Region Metropolitana

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

Fecha de aprobación: 29 de enero del 2026

INTRODUCCIÓN

La gestión de riesgos de seguridad y privacidad de la información es un componente esencial que le permite a la Región Metropolitana Bogotá Cundinamarca (RMBC) realizar la identificación, análisis y tratamiento a los riesgos asociados a los activos y la información de la Entidad, que pueden comprometer su confidencialidad, integridad y disponibilidad. Este plan tiene como propósito contribuir a diseñar, implementar y mantener un sistema de seguridad de la información eficaz, adaptado a las necesidades y objetivos estratégicos de la organización.

De otra parte, la resolución 019 de 30 de enero de 2024, integra y establece el reglamento de funcionamiento del Comité institucional de Gestión y Desempeño en la Región Metropolitana Bogotá – Cundinamarca y se adopta la implementación y operación del Modelo Integrado de Planeación y Gestión – MIPG., la guía para la administración del riesgo (DAFP) y políticas propias de la Entidad.

Por lo anterior y en cumplimiento de la normatividad establecida por el estado colombiano, la RMBC adoptó el Modelo de Seguridad y Privacidad de la Información - MPSI y la Política de Gobierno Digital, Decreto 767/22, emitidas por el Ministerio TIC. Igualmente, se incorporan lineamientos y buenas prácticas de los estándares ISO 27001, ISO 31000, entre otros

1. OBJETIVO GENERAL

Diseñar y documentar un plan de riesgos de seguridad y privacidad de la información de forma integral que garantice la protección de los activos de información de la organización, mediante la identificación, evaluación, manejo y mitigación de riesgos, con el fin de asegurar la confidencialidad, integridad y disponibilidad de la información.

1.1. OBJETIVOS ESPECIFICOS

- **Identificar** los riesgos potenciales que afectan a los activos de información de la organización.
- **Evaluar** el impacto y la probabilidad de materialización de dichos riesgos.
- **Desarrollar** estrategias de control y mitigación de riesgos alineadas con las políticas organizacionales.
- **Establecer** un proceso continuo de monitoreo y evaluación de la efectividad del plan de seguridad.
- **Garantizar** la capacitación continua del personal en cuanto a la seguridad de la información y mejores prácticas.

2. ALCANCE

Este plan de seguridad abarca todos los sistemas, aplicaciones, redes y procesos que involucran el manejo, almacenamiento y procesamiento de la información dentro de la organización, también se extiende a los proveedores y partes interesadas que manejan información crítica de la Entidad.

- **Ámbito geográfico:** Cobertura de todas las oficinas de la Entidad.
- **Ámbito operativo:** Incluye todas las actividades relacionadas con el procesamiento de información, desde el acceso hasta su eliminación.

3. RESPONSABILIDADES

Definir las responsabilidades de cada miembro del equipo de seguridad de la información y sus roles específicos dentro de La ejecución del plan, tales como:

- **Responsable del plan de seguridad**:
  Dependencia: Oficina de Tecnologías de la Información y las Comunicaciones (OTIC).
  Función: Encargado de supervisar la implementación y ejecución del plan.

- **Equipo de gestión de riesgos**:
  Dependencia: Oficina de Planeación / Gestión del Riesgo (con apoyo de la OTIC)
  Función: Encargados de la identificación, valoración y monitoreo de los riesgos.

- **Responsable de la infraestructura tecnológica**: Encargado de aplicar controles técnicos de seguridad en los sistemas.
  Dependencia: Oficina de Tecnologías de la Información y las Comunicaciones (OTIC).
  Función: Encargado de aplicar controles técnicos de seguridad en los sistemas.

4. DESARROLLO METODOLÓGICO

4.1. Identificación de riesgos de activos de información

En esta fase, se debe identificar los activos de información más críticos, como bases de datos, sistemas operativos, aplicaciones y redes, y los riesgos asociados a estos activos.

La identificación de estos riesgos se realizará teniendo en cuenta la matriz de riesgos del proceso de gestión TIC y los planes de manejo definidos por la entidad**,** con el fin de asegurar la coherencia entre el Plan de Seguridad de la Información y la gestión institucional del riesgo.

4.2. Establecimiento del Alcance, Contexto y Criterios

Definir el contexto del análisis de riesgos, incluyendo el entorno organizacional, los requisitos de seguridad, las leyes aplicables y las expectativas de los interesados.

4.3. Identificación y Valoración de riesgos

Determinar los riesgos potenciales que puedan afectar los activos identificados, basándose en su impacto y la probabilidad de su ocurrencia.

4.4. Análisis de Riesgos

Analizar los riesgos para comprender su naturaleza y sus posibles efectos en la organización. Esta etapa debe detallar los posibles escenarios de amenazas y vulnerabilidades.

4.5. Valoración del Riesgo

Establecer un sistema de clasificación de riesgos según el impacto y la probabilidad. Utilizar matrices de riesgos para priorizar aquellos riesgos que representan una mayor amenaza para los activos de información.

4.6. Manejo del Riesgo

Desarrollar estrategias y planes de acción para mitigar, transferir, aceptar o evitar los riesgos identificados. Este paso incluirá:

- Implementación de controles técnicos, como cifrado, autenticación y acceso restringido.
- Creación de políticas de gestión de incidentes de seguridad.

4.7. Monitoreo

Establecer un sistema de monitoreo continuo para detectar vulnerabilidades y amenazas. Esto incluye la implementación de herramientas de detección de intrusiones y auditorías periódicas de seguridad.

4.8. Evaluación de Riesgo Residual

Una vez implementadas las medidas de mitigación, evaluar el riesgo residual, es decir, el riesgo que persiste después de haber aplicado los controles.

4.9. Oportunidad de Mejora

Identificar áreas en las que el plan de seguridad puede mejorarse continuamente, con base en las evaluaciones periódicas y los resultados de los monitoreos.

4.10. Materialización

Planificar la puesta en marcha efectiva de los controles de seguridad definidos, asegurando que todos los recursos necesarios estén disponibles para su implementación.

4.11. Recursos

Detallar los recursos humanos, tecnológicos y financieros necesarios para implementar el plan de seguridad, incluyendo la contratación de personal especializado, adquisición de software de seguridad, y presupuesto para la capacitación.

4.12. Tiempo de ejecución – Plan de trabajo

Establecer un cronograma claro para la ejecución del plan de seguridad, incluyendo hitos, fechas de entrega y responsables de cada actividad.

4.13. Presupuesto

Determinar el presupuesto necesario para la ejecución del plan, especificando los costos asociados a la compra de equipos, software, personal y formación.

4.14. Medición del modelo de Seguridad y Privacidad de la Información

Establecer indicadores clave de rendimiento (KPI) para medir la eficacia del plan de seguridad. Estos indicadores deben evaluar tanto la implementación como los resultados obtenidos en términos de reducción de riesgos y mejora de la seguridad general de la organización.

El proceso de gestión de riesgos se articulará de manera permanente con la Matriz de Riesgos del Proceso de Gestión TIC de la entidad y con sus respectivos planes de manejo, garantizando consistencia, trazabilidad y alineación con el Sistema de Control Interno y el Modelo Integrado de Planeación y Gestión (MIPG).

5. CRONOGRAMA IMPLEMENTACIÓN PLAN DE TRATAMIENTO DE RIESGOS RMBC:

N°	Actividad	Tarea	Fecha de Inicio	Fecha de Finalización	Entregable	Responsables
1	Identificación de riesgos	Levantamiento de inventario de activos de información	1-mar-26	3-may-26	Matriz de activos de información	Líder de gestión de riesgos, quipo técnico de TI
		Realizar mesas de trabajo para identificación de riesgos asociados a los activos de información identificados.			Actas de reunión firmadas por las partes	
		Validar los de riesgos identificados y los responsables con el equipo de gestión			Matriz de riesgos identificados	
2	Evaluación de riesgos	Clasificar los riesgos según probabilidad e impacto.	4-abr-26	5-may-26	Matriz de riegos con su clasificación	Analistas de riesgos, equipo de TI
3	Desarrollo de estrategias de tratamiento	Asignar responsables para cada estrategia de tratamiento.	6-feb-26	10-feb-26	Documento de estrategias definidas para el tratamiento de los riesgos según su clasificación, valoración cuantitativa y cualitativa y priorización asignada, así como los controles a aplicar en cada caso.	Líder de riesgos, equipo técnico de TI
		Establecer medidas de control para la implementación de estrategias.				

N°	Actividad	Tarea	Fecha de Inicio	Fecha de Finalización	Entregable	Responsables
4	Planificación de recursos	Determinar recursos humanos necesarios (por ejemplo, personal experto).	11-feb-26	13-feb-26	Documento que establece los recursos necesarios para el tratamiento de los riesgos identificados	Recursos humanos, Dirección Regional, equipo financiero y equipo de TI
		Establecer presupuesto requerido para el tratamiento de riesgos.				
		Identificar herramientas y equipos necesarios.				
5	Implementación de estrategias	Asignar recursos y personal para implementar las estrategias.	1-ago-26	30-ago-26	Documento donde se establezcan los recursos asignados y las estrategias para la mitigación de riesgos	Gerentes de proyecto, líderes de área de TI
		Ejecutar actividades específicas según el plan (por ejemplo, establecer contratos de transferencia de riesgos).				
		Iniciar la mitigación de riesgos identificados.				
6	Monitoreo y seguimiento	Realizar revisiones periódicas del progreso de las estrategias de tratamiento.	1-dic-26	Continuo	Acta de revisión de los controles implementados y/o de la necesidad de implementar controles más efectivos, en caso de ser necesario	Líder de riesgos, equipo de proyecto de TI
		Evaluar si los riesgos tratados están bajo control.				
		Ajustar el plan de tratamiento en caso de nuevos riesgos o fallos.				
7	Revisión y evaluación final	Realizar análisis postratamiento de riesgos.	01/12/2026	30/12/2026	Matriz de riesgos residuales	Equipo de gestión de riesgos, partes interesadas
		Evaluar la efectividad de las estrategias implementadas.				
		Generar un informe final para las partes interesadas.				