacidad de la Información y Seguridad Digital.

Mejoramiento Continuo

El mejoramiento continuo del Modelo de Seguridad y Privacidad de la información es el resultado del seguimiento y revisión de todo el sistema de seguridad y privacidad de la información, donde se evalúa el alcance, la metodología de riesgo y la eficacia de los controles, que como resultado se identifican mejoras al sistema a través de planes de mejoramiento (acciones correctivas) y de esta manera mejorar continuamente el desempeño institucional del citado Modelo. Resultado del mejoramiento continuo, se retroalimentan los planes de seguridad, políticas, procedimientos y controles, que impacta de manera positiva, en el desempeño del sistema.

Hoja de Ruta

Programa/ Proyecto	Actividades	Responsable	Fecha Inicial	Fecha Final
Auditoría y Evaluación Inicial	• **Revisión de las Políticas de Seguridad Existentes**: Realizar una auditoría completa de las políticas actuales de seguridad y privacidad para identificar áreas de mejora. • **Evaluación de Vulnerabilidades**: Llevar a cabo una	Líder del Proceso – Control Interno	Febrero 2025	Diciembre 2025

Programa/ Proyecto	Actividades	Responsable	Fecha Inicial	Fecha Final
	evaluación de riesgos y vulnerabilidades tecnológicas en sistemas, infraestructuras y aplicaciones corporativas. • **Cumplimiento Regulatorio**: Analizar el estado de cumplimiento con las leyes de protección de datos (GDPR, Leyes locales de privacidad, etc.).			
Implementación de Nuevas Herramientas y Tecnologías	• **Mejoras en la Infraestructura de Seguridad**: Implementar herramientas avanzadas de protección como firewalls, sistemas de detección de intrusos (IDS), y cifrado de datos	Líder del Proceso	Febrero 2025	Diciembre 2025

Programa/ Proyecto	Actividades	Responsable	Fecha Inicial	Fecha Final
	en reposo y en tránsito. • **Autenticación Multifactor (MFA)**: Reforzar la seguridad en los accesos a sistemas críticos mediante la implementación de autenticación multifactor en todas las plataformas. • ***Backup* y Recuperación ante Desastres**: Actualizar los sistemas de respaldo y recuperación para garantizar que los datos puedan ser restaurados rápidamente en caso de incidentes.			

Programa/ Proyecto	Actividades	Responsable	Fecha Inicial	Fecha Final
Capacitación y Concienciación	• **Programa de Capacitación Continua**: Desarrollar un programa educativo anual en seguridad y privacidad de la información dirigido a todos los empleados. • **Simulacros de *Phishing* y Gestión de Incidentes**: Realizar simulacros de ciberataques (como *phishing)* para evaluar la respuesta del personal y mejorar la preparación ante posibles incidentes de seguridad. • **Campañas de Concienciación**: Promover	Líder del Proceso	Febrero 2025	Diciembre 2025

Programa/ Proyecto	Actividades	Responsable	Fecha Inicial	Fecha Final
	campañas de sensibilización sobre la importancia de la privacidad y cómo los empleados pueden contribuir a la protección de los datos.			
Revisión de Contratos y Relaciones con Terceros	• **Evaluación de Proveedores**: Realizar una auditoría de seguridad de todos los proveedores externos que gestionan datos de la organización, garantizando que cumplan con los estándares de seguridad y privacidad exigidos. • **Actualización de Contratos**:	Líder del Proceso	Febrero 2025	Diciembre 2025

Programa/ Proyecto	Actividades	Responsable	Fecha Inicial	Fecha Final
	Asegurar que los contratos con terceros incluyan cláusulas claras sobre protección de datos, seguridad cibernética y cumplimiento con las normativas vigentes. • **Evaluación de Transferencias Internacionales de Datos**: Garantizar que cualquier transferencia de datos fuera del país cumpla con los requisitos legales y de privacidad.			
Monitoreo y Mejora Continua	• **Monitoreo Continuo**: Implementar sistemas de monitoreo en tiempo real para	Líder del Proceso	Febrero 2025	Diciembre 2025

Programa/ Proyecto	Actividades	Responsable	Fecha Inicial	Fecha Final
	detectar y responder rápidamente a amenazas y vulnerabilidades. • **Revisión Anual de Políticas y Procedimientos**: Realizar una revisión exhaustiva de las políticas de seguridad y privacidad para asegurar su efectividad.			

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.