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

VIGENCIA 2026

TABLA DE CONTENIDO

SIGLAS

ISO: International Standard Organization.

MINTIC: Ministerio de Tecnología de la Información y las Comunicaciones.

MOP: Modelo de operación por procesos.

MSPI: Modelo de Seguridad y Privacidad de la Información.

SGSI: Sistema de Gestión de Seguridad de la Información.

TI: Tecnología de información.

TIC: Tecnologías de la información y la comunicación.

NORMOGRAMA

Ley 909 de 2004: "Por la cual se expiden normas que regulan el empleo público, la carrera administrativa, gerencia pública y se dictan otras disposiciones".

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 y se dictan otras disposiciones".

Decreto Municipal 500 de 2013: "Por el cual se aprueba la misión, visión, valores, principios orientadores de la función pública y el modelo institucional de la Administración Central del Municipio de Medellín y se dictan otras disposiciones".

Decreto Ministerial 1078 de 2015: "Por medio del cual se expide el Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones".

Decreto Presidencial 1083 de 2015: "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".

Decreto Municipal 883 de 2015: "Por el cual se adecúa la Estructura de la Administración Municipal de Medellín, las funciones de sus organismos, dependencias y entidades descentralizadas, se modifican unas entidades descentralizadas y se dictan otras disposiciones".

Decreto Presidencial 612 de 2018: "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 Municipal 0863 de 2020: "Por el cual se modifica la estructura orgánica y funcional del nivel central del Municipio de Medellín".

Decreto Presidencial 767 de 2022: "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".

Resolución Ministerial 00500 de 2021: "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".

ISO/IEC 27001:2013: Tecnología de la información-Técnicas de seguridad-

CONTEXTO

A partir del Decreto Distrital 863 de 2020, "Por el cual se modifica la estructura orgánica y funcional del nivel central del Municipio de Medellín", el cual estipula en el artículo 41 lo siguiente:
Adición al artículo al Decreto 883 de 2015, el cual quedará así:
"ARTÍCULO 333A. SECRETARÍA DE INNOVACIÓN DIGITAL:
Es una dependencia del nivel central, que tendrá como responsabilidad satisfacer las necesidades de servicios de tecnologías de la información a los diferentes grupos de valor y de interés, a través de Servicios Digitales, procesos eficientes, flujos de datos e información, y transformación digital del territorio, basados en la innovación y en una gestión enfocada en prácticas de arquitectura empresarial y la seguridad de la información."
Así mismo, en el artículo 333B del mismo Decreto señala las funciones de la Secretaría de Innovación Digital, en especial la contenida en el Núm. 7:

*"**Liderar la definición, implementación y mantenimiento del Sistema de Gestión de Seguridad de la Información** de la Alcaldía de Medellín acorde al marco específico y la estrategia de la entidad."*

La implementación del Sistema de Gestión de Seguridad de la Información surge en el contexto de lo expuesto en el Decreto Presidencial 1008 de 2018 referido a las obligaciones de los sujetos obligados en el artículo 2.2.9.1.1.2. para la implementación del habilitador de seguridad de la información, en atención a las orientaciones definidas en el Manual de Gobierno Digital, relacionadas con la adopción e implementación del Modelo de Seguridad y Privacidad de la Información, refrendadas y actualizadas a través del Decreto Presidencial 767 de 2022 en lo referente al habilitador de seguridad y privacidad de la información, el cual derogo el Decreto 1008 de 2018.

De igual manera es importante resaltar que es a través del Decreto Presidencial 612de 2018, 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", en su artículo 1, adiciona al Capítulo 3 del Título 22 de la Parte 2 del Libro 2 del Decreto Presidencial 1083 de 2015, Único Reglamentario del Sector de Función Pública, agregando al anterior Decreto el artículo 2.2.22.3.14, por medio del cual se integran los planes institucionales y estratégicos al Plan de Acción, considerando en su numeral 11 y 12 como obligación la elaboración anual del "Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información" y del "Plan de Seguridad y Privacidad de la Información" respectivamente de cada Entidad, y lo señalado en la Ley 1474 de 2011 por la cual se dictan normas orientadas a fortalecer los mecanismos de prevención, investigación y sanción de actos de corrupción y la efectividad del control de la gestión pública, señala en su artículo 74 denominado "Plan de acción de las entidades públicas", indicando que a partir de la vigencia de la presente Ley, todas las entidades del Estado a más tardar el 31 de enero de cada año, deberán publicar en su respectiva página web el Plan de Acción para el año siguiente".

Coherente con lo anterior, la Secretaría de Innovación Digital ha venido adelantando acciones en toda la entidad encaminadas a fortalecer las capacidades institucionales para dar cumplimiento a las disposiciones legales vigentes en materia de seguridad y privacidad de la información, atendiendo las orientaciones del Ministerio de Tecnologías de Información contenidas en la Resolución Ministerial0500 de 2021 y sus dos respectivos anexos.

INTRODUCCIÓN

En Colombia, la Política de Gobierno Digital se desarrolla conforme a los lineamientos definidos por la Presidencia de la República y el Ministerio de Tecnologías de la Información y las Comunicaciones (MinTIC), particularmente a través del Decreto 767 de 2022, el cual se encuentra incorporado en el Decreto Único Reglamentario del Sector TIC (Decreto 1078 de 2015), en el capítulo 1, título 9, parte 2, libro 2. Esta política constituye un pilar fundamental para el fortalecimiento de la gestión pública, al promover una relación más eficiente, transparente y cercana entre el Estado y la ciudadanía, en coherencia con el Modelo Integrado de Planeación y Gestión (MIPG). Dicho modelo orienta a las entidades públicas hacia el cumplimiento de objetivos estratégicos y políticas de desarrollo administrativo que aportan al mejor desempeño institucional.

El Manual de la Política de Gobierno Digital, emitido por el MinTIC, tiene como finalidad impulsar el uso estratégico de las tecnologías de la información y las comunicaciones (TIC) en el sector público, con el propósito de consolidar un Estado moderno y una ciudadanía más competitiva, participativa e innovadora, generando valor público dentro de un entorno basado en la confianza digital.

La implementación de esta política se estructura a partir de dos componentes principales: TIC para el Estado y TIC para la sociedad, los cuales se soportan en cuatro habilitadores transversales fundamentales:

- Arquitectura.
- Cultura y apropiación.
- Seguridad y privacidad de la información.
- Servicios ciudadanos digitales.

Estos componentes y habilitadores se desarrollan mediante lineamientos y estándares mínimos que deben ser adoptados por las entidades públicas, con el fin de garantizar el cumplimiento de los objetivos establecidos en la política.

En este marco, el habilitador de Seguridad y Privacidad de la Información tiene como propósito asegurar que las entidades públicas implementen medidas de protección en sus procesos, trámites, servicios, sistemas de información e infraestructura tecnológica, con el objetivo de salvaguardar la confidencialidad, integridad, disponibilidad y privacidad de la información.

De manera complementaria, el artículo 2.2.9.1.2.1 del Decreto 1078 de 2015 señala que la Política de Gobierno Digital debe articularse a través de elementos como la gobernanza, la innovación pública digital, los habilitadores, las líneas de acción y las iniciativas dinamizadoras. Dentro de este esquema, la Seguridad y Privacidad de la Información se reconoce como un aspecto transversal y esencial, que requiere el desarrollo de capacidades específicas y la adopción de lineamientos claros por parte de las entidades públicas.

El Modelo de Seguridad y Privacidad de la Información (MSPI), definido por el MinTIC, fortalece la implementación de esta política al establecer la obligación de gestionar los riesgos asociados a la información mediante prácticas orientadas a garantizar su confidencialidad, integridad y disponibilidad, incrementando así la confianza de las partes interesadas. Su adopción, implementación y evaluación son de carácter obligatorio, conforme a lo establecido en el artículo 2.2.9.1.3.2 del Decreto 767 de 2022.

Adicionalmente, el Decreto Presidencial 612 de 2018 establece directrices para la articulación de los planes institucionales y estratégicos con el Plan de Acción de las entidades del Estado, disponiendo, entre otros aspectos, la elaboración anual del Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información, así como del Plan de Seguridad y Privacidad de la Información.

En concordancia con lo anterior, la Resolución 0500 de 2021 del MinTIC define los lineamientos generales para la implementación del MSPI, resaltando la necesidad de adoptar medidas técnicas, administrativas y de gestión del talento humano que integren principios, políticas y procedimientos de seguridad digital dentro del Plan de Seguridad y Privacidad de la Información. Asimismo, enfatiza la importancia de realizar análisis de riesgos y de implementar controles adecuados para prevenir y mitigar incidentes de seguridad digital.

Finalmente, la adopción del MSPI en las entidades públicas se soporta en estándares internacionales como la NTC ISO/IEC 27001, así como en el marco normativo nacional establecido por la Ley 1712 de 2014 y la Ley 1581 de 2012. Estas disposiciones promueven un enfoque basado en la gestión del riesgo, facilitando la identificación, evaluación y tratamiento de los riesgos asociados a la seguridad y privacidad de la información, lo cual resulta fundamental para la toma de decisiones relacionadas con la implementación de controles y el diseño del Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información, en contribución al cumplimiento de los objetivos organizacionales del Distrito Especial de Ciencia, Tecnología e Innovación de Medellín.

OBJETIVO

Establecer un marco de actuación orientado al tratamiento de los riesgos asociados a la seguridad y privacidad de la información, con énfasis en los activos que soportan el logro de los objetivos institucionales. Dicho marco permitirá asegurar la confidencialidad, integridad y disponibilidad de la información institucional, considerando el contexto organizacional de la entidad, así como sus capacidades operativas y los recursos disponibles, con el propósito de fortalecer la confianza de ciudadanos, usuarios, aliados y demás partes interesadas.

La planeación se orientará al fortalecimiento de la ejecución de acciones específicas para el tratamiento de estos riesgos, en concordancia con los lineamientos definidos por el Ministerio de Tecnologías de la Información y las Comunicaciones (MinTIC) y el Departamento Administrativo de la Función Pública. Estas acciones estarán dirigidas a garantizar la protección de los activos de información del Distrito Especial de Ciencia, Tecnología e Innovación de Medellín a nivel central, como parte del cumplimiento de sus responsabilidades institucionales.

PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE ACTIVOS DE INFORMACIÓN POR CATEGORÍAS

De conformidad con lo establecido en la Guía para la Administración del Riesgo y el Diseño de Controles en Entidades Públicas, emitida por el Departamento Administrativo de la Función

Pública, el tratamiento de riesgos corresponde a la respuesta definida por la primera línea de defensa para mitigar los riesgos identificados. En este sentido, la presente planeación se enfoca en el tratamiento de los riesgos de Seguridad y Privacidad de la Información asociados a los activos de información bajo la responsabilidad del Distrito Especial de Ciencia, Tecnología e Innovación de Medellín a nivel central.

Para tal fin, durante la vigencia correspondiente se desarrollará un conjunto de actividades orientadas a la implementación de los controles de seguridad priorizados, de acuerdo con los resultados del análisis y valoración de riesgos. En atención a lo anterior, a continuación, se presentan las actividades más relevantes encaminadas al tratamiento de los riesgos de Seguridad y Privacidad de la Información.

Actividad	Responsable	1er Semestre 2026	2do Semestre 2026
Adquisición e implementación de controles de seguridad para mitigar riesgos identificados	Coordinador TI, Profesional de seguridad digital, Líder de comunicaciones	X	X
Seguimiento y monitoreo de la operación de controles implementados	Coordinador TI, Profesional de seguridad digital, Líder de comunicaciones	X	X
Evaluación y actualización de la identificación de riesgos y controles	Coordinador TI, Profesional de seguridad digital, Líder de comunicaciones	X	X
Capacitación y sensibilización en seguridad de la información a dependencias centrales	Secretaría de Innovación Digital	X	X
Revisión y actualización del Plan de Continuidad del Negocio	Coordinador TI, Profesional de seguridad digital		X

La ejecución de las actividades definidas estará condicionada a la disponibilidad de los recursos humanos, técnicos, tecnológicos y financieros necesarios para su desarrollo efectivo. Dichas acciones se implementarán en coherencia con la asignación presupuestal vigente, la capacidad institucional para la gestión y aceptación del riesgo, así como con los lineamientos y orientaciones establecidos por la alta dirección, responsable de definir los niveles de riesgo tolerables para la entidad.

Desde el proceso Gestión Sistemas de Información en articulación con la mesa de trabajo del Modelo de Seguridad y Privacidad de la Información – MSPI nos encargaremos de desarrollar acciones de sensibilización, capacitación y acompañamiento a las dependencias y sus áreas/procesos. Estas actividades se ejecutarán conforme a cronogramas previamente definidos y acordes con la planeación institucional.

Adicionalmente, desde el Plan de Acción Institucional se realiza el seguimiento continuo y el monitoreo del avance del plan de seguridad y privacidad de la información formulado. Este seguimiento permitirá verificar que las actividades asociadas a la elaboración, implementación y cumplimiento se desarrolle de manera oportuna, eficiente y alineada con los objetivos institucionales.