



|  |                            |  |
|--|----------------------------|--|
|  <p><b>Aldia de Medellín</b><br/>Distrito de<br/>Ciencia, Tecnología e Innovación</p> <p><b>SAPIENCIA</b><br/>Agencia de Educación<br/>Postsecundaria de Medellín</p> | <p>PROGRAMA ESPECÍFICO</p> | <p>Código: asignado por<br/>quien emite el documento<br/>(F-ES-GM-024)</p> <p>Versión: consecutivo en<br/>que va el documento<br/>(01)</p> |
| <p>NOMBRE DEL FORMATO<br/>(PLANTILLA ELABORACIÓN DE PROGRAMA ESPECÍFICO)</p>   |                            | <p>Página 1 de 16</p>  |

**DISTRITO ESPECIAL DE CIENCIA, TECNOLOGÍA E INNOVACIÓN DE MEDELLÍN**


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

**VIGENCIA 2025**

|   |                     |   |
|---|---------------------|---|
|  | PROGRAMA ESPECÍFICO | Código: asignado por quien emite el documento (F-ES-GM-024) |
|   |                     | Versión: consecutivo en que va el documento (01)            |
| NOMBRE DEL FORMATO (PLANTILLA ELABORACIÓN DE PROGRAMA ESPECÍFICO)                 |                     | Página 1 de 16  |

## Contenido

|  |    |
|--|----|
| NORMOGRAMA .....   | 4  |
| CONTEXTO .....   | 6  |
| INTRODUCCIÓN .....   | 8  |
| OBJETIVO.....  | 10 |
| PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE ACTIVOS DE INFORMACIÓN POR CATEGORÍAS..... | 10 |

|   |                     |   |
|---|---------------------|---|
|  | PROGRAMA ESPECÍFICO | Código: asignado por quien emite el documento (F-ES-GM-024) |
|   |                     | Versión: consecutivo en que va el documento (01)            |
| NOMBRE DEL FORMATO<br>(PLANTILLA ELABORACIÓN DE PROGRAMA ESPECÍFICO)              |                     | Página 1 de 16  |

## 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.

|   |                     |   |
|---|---------------------|---|
|  | PROGRAMA ESPECÍFICO | Código: asignado por quien emite el documento (F-ES-GM-024) |
|   |                     | Versión: consecutivo en que va el documento (01)            |
| NOMBRE DEL FORMATO (PLANTILLA ELABORACIÓN DE PROGRAMA ESPECÍFICO)                 |                     | Página 1 de 16  |

## 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”.

|   |                            |  |
|---|----------------------------|--|
|  | <p>PROGRAMA ESPECÍFICO</p> | <p>Código: asignado por quien emite el documento (F-ES-GM-024)</p> <p>Versión: consecutivo en que va el documento (01)</p> |
| <p>NOMBRE DEL FORMATO<br/>(PLANTILLA ELABORACIÓN DE PROGRAMA ESPECÍFICO)</p>      |                            | <p>Página 1 de 16</p>  |


**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-

|   |                     |   |
|---|---------------------|---|
|  | PROGRAMA ESPECÍFICO | Código: asignado por quien emite el documento (F-ES-GM-024) |
|   |                     | Versión: consecutivo en que va el documento (01)            |
| NOMBRE DEL FORMATO (PLANTILLA ELABORACIÓN DE PROGRAMA ESPECÍFICO)                 |                     | Página 1 de 16  |

## 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:

Adiciónese un 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 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”, en su artículo 1, adiciona al

|   |                            |  |
|---|----------------------------|--|
|  | <p>PROGRAMA ESPECÍFICO</p> | <p>Código: asignado por quien emite el documento (F-ES-GM-024)</p> <p>Versión: consecutivo en que va el documento (01)</p> |
| <p>NOMBRE DEL FORMATO<br/>(PLANTILLA ELABORACIÓN DE PROGRAMA ESPECÍFICO)</p>      |                            | <p>Página 1 de 16</p>  |

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 Ministerial 0500 de 2021 y sus dos respectivos anexos.

## INTRODUCCIÓN

En Colombia, la implementación de la política de gobierno digital se lleva a cabo siguiendo las disposiciones establecidas por la Presidencia de la República y el Ministerio de Tecnologías de la Información y las Comunicaciones (MinTIC), mediante el Decreto 767 de 2022. Estas disposiciones se integran en el Decreto Único Reglamentario del Sector TIC (Decreto 1078 de 2015), específicamente en el capítulo 1, título 9, parte 2, libro 2. Esta política es un instrumento clave para mejorar la gestión pública y fortalecer la interacción entre el Estado y los ciudadanos, enmarcándose dentro del Modelo Integrado de Planeación y Gestión (MIPG). Este modelo impulsa el cumplimiento de metas relacionadas con las políticas de desarrollo administrativo y otras políticas esenciales para la gestión pública en el país.

El Manual de la Política de Gobierno Digital, expedido por el MinTIC, tiene como propósito principal promover el uso estratégico de las tecnologías de la información y las comunicaciones (TIC). Su objetivo es consolidar un Estado y una ciudadanía más competitiva, proactivos e innovadores, generando valor público en un entorno de confianza digital.

La implementación de esta política se divide en dos componentes principales: TIC para el Estado y TIC para la sociedad, habilitados por cuatro elementos transversales:

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

Estos componentes y elementos se desarrollan mediante lineamientos y estándares mínimos que las entidades públicas deben cumplir para alcanzar los objetivos planteados.

El habilitador de Seguridad y Privacidad de la Información, según el manual, busca que las entidades públicas apliquen medidas de seguridad en todos sus procesos, trámites, servicios, sistemas de información e infraestructura. Su finalidad es garantizar la confidencialidad, integridad, disponibilidad y privacidad de los datos.



Por su parte, el artículo 2.2.9.1.2.1 del Decreto 1078 de 2015 establece que la Política de Gobierno Digital debe articularse mediante elementos como gobernanza, innovación pública digital, habilitadores, líneas de acción e iniciativas dinamizadoras. En este esquema, la Seguridad y Privacidad de la Información se destacan como aspectos fundamentales que las entidades públicas deben abordar mediante capacidades específicas y lineamientos definidos.

El Modelo de Seguridad y Privacidad de la Información (MSPI), expedido por el MinTIC, refuerza esta política. Este modelo establece que las entidades públicas deben gestionar riesgos relacionados con la información mediante prácticas que aseguren la confidencialidad, integridad y disponibilidad de los datos, aumentando la confianza de las partes interesadas. Su adopción, implementación y evaluación son obligatorias según el artículo 2.2.9.1.3.2 del Decreto 767 de 2022.

Adicionalmente, el Decreto Presidencial 612 de 2018 introduce directrices para integrar los planes institucionales y estratégicos al Plan de Acción de cada entidad estatal. Entre sus disposiciones, exige 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.

En complemento, la Resolución 0500 de 2021 del MinTIC establece lineamientos generales para implementar el MSPI. Esta resolución resalta la importancia de adoptar medidas técnicas, administrativas y de talento humano que integren principios, políticas y procedimientos de seguridad digital en el Plan de Seguridad y Privacidad de la Información. Además, establece que las entidades deben realizar análisis de riesgos y adoptar controles adecuados para mitigar posibles incidentes de seguridad digital.

Finalmente, la adopción del MSPI en las entidades públicas se fundamenta en estándares internacionales como la NTC ISO/IEC 27001 y principios regulatorios establecidos en leyes como la Ley 1712 de 2014 y la Ley 1581 de 2012. Estas normativas promueven un enfoque basado en la gestión del riesgo, facilitando la identificación, valoración y tratamiento de riesgos asociados a la seguridad y privacidad de la información. Este enfoque es esencial para la toma de decisiones sobre la implementación de controles y el diseño del Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información, que contribuyen al

cumplimiento de los objetivos organizacionales del Distrito Especial de Ciencia, Tecnología e Innovación de Medellín.

## **OBJETIVO**

Establecer un marco de acción que contribuya al tratamiento de riesgos relacionados con la seguridad y privacidad de la información, enfocado en los activos que respaldan el cumplimiento de los objetivos organizacionales. Este marco garantizará la preservación de la confidencialidad, integridad y disponibilidad de la información institucional, teniendo en cuenta el contexto organizacional de la entidad, así como sus capacidades y recursos disponibles, con el objetivo de fortalecer la confianza de ciudadanos, usuarios, socios y demás partes interesadas.


La planeación se centrará en fortalecer la implementación de acciones específicas para el tratamiento de estos riesgos, siguiendo los lineamientos establecidos por el Ministerio de Tecnologías de la Información y las Comunicaciones (MinTIC) y el Departamento Administrativo de la Función Pública. Estas acciones estarán orientadas a garantizar la seguridad de los activos de información del Distrito Especial de Ciencia, Tecnología e Innovación de Medellín a nivel central, como un aporte a:

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

Según lo expuesto 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 es la respuesta establecida por la primera línea de defensa para la mitigación de los diferentes riesgos, por lo tanto dicha planeación en este caso en particular, hace alusión al tratamiento de riesgos de Seguridad y Privacidad de la Información enfocado en la seguridad de la información sobre los activos de información a cargo del Distrito especial de ciencia, tecnología e innovación de Medellín a nivel central,

para lo cual se realizan un conjunto de actividades durante la vigencia orientadas a implementar los controles requeridos y priorizados. En atención a lo anterior, a continuación, se describen las actividades más relevantes orientadas al tratamiento de riesgos de Seguridad y Privacidad de la Información:

| Actividad  | Responsable  | 1 Semestre 2025 |   |   |   |   | 2 Semestre 2025 |   |   |  |   |
|--|--|-----------------|---|---|---|---|-----------------|---|---|--|---|
| Llevar a cabo la adquisición e implementación de controles de seguridad de la información que permitan abordar los riesgos relacionados con la seguridad y privacidad de la información. Estos controles estarán enfocados en mitigar los riesgos identificados, analizados, valorados y priorizados sobre los activos de información bajo la responsabilidad de cada dependencia a nivel central.     | Coordinador TI, Profesional de seguridad digital y líder del área de comunicaciones  |                 | X |   | X |   | X               |   | X |  | X |
| Llevar a cabo los procesos necesarios para realizar el seguimiento y monitoreo de la operación de los controles de seguridad de la información. Este seguimiento garantizará la adecuada gestión de los riesgos de seguridad y privacidad previamente identificados, analizados, valorados y priorizados sobre los activos de información bajo la responsabilidad de cada dependencia a nivel central. | Coordinador TI, Profesional de seguridad digital, y líder del área de comunicaciones |                 | X |   | X |   | X               |   | X |  | X |
| Realizar el seguimiento a las actividades de identificación y operación de controles de seguridad de la información para abordar los riesgos de seguridad y privacidad de la información identificados, analizados, valorados y priorizados sobre los activos de información bajo la responsabilidad de cada dependencia a nivel central.  | Coordinador TI, Profesional de seguridad digital, y líder del área de comunicaciones |                 |   | X |   | X |                 | X |   |  | X |

|   |                     |   |
|---|---------------------|---|
|  | PROGRAMA ESPECÍFICO | Código: asignado por quien emite el documento (F-ES-GM-024) |
|   |                     | Versión: consecutivo en que va el documento (01)            |
| NOMBRE DEL FORMATO (PLANTILLA ELABORACIÓN DE PROGRAMA ESPECÍFICO)                 |                     | Página 16 de 16   |

La realización de las actividades planificadas dependerá de la disponibilidad de recursos humanos, técnicos, tecnológicos y financieros que permitan su ejecución de manera efectiva. Estas acciones estarán alineadas con la disponibilidad presupuestal, la capacidad institucional para asumir riesgos y las directrices establecidas por la alta dirección, quienes definen el nivel de riesgo aceptable para la organización.

En este contexto, la Secretaría de Innovación Digital ha dispuesto la contratación de un equipo especializado, cuyo propósito será llevar a cabo actividades de sensibilización, formación y atención a las inquietudes de las dependencias del Distrito de Medellín a nivel central. Estas tareas se desarrollarán de acuerdo con cronogramas previamente establecidos.

Además, la Secretaría ha definido plazos específicos para ofrecer apoyo y monitorear el avance de los planes de seguridad y privacidad de la información presentados por las diferentes dependencias. Este proceso busca asegurar que las actividades relacionadas con la elaboración y cumplimiento de dichos planes se realicen de forma eficiente y acorde con los objetivos establecidos.

|                                    |  |                                      |
|------------------------------------|--|--------------------------------------|
| Elaboró: Profesional Apoyo Calidad | Revisó: Coordinadora de Planeación Estratégica | Aprobó: Sistema Integrado de Gestión |
| Fecha: 18 de mayo de 2020          | Fecha: 18 de mayo de 2020                      | Fecha: 18 de mayo de 2020            |