Region Metropolitana

POLÍTICA DE SEGURIDAD DIGITAL, PRIVACIDAD DE LA INFORMACIÓN Y DE DATOS PERSONALES

Fecha de aprobación: Diligencie la fecha de la aprobación - 31 de enero del 2025

ANTECEDENTES

De acuerdo con el artículo 2 de la Ley 2199 de 2022, la finalidad de la Región Metropolitana Bogotá-Cundinamarca es garantizar la formulación y ejecución de políticas públicas, planes, programas y proyectos de desarrollo sostenible, así como la prestación oportuna y eficiente de los servicios a su cargo, promoviendo el desarrollo armónico, la equidad, el cierre de brechas entre los territorios y la ejecución de obras de interés regional.

En virtud de lo dispuesto en el artículo 3 de la Ley 2199 de 2022, la Región Metropolitana Bogotá-Cundinamarca es una entidad administrativa de asociatividad regional con régimen especial, dotada de personería jurídica de derecho público, autonomía administrativa y patrimonio propio, a través de la cual las entidades territoriales que la integran concurren en el ejercido de las competencias que les corresponden, con el fin de hacer eficaces los principios constitucionales de coordinación, concurrencia, complementariedad y subsidiariedad en la función administrativa y en la planeación del desarrollo, dada su interdependencia geográfica, ambiental, social o económica.

Conforme al artículo 5 de la Ley 2199 de 2022 dentro de los principios que rigen el funcionamiento de la Región Metropolitana se encuentran los principios de gradualidad y economía y buen gobierno contemplados en los numerales 6 y 7 del artículo 5 de la Ley 2199 de 2022. La Región Metropolitana asumirá sus funciones y competencias de manera gradual, teniendo en cuenta su capacidad técnica y financiera y promoverá la autosostenibilidad económica, el saneamiento fiscal, la racionalización, la optimización del gasto público y el buen gobierno en su conformación y funcionamiento.

La RMBC como entidad del estado es sujeto obligado en el cumplimiento de la normatividad aplicable en materia de seguridad de la información y Protección de datos Personales, por lo anterior se encuentra adelantando la documentación y posterior implementación de políticas y procedimientos que permitan dar cumplimiento a dicha normatividad.

OBJETIVO

Establecer las directrices y medidas necesarias para asegurar la protección de la información digital y física, y los datos personales en la RMBC, garantizando la confidencialidad, integridad y disponibilidad de la información, y cumpliendo con las normativas legales y regulatorias aplicables.

ALCANCE

Esta política se aplica a toda la información gestionada, almacenada y procesada por la organización, incluyendo datos personales, y abarca a todos los empleados, contratistas, proveedores, y terceros que acceden a los sistemas, procesos y activos de información de la Región Metropolitana Bogotá - Cundinamarca.

DECLARACIÓN DE COMPROMISOS

Cumplimiento de la Normatividad Legal: La RMBC se compromete a cumplir con todas las leyes y regulaciones aplicables relacionadas con la seguridad de la información y la protección de los datos personales, incluyendo la **Ley 1581 de 2012** (Ley de Protección de Datos Personales), el **Decreto 1377 de 2013**, la **Ley 1266 de 2008**, la **Resolución 3100 de 2015**, y cualquier otra normativa relacionada con la protección de datos.

Confidencialidad de la Información: La RMBC se compromete a mantener la confidencialidad de la información sensible, asegurando que solo las personas autorizadas tengan acceso a la misma, de acuerdo con sus funciones y responsabilidades dentro de la organización.

Protección de Datos Personales: La RMBC se compromete a garantizar la protección de los datos personales que tratamos, adoptando las medidas necesarias para prevenir su uso indebido, acceso no autorizado, alteración, divulgación o destrucción de la misma. Esto incluye la recolección, almacenamiento, procesamiento, transmisión y eliminación de datos personales.

Implementación de Controles de Seguridad: La RMBC se compromete a implementar controles adecuados de seguridad, tanto tecnológicos como organizacionales, para proteger la información y los datos personales de posibles riesgos, amenazas y vulnerabilidades. Esto incluye el uso de tecnologías de encriptación, firewalls, acceso controlado y auditorías periódicas.

Derechos de los Titulares de Datos Personales: La RMBC se compromete a respetar los derechos de los titulares de los datos personales, permitiéndoles acceder, corregir, actualizar o solicitar la eliminación de sus datos cuando así lo deseen, conforme a lo establecido en la Ley 1581 de 2012 y demás normativas relacionadas.

Capacitación y Concienciación: La RMBC se compromete a realizar actividades continuas de capacitación y sensibilización sobre seguridad de la información y protección de datos personales para todos los empleados, proveedores y terceros, con el fin de garantizar el cumplimiento efectivo de esta política en todas las áreas de la organización.

Transparencia en el Tratamiento de Datos: La RMBC se compromete a garantizar que nuestros procesos de tratamiento de datos sean transparentes, permitiendo que los titulares de los datos personales sean informados sobre el propósito y la finalidad para la cual se recogen sus datos, así como sobre sus derechos conforme a la legislación vigente.

Gestión de Incidentes de Seguridad: La RMBC se compromete a establecer procedimientos claros para la identificación, reporte y gestión de incidentes de seguridad que puedan afectar la confidencialidad, integridad o disponibilidad de la información y los datos personales, así como a actuar de manera rápida y eficaz para mitigar cualquier impacto negativo.

Mejora Continua: La RMBC se compromete establecer un proceso de revisión continua y mejora de nuestras prácticas de seguridad de la información y protección de datos personales, a fin de adaptarnos a los cambios tecnológicos, legales y de negocio, y garantizar que nuestros controles sigan siendo eficaces y adecuados.

Responsabilidad de la Alta Dirección: La alta dirección de **RMBC** se compromete a proporcionar los recursos necesarios y a liderar el cumplimiento de la Política de Seguridad de la Información y Protección de Datos Personales, fomentando una cultura organizacional de respeto por la seguridad de la información y el tratamiento adecuado de los datos personales.

Compromiso de los Empleados y Colaboradores:

Los empleados, contratistas y terceros de **RMBC** se comprometen a cumplir con las disposiciones establecidas en esta política, actuando con responsabilidad, diligencia y cuidado en el manejo de la información y los datos personales. Cualquier violación a esta política será considerada una infracción grave y estará sujeta a medidas disciplinarias conforme a la normativa interna de la empresa.

MODELO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN (MSPI)

GESTIÓN DE ACCESOS

Control de Acceso
El acceso a la información debe ser concedido con base en el principio de "mínimo privilegio", donde los usuarios solo tendrán acceso a la información necesaria para realizar sus funciones.
Autenticación
Se utilizarán métodos de autenticación robustos, como contraseñas seguras y, cuando sea posible, autenticación multifactor (MFA).
Gestión de Identidades: Se llevará un registro detallado de las identidades y roles de los usuarios, con acceso revisado periódicamente.

PROTECCIÓN DE LA INFORMACIÓN

Clasificación de la Información
La información debe ser clasificada según su nivel de sensibilidad: Confidencial, Restringido, Interno y Uso Público.
Cifrado: Todos los datos sensibles, incluyendo los datos personales, deben ser cifrados tanto en tránsito como en reposo utilizando algoritmos de cifrado robustos.
Seguridad de la Red: Implementar medidas de seguridad perimetral, como firewalls y sistemas de detección y prevención de intrusiones (IDS/IPS), para proteger la infraestructura de red de la organización.
Copias de Seguridad
Realizarán copias de seguridad periódicas de la información crítica, que serán almacenadas en ubicaciones seguras y probadas regularmente para su recuperación en caso de incidentes o pérdida de información.

MANEJO DE INCIDENTES DE SEGURIDAD

Detección y Notificación
Todos los incidentes relacionados con la seguridad de la información, incluyendo brechas de datos personales, deben ser detectados y reportados de inmediato al equipo de seguridad.

Respuesta ante Incidentes: Establecer y aplicar procedimientos para la respuesta ante incidentes, que incluyen la contención, erradicación, recuperación y comunicación de los mismos.

Reporte de Incidentes

Todo incidente de seguridad debe ser reportado inmediatamente a la Oficina de TIC a través de los canales establecidos institucionalmente (mesa de servicios, Chat, correo electrónico).

Investigación y Remediación

La Oficina de TIC debe realizar un análisis detallado para identificar las causas raíz, implementar medidas correctivas y evitar recurrencias.

CONCIENTIZACIÓN Y CUMPLIMIENTO

Sensibilización Continua: Proporcionar mecanismos de sensibilización periódica sobre seguridad de la información y protección de datos personales a todos los empleados y colaboradores de la RMBC, así como a los terceros que deban conocer y acatar esta política.

Concientización

Promover una cultura de seguridad de la información mediante campañas de concienciación y la difusión de materiales informativos.

Cumplimiento Normativo: La RMBC velará por el cumplimiento con todas las leyes y normativas aplicables sobre protección de datos personales y seguridad de la información.

El incumplimiento de esta política será causal de sanciones disciplinarias según las normas aplicables y procedimientos internos de la RMBC.

REVISIÓN Y MEJORA CONTINUA

Evaluación Periódica: La política será revisada al menos una vez al año, o cuando ocurran cambios significativos en la organización o en las regulaciones aplicables.

Mejora Continua: La RMBC, basándose en los resultados de las auditorías, incidentes y cambios en el entorno de amenazas, se revisarán y actualizarán los controles de seguridad, políticas y procedimientos para mejorar la protección de la información.

Aprobación y Comunicación: Esta política debe ser aprobada por la alta dirección y comunicada a todos los empleados, contratistas y terceros para garantizar su comprensión y cumplimiento.

RESPONSABLES

Alta Dirección: Es responsable de establecer y promover la cultura de seguridad de la información, asegurando los recursos y apoyando las iniciativas de protección de datos.

Oficina de TIC

- Aseguran la implementación de medidas tecnológicas adecuadas para proteger los sistemas, redes y datos.
- Definir y mantener actualizadas las políticas de seguridad.
- Proporcionar las herramientas necesarias para la protección de la información.
- Realizar auditorías y revisiones periódicas de seguridad.

Responsables de Seguridad de la Información: Supervisan la implementación y el mantenimiento de las políticas de seguridad de la información, coordinando las acciones de protección de la información y datos personales.

Funcionarios y Contratistas

- Cumplir con las políticas de seguridad establecidas.
- Reportar cualquier incidente o vulnerabilidad de seguridad a la Oficina de TIC.
- Proteger las credenciales de acceso y no compartirlas con terceros no autorizados.

Terceros Autorizados

Asegurar el cumplimiento de las políticas de seguridad durante el manejo de información y datos personales de la entidad a que tenga acceso.

DEFINICIONES

- **Autenticación y No Repudio:** Implementar mecanismos de autenticación para asegurar la identidad de los usuarios y garantizar que no puedan negar sus acciones.
- **Confidencialidad:** Propiedad de la información de no ponerse a disposición o ser revelada a individuos, entidades o procesos no autorizados.
- **Disponibilidad:** Propiedad de la información de estar accesible y utilizable cuando lo requiera una entidad autorizada.
- **Integridad:** Propiedad de la información relativa a su exactitud y completitud.
- **Protección de Datos Personales:** Cumplir con las leyes y regulaciones de protección de datos personales Ley 1581 de 2012, y el Decreto 1377 de 2013, Ley 1266 de 2008, Norma ISO/IEC 27001 y las demás regulaciones aplicables, garantizando que los datos personales sean manejados de manera legal, ética y segura

DOCUMENTOS DE REFERENCIA

- **Ley 1581 de 2012:** Ley de Protección de Datos Personales en Colombia. https://www.funcionpublica.gov.co/documents/418537/0/Ley+1581+de+2012.pdf
- **Decreto 1377 de 2013:** Por el cual se reglamenta parcialmente la Ley 1581 de 2012. https://dapre.presidencia.gov.co/normativa/normativa/DECRETO%201377%20DEL%202013.pdf
- **Norma ISO/IEC 27001:** Tecnología de la información - Técnicas de seguridad - Sistemas de gestión de la seguridad de la información - Requisitos. https://www.iso.org/isoiec-27001-information-security.html
- **Guía de Seguridad de la Información de MinTIC:** Lineamientos y buenas prácticas para la gestión de seguridad de la información en entidades públicas. https://www.mintic.gov.co/portal/604/articles-55864_Guia_de_Seguridad.pdf

CONTROL DE DOCUMENTOS

Versión	Fecha de aprobación	Descripción de la modificación
1	31/01/2025	Creación del documento

ELABORÓ	Rosa Edilma López	Contratista	OTIC
REVISÓ TECNICAMENTE	Diego Urbano	Jefe OTIC	OTIC
REVISÓ METODOLÓGICAMENTE	Silvana Chaves	Contratista	OAPI