Alcaldía de Itagüí

PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN 2025.

MUNICIPIO DE ITAGÜÍ.

1. INTRODUCCIÓN

En cumplimiento del CONPES 3995 de 2020 y el Decreto Nacional 767 de 2022, que establecen los lineamientos generales de la Política de Gobierno Digital y sus habilitadores transversales, se resalta la Seguridad y Privacidad de la Información como un componente esencial. En este contexto, el Estado Colombiano ha adoptado el Modelo de Seguridad y Privacidad de la Información (MSPI) como instrumento fundamental para la implementación de estrategias de protección de datos, gestión de riesgos y cumplimiento normativo.

Este modelo se articula con los procesos, trámites, servicios, sistemas de información e infraestructura, y se complementa con los requisitos de la estrategia de seguridad digital establecidos en el artículo 5 de la Resolución 500 de 2021, emitida por el Ministerio de Tecnologías de la Información y las Comunicaciones (MinTIC), alineándose con los habilitadores de la Política de Gobierno Digital. En este marco, se formula el presente documento con el objetivo de fortalecer las capacidades institucionales, mitigar riesgos y establecer acciones necesarias para garantizar la confidencialidad, integridad, disponibilidad y privacidad de los datos en el Municipio de Itagüí. Además, se busca una integración efectiva con la estrategia de Seguridad Digital de la entidad y la Política de Seguridad de la Información.

El Municipio de Itagüí, mediante el Decreto Municipal Nro. 673 del 7 de mayo de 2018, adoptó el Modelo Integrado de Planeación y Gestión (MIPG), subrayando la importancia de articular modelos y sistemas de gestión con el sistema de control interno municipal. Este enfoque permite una gestión sostenible y una mejora continua, en concordancia con la Política de Gobierno Digital y las directrices de Gestión y Desempeño Institucional del MIPG. La Política de Gobierno Digital se ha integrado con el MIPG como un factor dinamizador para alcanzar las metas de desarrollo administrativo y fortalecer la gestión pública.

El artículo 2.2.9.1.2.1 del Decreto Nacional 1078 de 2015, modificado por el Decreto Nacional 767 de 2022, impone la obligación de desarrollar capacidades en seguridad y privacidad de la información en todos los procesos, trámites, servicios, sistemas de información e infraestructura, con el propósito de garantizar la protección de los datos. Así mismo, el Decreto Nacional 2106 de 2019 exige a las entidades que implementen procesos digitales contar con sistemas de gestión documental electrónica y archivo digital, asegurando la integridad, disponibilidad y autenticidad de la información.

En este sentido, la estrategia de seguridad digital del Municipio de Itagüí sigue los lineamientos de MinTIC, garantizando una correcta gestión y protección de la información en entornos digitales. La Resolución 500 de 2021 del MinTIC establece lineamientos y estándares para la estrategia de seguridad digital, obligando a las entidades a implementar el MSPI, gestionar riesgos y definir procedimientos para incidentes de seguridad digital.

El Gobierno Nacional, a través del Decreto 767 de 2022 y su reglamentación en el Decreto Único del Sector TIC (1078 de 2015) y (338 de 2022), ha consolidado la Política de Gobierno Digital como un instrumento para mejorar la gestión pública y la relación con los ciudadanos. El Manual de la Política de Gobierno Digital del MinTIC destaca su impacto en la calidad de vida de los ciudadanos y la competitividad del país, promoviendo la generación de valor público mediante la transformación digital del Estado. Esta política se implementa a través de un esquema que articula gobernanza, innovación pública digital, habilitadores, líneas de acción e iniciativas dinamizadoras. 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 este contexto, el Municipio de Itagüí ha actualizado su Plan de Seguridad y Privacidad de la Información, el cual fue socializado y aprobado por el Comité Institucional de Gestión de Desempeño de la Administración Municipal. Este plan representa un paso clave para fortalecer la seguridad digital, mitigar riesgos y garantizar la protección de la información en la entidad.

2. OBJETIVO

Establecer una hoja de ruta que fortalezca las capacidades institucionales, minimice riesgos y defina las actividades necesarias para garantizar la confidencialidad, integridad, disponibilidad y privacidad de los datos en el Municipio de Itagüí. Esto se realizará en conformidad con el Modelo de Seguridad y Privacidad de la Información (MSPI) de la Política de Gobierno Digital, alineado con las normas de calidad, en especial la NTC/IEC ISO 27001, la Política de Seguridad Digital y los criterios de continuidad operativa de los servicios.

Las acciones propuestas están diseñadas para asegurar la protección de la información en los procesos administrativos del Municipio de Itagüí, fortaleciendo la integridad, confidencialidad y disponibilidad de los activos de información de la entidad. Esto permitirá mitigar los riesgos a los que está expuesta la administración municipal hasta niveles aceptables, mediante la implementación de estrategias de seguridad digital establecidas en este documento para la vigencia 2024.

Este enfoque responde a los objetivos fundamentales del Modelo de Seguridad y Privacidad de la Información, que destaca la importancia de garantizar un manejo adecuado de la información pública en manos de las entidades responsables. Dicha información es un activo fundamental para la toma de decisiones, por lo que el modelo se basa en un enfoque dual:

I. **Seguridad de la Información**: Proporciona directrices para que las entidades implementen políticas que protejan la información tanto en el ámbito físico como lógico, garantizando su integridad, disponibilidad y autenticidad en todo momento.

II. **Privacidad de la Información**: Complementa la seguridad con un enfoque centrado en la protección de los derechos a la intimidad, el buen nombre y la reserva de secretos profesionales, industriales o información privilegiada en posesión de la administración. También se consideran los principios de acceso a la información pública, especialmente cuando esta no se encuentra sujeta a reserva.

Para alcanzar estos objetivos, el modelo de Seguridad de la Información incorpora un componente específico de privacidad, permitiendo así una gestión integral que abarque tanto la seguridad como la protección de la privacidad en el manejo de la información pública y privada por parte de las entidades responsables.

2. ALCANCE

Este plan se dirige a todos los procesos del Municipio de Itagüí, en consonancia con el alcance del modelo de Seguridad y Privacidad de la Información, la estrategia de Seguridad Digital de la entidad y las demás políticas y lineamientos relacionados vigentes. Para ello, el presente documento abarca todo el modelo de operación por procesos de esta Alcaldía Municipal, cumpliendo con lo establecido en el Decreto 1083 de 2015, que expide el Decreto Único Reglamentario del Sector de Función Pública, así como con el Decreto Nacional 1078 de 2015 en lo referente a la Política de Gobierno Digital y su Modelo de Seguridad y Privacidad de la Información de la Resolución 500 de 2021 (MINTIC).

3. NORMATIVIDAD.

Constitución Política de Colombia: Artículos 15, 20, 23 y 74.
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”.
Ley 23 de 1982: Sobre derechos de autor.
Ley 44 de 1993: Por la cual se modifica y adiciona la Ley 23 de 2082 y se modifica la Ley 29 de 2044 y Decisión Andina 351 de 2015 (Derechos de autor).
Ley 527 de 1999: “Por la cual se define y reglamenta el acceso y uso de los mensajes de datos, del comercio electrónico y de las firmas digitales y se establecen las entidades de certificación y se dictan otras disposiciones”.
Ley 594 de 2000: “Por medio de la cual se regula el Derecho Fundamental de Petición y se sustituye un título del Código de Procedimiento Administrativo y de lo Contencioso Administrativo”.

Ley 962 de 2005: “Por la cual se dictan disposiciones sobre racionalización de trámites y procedimientos administrativos de los organismos y entidades del Estado y de los particulares que ejercen funciones públicas o prestan servicios públicos”.
Ley 1266 de 2008: “Por la cual se dictan las disposiciones generales del Hábeas data y se regula el manejo de la información contenida en bases de datos personales, en especial la financiera, crediticia, comercial, de servicios y la proveniente de terceros países y se dictan otras disposiciones”.
Ley 1273 de 2009: “Por medio de la cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado - denominado "de la protección de la información y de los datos"- y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones”.
Ley 1437 de 2011: “Por la cual se expide el código de procedimiento administrativo y de lo contencioso administrativo”.
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 Nacional 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 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 Nacional 1008 de 2018: “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”.
Decreto 728 de 2017. “Por el cual se adiciona el capítulo 2 al título 9 de la parte 2 del libro 2 del Decreto Único Reglamentario del sector TIC, Decreto 1078 de 2015, para fortalecer el modelo de Gobierno Digital en las entidades del orden nacional del Estado colombiano, a través de la implementación de zonas de acceso público a Internet inalámbrico.”
-**Decreto 1008 del 2018.** “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.”
Decreto Nacional 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”.

Decreto Nacional 338 de 2022. "Por el cual se adiciona el Titulo 21 a la parte 2 del libro 2 del Decreto Único 1078 de 2015, Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones, con el fin de establecer los lineamientos generales para fortalecer la gobernanza de la seguridad digital, se crea el Modelo y las instancias de Gobernanza de Seguridad Digital y se dictan otras disposiciones."

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 113 de 2023: "Por medio del cual se modifican, actualizan e integran el comité municipal de gestión y desempeño y el comité institucional de gestión y desempeño del municipio de Itagüí y se reglamenta su funcionamiento".

Decreto Municipal 1545 de 2023: "Por medio del cual se modifica la estructura orgánica de la administración municipal de Itagüí y las funciones generales de las dependencias"

Resolución 500 de 2021 (MINTIC): "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".

Resolución 746 de 2022 (MINTIC): "Por la cual se fortalece el Modelo de Seguridad y Privacidad de la Información y se definen lineamientos adicionales a los establecidos en la Resolución No. 500 de 2021".

CONPES 3995 de 2020: Confianza y Seguridad Digital

CONPES 3854 de 2017: Política Nacional de Seguridad digital. CONPES 3701 de 2011: Lineamientos de Política para Ciberseguridad y Ciberdefensa.

CONPES 4069 de 2022: Política Nacional de Ciencia, tecnología e innovación 2022-2031.

ISO/IEC 27001:2013: Tecnología de la información-Técnicas de seguridad. Sistemas de Gestión de la Seguridad de la Información (SGSI)- Requisitos.

4. DEFINICIONES:

Acceso a la Información Pública: Derecho fundamental consistente en la facultad que tienen todas las personas de conocer sobre la existencia y acceder a la información pública en posesión o bajo control de sujetos obligados. (Ley 1712 de 2014, art 4).

Activo: En relación con la seguridad de la información, se refiere a cualquier información o elemento relacionado con el tratamiento de la misma (sistemas, soportes, edificios, personas…) que tenga valor para la organización. (ISO/IEC 27000).

Activo de Información: En relación con la privacidad de la información, se refiere al activo que contiene información pública que el sujeto obligado genere, obtenga, adquiera, transforme o controle en su calidad de tal. Ciberseguridad: Capacidad del Estado para minimizar el nivel de riesgo al que están expuestos los ciudadanos, ante amenazas o incidentes de naturaleza cibernética. (CONPES 3701).

Ciberespacio: Es el ambiente tanto físico como virtual compuesto por computadores, sistemas computacionales, programas computacionales (software), redes de telecomunicaciones, datos e información que es utilizado para la interacción entre usuarios. (Resolución CRC 2258 de 2009).

Gestión de incidentes de seguridad de la información: Procesos para detectar, reportar, evaluar, responder, tratar y aprender de los incidentes de seguridad de la información. (ISO/IEC 27000).

Seguridad de la información: Preservación de la confidencialidad, integridad, y disponibilidad de la información. (ISO/IEC 27000).

Sistema de Gestión de Seguridad de la Información (SGSI): Conjunto de elementos interrelacionados o interactuantes (estructura organizativa, políticas, planificación de actividades, responsabilidades, procesos, procedimientos y recursos) que utiliza una organización para establecer una política y unos objetivos de seguridad de la información y alcanzar dichos objetivos, basándose en un enfoque de gestión y de mejora continua.

(ISO/IEC 27000). 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

MPIG: Modelo integrado de planeación y gestión

5. RESPONSABILIDAD PRINCIPAL.

La Dirección Administrativa de las Tecnologías de la Información y las Comunicaciones TIC, será la unidad administrativa encargada de liderar y dar continuidad a las actividades descritas en este plan. Así mismo, se desarrollará en articulación todo el proceso con el Comité Institucional de Gestión y Desempeño de la Administración de Itagüí y con las demás unidades administrativas de la entidad.

6. PRINCIPIOS RECTORES.

I. Salvaguardar los derechos humanos y los valores fundamentales de los ciudadanos en el municipio de Itagüí, garantizando la libertad de expresión, el acceso y flujo libre de información, la confidencialidad de datos y comunicaciones, así como la protección de la intimidad y los datos personales, en concordancia con los principios establecidos en la Constitución Política de Colombia.

II. Implementar un enfoque inclusivo y colaborativo que integre activamente a todas las partes interesadas, promoviendo la creación de alianzas estratégicas para fortalecer la seguridad digital del municipio y la protección de sus habitantes. Esto permitirá incrementar la resiliencia ante incidentes en el entorno digital.

III. Fomentar una responsabilidad compartida entre los actores involucrados, impulsando la cooperación y coordinación efectiva, con un enfoque claro sobre el rol y la responsabilidad de cada parte en la gestión de los riesgos de seguridad digital y la protección del ecosistema digital municipal.

IV. Aplicar un enfoque basado en la gestión de riesgos, que garantice un entorno digital seguro y confiable para el desarrollo de actividades económicas y sociales. Esto contribuirá al crecimiento y fortalecimiento de la economía local, impulsando la innovación, la productividad, la competitividad y la generación de empleo en todos los sectores.

7. PLAN DE IMPLEMENTACIÓN DEL MODELO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN.

La Alcaldía de Itagüí ha integrado la Política de Seguridad Digital dentro de MIPG como un pilar esencial dentro de su sistema de gestión institucional. Para su implementación y fortalecimiento, ha diseñado un conjunto de planes estratégicos orientados a desarrollar actividades alineadas con las directrices del Ministerio de Tecnologías de la Información y las Comunicaciones, en particular, la adopción e implementación del Modelo de Seguridad y Privacidad de la Información (MSPI).

En este marco, el Municipio de Itagüí establece un plan general que contribuye al fortalecimiento del MSPI, considerándolo un elemento clave para el cumplimiento de la Política de Gobierno Digital. Además, se aborda de manera integral la identificación, valoración, tratamiento y gestión de los riesgos de seguridad de la información, conforme a los lineamientos del modelo de seguridad y privacidad y en cumplimiento del estándar NTC ISO 27001:2013. Estas acciones son fundamentales para garantizar un entorno digital seguro y fortalecer la gestión de la información dentro de la entidad.

8. DESARROLLO DE LA POLÍTICA.

La Alcaldía de Itagüí ha integrado el proceso de Sistemas de Información e Infraestructura Tecnológica dentro de su modelo de procesos a nivel estratégico. Esta incorporación garantiza de manera continua la seguridad y privacidad de la información, la protección del entorno digital y la continuidad operativa de los servicios en el municipio.

9. ESTRATEGIAS DE SEGURIDAD DIGITAL, COMO ELEMENTOS ARTICULADORES

El Municipio de Itagüí, a través de la adopción e implementación del Modelo de Seguridad y Privacidad de la Información, enmarcado dentro del Sistema de Gestión de Seguridad de la Información, reafirma su compromiso con la protección, administración y resguardo de la confidencialidad, integridad, disponibilidad, autenticidad, privacidad y no repudio de la información en su operación por procesos.

Para ello, se lleva a cabo una gestión integral de riesgos y la implementación de controles digitales que permitan prevenir incidentes, garantizar la continuidad de los servicios y asegurar el cumplimiento de las normativas legales y regulatorias vigentes.

Este enfoque se basa en la mejora continua y el alto desempeño del Sistema de Gestión de Seguridad de la Información, impulsando el acceso, uso eficiente y apropiación generalizada de las Tecnologías de la Información y las Comunicaciones.

9.1. ÁMBITO DE APLICACIÓN.

La Política de Seguridad y Privacidad de la Información se aplica a todos los niveles funcionales y organizacionales del Municipio de Itagüí, incluyendo funcionarios, contratistas, proveedores, operadores y entidades descentralizadas de orden municipal. También abarca a terceros que, en el ejercicio de sus funciones, compartan, utilicen, recolectan, procesen, intercambien o consulten información del municipio. Así mismo, esta política se extiende a entidades de control y otras organizaciones que accedan, de forma interna o externa, a cualquier activo de información, sin importar su ubicación. Su alcance abarca toda la información creada, procesada o utilizada por el Municipio de Itagüí, independientemente del medio, formato o ubicación en la que se encuentre.

9.2. ESTRATEGIA DE SEGURIDAD DIGITAL.

La Alcaldía de Itagüí implementará una estrategia integral de seguridad digital que articule principios, políticas, procedimientos, guías, manuales, formatos y lineamientos para la gestión eficaz de la seguridad de la información. Esta estrategia estará enfocada en la adopción del Modelo de Seguridad y Privacidad de la Información (MSPI), complementada por la guía de gestión de riesgos de seguridad de la información y el establecimiento de un procedimiento formal para la gestión de incidentes.

9.3 DESCRIPCIÓN DE LAS ESTRATEGIAS ESPECIFICAS (EJES).

ESTRATEGIA / EJE	DESCRIPCIÓN / OBJETIVO
Liderazgo de seguridad de la información	Asegurar el establecimiento del Modelo de Seguridad y Privacidad de la Información (MSPI) mediante la aprobación de la política general y otros lineamientos definidos, con el objetivo de proteger la confidencialidad, integridad y disponibilidad de la información. Este proceso se fundamenta en el compromiso de la alta dirección y de los líderes de las diferentes dependencias o procesos de la Entidad, quienes establecerán roles y responsabilidades claras en seguridad de la información.
Gestión de riesgos	Identificar los riesgos de seguridad de la información mediante una planificación y valoración definida, con el objetivo de prevenir o reducir los efectos no deseados. Esto se basa en la implementación de controles de seguridad para abordar los riesgos identificados.

Apropiación	Fortalecer la construcción de una cultura organizacional centrada en la seguridad de la información, de manera que se convierta en un hábito arraigado. Esto se logrará promoviendo el cumplimiento de políticas, procedimientos, normas, buenas prácticas y otros lineamientos relacionados. Además, se fomentará la transferencia de conocimiento, la asignación y divulgación de responsabilidades a todo el personal de la entidad en materia de seguridad y privacidad de la información.
Implementación de controles	Planificar e implementar las acciones necesarias para alcanzar los objetivos de seguridad y privacidad de la información y mantener la confianza en la ejecución de los procesos de la entidad implica la subdivisión en controles tecnológicos y/o administrativos.
Gestión de incidentes	Garantizar una gestión efectiva de incidentes de seguridad de la información mediante un enfoque integral que incluya la integración, análisis y comunicación de eventos e incidentes, así como de las debilidades de seguridad. Esto tiene como objetivo identificar y resolver estos incidentes para minimizar su impacto negativo en la Entidad.

9.4. ROLES Y RESPONSABILIDADES DE ARTICULACIÓN.

Para el cumplimiento de la Política de Seguridad y Privacidad de la Información del municipio de Itagüí, se definen los siguientes roles y responsabilidades.

1. El Departamento Administrativo de Planeación, la Secretaría General por medio del Equipo de Gestión Documental y la Dirección Administrativa de las TIC por medio del Grupo de Infraestructura Tecnológica y Gobierno Digital, revisarán y actualizarán los activos de información, y para ello tendrán en cuenta la clasificación según su naturaleza, como, por ejemplo, documentos, información, software, hardware y/o componentes de red.

2. El Grupo de Infraestructura Tecnológica y Gobierno Digital, realizará el levantamiento de la Infraestructura Tecnológica Crítica de la Entidad.

3. El Grupo de Infraestructura Tecnológica y Gobierno Digital, apoyará la actualización de los riesgos de seguridad digital, siguiendo la metodología dispuesta por el Departamento Administrativo de la Función Pública (DAFP) y el Ministerio de Tecnologías de la Información y las Comunicaciones (MINTIC).

4. Todas las Unidades Administrativas con el apoyo de la Dirección Administrativa de las Tecnologías y Sistemas de la Información y las Comunicaciones TIC y la Secretaría de Evaluación y Control, implementarán el Modelo de Seguridad y Privacidad de la Información (MSPI) con las herramientas que el Ministerio de Tecnologías de la Información y las Comunicaciones destine para ello, el cual integra en cada una de sus fases, tareas asociadas a la gestión de riesgos de seguridad digital.

5. La Dirección Administrativa de las Tecnologías y Sistemas de la Información y las Comunicaciones TIC y la Secretaría de Evaluación y Control, Grupo de Infraestructura Tecnológica y Gobierno Digital, establecerán los controles definidos en el Anexo A de la ISO 27001, que en el MSPI se define como la Declaración de Aplicabilidad.

6. La Dirección Administrativa de las Tecnologías y Sistemas de la Información y las Comunicaciones TIC, con el apoyo del Departamento Administrativo de Planeación y la Secretaría de Evaluación y Control, evaluarán el desempeño del Modelo de Seguridad y Privacidad de la Información (MSPI), a través de la aplicación de la Política de Seguridad y Privacidad de la Información, la ejecución de los controles definidos en la declaración de aplicabilidad y el monitoreo de los indicadores de seguridad de la información.

7. La Dirección Administrativa de las Tecnologías y Sistemas de la Información y las Comunicaciones TIC por medio del Grupo de Infraestructura Tecnológica y Gobierno Digital, desarrollará el Procedimiento de Gestión de Incidentes de Seguridad de la Información y en él se establecerá como actividad el reporte de los incidentes a las autoridades competentes y designadas para tal fin.

8. La Secretaría de Servicios Administrativos a través de la Oficina de Talento Humano, brindará capacitación técnica y tecnológica para atender riesgos de seguridad digital y fortalecerá la capacidad humana de los servidores públicos adscritos al Municipio de Itagüí, esto en articulación con la Dirección Administrativa de las Tecnologías y Sistemas de la Información y las Comunicaciones TIC.

9. La Dirección Administrativa de las Tecnologías y Sistemas de la Información y las Comunicaciones TIC por medio del Grupo de Gobierno Digital y la Oficina de Talento Humano, sensibilizan a usuarios internos en el uso de medios digitales y en buenas prácticas para mitigar los riesgos de seguridad digital que puedan afectar a la Entidad. Para tal fin, se articulará con la Secretaría de Comunicaciones.

10.El Comité Institucional de Gestión y Desempeño de la Administración Municipal de Itagüí será el responsable de aprobar la Política de Seguridad y Privacidad de la Información de la Entidad.

Así mismo deberá asegurar la implementación y desarrollo de políticas de gestión y directrices en materia de seguridad y privacidad de la información, mediante el cumplimiento de las siguientes actividades:

10.1. Aprobación seguimiento a los planes, programas, proyectos, estrategias y herramientas necesarias para la implementación interna de las políticas digitales.

10.2. Socializar la importancia de adoptar la cultura de seguridad y privacidad de la información a los procesos de la entidad.

10.3. Aprobar acciones y mejores prácticas en la implementación del MSPI.

10.4. Adoptar las decisiones que permitan la gestión y minimización de riesgos críticos de seguridad de la información.

10.5. Las demás que tengan relación con el estudio, análisis y recomendaciones en materia de seguridad y privacidad de la información.

9.5. MEJORAMIENTO CONTINUO.

La entidad consolidará los resultados obtenidos en la evaluación del desempeño para diseñar un plan integral de mejora continua en seguridad y privacidad de la información. Este plan estará enfocado en la implementación de estrategias que fortalezcan el sistema y reduzcan las vulnerabilidades detectadas.

Para ello, se estructurará un plan de optimización basado en los siguientes aspectos clave:

I. Los hallazgos obtenidos a partir del seguimiento, evaluación y análisis del Sistema de Seguridad y Privacidad de la Información (SSPI).
II. Los resultados derivados de auditorías y revisiones independientes realizadas al SSPI.

Con esta información, la entidad ajustará los controles, procedimientos y entregables del sistema, garantizando su alineación con las mejores prácticas en seguridad de la información. Además, se desarrollará un plan integral de mejora y una estrategia de comunicación para su implementación efectiva.

Antes de su ejecución, estos planes serán sometidos a revisión y aprobación por parte de la mesa técnica de gobierno digital, y posteriormente presentados ante el comité municipal de gestión y desempeño para su validación final.

10. ACTIVIDADES DE SEGUIMIENTO AL PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN EN ARTICULACIÓN CON EL PLAN DE ACCIÓN DE LA DIRECCIÓN ADMINISTRATIVA DE LAS TECNOLOGÍAS Y SISTEMAS DE LA INFORMACIÓN Y LAS COMUNICACIONES TIC.

En virtud de las competencias y facultades de la Dirección Administrativa de las Tecnologías de la Información y las Comunicaciones TIC, se articulan las siguientes actividades de seguimiento al plan, las cuales aportan al proceso estratégico de esta unidad administrativa de cara a la administración municipal. (Ver Anexo 1)

11.CONTROL DE APROBACIONES

PROYECTÓ	APROBÓ	SOCIALIZADO
EQUIPO MSPI	SANTIAGO ECHAVARRIA GALLEGO	COMITÉ INSTITUCIONAL DE GESTIÓN Y DESEMPEÑO
Contratistas - Dirección Administrativa de las TIC	Director Administrativo de las Tecnologías de la Información y las Comunicaciones TIC.	

12. CONTROL DE VERSIONES

VERSIÓN	FECHA	DESCRIPCIÓN	PROYECTÓ	REVISÓ / APROBÓ
Versión 01	2024	Elaboración del Plan.	EQUIPO MSPI	SANTIAGO ECHAVARRIA GALLEGO
Versión 02	2025	Actualización del Plan.	EQUIPO MSPI	SANTIAGO ECHAVARRIA GALLEGO

Alcaldía de Itagüí

PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

UNIDAD ADMINISTRATIVA: DIRECCIÓN ADMINISTRATIVA DE LAS TECNOLOGÍAS Y SISTEMAS DE LA INFORMACIÓN Y LAS COMUNICACIONES TIC

VIGENCIA: 2025

ESTRATEGIA	ACTIVIDAD	FUENTE DE VERIFICACIÓN	RESPONSABLES	CORRESPONSABLES	AVANCE DE EJECUCIÓN DE LAS ACTIVIDADES (EN % DE CUMPLIMIENTO)																	
					MARZO		ABRIL		MAYO		JUNIO		JULIO		AGOSTO		SEPTIEMBRE		OCTUBRE		NOVIEMBRE	
					P	E	P	E	P	E	P	E	P	E	P	E	P	E	P	E	P	E
Liderazgo de seguridad de la información.	Realizar el Autodiagnóstico de Seguridad y privacidad de la información de la Entidad, con el instrumento del MSPI.	Instrumento de autodiagnóstico diligenciado	. Equipo MSPI Equipo Infraestructura				25%		25%		25%		25%									
	Definirr/actualizar la política de Seguridad de la Información de la Entidad.	Política de Seguridad y privacidad de la información actualizada,aprobada e Implementada.	Equipo MSPI				33%		33%		33%											
	Definiir roles y responsabilidades de Seguridad de la Información.	Definición de los Roles y Responsabilidades en Seguridad de la Información, formalizados dentro de las políticas de Seguridad.	Equipo MSPI				33%		33%		33%											
	Definir/actualizar el Manual de políticas de Seguridad de la información de la Entidad.	Manual de políticas de Seguridad de la información actualizado, aprobado e implementado.	. Equipo MSPI								50%		50%									
	Acompañar a las diferentes dependencias que tengan relación con MIPG y FURAG mediante la implementación de la política de seguridad digital	Formulario diligenciado	. Equipo MSPI			**100%**							100%									
Gestión de riesgos	Actualizar el Plan de Tratamiento de Riesgos de seguridad y privacidad de la información, que incluya la identificación, valoración y clasificación de los riesgos asociados a los activos de información de la Entidad.	Plan de Tratamiento de Riesgos actualizado, aprobado e implementado.	. Equipo MSPI	Unidad Admnistrativa Planeación--Calidad Gestión Documental					20%		20%		20%		20%		20%					
	Realizar revisión/ actualización, monitoreo, seguimiento y control a los riesgos de Seguridad de la Información identificados.	Matriz de Riesgos de Seguridad y Privacidad de la información actualizada.	. Equipo MSPI Equipo Calidad	Unidad Admnistrativa Planeación--Calidad Gestión Documental							20%		20%		20%		20%		20%			
Apropiación	Establecer capacitaciones, sensibilización y comunicación en Seguridad de la Información en la Entidad.	Plan de capacitación, sensibilización y comunicación de Seguridad de la Información, aprobado.	. Equipo MSPI	Talento Humano Comunicaciones			10%		10%		10%		10%		10%		10%		10%		10%	
	Realizar jornadas de sensibilización a todos los grupos de valor e interés de la Entidad.	Actas de reunión, eventos realizados.	. Equipo MSPI	Talento Humano Comunicaciones					20%		20%		20%		20%		20%					
	Realizar trasferencia de conocimiento a los diferentes grupos de valor e interés de la Entidad, a través de cursos especializados en temas de Seguridad de la Información.	Certificaciones/evidencias de cursos realizados.	. Equipo MSPI	Talento Humano			10%		10%		10%		10%		10%		10%		10%		10%	

	Medir el grado de sensibilización a toda la Entidad.	Resultado de encuestas de satisfacción y de medición respecto a la implementación del Plan de sensibilización.	. Equipo MSPI								33%				33%				33%				
Implementación de controles	**Implementar Control A.5.1.1** Políticas para la seguridad de la información Definir un conjunto de políticas para la seguridad de la información, aprobada por la dirección, publicada y comunicada a los diferentes grupos de valor e interés de la Entidad.	Políticas para la seguridad de la información, aprobadas e implementadas.	. Equipo MSPI						50%		50%												
	Implementar Control A.8.1.1 Inventario de activos Identificar los activos asociados con la información y las instalaciones de procesamiento de información.	Inventario de activos actualizado.	. Equipo MSPI Equipo Calidad	Unidad Admnistrativa Planeación--Calidad		80%	10%		10%														
	Implementar Control A.8.2.1 Clasificación de la información Clasificar la información en función de los requisitos legales, valor, criticidad y susceptibilidad a divulgación o a modificación no autorizada.	Información debidamente clasificada de acuerdo con los parámetros establecidos.	. Equipo MSPI	Unidad Admnistrativa Planeación--Calidad Gestión Documental					33%		33%		33%										
	Implementar Control A.12.1.2 Gestión de cambios Controlar los cambios en la organización, en los procesos de negocio, en las instalaciones y en los sistemas de procesamiento de información que afectan la seguridad de la información.	Procedimiento de Gestión de cambios aprobado e implementado.	. Equipo MSPI Equipo Calidad								50%		50%										
Gestión de incidentes	Realizar la identificación, clasificación, tratamiento y divulgación de Incidentes Seguridad de la Información, sobre los activos de información, bajo la responsabilidad de cada Unidad Administrativa.	Incidentes de Seguridad de la Información identificados, clasificados, tratados y divulgados. -Matriz de riesgos de seguridad y privacidad de la información actualizada.	. Equipo MSPI Equipo Calidad	Unidad Admnistrativa Planeación--Calidad Gestión Documental							50%		50%										
	Capacitar con relación la gestión de incidentes de seguridad de la información.	Sesiones de capacitación desarrolladas, actas de capacitación.	. Equipo MSPI	Unidad Admnistrativa Planeación--Calidad Gestión Documental							50%		50%										