Resolución No. 065
(04 de marzo de 2025)

"Por medio de la cual se adopta la Política de Seguridad Digital, Privacidad de la Información y de Datos Personales de la Región Metropolitana Bogotá – Cundinamarca"

EL DIRECTOR DE LA REGIÓN METROPOLITANA BOGOTÁ – CUNDINAMARCA

En ejercicio de las facultades constitucionales y legales, en especial las conferidas en los artículos 209, 211 y 269 de la Constitución Política de Colombia, el artículo 9 de la Ley 489 de 1998 y los Acuerdos Regionales 001 y 003 de 2022, y

CONSIDERANDO:

Que la Constitución Política Colombiana en su artículo 15 consagra *"Todas las personas tienen derecho a su intimidad personal y familiar y a su buen nombre, y el Estado debe respetarlos y hacerlos respetar. De igual modo, tienen derecho a conocer, actualizar y rectificar las informaciones que se hayan recogido sobre ellas en bancos de datos y en archivos de entidades públicas y privadas.*

Que el artículo 74 de la Carta Política preceptúa que *"Todas las personas tienen derecho a acceder a los documentos públicos salvo los casos que establezca la Ley. El secreto profesional es inviolable."*

Que el artículo 209 ídem establece que la función administrativa está al servicio de los intereses generales y se desarrolla con fundamento en los principios de igualdad, moralidad, eficacia, economía, celeridad, imparcialidad y publicidad, mediante la descentralización, la delegación y la desconcentración de funciones.

Que en su artículo 269 ibidem señala que, *"En las entidades públicas, las autoridades correspondientes están obligadas a diseñar y aplicar, según la naturaleza de sus funciones, métodos y procedimientos de control interno, de conformidad con lo que disponga la ley, la cual podrá establecer excepciones y autorizar la contratación de dichos servicios con empresas privadas colombianas."*

Que la Ley 1273 de 2009 crea un nuevo bien jurídico tutelado denominado *"de la protección de la información y de los datos"*, estableciendo las conductas punibles que atentan contra dicho bien jurídico, entre las cuales se encuentran, acceso

abusivo a un sistema informático, obstaculización ilegítima de sistema informático o red de comunicación, interceptación de datos informáticos, daño informático, uso de software malicioso, violación de datos personales, suplantación de sitios web para capturar datos personales, entre otros.

Que la Ley Estatutaria 1581 de 2012, por la cual se dictan disposiciones generales para la protección de datos personales, tiene como objeto *"(…) desarrollar el derecho constitucional que tienen todas las personas a conocer, actualizar y rectificar las informaciones que se hayan recogido sobre ellas en bases de datos o archivos, y los demás derechos, libertades y garantías constitucionales"*, estableciendo, además, las disposiciones generales para la protección de datos personales.

Que la Norma ISO 27001:2013 es la norma estándar para la seguridad de la información expedida por la Organización Internacional de Normalización.

Que la Ley Estatutaria 1712 de 2014, Ley de Transparencia y del Derecho de Acceso a la Información Pública, tiene por objeto adoptar disposiciones tendientes a prevenir los actos de corrupción, a reforzar la articulación y coordinación de las entidades del Estado y a recuperar los daños ocasionados por dichos actos con el fin de asegurar promover la cultura de la legalidad e integridad y recuperar la confianza ciudadana y el respeto por lo público.

Que el Decreto 2573 de 2014 define los lineamientos, instrumentos y plazos de la estrategia de Gobierno en Línea, especialmente en temas de seguridad, privacidad, gestión de tecnologías de información e interoperabilidad.

Que el Decreto 1078 de 2015 dispone que las entidades que conforman la administración pública serán sujetos obligados para el cumplimiento de las políticas y los lineamientos de la Estrategia de Gobierno en Línea, estableciendo en su artículo 2.2.9.1.2.1 como uno de sus cuatro componentes, el habilitador de la Seguridad y privacidad de la Información, comprendido por las acciones transversales a los componentes de TIC para Servicios, TIC para el Gobierno Abierto y TIC para la Gestión, tendientes a proteger la información y sistemas de información, del acceso, divulgación, interrupción o destrucción no autorizada.

Resolución No. 065
(04 de marzo de 2025)

"Por medio de la cual se adopta la Política de Seguridad Digital, Privacidad de la Información y de Datos Personales de la Región Metropolitana Bogotá – Cundinamarca"

Que el Decreto 103 de 2015 compilado en el Decreto Único Reglamentario 1081 de 2015, reglamenta parcialmente la ley de transparencia y el derecho de acceso a la información pública.

Que el Decreto 1499 de 2017 *"Por medio del cual se modifica el Decreto 1083 de 2015, Decreto Único Reglamentario del Sector Función Pública, en lo relacionado con el Sistema de Gestión establecido en el artículo 133 de la Ley 1753 de 2015"*, sentó las bases del nuevo Sistema Integrado de Gestión, estableció el Modelo Integrado de Planeación y de Gestión para implementar dicho sistema, e hizo énfasis en que dentro de las políticas de gestión y de desempeño institucional se encuentran, según el artículo 2.2.22.2.1 del Decreto 1083 de 2015, numerales 11 y 12, las Políticas de Gobierno Digital y de Seguridad Digital, con las cuales debe alinearse la Política de Seguridad y Privacidad de la Información de la Región Metropolitana Bogotá - Cundinamarca.

Que mediante el Decreto 1008 de 2018, que modificó el Decreto 1078 de 2015, antes mencionado, se establecen *"(…) lineamientos generales de la Política de Gobierno Digital para Colombia, antes estrategia de Gobierno en Línea, la cual desde ahora debe ser entendida como: el uso y aprovechamiento de las tecnologías de la información y las comunicaciones para consolidar un Estado y ciudadanos competitivos, proactivos, e innovadores, que generen valor público en un entorno de confianza digital."*.

Que la Resolución 5569 del 11 de diciembre de 2018 de la Comisión de Regulación de Comunicaciones *"Por la cual se modifica el artículo 5.1.2.3 del Capítulo 1 del Título V de la Resolución CRC 5050 de 2016 en materia de gestión de seguridad en redes de telecomunicaciones y se dictan otras disposiciones"*, consagra en el artículo 1º de definiciones, el término *"Incidente de seguridad de la información: un evento o serie de eventos de seguridad de la información no deseados o inesperados, que tienen una probabilidad significativa de comprometer las operaciones del negocio y amenazar la seguridad de la información*".

Que en el artículo 2º ídem, referente a la Gestión de Seguridad en Redes de Telecomunicaciones, subnumeral 5.1.2.3.1. Políticas de seguridad de la información, define las categorías de los incidentes, así: a) Denegación de servicio,

b) Acceso no autorizado, c) Malware (software malintencionado), d) Abuso y e) Recopilación de información de sistema.

Que mediante el Documento CONPES 3854 de 2016 *"POLÍTICA NACIONAL DE SEGURIDAD DIGITAL"* se establecen los lineamientos y directrices de seguridad digital, incluyendo componentes tales como la gobernanza, educación, la regulación, la cooperación internacional y nacional, la investigación, el desarrollo y la innovación. Que el Decreto 620 de 2020, establece los lineamientos generales en el uso y operación de los servicios ciudadanos digitales" indicando,

> *"ARTÍCULO 2.2.17.5.6. Seguridad de la información y Seguridad Digital. Los actores que traten información en el marco del presente título deberán contar con una estrategia de seguridad y privacidad de la información, seguridad digital y continuidad de la prestación del servicio en la cual, deberán hacer periódicamente una evaluación del riesgo de seguridad digital, que incluya una identificación de las mejoras a implementar en su Sistema de Administración del Riesgo Operativo. Para lo anterior, deben contar con normas, políticas, procedimientos, recursos técnicos, administrativos y humanos necesarios para gestionar efectivamente el riesgo. En ese sentido, deben adoptar los lineamientos para la gestión de la seguridad de la información y seguridad digital que emita el Ministerio de Tecnologías de la Información y las Comunicaciones".*

Que mediante Documento CONPES 3995 de 2020 - "POLÍTICA NACIONAL DE CONFIANZA Y SEGURIDAD DIGITAL" la cual formula una política nacional que tiene como objetivo, establecer medidas para ampliar la confianza digital y mejorar la seguridad digital de manera que Colombia sea una sociedad incluyente y competitiva en el futuro digital, y estableciendo medidas para desarrollar la confianza digital a través de la mejora de la seguridad digital de manera que Colombia sea una sociedad incluyente y competitiva en el futuro digital mediante el fortalecimiento de capacidades y la actualización del marco de gobernanza en seguridad digital, así como con la adopción de modelos con énfasis en nuevas tecnologías.

Resolución No. 065
(04 de marzo de 2025)

"Por medio de la cual se adopta la Política de Seguridad Digital, Privacidad de la Información y de Datos Personales de la Región Metropolitana Bogotá – Cundinamarca"

Que, a través del Acto Legislativo 02 del 22 de julio de 2020, que modificó el artículo 325 de la Constitución Política, se creó la Región Metropolitana Bogotá-Cundinamarca, reglamentada por la Ley 2199 del 2022.

Que, 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 ejercicio 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.

Que el artículo 22 de la Ley 2199 del 2022 señala que 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.

Que el numeral 6 del artículo 27 de la Ley 2199 de 2022, estableció que dentro de las funciones del Director de la Región Metropolitana, se encuentra dirigir la acción administrativa de la Región Metropolitana, con sujeción a la Constitución Política, la ley y los Acuerdos Regionales, y expedir los correspondientes actos administrativos.

Que la Región Metropolitana Bogotá – Cundinamarca RMBC, recolecta, procesa, modifica, almacena y transfiere información en formato físico y digital. Esta información es un activo fundamental para el cumplimiento de la misión de la Entidad y proviene de diversas fuentes como funcionarios, contratistas, proveedores y entidades públicas y privadas; por lo cual la gestión de dicha información requiere un manejo responsable y seguro, que permita realizar un buen uso de esta y mitigar los riesgos sobre su confidencialidad, disponibilidad e integridad.

Resolución No. 065
(04 de marzo de 2025)

"Por medio de la cual se adopta la Política de Seguridad Digital, Privacidad de la Información y de Datos Personales de la Región Metropolitana Bogotá – Cundinamarca"

Que la Política de Seguridad y Privacidad de la Información, es la declaración donde se establece el compromiso y el enfoque de la Región Metropolitana Bogotá – Cundinamarca RMBC, respecto a la gestión de la seguridad y privacidad de la información, indicando las responsabilidades y la conducta aceptada para funcionarios, contratistas, proveedores y terceros que debido al cumplimiento de sus funciones u obligaciones tienen acceso a la información de la entidad.

Que Política de Seguridad Digital, Privacidad de la Información y de Datos Personales de la Región Metropolitana Bogotá – Cundinamarca fue adoptada en sesión del 31 de enero de 2025 del Comité Institucional de Gestión y Desempeño de la RMBC.

Con fundamento en lo expuesto, se hace necesario adoptar la Política de Seguridad Digital, Privacidad de la Información y de Datos Personales de la Región Metropolitana Bogotá – Cundinamarca RMBC.

En mérito de lo expuesto,

RESUELVE:

Artículo 1. Adopción. Adoptar Política de Seguridad Digital, Privacidad de la Información y de Datos Personales de la Región Metropolitana Bogotá – Cundinamarca, la cual hace parte integral de este documento.

Artículo 2. Ámbito de Aplicación y alcance. La Política de Seguridad Digital, Privacidad de la Información y de Datos Personales aplica a todos los niveles de la Región Metropolitana Bogotá – Cundinamarca, a todos sus funcionarios, contratistas, proveedores, operadores, entes de control, terceros y ciudadanía en general que compartan, utilicen, recolecten, procesen, intercambien o consulten su información de forma interna o externa, independientemente de su ubicación.
De igual forma, esta política aplica a toda la información creada, procesada o utilizada por la Entidad, sin importar el medio, formato, presentación o lugar en la

cual se encuentre, a todos los recursos y activos de información de la Entidad; los procesos y procedimientos de la Entidad; y a toda la infraestructura tecnológica y sistemas de información que soportan la misionalidad de la Entidad;

Artículo 3. Componentes de la Política. La Política de Seguridad Digital, Privacidad de la Información y de Datos Personales está conformada por estándares técnicos de seguridad aplicables en los procesos, procedimientos, estructura organizacional, mecanismos de verificación y control, infraestructura tecnológica para garantizar espacios digitales seguros, con una gestión documentada, sistemática, estructurada, eficiente y adaptable a los cambios que se produzcan en los riesgos, el entorno y las tecnologías.

Artículo 4. Gestión Integral de Riesgos de seguridad digital. La Región Metropolitana Bogotá Cundinamarca preservará la confidencialidad, integridad, disponibilidad y privacidad de sus activos de información, realizando sobre estos una gestión integral de los riesgos de seguridad digital con el fin de mitigar su impacto, en un proceso de mejora continua, para lo cual implementará los controles necesarios, que son de estricto cumplimiento para todos los funcionarios, contratistas y terceros que en el cumplimiento de sus funciones u obligaciones accedan a los activos de información de la Entidad. De igual manera implementará los controles sobre los activos de información que son accedidos por la ciudadanía, la cual deberá darles cumplimiento a los lineamientos establecidos.

Artículo 5. Revisión de la Política. La Región Metropolitana Bogotá Cundinamarca revisará la Política de Seguridad Digital, Privacidad de la Información y de Datos Personales y las políticas detalladas derivadas con una periodicidad mínima anual o cuando se considere pertinente por cambios normativos, necesidades del servicio o riesgos de seguridad detectados que así lo ameriten.

Artículo 6. Comunicación. Comunicar la Política de Seguridad Digital, Privacidad de la Información y de Datos Personales a todos los servidores y contratistas de la Región Metropolitana Bogotá Cundinamarca, así como a los grupos de valor, de interés y ciudadanía en general mediante su publicación en la página web de la Entidad.

Resolución No. 065
(04 de marzo de 2025)

"Por medio de la cual se adopta la Política de Seguridad Digital, Privacidad de la Información y de Datos Personales de la Región Metropolitana Bogotá – Cundinamarca"

Artículo 7. Publicación y Vigencia. El presente acto administrativo rige a partir de la fecha de su publicación en la página web, el registro distrital y la gaceta de Cundinamarca, de conformidad con lo establecido en el art. 44 del Acuerdo regional 001 de 2022 y deroga las disposiciones que le sean contrarias.

COMUNÍQUESE Y CÚMPLASE.

Dada en Bogotá D.C., a los cuatro (04) días del mes de marzo del año dos mil veinticinco (2025)

LOTA LUIS FELIPE
Firmado digitalmente por LOTA LUIS FELIPE

LUIS FELIPE LOTA
Director

ROL	NOMBRES Y APELLIDOS	CARGO	Firma
Revisó / Aprobó	Diego Fernando Urbano Chaves	Jefe Oficina de TIC	
	Clara Inés Márquez Vásquez	Jefe Oficina Jurídica	
	Angélica Ma. Avendaño Ortegón	Asesora de la Dirección General	
	Rosa Edilma López	Contratista	
Proyectó	José Manuel Sánchez Jaramillo	Profesional Universitario	

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