



Alcaldía de Medellín
Distrito de
Ciencia, Tecnología e Innovación

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

PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

VIGENCIA 2026



Alcaldía de Medellín
Distrito de
Ciencia, Tecnología e Innovación

CONTENIDO

SIGLAS.....	3
NORMOGRAMA	4
CONTEXTO	6
INTRODUCCIÓN	7
CONTEXTO DEL DESARROLLO DEL PLAN 2025	11
Acompañamientos	11
Tipo de ejecución del plan.....	11
OBJETIVO	12
PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN	13



Alcaldía de Medellín
Distrito de
Ciencia, Tecnología e Innovación

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”.

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...”.

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.

CONTEXTO

En el marco de las responsabilidades del Distrito Especial de Ciencia, Tecnología e Innovación de Medellín y de la Secretaría de Innovación Digital, la entidad adelanta la implementación y fortalecimiento del Sistema de Gestión de Seguridad de la Información (SGSI) y del Modelo de Seguridad y Privacidad de la Información (MSPI) como habilitador de la Política de Gobierno Digital. Este plan se integra al Plan de Acción institucional y se desarrolla bajo un enfoque de gestión del riesgo, preservando la confidencialidad, integridad, disponibilidad y privacidad de la información.

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, título 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.

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.

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 principios, políticas, procedimientos, guías, manuales, formatos y lineamientos para la gestión de la seguridad de la información digital, e incluirla en el Plan de



Alcaldía de Medellín
Distrito de
Ciencia, Tecnología e Innovación

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. En atención a lo anterior, se presenta el plan de seguridad y privacidad de la información para la vigencia 2026.

CONTEXTO DEL DESARROLLO DEL PLAN 2025

Durante la vigencia 2025 se evidenciaron avances de madurez y participación de algunas dependencias en la ejecución del Plan de Seguridad y Privacidad de la Información. Se realizaron jornadas de acompañamiento para resolución de dudas e inquietudes y se consolidó la modalidad de ejecución individual por dependencia, facilitando una identificación más precisa de activos, riesgos y controles, y una asignación clara de responsabilidades.

Acompañamientos

Se continuarán las jornadas de acompañamiento para apoyar a las dependencias en la autoevaluación, la gestión de activos y la gestión de riesgos, con enfoque diferenciado según nivel de avance y madurez.

Tipo de ejecución del plan

Se ratifica la ejecución bajo modalidad individual, mediante planes específicos por subsecretaría, subdirección, unidad y/o equipo, de acuerdo con la estructura organizacional y responsabilidades sobre activos de información.

OBJETIVO

Establecer o actualizar el marco de acción para la ejecución del Plan de Seguridad y Privacidad de la Información 2026, orientado a la implementación del MSPI, sobre los activos de información que soportan los objetivos institucionales, con el fin de preservar la confidencialidad, integridad y disponibilidad de la información y fortalecer la confianza de los grupos de valor e interés.

PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

La presente propuesta unificada estructura el plan en dos componentes: (i) fortalecimiento de capacidades institucionales y (ii) fortalecimiento de procesos institucionales relacionados con seguridad y privacidad de la información. A continuación, se detallan las acciones, recursos y productos relacionados con cada el avance en cada uno de los componentes.

A. FORTALECIMIENTO DE LAS CAPACIDADES INSTITUCIONALES RESPECTO A LA SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

Este componente consolida acciones para fortalecer el gobierno de seguridad de la información, los mecanismos de planeación y seguimiento, los documentos y artefactos del sistema de gestión, la identificación de recursos y capacidades, la cultura de seguridad y privacidad, y la gestión institucional transversal.

Código de referenciación de la observación	Asunto
1	Gobierno de Seguridad de la Información.
2	Mecanismos de Planificación y Seguimiento – Seguridad de la Información.
3	Documentos de Calidad – Seguridad de la Información.
5	Recurso humano y experticia en la Seguridad de la Información.

PLAN DE FORTALECIMIENTO DE LAS CAPACIDADES INSTITUCIONALES RESPECTO A LA SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN													
Actividad	Responsable / Corresponsable	1 semestre 2025						2 semestre 2025					
		E	F	M	A	M	J	J	A	S	O	N	D
Fortalecimiento del Gobierno de Seguridad de la Información.	• Secretaría De Innovación Digital. / Comité de Seguridad de la Información.		X	X	X	X	X	X	X	X	X	X	X
Fortalecimiento de los mecanismos de Planificación y Seguimiento de la Seguridad de la Información.	• Secretaría De Innovación Digital. / Comité de Seguridad de la Información.		X	X	X	X	X	X	X	X	X	X	X
Fortalecimiento de los Documentos asociados al sistema de Gestión de Calidad, relacionados con Seguridad de la Información.	• Secretaría De Innovación Digital / Secretaria Gestión Humana Y Servicio a la Ciudadanía. / Comité de Seguridad de la Información		X	X	X	X	X	X	X	X	X	X	X
Fortalecimiento de la identificación de los recursos y capacidades para la gestión de la Seguridad y privacidad de la Información.	• Secretaría De Innovación Digital. / Comité de Seguridad de la Información.		X	X	X	X	X	X	X	X	X	X	X
Fortalecimiento de la Cultura de la seguridad y privacidad de la información	• Secretaría De Innovación Digital. / Comité de Seguridad de la Información / Todas las Secretarías, Departamentos Administrativos y Gerencias a nivel central del Distrito.		X	X	X	X	X	X	X	X	X	X	X
Fortalecimiento de la gestión de la seguridad y privacidad de la información institucional	• Secretaría De Innovación Digital. / Comité de Seguridad de la Información / Las Secretarías, Departamentos Administrativos y Gerencias a nivel central del Distrito Priorizadas.		X	X	X	X	X	X	X	X	X	X	X

RECURSOS PARA EL FORTALECIMIENTO DE LAS CAPACIDADES INSTITUCIONALES RESPECTO A LA SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

La seguridad 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 fortalecer las capacidades institucionales respecto a la seguridad y privacidad de la información es clave para desarrollar, implementar y gestionar estrategias efectivas que respondan adecuadamente a las necesidades directivas y faciliten la gestión integral de los procesos relacionados con la seguridad y privacidad de la información. Por ello, es necesario integrar el siguiente factor humano para cumplir con las necesidades de fortalecimiento de las capacidades institucionales en materia de seguridad y privacidad de la información:

Actividad	Tipo de recurso	Numero de recurso	Presupuesto mensual por recurso	Presupuesto Anual
Fortalecimiento del Gobierno de Seguridad y Privacidad de la Información.	Humano Especializado	1	\$10.510.329	\$115.613.629
Fortalecimiento de los mecanismos de Planificación y Seguimiento de la Seguridad y Privacidad de la Información				
Fortalecimiento de los Documentos asociados al sistema de Gestión de Calidad, relacionados con Seguridad y Privacidad de la Información				
Fortalecimiento de los recursos y capacidades para la gestión de la Seguridad y Privacidad de la Información	Humano Especializado	1	\$ 7.590.793	\$ 83.498.732
Fortalecimiento de la cultura de la seguridad y privacidad de la información				
Fortalecimiento de la gestión de la seguridad y privacidad de la información institucional				
TOTAL				\$ 199.112.361

PRODUCTOS DE LAS ACTIVIDADES PARA EL FORTALECIMIENTO DE LAS CAPACIDADES 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
Fortalecimiento del Gobierno de Seguridad y Privacidad de la Información.	Humano Especializado	1/3	✓ Informes de avance trimestral en la ejecución del plan seguridad y privacidad de la información. ✓ Informe de avance trimestral en la ejecución del plan de tratamiento de riesgos de seguridad y privacidad de la información. ✓ Informe de acompañamiento para la aprobación de la política general de seguridad y privacidad de la información.
Fortalecimiento de los mecanismos de Planificación y Seguimiento de la Seguridad y Privacidad de la Información	Humano Especializado	1/3	✓ Diagnóstico de brechas de recursos financieros asociados a seguridad y privacidad de la información para 10 dependencias priorizadas (Inversión vs Necesidad).
Fortalecimiento de los Documentos asociados al sistema de Gestión de Calidad, relacionados con Seguridad y Privacidad de la Información	Humano Especializado	1/3	✓ Propuesta de proceso de Gestión de Seguridad y Privacidad de la Información. ✓ Propuesta de Manual de Seguridad y Privacidad de la información.
Fortalecimiento de los recursos y capacidades para la gestión de la Seguridad y Privacidad de la Información	Humano Especializado	1/3	✓ Diagnóstico de Recursos y Capacidades para la Gestión de la Seguridad y Privacidad de la Información para una dependencia/proceso priorizado.
Fortalecimiento de la cultura de la seguridad y privacidad de la información	Humano Especializado	1/3	✓ Actas de Asistencia de 20 jornadas de sensibilización en materia de seguridad y privacidad de la información.
Fortalecimiento de la gestión de la seguridad y privacidad de la información institucional	Humano Especializado	1/3	✓ Consolidado de la Matriz de Activos de Información clasificados como Altos de 5 dependencias priorizadas ✓ Consolidado de la Matriz de Riesgos de Seguridad y Privacidad de la Información clasificados como Altos de 5 dependencias priorizadas

B. FORTALECIMIENTO DE LOS PROCESOS INSTITUCIONALES RELACIONADOS CON LA SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

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.

el cual se divide en 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 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:

FORTALECIMIENTO DE LOS PROCESOS INSTITUCIONALES RELACIONADOS CON LA SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN- GRUPO 1									
Actividad	Responsable	1 semestre 2025							
		E	F	M	A	M	J	J	A
Realizar la autoevaluación de seguridad y privacidad de la información de cada dependencia a nivel central con corte a diciembre de 2025.	Todas las Secretarías, Departamentos Administrativos y Gerencias a nivel central del Distrito, así como sus respectivas subsecretarías, unidades, equipos, etcétera en caso de realizar la ejecución del plan de forma individual.		X	X					
Realizar la identificación, clasificación y valoración de 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 subsecretarías, unidades, equipos, etcétera en caso de realizar la ejecución del plan de forma individual.				X	X			
Realizar la identificación, análisis y valoración de los riesgos de seguridad y privacidad de la 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 subsecretarías, unidades, equipos, etcétera en caso de realizar la ejecución del plan de forma individual.						X	X	X
Realizar el acompañamiento a los diferentes procesos de seguridad de la información (Autoevaluación, Gestión de activos y riesgos de seguridad y privacidad de la información), enmarcados en el plan de seguridad y privacidad de la información, lo anterior bajo la responsabilidad de las dependencias que estructuran el Distrito especial de ciencia, tecnología e innovación de Medellín a nivel central.	Secretaría de Innovación Digital		X	X	X	X	X	X	X
Realizar el seguimiento al cumplimiento de los diferentes procesos de seguridad de la información (Autoevaluación, Gestión de activos y riesgos de seguridad y privacidad de la información), enmarcados en el plan de seguridad y privacidad de la información, lo anterior bajo la responsabilidad de las dependencias que estructuran el Distrito especial de ciencia, tecnología e innovación de Medellín a nivel central.	Todas las Secretarías, Departamentos Administrativos y Gerencias a nivel central del Distrito, así como sus respectivas subsecretarías, unidades, equipos, etcétera en caso de realizar la ejecución del plan de forma individual.		X	X	X	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 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:

FORTALECIMIENTO DE LOS PROCESOS INSTITUCIONALES RELACIONADOS CON LA SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN- GRUPO 2									
Actividad	Responsable	1 semestre 2025							
		E	F	M	A	M	J	J	A
Realizar la entrega de las actividades restantes referente a los procesos de gestión de seguridad y privacidad de la información ejecutados en el marco del cierre de las brechas del plan de seguridad y privacidad de la información en la vigencia 2025.	Todas las Secretarías, Departamentos Administrativos y Gerencias a nivel central del Distrito, así como sus respectivas subsecretarías, unidades, equipos, etcétera en caso de realizar la ejecución del plan de forma individual.	X	X	X					
Realizar la autoevaluación de seguridad de la información de cada dependencia a nivel central con corte a diciembre de 2025.	Todas las Secretarías, Departamentos Administrativos y Gerencias a nivel central del Distrito, así como sus respectivas subsecretarías, unidades, equipos, etcétera en caso de realizar la ejecución del plan de forma individual.		X	X					
Realizar la identificación, clasificación y valoración de 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 subsecretarías, unidades, equipos, etcétera en caso de realizar la ejecución del plan de forma individual.				X	X			
Realizar la identificación, análisis y valoración de los riesgos de seguridad y privacidad de la	Todas las Secretarías, Departamentos Administrativos y Gerencias a nivel central						X	X	X



Alcaldía de Medellín
 Distrito de
Ciencia, Tecnología e Innovación

información bajo la responsabilidad de cada dependencia a nivel central.	del Distrito, así como sus respectivas subsecretarías, unidades, equipos, etcétera en caso de realizar la ejecución del plan de forma individual.							
Realizar el acompañamiento a los diferentes procesos de seguridad de la información (Autoevaluación, Gestión de activos y riesgos de seguridad y privacidad de la información), enmarcados en el plan de seguridad y privacidad de la información, lo anterior bajo la responsabilidad de las dependencias que estructuran el Distrito especial de ciencia, tecnología e innovación de Medellín a nivel central.	Secretaría de Innovación Digital		X	X	X	X	X	X
Realizar el seguimiento al avance en las entregas de los diferentes procesos de seguridad de la información (Autoevaluación, Gestión de activos y riesgos de seguridad y privacidad de la información), enmarcados en el plan de seguridad y privacidad de la información, lo anterior bajo la responsabilidad de las dependencias que estructuran el Distrito especial de ciencia, tecnología e innovación de Medellín a nivel central.	Secretaría de Innovación Digital		X	X	X	X	X	X

RECURSOS PARA APOYAR AL FORTALECIMIENTO PARA LA GESTIÓN DE ACTIVOS DE INFORMACIÓN, DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN Y DE LA CULTURA 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 y privacidad de la información es clave para desarrollar y ejecutar estrategias efectivas que faciliten la gestión integral de los procesos relacionados con la seguridad y privacidad de la información.

Para el desarrollo de las actividades bajo la responsabilidad de las dependencias, cada responsable de dependencia deberá disponer de un enlace de seguridad y privacidad de la información para facilitar la interacción entre el equipo de acompañamiento y seguimiento al modelo de seguridad y privacidad de la información y la disposición del personal adscrito a su dependencia, para facilitar el desarrollo de la actividad a nivel de equipos de trabajo, unidades y subsecretarías, de manera que se pueda tener claridad sobre la exposición de riesgo de cada dependencia de manera integral.

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:



Alcaldía de Medellín
 Distrito de
 Ciencia, Tecnología e Innovación

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 (Autoevaluación, Gestión de activos y riesgos), enmarcados en el plan de seguridad y privacidad de la información, lo anterior bajo la responsabilidad de las dependencias que estructuran el Distrito especial de ciencia, tecnología e innovación de Medellín a nivel central.	Humano Especializado	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	\$7.006.887	\$77.075.753



Alcaldía de Medellín
 Distrito de
Ciencia, Tecnología e Innovación

Realizar el seguimiento al cumplimiento de los diferentes procesos de seguridad y privacidad de la información (Autoevaluación, Gestión de activos y riesgos de seguridad y privacidad de la información), enmarcados en el plan de seguridad y privacidad de la información, lo anterior bajo la responsabilidad de las dependencias que estructuran el Distrito especial de ciencia, tecnología e innovación de Medellín a nivel central.		➤ Gerencia étnica ➤ 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				\$ 77.075.753

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 entrega de las actividades restantes referente a los procesos de gestión de seguridad y privacidad de la información ejecutados en el marco del cierre de las brechas del plan de seguridad y privacidad de la información en la vigencia 2025.	Disposición de cada Dependencia	Disposición de cada Dependencia	✓ Consolidado de Informes de Seguimiento Pendientes
Realizar la autoevaluación de seguridad de la información de cada dependencia a nivel central con corte a diciembre de 2025.			✓ Autoevaluación 2026 de la Dependencia
Realizar la identificación, clasificación y valoración de los activos de información bajo la responsabilidad de cada dependencia a nivel central.			✓ Catálogo de Activos de Información 2026 de la Dependencia
Realizar la identificación, análisis y valoración de los riesgos de seguridad y privacidad de la información bajo la responsabilidad de cada dependencia a nivel central.			✓ Catálogo de Riesgos de Seguridad y Privacidad de la Información 2026 de la Dependencia
Realizar el acompañamiento a los diferentes procesos de seguridad de la información (Autoevaluación, Gestión de activos y riesgos de seguridad y privacidad de la información), enmarcados en el plan de seguridad y privacidad de la información, lo anterior bajo la responsabilidad de las dependencias que estructuran el Distrito especial de ciencia, tecnología e innovación de Medellín a nivel central.	Humano Especializado	1	✓ Informes 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
Realizar el seguimiento al avance en las entregas de los diferentes procesos de seguridad de la información (Autoevaluación, Gestión de activos y riesgos de seguridad y privacidad de la información), enmarcados en el plan de seguridad y privacidad de la información, lo anterior bajo la responsabilidad de las dependencias que estructuran el Distrito especial de ciencia, tecnología e innovación de Medellín a nivel central.			

Los responsables adelantaran las actividades concernientes con el propósito de aportar al fortalecimiento del Modelo de Seguridad y Privacidad de la Información institucional, 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 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 SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

Para facilitar el seguimiento a la ejecución del plan 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 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.

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

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

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

En relación con el avance en la implementación, tomada a partir de la autoevaluación propuesta por el Ministerio de Tecnologías de Información y de las Comunicaciones, se define como meta de implementación:

Incremento de 8 puntos porcentuales en la valoración del componente P-H-V-A asociados a la Gestión de la Seguridad y Privacidad de la Información, respecto de la última medición alcanzada.