Alcaldía de Itagüí

PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN 2025.

MUNICIPIO DE ITAGÜÍ.

1. INTRODUCCIÓN

La creciente digitalización de los procesos administrativos y la prestación de servicios en el sector público colombiano ha generado nuevos retos en materia de protección de la información, continuidad operativa y confianza institucional. En este contexto, el Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información de la Alcaldía de Itagüí se formula como un instrumento estratégico esencial para la gestión integral de los riesgos que puedan afectar la confidencialidad, integridad, disponibilidad y trazabilidad de los activos de información institucionales.

Este plan responde a una necesidad estructural de fortalecer la cultura de la gestión del riesgo dentro de la administración pública, mediante la implementación de acciones preventivas, correctivas y de mejora continua, orientadas a reducir la probabilidad e impacto de eventos que puedan comprometer el cumplimiento de los objetivos institucionales. La gestión de riesgos se enmarca en un enfoque sistémico, basado en estándares internacionales como la norma ISO/IEC 27001, y guiado por los lineamientos establecidos en el Modelo de Seguridad y Privacidad de la Información (MSPI) del Ministerio de Tecnologías de la Información y las Comunicaciones (MinTIC).

La elaboración del presente plan tiene su fundamento normativo en la Política de Gobierno Digital, establecida por el Decreto 767 de 2022, que subroga parcialmente el Decreto 1078 de 2015, y que define la seguridad y privacidad de la información como habilitadores fundamentales para la transformación digital del Estado. Esta política, a su vez, se articula con el Modelo Integrado de Planeación y Gestión (MIPG), estableciendo que la gestión de riesgos debe integrarse a los procesos de planeación institucional y a los sistemas de control interno, como garantía del cumplimiento misional y de la generación de valor público.

Adicionalmente, en cumplimiento de lo dispuesto por el artículo 2.2.22.3.14 del Decreto 1083 de 2015, adicionado por el Decreto 612 de 2018, todas las entidades públicas del orden nacional y territorial deben adoptar anualmente el Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información, en el marco de los planes institucionales y estratégicos que conforman el Plan de Acción, según lo estipulado en el artículo 74 de la Ley 1474 de 2011.

En concordancia con esta normativa nacional, la Alcaldía de Itagüí adoptó mediante el Decreto Municipal N.º 056 del 30 de enero de 2025 los planes institucionales y estratégicos de la administración municipal, entre los cuales se incluye, en su numeral 11, el Plan de Seguridad y Privacidad de la Información, así como el correspondiente Plan de Tratamiento de Riesgos,

en cumplimiento del marco normativo vigente. Este acto administrativo reafirma el compromiso del municipio con la gestión responsable de la información pública y la incorporación efectiva de lineamientos nacionales a nivel territorial.

Por su parte, la Resolución 0500 de 2021 del MinTIC establece directrices técnicas para la implementación del MSPI, así como para la gestión de riesgos, el manejo de incidentes de seguridad digital y la adopción de controles técnicos, administrativos y organizacionales. El artículo 5 de dicha resolución destaca la importancia del análisis y tratamiento de riesgos como eje transversal del plan de seguridad de la información de cada entidad. Asimismo, el Anexo 1, en su capítulo de planificación, señala que toda entidad debe estructurar un plan específico de tratamiento de riesgos, alineado con su contexto interno y externo, y con base en metodologías internacionales.

Este plan, por tanto, se convierte en una herramienta de planeación estratégica y operativa que permite gestionar de forma estructurada los riesgos asociados a la información, promover la resiliencia institucional, y proteger los derechos de los ciudadanos en el entorno digital, de acuerdo con los principios de legalidad, transparencia, eficiencia, responsabilidad y protección de datos personales establecidos en la Ley 1581 de 2012 y demás disposiciones complementarias.

La Alcaldía de Itagüí, consciente de su rol como entidad territorial comprometida con la modernización del Estado y la garantía de un servicio público eficiente y seguro, adopta este Plan de Tratamiento de Riesgos como parte de su compromiso con la mejora continua, el uso responsable de las tecnologías de la información y la generación de confianza en sus ciudadanos, consolidando así un modelo de gobernanza digital sólido y orientado al cumplimiento misional.

2. OBJETIVO

Establecer un marco integral para la identificación, análisis, evaluación, tratamiento, seguimiento y control de los riesgos asociados a la Seguridad y Privacidad de la Información, la Seguridad Digital y la Continuidad de la Operación de los servicios tecnológicos de la Alcaldía de Itagüí, con el fin de proteger la confidencialidad, integridad, disponibilidad, autenticidad y privacidad de la información institucional. Este objetivo se enmarca en el cumplimiento de los lineamientos establecidos en la Política de Gobierno Digital, el Modelo de Seguridad y Privacidad de la Información (MSPI), el Decreto Nacional 767 de 2022, la Resolución MinTIC 0500 de 2021, el Decreto Presidencial 612 de 2018,

, que adopta los planes institucionales y estratégicos en el municipio. De esta manera, el plan contribuye al fortalecimiento de la cultura organizacional en materia de gestión de riesgos, al cumplimiento normativo, a la mejora continua de los procesos institucionales y a la garantía de la continuidad de los servicios públicos digitales, en coherencia con la misión, visión y objetivos estratégicos de la entidad territorial.

3. ALCANCE

El alcance del Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información para la Alcaldía de Itagüí abarca la gestión integral de los riesgos relacionados con la Seguridad y Privacidad de la Información, Seguridad Digital y Continuidad de la Operación de los servicios institucionales, buscando integrar buenas prácticas y principios de gestión de riesgos en todos los procesos de la entidad. Este plan tiene como objetivo prevenir incidentes que puedan comprometer la consecución de los objetivos estratégicos del municipio, contribuyendo a una toma de decisiones informada y a la adopción de medidas que aseguren la protección de la información en un entorno digital.

El Plan considerará especialmente aquellos riesgos clasificados en los niveles Moderado, Alto y Extremo, conforme a las directrices del Ministerio de Tecnologías de la Información y las Comunicaciones (MinTIC), priorizando la atención y tratamiento de los riesgos más críticos para la Alcaldía de Itagüí. Los riesgos clasificados en niveles inferiores serán gestionados de acuerdo con la política institucional, aceptando y monitorizando aquellos que no requieran acciones correctivas inmediatas.

El ámbito del plan incluye la aplicación de los principios metodológicos establecidos para la gestión de riesgos de seguridad de la información en todos los procesos de la Alcaldía de Itagüí. Se contemplan todas las fases del ciclo de gestión de riesgos, desde la identificación del contexto y de los riesgos, pasando por su análisis y evaluación, hasta el tratamiento y la implementación de los controles necesarios. Además, se establecerán mecanismos para el seguimiento, monitoreo y evaluación continua de los riesgos, garantizando la adecuación y efectividad de las acciones implementadas a lo largo del tiempo.

El Plan de Tratamiento de Riesgos se aplicará a todos los procesos, sistemas de información, infraestructura tecnológica y activos digitales de la Alcaldía de Itagüí, permitiendo una gestión proactiva y dinámica de los riesgos, en congruencia con los

marcos normativos y las políticas de seguridad y privacidad establecidas a nivel nacional y local.

4. 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 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 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 00500 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.

CONPES 4144 DE 2025: Política Nacional de Inteligencia Artificial.

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

5. 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).

Seguridad de la Información: Conjunto de prácticas, políticas y medidas que buscan garantizar la confidencialidad, integridad, disponibilidad, autenticidad y privacidad de la información, protegiéndola contra accesos no autorizados, alteraciones, destrucción o divulgación inapropiada.

Privacidad de la Información: El derecho y la práctica de asegurar que los datos personales de los individuos sean recopilados, almacenados, procesados y compartidos de acuerdo con las leyes y principios que protegen la intimidad y los derechos fundamentales de las personas.

Riesgo de Seguridad de la Información: Posibilidad de que ocurra un evento o incidente que afecte la confidencialidad, integridad, disponibilidad o privacidad de la información dentro de los sistemas y procesos de la entidad, con consecuencias que puedan comprometer los objetivos de la organización.

Continuidad de la Operación: Capacidad de una organización para seguir funcionando durante y después de un evento disruptivo que afecte sus servicios, procesos o infraestructura tecnológica, asegurando la mínima interrupción en la prestación de los servicios y el mantenimiento de las operaciones esenciales.

Riesgo de Interrupción de los Servicios: Probabilidad de que ocurra una interrupción o suspensión de los servicios digitales de la Alcaldía de Itagüí, ya sea por fallas en los

sistemas de información, ciber incidentes, desastres naturales, u otros eventos imprevistos que impacten la continuidad de las operaciones.

Tratamiento de Riesgos: Proceso mediante el cual se identifican, evalúan, priorizan y gestionan los riesgos asociados a los activos de información, con el objetivo de implementar controles y medidas para mitigar, transferir, aceptar o evitar los riesgos identificados, según corresponda.

Seguridad Digital: Conjunto de estrategias, herramientas y medidas que buscan proteger los activos digitales, incluyendo redes, dispositivos y datos electrónicos, frente a amenazas cibernéticas y ataques que puedan comprometer la operatividad y la protección de la información en entornos digitales.

Incidente de Seguridad Digital: Cualquier evento o serie de eventos no planeados que puedan afectar la seguridad de la información, como brechas de seguridad, ciberataques, accesos no autorizados, o cualquier actividad maliciosa que comprometa los sistemas, redes o datos de la entidad.

Política de Gobierno Digital: Conjunto de directrices establecidas por el gobierno nacional para promover la transformación digital de las entidades públicas, con el fin de mejorar la interacción con los ciudadanos, la eficiencia administrativa y la prestación de servicios públicos mediante el uso de tecnologías de la información.

Modelo de Seguridad y Privacidad de la Información (MSPI): Marco establecido por el Ministerio de Tecnologías de la Información y las Comunicaciones (MinTIC) que define las directrices y mejores prácticas para la protección de la información, orientado a garantizar la seguridad y la privacidad de los datos en las entidades públicas y en los servicios digitales del gobierno.

Gestión de Riesgos: Proceso sistemático de identificación, evaluación, tratamiento, monitoreo y comunicación de los riesgos, con el fin de minimizar las consecuencias de eventos adversos y maximizar las oportunidades para la organización.

Vulnerabilidad: Debilidad en un sistema, proceso o infraestructura que puede ser explotada por amenazas, dando lugar a un riesgo potencial para la seguridad o la privacidad de la información.

Amenaza: Cualquier evento o circunstancia que, de materializarse, puede causar daño o impacto negativo sobre los sistemas, activos de información o servicios de la Alcaldía de Itagüí.

Impacto: El efecto o consecuencia que un evento riesgoso tiene sobre los activos, procesos, personas o servicios de la organización, medido en términos de daño, pérdida o afectación.

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).

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

MOP: Modelo de operación por procesos.

ISO: International Standard Organization.

Probabilidad: Se entiende la posibilidad de ocurrencia del riesgo. Estará asociada a la exposición al riesgo del proceso o actividad que se esté analizando.

TI: Tecnología de información.

TIC: Tecnologías de la información y la comunicación

Vulnerabilidad: Es una falencia o debilidad que puede estar presente en la tecnología, las personas o en las políticas y procedimientos

6. 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 de Desempeño de la Administración de Itagüí y las demás unidades administrativas de la entidad

7. PRINCIPIOS RECTORES

I. Protección de los Derechos Fundamentales: Garantizar el respeto y la promoción de los derechos humanos, especialmente aquellos relacionados con el entorno digital, como la libertad de expresión, el acceso libre a la información, la protección de la intimidad y la confidencialidad de los datos personales. Este principio se fundamenta en los valores esenciales consagrados en la Constitución Política de Colombia y en el marco normativo vigente.

II. Participación Inclusiva y Gobernanza Colaborativa: Fomentar la construcción de un entorno digital seguro a través de la participación activa y coordinada de todos los grupos de interés, tanto internos como externos. Esto incluye entidades públicas, ciudadanos, organizaciones civiles y sector privado, promoviendo la articulación de esfuerzos y la generación de alianzas estratégicas para fortalecer la seguridad digital en el municipio.

III. Responsabilidad compartida

Reconocer que la gestión de la seguridad y privacidad de la información es un deber colectivo que debe ser asumido por todas las partes involucradas. Cada actor, desde su competencia, deberá asumir con compromiso su rol en la implementación de medidas preventivas y correctivas para mitigar riesgos y garantizar la resiliencia institucional frente a amenazas digitales.

IV. Enfoque Basado en Gestión de Riesgos: Adoptar un enfoque preventivo y proactivo en la identificación, evaluación, tratamiento y monitoreo de los riesgos relacionados con la seguridad de la información, la seguridad digital y la continuidad operativa. Este enfoque busca anticiparse a los eventos disruptivos, proteger los activos de información y asegurar el desarrollo sostenible y seguro de las operaciones institucionales.

V. Confianza y Transparencia en el Entorno Digital: Impulsar la confianza pública en los servicios digitales de la Alcaldía de Itagüí mediante prácticas transparentes, responsables y verificables en el manejo de la información. Se prioriza la implementación de controles y medidas de protección que generen credibilidad en los procesos institucionales frente a los ciudadanos y usuarios del ecosistema digital.

VI. Mejora Continua e Innovación Tecnológica: Promover la evaluación constante de los procesos y herramientas utilizadas para la gestión de riesgos, así como la incorporación de tecnologías emergentes y buenas prácticas internacionales que fortalezcan la seguridad digital y la protección de la información en la entidad. La adaptación al cambio y la innovación serán claves para responder a los desafíos del entorno dinámico actual.

8. PLAN DE IMPLEMENTACIÓN DEL MODELO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN (MSPI)

La Alcaldía de Itagüí ha adoptado el Modelo de Seguridad y Privacidad de la Información (MSPI) como un componente estratégico y transversal de su sistema de gestión institucional, en concordancia con lo establecido en la Política de Gobierno Digital (Decreto 767 de 2022), el Modelo Integrado de Planeación y Gestión (MIPG) y el Decreto Municipal No. 056 de 2025, que formaliza la integración de los planes institucionales y estratégicos en el marco del Plan de Acción anual.

Este modelo constituye un habilitador clave para garantizar la confidencialidad, integridad, disponibilidad y privacidad de la información, fortaleciendo la confianza digital entre los ciudadanos, las entidades públicas y los demás actores del entorno digital local. En este contexto, el presente Plan de Implementación articula un conjunto de acciones y directrices orientadas al despliegue progresivo del MSPI en la entidad territorial, en coherencia con los lineamientos definidos por el Ministerio de Tecnologías de la Información y las Comunicaciones (MinTIC), en especial los contenidos en la Resolución 0500 de 2021 y el estándar NTC ISO/IEC 27001:2013.

9. DESARROLLO DE LA POLÍTICA DE TRATAMIENTO DE RIESGOS.

El tratamiento de riesgos en el Municipio de Itagüí se desarrolla como una acción estratégica dentro del Modelo Integrado de Planeación y Gestión (MIPG), que busca preservar la integridad, disponibilidad, confidencialidad y continuidad de la información y los servicios institucionales. Esta política se articula con los lineamientos del Ministerio de Tecnologías de la Información y las Comunicaciones (MinTIC), las normas técnicas vigentes como la NTC ISO/IEC 27001:2013 y la Guía para la Administración del Riesgo y el Diseño de Controles en Entidades Públicas del DAFP.

El enfoque adoptado permite implementar mecanismos y controles que fortalezcan la capacidad institucional para anticiparse, mitigar y responder a eventos de riesgo, principalmente en materia de Seguridad y Privacidad de la Información, Seguridad Digital y Continuidad de la Operación. De esta manera, se busca garantizar la protección de los activos de información, minimizar interrupciones y apoyar el cumplimiento de los objetivos institucionales y la prestación de los servicios a la ciudadanía.

La ejecución de esta política se desarrolla mediante una gestión estructurada que comprende las siguientes etapas: identificación del contexto, análisis del riesgo, valoración, definición del tratamiento, implementación de medidas y seguimiento. El tratamiento del riesgo es asumido por las unidades responsables del proceso, quienes

constituyen la primera línea de defensa, con el acompañamiento de la Alta Dirección y las instancias de control.

Las estrategias de tratamiento que se pueden aplicar son:

- **Aceptar el riesgo:** Se contempla cuando el riesgo es bajo o no resulta viable su mitigación. No obstante, se requiere un monitoreo constante para garantizar que no aumente su nivel.
- **Reducir el riesgo:** Consiste en implementar controles que disminuyan la probabilidad de ocurrencia y/o el impacto del riesgo, como segregación de funciones, ajustes tecnológicos o fortalecimiento de capacidades internas.
- **Evitar el riesgo:** Implica suspender, cancelar o no iniciar la actividad que origina el riesgo, en los casos en que su materialización pueda comprometer de forma crítica la operación o la seguridad de la información.
- **Compartir el riesgo:** Consiste en transferir parte de la exposición al riesgo mediante seguros, alianzas estratégicas o contratación con terceros, sin que esto implique delegar la responsabilidad institucional.

La aplicación de estas estrategias debe estar alineada con el nivel de riesgo aceptable definido por la entidad y con los principios de eficiencia, transparencia y responsabilidad institucional. Además, se busca fortalecer la toma de decisiones basadas en el análisis de riesgos, promover una cultura organizacional orientada a la gestión preventiva y garantizar el cumplimiento de la Política de Seguridad y Privacidad de la Información.

10. POLÍTICA GENERAL TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

Tal y como se había esbozado anteriormente, según lo establecido en la Guía para la Administración del Riesgo y el Diseño de Controles en Entidades Públicas emitida por el Departamento Administrativo de la Función Pública DAFP, el tratamiento de riesgos se refiere a la respuesta diseñada por la primera línea de defensa para mitigar los diferentes riesgos. En este contexto, la planificación se centra en el tratamiento de riesgos de Seguridad y Privacidad de la Información, específicamente enfocado en la seguridad de la información relacionada con los activos a cargo del Municipio de Itagüí a nivel central. Durante el período vigente, se llevan a cabo una serie de acciones orientadas a implementar los controles necesarios y priorizados para garantizar la seguridad de la

información sobre estos activos. Este plan está dirigido a los participantes de todas las dependencias a nivel central de la Alcaldía de Itagüí.

11. METODOLOGÍA

FASE	ACTIVIDAD	RESPONSABLES
Revisión, actualización y publicación de Activos de Información	Identificar los activos de información que van a hacer parte del Inventario de activos de la Entidad.	Equipo MSPI Secretaria General
	Clasificar los activos de información de acuerdo con los tres principios de seguridad de la información: integridad, confidencialidad y disponibilidad.	Equipo MSPI Secretaria General
	Actualizar el inventario y la clasificación de los activos, por los propietarios y custodios de los activos, de forma periódica o toda vez que exista un cambio en el proceso.	Equipo MSPI Secretaria General
Valoración de Riesgos de Seguridad de la Información	Identificar, analizar, valorar y priorizar los riesgos sobre los activos de información, que causen la pérdida de confidencialidad, integridad, disponibilidad y privacidad de la información, bajo la responsabilidad de cada Unidad Administrativa.	Equipo MSPI Equipo Calidad
Identificación de incidentes de seguridad	Definir y formalizar el Procedimiento de Gestión de Incidentes de Seguridad de la información, de la Entidad.	Equipo MSPI Equipo Infraestructura Equipo Calidad

	Realizar la identificación, clasificación, tratamiento y divulgación de Incidentes Seguridad de la Información, sobre los activos de información, a partir del Procedimiento de Gestión de Incidentes de Seguridad de la Información y bajo la responsabilidad de cada Unidad Administrativa.	Equipo MSPI Equipo Infraestructura
	Capacitar con relación la gestión de incidentes de Seguridad de la Información.	Equipo MSPI Equipo Infraestructura
Identificación e Implementación de controles	Identificar los controles para abordar los riesgos e incidentes de Seguridad y Privacidad de la Información sobre los activos de información, para su posterior análisis, valoración y priorización, bajo la responsabilidad de cada Unidad Administrativa.	Equipo MSPI Equipo Infraestructura
Seguimiento	Realizar acciones de seguimiento al Plan, de acuerdo con el formato (informe, matriz, etc..) y periodicidad definida.	Equipo MSPI Equipo Infraestructura

12. DEFINICIÓN DEL CONTEXTO

El contexto general abarca los aspectos externos, internos y del proceso que son relevantes para gestionar los riesgos de Seguridad y Privacidad de la Información, Seguridad Digital y Continuidad de la Operación de los Servicios del Municipio de Itagüí. A partir de este contexto, es posible identificar las posibles causas de los riesgos. Para definir el contexto, se seguirán las metodologías establecidas por los entes reguladores y el MSPI, lo que permitirá determinar las posibles causas y llevar a cabo la identificación de los riesgos de manera efectiva. Esto implica considerar tanto los factores externos que pueden influir en la seguridad y privacidad de la información, como los aspectos internos de la entidad y los procesos que podrían afectar la continuidad de la operación de los servicios digitales.

13. IDENTIFICACIÓN DEL RIESGO.

La identificación del riesgo en materia de Seguridad y Privacidad de la Información, Seguridad Digital y Continuidad de la Operación de los Servicios constituye un paso fundamental en la gestión integral del riesgo dentro de la administración municipal de

Itagüí. Esta fase permite reconocer anticipadamente las situaciones que puedan afectar la confidencialidad, integridad y disponibilidad de los activos de información, así como interrumpir la prestación efectiva de los servicios públicos.

Este proceso parte del conocimiento detallado de la infraestructura tecnológica, los entornos físicos de operación, las áreas funcionales y los procesos misionales y de apoyo de la entidad. Cada dependencia deberá identificar los activos de información asociados a sus actividades, teniendo en cuenta su criticidad, clasificación, valor y función dentro del cumplimiento de los objetivos institucionales.

14. VALORACIÓN DEL RIESGO

La valoración de los riesgos de Seguridad y Privacidad de la Información, Seguridad Digital y Continuidad de la Operación en el Municipio de Itagüí se realizará conforme a la metodología establecida por el Departamento Administrativo de la Función Pública (DAFP). Este proceso evalúa la probabilidad de ocurrencia y el impacto potencial del riesgo, permitiendo su clasificación en niveles que orientan el tipo de tratamiento requerido. Se tendrán en cuenta variables como la asignación de responsables, el tipo de control (preventivo, detectivo o correctivo), su frecuencia de ejecución y la evidencia de su aplicación. La consistencia y eficacia de estos controles serán evaluadas para asegurar una mitigación adecuada. Esta valoración se actualiza periódicamente y es clave para la toma de decisiones y la protección de los activos de información de la entidad.

15. MATERIALIZACIÓN Y OPORTUNIDAD DE MEJORA

En caso de que se materialice un riesgo, este debe ser reportado de acuerdo con la gestión de incidentes de seguridad y privacidad de la información. Además, se debe analizar el riesgo y validar en qué nivel queda posterior a su materialización, registrando los cambios respectivos en el mapa de riesgos. Si se materializa un riesgo que no esté previamente identificado, también debe ser reportado para que se inicie su correspondiente identificación en el mapa de riesgos y se puedan tomar las medidas adecuadas para su gestión. La Alcaldía de Itagüí no solo se centrará en los riesgos identificados, sino que este análisis o apreciación del riesgo debe servir como base para identificar oportunidades. En este contexto, una oportunidad se define como la consecuencia positiva que resulta del tratamiento del riesgo, lo que significa que, al gestionar adecuadamente los riesgos, se pueden obtener beneficios adicionales o mejoras en los procesos y resultados

16. ACTIVIDADES DE SEGUIMIENTO AL PLAN DE TRATAMIENTO DE RIESGOS 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)

17. 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.	

18. 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 TRATAMIENTO DE RIESGOS DESEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

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

VIGENCIA: 2025

FASE	ACTIVIDAD	FUENTE DE VERIFICACIÓN	RESPONSABLES	CORRESPONSABLES	AVANCE DE EJECUCIÓN DE LAS ACTIVIDADES (EN % DE CUMPLIMIENTO)																	
					ABRIL		MAYO		JUNIO		JULIO		AGOSTO		SEPTIEMBRE		OCTUBRE		NOVIEMBRE		DICIEMBRE	
					P	E	P	E	P	E	P	E	P	E	P	E	P	E	P	E	P	E
Revisión, actualización y publicación de Activos de Información	Identificar los activos de información que van a hacer parte del Inventario de activos de la Entidad.	Inventario de Activos de Información de la Entidad.	Equipo MSPI Secretaria General	Unidad Admnistrativa Planeación--Calidad Gestión Documental		100%																
	Clasificar los activos de información de acuerdo con los tres principios de seguridad de la información: integridad, confidencialidad y disponibilidad.	Inventario de Activos de Información de la Entidad.	Equipo MSPI Secretaria General	Unidad Admnistrativa Planeación--Calidad Gestión Documental		80%		10%		10%												
	Actualizar el inventario y la clasificación de los activos, por los propietarios y custodios de los activos, de forma periódica o toda vez que exista un cambio en el proceso.	Inventario de Activos de Información de la Entidad, aprobado y actualizado.	Equipo MSPI Secretaria General	Unidad Admnistrativa Planeación--Calidad Gestión Documental		40%		60%														
Valoración de Riesgos de Seguridad de la Información	Identificar, analizar, valorar y priorizar los riesgos sobre los activos de información, que causen la pérdida de confidencialidad, integridad, disponibilidad y privacidad de la información, bajo la responsabilidad de cada Unidad Administrativa.	-Matriz de riesgos de Seguridad y Privacidad de la Información aprobada y actualizada.	Equipo MSPI Equipo Calidad	Unidad Admnistrativa Planeación--Calidad Gestión Documental					25%		25%		25%		25%							
Identificación de incidentes de seguridad	Definir y formalizar el Procedimiento de Gestión de Incidentes de Seguridad de la información, de la Entidad.	Procedimiento de Gestión de Incidentes de Seguridad, aprobado e implementado.	Equipo MSPI Equipo Infraestructura Equipo Calidad						50%		50%											
	Realizar la identificación, clasificación, tratamiento y divulgación de Incidentes Seguridad de la Información, sobre los activos de información, a partir del Procedimiento de Gestión de Incidentes de Seguridad de la Información y bajo la responsabilidad de cada Unidad Administrativa.	Incidentes seguridad de la información identificados, clasificados, tratados y divulgados. -Matriz de riesgos de seguridad y privacidad de la información actualizada.	Equipo MSPI Equipo Infraestructura	Unidad Admnistrativa Planeación--Calidad Gestión Documental					33%		33%		33%									
	Capacitar con relación la gestión de incidentes de Seguridad de la Información.	Sesiones de capacitación desarrolladas, actas de capacitación.	Equipo MSPI Equipo Infraestructura	Unidad Admnistrativa Planeación--Calidad Gestión Documental							33%		33%		33%							
Identificación e Implementación de controles	Identificar los controles para abordar los riesgos e incidentes de Seguridad y Privacidad de la Información sobre los activos de información, para su posterior a{aalisis, valoración y priorización, bajo la responsabilidad de cada Unidad Administrativa.	Matriz de riesgos de seguridad y privacidad de la información actualizada.	Equipo MSPI Equipo Infraestructura				33%		33%		33%											
Seguimiento	Realizar acciones de seguimiento al Plan, de acuerdo al formato (informe, matriz, etc..) y periodicidad definida.	Informe/matriz de seguimiento trimestral.	Equipo MSPI Equipo Infraestructura		25%				25%						25%				25%			