Alcaldía de Medellín
Distrito de
Ciencia, Tecnología e Innovación

DISTRITO ESPECIAL DE CIENCIA, TECNOLOGÍA E INNOVACIÓN DE MEDELLÍN

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

VIGENCIA 2026

www.medellin.gov.co
Centro Administrativo Distrital CAD
Calle 44 N° 52-165. Código Postal 50015
Línea de Atención a la Ciudadanía: (604) 44 44 144
Conmutador: (604) 385 55 55 Medellín - Colombia

CONTENIDO

Centro Administrativo Distrital CAD
Calle 44 N° 52-165. Código Postal 50015
Línea de Atención a la Ciudadanía: (604) 44 44 144
Conmutador: (604) 385 55 55 Medellín - Colombia
www.medellin.gov.co

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.

Centro Administrativo Distrital CAD
Calle 44 N° 52-165. Código Postal 50015
Línea de Atención a la Ciudadanía: (604) 44 44 144
Conmutador: (604) 385 55 55 Medellín - Colombia
www.medellin.gov.co

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”.

Decreto Municipal 883 de 2015: “Por el cual se adecúa la Estructura de la Administración Municipal de Medellín…”.

Decreto 612 de 2018: “Por el cual se fijan directrices para la integración de los planes institucionales y estratégicos al Plan de Acción…”.

Centro Administrativo Distrital CAD
Calle 44 N° 52-165. Código Postal 50015
Línea de Atención a la Ciudadanía: (604) 44 44 144
Conmutador: (604) 385 55 55 Medellín - Colombia
www.medellin.gov.co

Decreto Municipal 0863 de 2020: “Por el cual se modifica la estructura orgánica y funcional…”.

Decreto 767 de 2022: “Por el cual se establecen los lineamientos generales de la Política de Gobierno Digital…”.

Resolución 00500 de 2021: “Por la cual se establecen los lineamientos y estándares para la estrategia de seguridad digital…”.

Resolución 1519 de 2020: “Por la cual se establecen los lineamientos y estándares para la estrategia de seguridad digital…”.

Resolución 02277 de 2025: “Por la cual se actualiza el Anexo 1 de la Resolución número 500 de 2021 y se derogan otras disposiciones relacionadas con la materia.”

ISO/IEC 27001:2022: Seguridad de la información, ciberseguridad y protección de la privacidad — Sistemas de gestión de la seguridad de la información — Requisitos.

Centro Administrativo Distrital CAD
Calle 44 N° 52-165. Código Postal 50015
Línea de Atención a la Ciudadanía: (604) 44 44 144
Conmutador: (604) 385 55 55 Medellín - Colombia
www.medellin.gov.co

CONTEXTO

El Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información es un instrumento institucional que permite definir acciones para gestionar los riesgos priorizados a través de la implementación de controles orientados a preservar la confidencialidad, integridad y disponibilidad de los activos de información institucionales, atendiendo la normatividad vigente y las lineamientos nacionales que se definen a través del Modelo de Seguridad y Privacidad de la Información (MSPI).

Centro Administrativo Distrital CAD
Calle 44 N° 52-165. Código Postal 50015
Línea de Atención a la Ciudadanía: (604) 44 44 144
Conmutador: (604) 385 55 55 Medellín - Colombia
www.medellin.gov.co

INTRODUCCIÓN

En Colombia se viene adelantando la implementación de la política de gobierno digital, tal como lo establece La Presidencia de la Republica y el Ministerio de Tecnologías de la Información y las Comunicaciones a través del Decreto 767 de 2022, cuyas disposiciones se compilan en el Decreto Único Reglamentario del Sector TIC, 1078 de 2015, específicamente en el capítulo 1, titulo 9, parte 2, libro 2, como un instrumento fundamental para mejorar la gestión pública y la relación del estado con los ciudadanos, la cual se ha articulado con el Modelo Integrado de Planeación y Gestión, como una herramienta dinamizadora para cumplir las metas de las políticas de desarrollo administrativo, articulada a otras políticas esenciales para la gestión pública en Colombia.

El Manual de la política de Gobierno Digital expedido por el MinTIC establece que la política tiene como propósito promover 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.

Según el manual, la implementación de la política de gobierno digital se ha definido en dos componentes: TIC para el estado y TIC para la sociedad, que son habilitados por cuatro elementos transversales: Arquitectura, Cultura y Apropiación, Seguridad y Privacidad de la Información y Servicios Ciudadanos Digitales. Estos seis elementos, se desarrollan a través de lineamientos y estándares, que son requerimientos mínimos que todos los sujetos obligados deben cumplir para alcanzar los logros de la política.

Centro Administrativo Distrital CAD
Calle 44 N° 52-165. Código Postal 50015
Línea de Atención a la Ciudadanía: (604) 44 44 144
Conmutador: (604) 385 55 55 Medellín - Colombia
www.medellin.gov.co

El manual en mención, precisa que el habilitador de Seguridad y Privacidad de la Información busca que las entidades públicas implementen los lineamientos de seguridad de la información en todos sus procesos, tramites, servicios, sistemas de información, infraestructura y en general, en todos los activos de información con el fin de preservar la confidencialidad, integridad, disponibilidad y privacidad de los datos.

No obstante, el Artículo 2.2.9.1.2.1 del Decreto Ministerial 1078 de 2015 establece que La Política de Gobierno Digital se desarrollará a través de un esquema que articula los elementos que la componen, a saber: gobernanza, innovación pública digital, habilitadores, líneas de acción, e iniciativas dinamizadoras, con el fin de lograr su objetivo. En el mencionado artículo, en su numeral 3.2 recalca como habilitador, la Seguridad y Privacidad de la Información donde los sujetos obligados deben desarrollar capacidades a través de la implementación de los lineamientos de seguridad y privacidad de la información en todos sus procesos, trámites, servicios, sistemas de información, infraestructura y en general, en todos los activos de información, con el fin de preservar la confidencialidad, integridad, disponibilidad y privacidad de los datos.

El documento denominado Modelo de Seguridad y Privacidad de la Información (MSPI), expedido por el Ministerio de Tecnologías de Información y de las Comunicaciones, expresa que la adopción de este, por las entidades del estado, conduce a la preservación de la confidencialidad, integridad, disponibilidad de la información, apoyada en un proceso de gestión del riesgo, brindando confianza a las partes interesadas acerca de la adecuada gestión de riesgos.

Centro Administrativo Distrital CAD
Calle 44 N° 52-165. Código Postal 50015
Línea de Atención a la Ciudadanía: (604) 44 44 144
Conmutador: (604) 385 55 55 Medellín - Colombia
www.medellin.gov.co

La adopción, implementación y evaluación del modelo mencionado, es una actividad obligatoria según lo expresado en el artículo 2.2.9.1.3.2 del Decreto 767 de 2022. 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 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.

Así mismo, la resolución 0500 de marzo 10 del 2021 expedida por el Ministerio de Tecnologías de Información y de las Comunicaciones, que tiene como objeto establecer los lineamientos generales para la implementación del Modelo de Seguridad y Privacidad de la Información, la guía de gestión de riesgos de Seguridad de la Información y el procedimiento para la gestión de los incidentes de seguridad digital, y establecer los lineamientos y estándares para la estrategia de seguridad digital. La resolución en mención precisa la necesidad de que los sujetos obligados deban adoptar las medidas técnicas, administrativas y de talento humano para garantizar que la seguridad digital se incorpore al Plan de Seguridad y Privacidad de la Información y así mitigar los riesgos relacionados con la protección y la privacidad de la información e incidentes de seguridad digital. Es precisamente a través del artículo 5 de la resolución 0500 que se precisa la necesidad de adoptar la estrategia de seguridad digital en la que se integren los

Centro Administrativo Distrital CAD
Calle 44 N° 52-165. Código Postal 50015
Línea de Atención a la Ciudadanía: (604) 44 44 144
Conmutador: (604) 385 55 55 Medellín - Colombia
www.medellin.gov.co

principios, políticas, procedimientos, guías, manuales, formatos y lineamientos para la gestión de la seguridad de la información digital, e incluirla en el Plan de Seguridad y Privacidad de la Información que se integra al Plan de Acción en los términos del artículo 2.22.22.3.14 del capítulo 3 del título 22 de la parte 2 del libro 2 del decreto 1083 de 2015.

Considerando que, la Resolución Ministerial 0500 de 2021, establece en su artículo 5, denominado “Estrategia de Seguridad Digital”, en especial en el numeral 2, indicando que se debe “Contar con un análisis y tratamiento de riesgos de seguridad digital e implementar controles que permitan gestionarlos”, además, en la el anexo 1 de la misma Resolución, en su acápite “Planificación”, señala “Determinar las necesidades y objetivos de seguridad y privacidad de la información teniendo en cuenta su mapa de procesos, el tamaño y en general su contexto interno y externo. Esta fase define el plan de valoración y tratamiento de riesgos, siendo ésta la parte más importante del ciclo, teniendo el Plan de Tratamiento de Riesgos como el documento que define las acciones para gestionar los riesgos de seguridad de la información inaceptables e implantar los controles necesarios para proteger la misma. (ISO/IEC 27000), y en el mencionado anexo, en su numeral 7.3.3 Plan de tratamiento de los riesgos de seguridad de la información, tiene como lineamiento que la Entidad debe definir y aplicar un proceso de tratamiento de riesgos de la seguridad de la información.

La adopción e implementación del Modelo de Seguridad y Privacidad de la información en las entidades públicas toma como sustento el estándar NTC ISO 27001:2022, así como principios regulatorios definidos por el Gobierno Nacional, tal como la Ley 1712 de 2014 o la Ley 1581 de 2012; así mismo, apoyan su enfoque en la implementación de un ciclo de identificación, valoración y tratamiento de riesgos de seguridad y privacidad de la información, para lo cual

Centro Administrativo Distrital CAD
Calle 44 N° 52-165. Código Postal 50015
Línea de Atención a la Ciudadanía: (604) 44 44 144
Conmutador: (604) 385 55 55 Medellín - Colombia
www.medellin.gov.co

se ha expedido desde el Departamento Administrativo de la Función Pública la guía para la administración del riesgo y el diseño de controles en entidades públicas, como referente para abordar los riesgos de gestión, corrupción y de seguridad de la información. La adopción de prácticas de gestión de riesgos en las entidades públicas permitirá fortalecer la toma de decisiones en cuanto a la implementación de controles de acuerdo con el plan de tratamientos definido.

Estos referentes constituyen el fundamento para la definición del plan de tratamiento de riesgos de seguridad y privacidad de la información del Distrito Especial de Ciencia, Tecnología e Innovación de Medellín a nivel central sobre activos de información que aportan al logro de los objetivos organizacionales.

Centro Administrativo Distrital CAD
Calle 44 N° 52-165. Código Postal 50015
Línea de Atención a la Ciudadanía: (604) 44 44 144
Conmutador: (604) 385 55 55 Medellín - Colombia
www.medellin.gov.co

CONTEXTO DEL DESARROLLO DEL PLAN 2025

Durante la vigencia 2025 se evidenció consolidación y madurez en la ejecución del Plan de Tratamiento de Riesgos, con acompañamientos orientados a la gestión de planes de tratamiento y la gestión de incidentes, con ejecución bajo modalidad individual por dependencia. Las lecciones aprendidas se incorporan en el enfoque 2026.

Acompañamientos

Se realizarán acompañamientos metodológicos a las dependencias para fortalecer la identificación e implementación de controles, la gestión de incidentes y el cierre de acciones del plan de tratamiento, con enfoque diferenciado según nivel de avance (Grupo 1 y Grupo 2).

Tipo de ejecución del plan

Se mantiene la modalidad de ejecución individual, mediante planes específicos por subsecretaría, subdirección, unidad y/o equipo, en coherencia con la asignación de responsabilidades sobre activos de información, controles y tratamiento de incidentes.

Centro Administrativo Distrital CAD
Calle 44 N° 52-165. Código Postal 50015
Línea de Atención a la Ciudadanía: (604) 44 44 144
Conmutador: (604) 385 55 55 Medellín - Colombia
www.medellin.gov.co

OBJETIVO

Establecer o actualizar el marco de acción para aportar al tratamiento de riesgos de seguridad y privacidad de la información sobre los activos de información que soportan el cumplimiento de los objetivos institucionales, conducentes a preservar la confidencialidad, integridad y disponibilidad de la información, considerando el contexto organizacional, capacidades y recursos disponibles, y fortaleciendo la confianza de las partes interesadas.

www.medellin.gov.co
Centro Administrativo Distrital CAD
Calle 44 N° 52-165. Código Postal 50015
Línea de Atención a la Ciudadanía: (604) 44 44 144
Conmutador: (604) 385 55 55 Medellín - Colombia

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

El plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información para la vigencia 2026, se abordará desde 2 componentes, (i) orientado al fortalecimiento de las capacidades institucionales de seguridad informática frente a ciberamenazas y (ii) orientado al fortalecimiento de los procesos institucionales para la identificación y gestión de controles de seguridad y privacidad de la información, así como de eventos e incidentes de seguridad y privacidad de la información.

A. FORTALECIMIENTO DE LAS CAPACIDADES INSTITUCIONALES DE SEGURIDAD INFORMÁTICA FRENTE A CIBERAMENAZAS

En atención a la creciente ola de ataques a las organizaciones públicas y privadas alrededor del mundo, se abordará un componente en el que se puedan evidenciar los esfuerzos institucionales para enfrentar las amenazas digitales, en el contexto del alcance del centro de datos bajo la responsabilidad de la secretaría de innovación digital, tal como se presenta a continuación:

Centro Administrativo Distrital CAD
Calle 44 N° 52-165. Código Postal 50015
Línea de Atención a la Ciudadanía: (604) 44 44 144
Conmutador: (604) 385 55 55 Medellín - Colombia
www.medellin.gov.co

PLAN DE FORTALECIMIENTO DE LAS CAPACIDADES INSTITUCIONALES DE SEGURIDAD INFORMÁTICA FRENTE A CIBERAMENAZAS													
Actividad	**Responsable / Corresponsable**	**1 semestre 2025**						**2 semestre 2025**					
		E	F	M	A	M	J	J	A	S	O	N	D
Fortalecimiento del Control para la Protección de la Navegación Institucional	Secretaría De Innovación Digital.	X	X	X	X	X	X	X	X	X	X	X	X
Fortalecimiento del Control para la Protección del Correo Electrónico Institucional	Secretaría De Innovación Digital.	X	X	X	X	X	X	X	X	X	X	X	X
Fortalecimiento del Control para la Protección del acceso a Sitios y Aplicaciones Web Institucionales	Secretaría De Innovación Digital.	X	X	X	X	X	X	X	X	X	X	X	X
Fortalecimiento del Control Antimalware de los Equipos y Servidores de Computo Institucionales	Secretaría De Innovación Digital.	X	X	X	X	X	X	X	X	X	X	X	X
Fortalecimiento del Control para la Protección del Acceso a Bases de Datos	Secretaría De Innovación Digital.	X	X	X	X	X	X	X	X	X	X	X	X
Fortalecimiento del Control para la Detección de Eventos e Incidentes de Seguridad Informática	Secretaría De Innovación Digital.	X	X	X	X	X	X	X	X	X	X	X	X
Fortalecimiento del Control para la Identificación de Vulnerabilidades Técnicas sobre la Infraestructura Tecnológica	Secretaría De Innovación Digital.	X	X	X	X	X	X	X	X	X	X	X	X
Fortalecimiento del Control para la Protección de los Perímetros de Red Institucionales	Secretaría De Innovación Digital.	X	X	X	X	X	X	X	X	X	X	X	X

RECURSOS FORTALECIMIENTO DE LAS CAPACIDADES INSTITUCIONALES DE SEGURIDAD INFORMÁTICA FRENTE A CIBERAMENAZAS

La implementación de controles frente a ciberamenazas y su mantenimiento y actualización son esenciales para minimizar la materialización de riesgos en el entorno digital institucional, por lo anterior, el Distrito de Medellín ha priorizado una inversión en tecnologías de información y de las comunicaciones diseñadas como controles de seguridad informática que se deben mantener implementadas y actualizadas para la protección de los activos informáticos institucionales. A continuación, se detallan las actividades más relevantes:

Actividad	Tipo de recurso	Presupuesto Anual
Fortalecimiento del Control para la Protección de la Navegación Institucional	Financiero	$ 454.510.314
Fortalecimiento del Control para la Protección del Correo Electrónico Institucional	Financiero	$ 716.539.200
Fortalecimiento del Control para la Protección del acceso a Sitios y Aplicaciones Web Institucionales	Financiero	$ 724.802.201
Fortalecimiento del Control Antimalware de los Equipos y Servidores de Computo Institucionales	Financiero	$ 2.270.392.944
Fortalecimiento del Control para la Protección del Acceso a Bases de Datos	Financiero	$ 1.562.765.471
Fortalecimiento del Control para la Detección de Eventos e Incidentes de Seguridad Informática	Financiero	$ 897.285.758
Fortalecimiento del Control para la Identificación de Vulnerabilidades Técnicas sobre la Infraestructura Tecnológica	Financiero	$ 650.000.000
Fortalecimiento del Control para la Protección de los Perímetros de Red Institucionales	Financiero	$ 2.998.967.053
TOTAL		$ 10.275.262.941

PRODUCTOS FORTALECIMIENTO DE LAS CAPACIDADES INSTITUCIONALES DE SEGURIDAD INFORMÁTICA FRENTE A CIBERAMENAZAS

A partir de los recursos definidos, se podrán obtener los siguientes productos:

Actividad	Tipo de recurso	PRODUCTOS
Fortalecimiento del Control para la Protección de la Navegación Institucional	Financiero	✓ Licenciamiento anual renovado
Fortalecimiento del Control para la Protección del Correo Electrónico Institucional	Financiero	✓ Licenciamiento anual renovado
Fortalecimiento del Control para la Protección del acceso a Sitios y Aplicaciones Web Institucionales	Financiero	✓ Licenciamiento anual renovado
Fortalecimiento del Control Antimalware de los Equipos y Servidores de Computo Institucionales	Financiero	✓ Licenciamiento anual renovado
Fortalecimiento del Control para la Protección del Acceso a Bases de Datos	Financiero	✓ Licenciamiento anual renovado
Fortalecimiento del Control para la Detección de Eventos e Incidentes de Seguridad Informática	Financiero	✓ Licenciamiento anual renovado
Fortalecimiento del Control para la Identificación de Vulnerabilidades Técnicas sobre la Infraestructura Tecnológica	Financiero	✓ Licenciamiento anual renovado
Fortalecimiento del Control para la Protección de los Perímetros de Red Institucionales	Financiero	✓ Licenciamiento anual renovado

B. FORTALECIMIENTO DE LOS PROCESOS ASOCIADOS AL PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE ACTIVOS DE INFORMACIÓN POR CATEGORÍAS

En atención a las recomendaciones del “INFORME FINAL DE AUDITORIA”, con radicado 202120115527, y la remisión de este bajo el oficio 202120116604, se tiene presente la observación:

Código de referenciación de la observación	Asunto
8	Gestión activos de información y Gestión de Riesgos de Seguridad de la Información.

Así mismo, atendiendo 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 y privacidad 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 se estructura la división de dos grupos:

El primer grupo del plan está destinado a los participantes de todas las dependencias a nivel central del Distrito Especial de Ciencia, Tecnología e Innovación de Medellín que no demostraron avances en las actividades contempladas en el marco de ejecución del plan de tratamiento de riesgos de seguridad y privacidad de la información durante la vigencia 2025. Estos participantes serán asignados al grupo número uno, y su participación y ejecución de los planes para la vigencia 2026 seguirán el siguiente cronograma:

Centro Administrativo Distrital CAD
Calle 44 N° 52-165. Código Postal 50015
Línea de Atención a la Ciudadanía: (604) 44 44 144
Conmutador: (604) 385 55 55 Medellín - Colombia
www.medellin.gov.co

PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN - GRUPO 1					
Actividad	**Responsable**	**2 semestre 2026**			
		S	**O**	**N**	**D**
Realizar la identificación, adquisición e implementación de controles de seguridad y privacidad 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.	Todas las Secretarías, Departamentos Administrativos y Gerencias a nivel central del Distrito, así como sus respectivas subsecretarias, unidades, equipos, etcétera en caso de realizar la ejecución del plan de forma individual.	X	X		
Realizar la gestión y seguimiento de los controles de seguridad y privacidad de la información implementados, verificando su eficacia y eficiencia para el tratamiento de 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.	Todas las Secretarías, Departamentos Administrativos y Gerencias a nivel central del Distrito, así como sus respectivas subsecretarias, unidades, equipos, etcétera en caso de realizar la ejecución del plan de forma individual.	X	X		
Realizar la identificación, registro y clasificación de eventos e incidentes de seguridad y privacidad de la información materializados, en atención a 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.	Todas las Secretarías, Departamentos Administrativos y Gerencias a nivel central del Distrito, así como sus respectivas subsecretarias, unidades, equipos, etcétera en caso de realizar la ejecución del plan de forma individual.			X	X
Realizar la atención, tratamiento y cierre de los incidentes de seguridad de la información identificados, incluyendo las acciones de contención, corrección y mejora, en función de los riesgos de seguridad y privacidad de la información identificados, analizados, valorados	Todas las Secretarías, Departamentos Administrativos y Gerencias a nivel central del Distrito, así como sus respectivas subsecretarias, unidades, equipos, etcétera en caso de realizar la ejecución del plan de forma individual.			X	X

y priorizados sobre los activos de información bajo la responsabilidad de cada dependencia a nivel central.					
Realizar el acompañamiento a las actividades de identificación, adquisición e implementación de controles de seguridad de la información, así como al tratamiento de incidentes de seguridad y privacidad 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.	Secretaría de innovación digital	X	X	X	X
Realizar el seguimiento a las actividades de identificación, adquisición, implementación y gestión de controles de seguridad de la información, así como al tratamiento de incidentes 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.	Secretaría de innovación digital	X	X	X	X

El segundo grupo del plan está destinado a los participantes de todas las dependencias a nivel central del Distrito Especial de Ciencia, Tecnología e Innovación de Medellín que demostraron avances en la entrega o seguimiento en la ejecución de las actividades contempladas en el marco del plan de tratamiento de riesgos de seguridad y privacidad de la información durante la vigencia 2025. Estos participantes serán asignados al grupo número dos, y su participación y ejecución de los planes para el año 2026 seguirán el siguiente cronograma:

PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN - GRUPO 2													
Actividad	**Responsable**	**1 semestre 2026**						**2 semestre 2026**					
		E	**F**	**M**	**A**	**M**	**J**	**J**	**A**	**S**	**O**	**N**	**D**
Realizar la actualización de la matriz de identificación de controles de seguridad y privacidad de la información consolidada en la vigencia 2025, bajo la responsabilidad de cada dependencia a nivel central, en atención a las modificaciones que puedan ser requeridas para abordar los riesgos de seguridad y privacidad de la información identificados, analizados, valorados y priorizados sobre los activos de información.	Todas las Secretarías, Departamentos Administrativos y Gerencias a nivel central del Distrito, así como sus respectivas subsecretarias, unidades, equipos, etcétera en caso de realizar la ejecución del plan de forma individual.								X	X	X	X	
Realizar la adquisición e implementación de controles de seguridad y privacidad 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.	Todas las Secretarías, Departamentos Administrativos y Gerencias a nivel central del Distrito, así como sus respectivas subsecretarias, unidades, equipos, etcétera en caso de realizar la ejecución del plan de forma individual.		X	X	X	X	X	X	X	X	X	X	X
Realizar la gestión y seguimiento de los controles de seguridad y privacidad de la información implementados, verificando su eficacia y eficiencia para el tratamiento de 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.	Todas las Secretarías, Departamentos Administrativos y Gerencias a nivel central del Distrito, así como sus respectivas subsecretarias, unidades, equipos, etcétera en caso de realizar la ejecución del plan de forma individual.		X	X	X	X	X	X	X	X	X	X	X
Realizar la identificación, registro y clasificación de eventos e incidentes de seguridad de la información materializados, en atención a los riesgos de seguridad y privacidad de la	Todas las Secretarías, Departamentos Administrativos y Gerencias a nivel central del Distrito, así como sus respectivas		X	X	X	X	X	X	X	X	X	X	X

información identificados, analizados, valorados y priorizados sobre los activos de información bajo la responsabilidad de cada dependencia a nivel central.	subsecretarias, unidades, equipos, etcétera en caso de realizar la ejecución del plan de forma individual.												
Realizar el seguimiento a la atención, tratamiento, divulgación y cierre de eventos e incidentes de seguridad y privacidad de la información identificados, incluyendo las acciones de contención, corrección y mejora, en función de 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.	Todas las Secretarías, Departamentos Administrativos y Gerencias a nivel central del Distrito, así como sus respectivas subsecretarias, unidades, equipos, etcétera en caso de realizar la ejecución del plan de forma individual.		X	X	X	X	X	X	X	X	X	X	X
Realizar el acompañamiento a los diferentes procesos de seguridad y privacidad de la información, en particular a la gestión de planes de tratamiento y a la gestión de incidentes, para fortalecer la eficacia y eficiencia de las acciones orientadas al tratamiento de los riesgos de seguridad y privacidad de la información sobre los activos de información bajo la responsabilidad de cada dependencia a nivel central.	Secretaría de Innovación Digital		X	X	X	X	X	X	X	X	X	X	X
Realizar el seguimiento a las actividades de actualización, adquisición, implementación y gestión de controles de seguridad y privacidad de la información, así como al tratamiento de incidentes 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.	Secretaría de Innovación Digital		X	X	X	X	X	X	X	X	X	X	X

RECURSOS PARA APOYAR EL FORTALECIMIENTO EN LA GESTIÓN DE CONTROLES DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN, ASÍ COMO DE INCIDENTES DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN EN LAS DEPENDENCIAS A NIVEL CENTRAL DEL DISTRITO

La seguridad y privacidad de la información es esencial para proteger la información crítica del distrito, y su fortalecimiento depende en gran medida del recurso humano. Contar con personal capacitado y especializado para el fortalecimiento de los procesos institucionales relacionados con la seguridad de la información es clave para desarrollar y ejecutar estrategias efectivas que faciliten la gestión integral de los procesos relacionados con la seguridad de la información. Por ello, es necesario integrar el siguiente factor humano para cumplir con las necesidades de fortalecimiento de los procesos institucionales relacionados con la seguridad y privacidad de la información:

Actividad	Tipo de recurso	Numero de recurso	Dependencia	Presupuesto mensual	Presupuesto Anual
Realizar el acompañamiento a los diferentes procesos de seguridad y privacidad de la información, en particular a la gestión de planes de tratamiento y a la gestión de incidentes, para fortalecer la eficacia y eficiencia de las acciones orientadas al tratamiento de los riesgos de seguridad y privacidad de la información sobre los activos de información bajo la responsabilidad de cada dependencia a nivel central	Humano Profesional	1	➢ Departamento administrativo de gestión del riesgo de desastres ➢ Secretaria del medio ambiente ➢ Gerencia de corregimientos ➢ Departamento administrativo de planeación ➢ Secretaria de hacienda ➢ Secretaria de desarrollo económico ➢ Gerencia del centro ➢ Secretaria de gestión humana y servicio a la ciudadanía ➢ Secretaria de inclusión social y familia ➢ Secretaria de las mujeres ➢ Secretaria de la juventud ➢ Secretaria de salud ➢ Secretaria de educación ➢ Secretaria de cultura ciudadana ➢ Secretaria de paz y derechos humanos ➢ Gerencia de Diver. Sexuales e identidad de genero ➢ Secretaria de gestión y control territorial ➢ Secretaria de movilidad ➢ Secretaria de infraestructura física ➢ Secretaria de turismo y entretenimiento ➢ Secretaria de seguridad y convivencia ➢ Secretaria de gobierno y gestión del gabinete ➢ Gerencia de proyectos estratégicos ➢ Secretaria privada ➢ Secretaria de innovación digital ➢ Secretaria de suministros y servicios ➢ Secretaria de comunicaciones ➢ Secretaria de evaluación y control ➢ Secretaria de participación ciudadana ➢ Secretaria general	$ 5.488.728	$ 60.376.006

			➢ Gerencia étnica		
Realizar el seguimiento a las actividades de actualización, adquisición, implementación y gestión de controles de seguridad y privacidad de la información, así como al tratamiento de incidentes 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			➢ Departamento administrativo de gestión del riesgo de desastres ➢ Secretaria del medio ambiente ➢ Gerencia de corregimientos ➢ Departamento administrativo de planeación ➢ Secretaria de hacienda ➢ Secretaria de desarrollo económico ➢ Gerencia del centro ➢ Secretaria de gestión humana y servicio a la ciudadanía ➢ Secretaria de inclusión social y familia ➢ Secretaria de las mujeres ➢ Secretaria de la juventud ➢ Secretaria de salud ➢ Secretaria de educación ➢ Secretaria de cultura ciudadana ➢ Secretaria de paz y derechos humanos ➢ Gerencia de Diver. Sexuales e identidad de genero ➢ Secretaria de gestión y control territorial ➢ Secretaria de movilidad ➢ Secretaria de infraestructura física ➢ Secretaria de turismo y entretenimiento ➢ Secretaria de seguridad y convivencia ➢ Secretaria de gobierno y gestión del gabinete ➢ Gerencia de proyectos estratégicos ➢ Secretaria privada ➢ Secretaria de innovación digital ➢ Secretaria de suministros y servicios ➢ Secretaria de comunicaciones ➢ Secretaria de evaluación y control ➢ Secretaria de participación ciudadana ➢ Secretaria general ➢ Gerencia étnica		
TOTAL					$ 60.376.006

PRODUCTOS DE LAS ACTIVIDADES PARA EL FORTALECIMIENTO DE LOS PROCESOS INSTITUCIONALES RESPECTO A LA SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

A partir de los recursos definidos, se podrán obtener los siguientes productos:

Actividad	Tipo de recurso	Dedicación	PRODUCTOS
Realizar la identificación, adquisición e implementación de controles de seguridad y privacidad 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.	Disposición de cada Dependencia		✓ Catálogo de Controles de Seguridad y Privacidad de la Información 2026 por Dependencia
Realizar la gestión y seguimiento de los controles de seguridad y privacidad de la información implementados, verificando su eficacia y eficiencia para el tratamiento de 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.			✓ Informe de Seguimiento a los Controles de Seguridad y Privacidad de la Información 2026 por Dependencia
Realizar la identificación, registro y clasificación de eventos e incidentes de seguridad y privacidad de la información materializados, en atención a 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.			✓ Inventario de Eventos de Seguridad y Privacidad de la Información 2026 Registrados por la Dependencia
Realizar la atención, tratamiento y cierre de los incidentes de seguridad de la información identificados, incluyendo las acciones de contención, corrección y mejora, en función de 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.			✓ Inventario de Incidentes de Seguridad y Privacidad de la Información Materializados en la vigencia 2026 en la Dependencia

Realizar el acompañamiento a las actividades de identificación, adquisición e implementación de controles de seguridad de la información, así como al tratamiento de incidentes de seguridad y privacidad 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. Realizar el seguimiento a las actividades de identificación, adquisición, implementación y gestión de controles de seguridad de la información, así como al tratamiento de incidentes 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.	Humano Especializado	1	✓ Informe de Acompañamiento por Dependencia con brechas identificadas y compromisos acordados ✓ Informes de Seguimiento Trimestral de Avance de las Dependencias en el Desarrollo de las Actividades

www.medellin.gov.co
Centro Administrativo Distrital CAD
Calle 44 N° 52-165. Código Postal 50015
Línea de Atención a la Ciudadanía: (604) 44 44 144
Conmutador: (604) 385 55 55 Medellín - Colombia

El desarrollo de las actividades para lograr su consecución estará sujeto a la **disponibilidad de recursos** (humanos, técnicos, tecnológicos, financieros) que faciliten el cumplimiento de las actividades; de acuerdo con la disponibilidad presupuestal oportuna, al apetito de riesgo institucional y a las orientaciones de la alta dirección, en cuanto al apetito de riesgo institucionales que han adoptado para afrontar el desarrollo y cumplimiento de las actividades planificadas.

Todas las dependencias del nivel central serán responsables de la participación, atención, ejecución de las actividades propuestas y suministro de la información solicitada durante la ejecución del plan. El equipo responsable de la ejecución de las actividades por parte de la Secretaría de Innovación Digital reportará a los directivos responsables de las dependencias, al comité de seguridad de la información y al comité institucional de gestión y desempeño las situaciones que ocasionen desviación o incumplimiento de las dependencias, de manera que se pueda retroalimentar la estrategia de decisión institucional de manera más oportuna.

INDICADORES DE SEGUIMIENTO AL PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

Para facilitar el seguimiento a la ejecución del plan de tratamiento de riesgos de seguridad y privacidad de la información, se define el siguiente indicador:

Indicador	Unidad de Medida	Meta
Porcentaje de Avance a la Ejecución del Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información	Porcentaje	100%

El indicador será específico para la vigencia 2026 orientado a garantizar el seguimiento al cumplimiento de las actividades previstas.

Centro Administrativo Distrital CAD
Calle 44 N° 52-165. Código Postal 50015
Línea de Atención a la Ciudadanía: (604) 44 44 144
Conmutador: (604) 385 55 55 Medellín - Colombia
www.medellin.gov.co

METAS DE SEGUIMIENTO AL PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

Respecto de la ejecución del Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información de la Vigencia 2026, se define como meta:

100% de la Ejecución del Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información

Centro Administrativo Distrital CAD
Calle 44 N° 52-165. Código Postal 50015
Línea de Atención a la Ciudadanía: (604) 44 44 144
Conmutador: (604) 385 55 55 Medellín - Colombia
www.medellin.gov.co