TABLA DE CONTENIDO

1. 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 - MSPI 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

2. OBJETIVO

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.

2.1. Objetivos Específicos

- **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.

3. 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.

4. DEFINICIONES

Aceptación de riesgo: decisión de asumir un riesgo.

Activo de información: cualquier elemento que contenga, genere, adquiera, gestione y/o procese información, que tiene valor para uno o más procesos de la organización y debe protegerse (ISO/IEC 27001).

Análisis de riesgo: uso sistemático de la información para identificar fuentes y estimar el riesgo.
Apetito al riesgo: magnitud y tipo de riesgo que una organización está dispuesta a buscar o retener.

Evaluación del riesgo: proceso de comparar el riesgo estimado contra criterios de riesgo definidos para determinar su importancia.

Gestión de riesgos: actividades coordinadas para dirigir y controlar una organización con respecto al riesgo. Incluye la identificación, valoración, tratamiento, monitoreo y seguimiento de los riesgos que afecten el logro de los objetivos institucionales.

Impacto: consecuencias o efectos que genera la materialización de un riesgo.
Mapa de riesgos: documento que consolida la información resultante del proceso de gestión de riesgos.

Probabilidad: posibilidad de que una amenaza aproveche una vulnerabilidad para materializar un riesgo.

Riesgo de seguridad de la información: combinación de amenazas y vulnerabilidades en el entorno físico, digital o humano que puede afectar la confidencialidad, integridad y disponibilidad de la información.

Riesgo inherente: nivel de riesgo propio de una actividad antes de la aplicación de controles.

Riesgo residual: nivel de riesgo que permanece después de implementar las medidas de tratamiento y control.

Vulnerabilidad: debilidad, falla o ausencia de controles que puede ser explotada por una amenaza para afectar los activos de información o los procesos de la organización.

5. MARCO NORMATIVO

Ley 1273 de 2009. Por medio de la cual se modifica el Código Penal y se crea el bien jurídico de protección de la información y de los datos.

Ley 1581 de 2012. Por la cual se dictan disposiciones generales para la protección de datos personales.

Ley 1712 de 2014. Por medio de la cual se crea la Ley de Transparencia y del Derecho de Acceso a la Información Pública Nacional.

Decreto 886 de 2014. Por el cual se reglamenta el Registro Nacional de Bases de Datos.

Decreto 1068 de 2015. Reglamenta aspectos relacionados con la protección de datos personales y el Registro Nacional de Bases de Datos.

Decreto 612 de 2018. Establece directrices para la integración de los planes institucionales y estratégicos al Plan de Acción.

Decreto 1008 de 2018. Establece los lineamientos generales de la Política de Gobierno Digital.

Ley 1915 de 2018. Modifica disposiciones relacionadas con derechos de autor y derechos conexos.

Resolución 1519 de 2020. Define estándares y directrices para la publicación de información pública, accesibilidad web, seguridad digital y datos abiertos.

Resolución 500 de 2021. Adopta el Modelo de Seguridad y Privacidad de la Información como habilitador de la Política de Gobierno Digital.

Directiva Presidencial 03 de 2021. Establece lineamientos para el uso de servicios en la nube, inteligencia artificial, seguridad digital y gestión de datos.

Resolución 746 de 2022. Fortalece el Modelo de Seguridad y Privacidad de la Información y establece lineamientos adicionales.

Guía para la Administración del Riesgo y el Diseño de Controles en Entidades Públicas – Versión 6 (DAFP, 2022). Define la metodología para la identificación, valoración, tratamiento y monitoreo de riesgos.

Resolución 2277 de 2025. Actualiza el Anexo 1 de la Resolución 500 de 2021 y establece disposiciones relacionadas con el Modelo de Seguridad y Privacidad de la Información.

6. PÚBLICO OBJETIVO

El presente plan está dirigido a los servidores públicos, contratistas, directivos y líderes de proceso de la Región Metropolitana Bogotá–Cundinamarca (RMBC), quienes participan en la identificación, valoración, tratamiento, monitoreo y seguimiento de los riesgos institucionales y de seguridad de la información.

De igual forma, involucra a las dependencias responsables de la implementación de controles, la Oficina de Tecnologías de la Información y las Comunicaciones (OTIC), la Oficina Asesora de Planeación, el Comité Institucional de Gestión y Desempeño y demás actores que, en el marco de sus funciones, contribuyen a la gestión integral del riesgo en la entidad.

7. DESARROLLO METODOLÓGICO

El presente Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información complementa la Política para la Gestión Integral del Riesgo de la Región Metropolitana Bogotá–Cundinamarca (RMBC) y desarrolla los lineamientos específicos para la gestión de los riesgos asociados a la seguridad y privacidad de la información.

La identificación, análisis, valoración, tratamiento y seguimiento de los riesgos se realizará conforme a la metodología institucional adoptada por la entidad, basada en los lineamientos del Departamento Administrativo de la Función Pública (DAFP), el Modelo de Seguridad y Privacidad de la Información (MSPI) y la Política para la Gestión Integral del Riesgo de la RMBC. Para tal fin, se utilizará la Matriz de Riesgos y Controles institucional y los demás instrumentos definidos por la entidad para la administración del riesgo.

El proceso de gestión de riesgos de seguridad y privacidad de la información se articulará permanentemente con el Mapa de Riesgos Institucional, los planes de manejo asociados y las instancias de seguimiento definidas por la entidad, garantizando la trazabilidad, coherencia y alineación con el Sistema de Control Interno y los lineamientos institucionales para la gestión integral del riesgo.

7.1. Etapas para la Gestión y tratamiento de Riesgos de Seguridad y Privacidad de la Información

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.

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.

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. 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.

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.

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.

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.

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.

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.

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.

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.

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.

13. Presupuesto

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

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).

8. CRONOGRAMA IMPLEMENTACIÓN PLAN DE TRATAMIENTO DE RIESGO RMBC

N°	Actividad	Tarea	Fecha de inicio	Fecha de finalización	Entregable	Responsable
1	Identificación de activos	Creación y aprobación de Metodología de levantamiento de activos	mar-26	jul-26	Metodología de levantamiento de activos	Oficina de TIC
	Identificación de activos	Asignación de enlaces de cada oficina para levantamiento de riesgos	mar-26	jul-26	Memorando con asignación de enlaces	Todas las dependencias
	Identificación de activos	Socialización de metodología de levantamiento de activos	mar-26	jul-26	Registros de asistencia y grabación de reuniones	Oficina de TIC
	Identificación de activos	Mesas de trabajo levantamiento de inventario de activos	mar-26	jul-26	Registros de asistencia y grabación de reuniones	Oficina de TIC
	Identificación de activos	Radicación de memorando con activos de información identificados	mar-26	jul-26	Memorando con inventario de activos	Todas las dependencias
	Identificación de activos	Presentación final de inventario de activos a CIGD	mar-26	jul-26	Documento inventario de activos	Oficina de TIC

N°	Actividad	Tarea	Fecha de inicio	Fecha de finalización	Entregable	Responsable
	Identificación de activos	Aprobación de inventario activos de información	mar-26	jul-26	Acta en CIGD aprobando inventario de activos	CIGD
2	Identificación y evaluación de riesgos	Realizar mesas de trabajo para identificación de riesgos asociados a los activos de información identificados	ago-26	nov-26	Registros de asistencia y grabación de reuniones	Todas las dependencias
	Identificación y evaluación de riesgos	Levantamiento de matriz de riesgos de información	ago-26	nov-26	Matriz de riesgos identificados	Oficina de TIC
	Identificación y evaluación de riesgos	Validar los riesgos identificados y los responsables con el equipo de gestión	ago-26	nov-26	Matriz de riesgos identificados	Oficina de TIC
	Identificación y evaluación de riesgos	Clasificar los riesgos según probabilidad e impacto	ago-26	nov-26	Matriz de riesgos identificados	Oficina de TIC
3	Implementación de estrategias	Iniciar la mitigación de riesgos identificados	sep-26	nov-26	Documento donde se establezcan las estrategias para la mitigación de riesgos	Oficina de TIC
4	Monitoreo y seguimiento	Realizar revisiones periódicas del progreso de las estrategias de tratamiento	sep-26	nov-26	Acta de revisión de los controles implementados y/o de la necesidad de implementar controles más efectivos	Oficina de TIC
	Monitoreo y seguimiento	Evaluar si los riesgos tratados están bajo control	sep-26	nov-26	Acta de revisión de los controles implementados y/o de la necesidad de implementar controles más efectivos	Oficina de TIC
	Monitoreo y seguimiento	Ajustar el plan de tratamiento en caso de nuevos riesgos o fallos	sep-26	nov-26	Acta de revisión de los controles implementados y/o de la necesidad de	Oficina de TIC

N°	Actividad	Tarea	Fecha de inicio	Fecha de finalización	Entregable	Responsable
					implementar controles más efectivos	
5	Revisión y evaluación final	Evaluar la efectividad de las estrategias implementadas	sep-26	nov-26	Matriz de riesgos residuales	Oficina de TIC
	Revisión y evaluación final	Generar un informe final para las partes interesadas	sep-26	nov-26	Matriz de riesgos residuales	Oficina de TIC

8.1. Monitoreo y Revisión a la Administración de Riesgos.

El monitoreo y revisión de los riesgos y controles estará a cargo de los líderes de proceso, responsables de activos de información y demás servidores o contratistas que participen en la gestión del riesgo, en el marco de la primera línea de defensa. Su propósito es verificar la efectividad de los controles implementados, identificar cambios en el contexto interno o externo y promover las acciones de mejora que se requieran para una adecuada gestión de los riesgos.

El seguimiento a los riesgos se realizará de acuerdo con la periodicidad definida por la entidad para el reporte y revisión de riesgos. No obstante, cuando se presenten cambios significativos en los procesos, la tecnología, la normatividad o el contexto institucional, los riesgos y controles podrán ser revisados y actualizados en cualquier momento.

8.2. Seguimiento y Evaluación Independiente

La Oficina de Control Interno, como tercera línea de defensa, realizará evaluaciones independientes sobre la gestión de riesgos y la efectividad de los controles, de acuerdo con su plan de auditoría y la normatividad vigente, promoviendo la mejora continua de la gestión institucional.

9. DOCUMENTOS INTERNOS ASOCIADOS

TIPO DE DOCUMENTO	NOMBRE DEL DOCUMENTO
Política	**PL-DES-001** POLÍTICA PARA LA GESTIÓN INTEGRAL DEL RIESGO
Formato	Guía para la Administración del Riesgo y el Diseño de Controles en Entidades Públicas – Versión 6 DAFP

10. PRODUCTO O SERVICIO GENERADO

Producto / Servicio Generado	Descripción del Producto / Servicio
Power Bi	Tablero de Power BI para la visualización, seguimiento y análisis de los riesgos institucionales, controles y planes de tratamiento definidos por la entidad.

11. CONTROL DE DOCUMENTOS

Versión	Fecha de aprobación	Descripción de la modificación
1	29/01/2026	Creación del documento
2	26/06/2026	Actualización de formato, adaptación a política de riesgos institucional, cambio de metodología y actualización de cronograma

ELABORÓ	Brahiam Alirio Cruz Aleman	Contratistas	Oficina de las Tecnologías de la Información y las comunicaciones
REVISÓ	Silvana Lorena Chaves Patiño	Contratista	Oficina Asesora de Planeación Institucional
APROBÓ	LILIANA MORALES	Jefe	Oficina de las Tecnologías de la Información y las comunicaciones
FECHA DE APROBACIÓN	***COMITÉ INSTITUCIONAL DE GESTIÓN Y DESEMPEÑO*** 26-06-2026		