Alcaldía de Itagüí

PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN 2024.

MUNICIPIO DE ITAGÜÍ.

DIEGO LEÓN TORRES SÁNCHEZ
Alcalde de Itagüí.

CONTENIDO:

1. INTRODUCCIÓN:

En consonancia con el CONPES 3995/2020 y el Decreto Nacional 767 de 2022 que establece los lineamientos generales de la Política de Gobierno Digital, y el cual define los habilitadores transversales, entre los cuales se encuentra el de Seguridad y Privacidad de la Información, se destaca la adopción del Modelo de Seguridad y Privacidad de la Información (MSPI) por parte del Estado Colombiano. Este marco se establece como un instrumento para la implementación de los lineamientos de seguridad de la información desde su función, articulado con los procesos, trámites, servicios, sistemas de información e infraestructura. Además, se complementa con los requisitos establecidos para la estrategia de seguridad digital, según lo dispuesto en el artículo 5 de la Resolución 500 de 2021, emitida por el Ministerio de las Tecnologías de la Información y las Comunicaciones, alineándose adicionalmente con los habilitadores de la política de gobierno digital.

En este contexto, se estructura el presente documento que tiene como objetivo formular una hoja de ruta que permita fortalecer las capacidades institucionales, reducir riesgos y visualizar las actividades necesarias para preservar la confidencialidad, integridad, disponibilidad y privacidad de los datos en el Municipio de Itagüí. Así mismo se tendrá como elementos articuladores y vinculantes, la estrategia de Seguridad Digital de la entidad y la Política de Seguridad de la información.

El Municipio de Itagüí, a través del Decreto Municipal Nro. 673 del 7 de mayo de 2018, titulado "Por medio del cual se adopta el Modelo Integrado de Planeación y Gestión (MIPG)", estableció la importancia de integrar de manera articulada los modelos y sistemas de gestión de la entidad con el Modelo Integrado de Gestión. Esto se hizo con el fin de facilitar la integración del sistema de gestión y su articulación con el sistema de control interno del municipio de Itagüí.

Así mismo, se establece que, para asegurar la sostenibilidad y el mejoramiento continuo del Modelo Integrado de Planeación y Gestión, es necesario cumplir con la Política de Gobierno Digital, en relación con las políticas de Gestión y Desempeño Institucional del MIPG.

La política de gobierno digital se ha integrado con el Modelo Integrado de Planeación y Gestión como una herramienta dinamizadora para alcanzar las metas de las políticas de desarrollo administrativo, en conjunto con otras políticas esenciales para la gestión pública en Colombia.

En el mismo sentido, el Decreto Municipal Nro. 194 del 31 de enero de 2024, "Por medio de la cual se adoptan los planes institucionales y estratégicos en la administración municipal de Itagüí", sigue la disposición del Decreto Nacional 612 de 2018. Este último, en su artículo 2.2.22.3.14, establece que las entidades del

Estado deben integrar los planes institucionales y estratégicos, según el ámbito de aplicación del Modelo Integrado de Planeación y Gestión y el Plan de Acción previsto en el artículo 74 de la Ley 1474 de 2011. Además, deben publicarlos en sus respectivas páginas web antes del 31 de enero de cada año.

En este contexto, el Decreto Municipal de Itagüí adopta los Planes Institucionales y Estratégicos mencionados, entre los cuales se destaca el Plan de Seguridad y Privacidad de la Información, establecido en el numeral 12.

De ahí que, la normativa hace referencia al proceso de Seguridad y Privacidad de la Información como parte del acompañamiento en el habilitador de seguridad y privacidad de la información de la Política de Gobierno Digital. Esto se basa en el artículo 2.2.9.1.2.1. del Decreto Nacional 1078 de 2015, subrogado por el artículo primero del Decreto Nacional 767 de 2022 titulado " 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".

Este artículo establece la obligación de los sujetos obligados a 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. El objetivo es preservar la confidencialidad, integridad, disponibilidad y privacidad de los datos.

En otro sentido, el Decreto Nacional 2106 de 2019, titulado "por el cual se dictan normas para simplificar, suprimir y reformar trámites, procesos y procedimientos innecesarios existentes en la administración pública", establece en su artículo 16 que las autoridades que realicen trámites, procesos y procedimientos por medios digitales deben contar con sistemas de gestión documental electrónica y archivo digital. Esto garantiza la conformación de expedientes electrónicos con características de integridad, disponibilidad y autenticidad de la información.

En este sentido, es esencial disponer de una estrategia de seguridad digital que siga los lineamientos emitidos por el Ministerio de Tecnologías de la Información y las Comunicaciones, asegurando así la correcta gestión y protección de la información en entornos digitales.

A su vez la Resolución 500 de 2021 del Ministerio de Tecnologías de la Información y las Comunicaciones (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", forma parte de la Política de Gobierno Digital reglamentada por el Decreto 1078 de 2015.

Esta resolución indica que las entidades mencionadas en el artículo 2.2.9.1.1.2. del Decreto Nacional 1078 de 2015, subrogado por el Decreto Nacional 767 de 2022, están obligadas a cumplir con la Política de Gobierno Digital. En consecuencia, deben definir lineamientos generales para la implementación del Modelo de Seguridad y Privacidad de la Información (MSPI), la guía de gestión de riesgos de seguridad de la Información y el procedimiento para la gestión de los incidentes de seguridad digital. Además, deben establecer los lineamientos y estándares para la estrategia de seguridad digital.

En Colombia, se está llevando a cabo la implementación de la política de gobierno digital, según lo establecido por La Presidencia de la República y el Ministerio de Tecnologías de la Información y las Comunicaciones mediante el Decreto 767 de 2022. Estas disposiciones se encuentran recopiladas en el Decreto Único Reglamentario del Sector TIC, Decreto 1078 de 2015, específicamente en el capítulo 1, título 9, parte 2, libro 2. Este marco legal se considera un instrumento fundamental para mejorar la gestión pública y la relación del Estado con los ciudadanos.

El Manual de la política de Gobierno Digital expedido por el MinTIC establece que su objetivo es impactar positivamente la calidad de vida de los ciudadanos y, en general, los habitantes del territorio nacional y la competitividad del país, promoviendo la generación de valor público a través de la transformación digital del Estado, de manera proactiva, confiable, articulada y colaborativa entre los Grupos de Interés y permitir el ejercicio de los derechos de los usuarios del ciberespacio.

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, se formula e implementa la actualización del Plan de Seguridad y Privacidad de la Información al interior del Municipio de Itagüí. Este proceso fue socializado y posteriormente aprobado mediante acta de la sesión 002-2024 del Comité Institucional de Gestión de Desempeño de la Administración de Itagüí.

2. OBJETIVO.

El objetivo es formular una hoja de ruta que permita fortalecer las capacidades institucionales, reducir riesgos y establecer las actividades necesarias para preservar la confidencialidad, integridad, disponibilidad y privacidad de los datos en el Municipio de Itagüí conforme al Modelo de Seguridad y Privacidad de la Información (MSPI) de la política de Gobierno Digital, alineadas con las normas de calidad, en especial la NTC/IEC ISO 27001, la Política de Seguridad Digital y los criterios de continuidad de la operación de los servicios. Estas actividades están

diseñadas para mantener la seguridad y privacidad de la información que circula en los procesos del Municipio de Itagüí.

Para lograr esto, se busca fortalecer la integridad, confidencialidad y disponibilidad de los activos de información de la Entidad. Esto se traduce en la reducción de los riesgos a los que está expuesta la administración municipal hasta niveles aceptables. Todo ello se lleva a cabo mediante la implementación de las estrategias de seguridad digital definidas en este documento para la vigencia 2024.

Lo anterior, con el fin de abordar los objetivos fundamentales del modelo de Seguridad y Privacidad de la Información, teniendo en cuenta que el mismo establece la importancia de asegurar un manejo adecuado de la información pública en manos de las entidades destinatarias. Esta información es uno de los activos más valiosos para la toma de decisiones. El modelo busca lograr este objetivo a través de un enfoque dual:

1. **Seguridad de la Información:** Este enfoque establece directrices para que las entidades destinatarias desarrollen políticas de seguridad que protejan la información tanto a nivel físico como lógico. El objetivo es salvaguardar la integridad, disponibilidad y autenticidad de la información en todo momento.

2. **Privacidad de la Información:** Además de asegurar los procesos relacionados con los sistemas de información, el modelo integra un enfoque de privacidad. Esto implica garantizar la protección de los derechos a la intimidad, el buen nombre y la salvaguarda de secretos profesionales, industriales o de información privilegiada de particulares en manos de la administración. También se considera el acceso a la información pública, especialmente cuando no está sujeta a reserva.

Para cumplir con estos objetivos, es necesario incorporar al modelo de Seguridad de la Información un componente específico dedicado a la privacidad. Esto permite abordar de manera integral tanto la seguridad como la protección de la privacidad en el manejo de la información pública y privada por parte de las entidades destinatarias.

3. 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).

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.

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

5. DEFINICIONES, SIGLAS Y ABREVIATURAS.

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.

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 con las demás unidades administrativas de la entidad.

7. PRINCIPIOS RECTORES.

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

II. Adoptar un enfoque inclusivo y colaborativo que involucre activamente a todas las partes interesadas, facilitando la creación de condiciones para establecer alianzas eficientes que promuevan la seguridad digital del territorio y sus habitantes. Esto aumentará la capacidad de resiliencia municipal ante eventos no deseados en el entorno digital.

III. Garantizar una responsabilidad compartida entre las partes interesadas, promoviendo la colaboración y cooperación máximas. Esto considerará el rol y la responsabilidad de cada parte en la gestión de los riesgos de seguridad digital y la protección del entorno digital.

IV. Adoptar un enfoque basado en la gestión de riesgos, que facilite a los individuos el desarrollo seguro y confiable de sus actividades en el entorno digital. Esto fomentará la prosperidad económica y social, buscando generar riqueza, innovación, productividad, competitividad y empleo en todos los sectores de la economía.

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

La Alcaldía de Itagüí ha incorporado la Política de Seguridad Digital MIPG como parte integral de su sistema de gestión institucional. Para llevar a cabo su implementación y fortalecimiento, ha diseñado una serie de planes destinados a avanzar en diversas actividades que se alinean con las directrices del Ministerio de Tecnologías de la Información y las Comunicaciones, específicamente en lo referente a la adopción e implementación del Modelo de Seguridad y Privacidad de la Información (MSPI).

En este contexto, el Municipio de Itagüí a nivel central establece este plan general para contribuir a las acciones destinadas a fortalecer el Modelo de Seguridad y Privacidad de la Información de la Entidad, considerado como un habilitador fundamental para cumplir con lo establecido en la Política de Gobierno Digital.

Asimismo, se aborda la identificación, valoración, tratamiento y gestión de riesgos de seguridad de la información, conforme a lo especificado tanto en el modelo de seguridad y privacidad como en el estándar NTC ISO 27001:2013. Estas acciones se consideran fundamentales para el desarrollo de las actividades dentro del marco del Modelo de Seguridad y Privacidad de la Información de la entidad.

8.1 ESTADO ACTUAL DE LA ENTIDAD RESPECTRO AL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN.

La Entidad ha estado fortaleciendo el modelo de seguridad y privacidad de la información, abordando tanto un enfoque técnico como estratégico. En el ámbito técnico, se han adquirido herramientas para el monitoreo y correlación de eventos, se ha contratado servicios para el análisis de vulnerabilidades, se han implementado servicios de monitoreo de seguridad y se ha llevado a cabo la revisión de la marca.

Por otro lado, desde el punto de vista estratégico, se ha trabajado en fortalecer el Modelo de Seguridad y Privacidad de la Información (MSPI). Esto ha implicado

actualizar las políticas de seguridad, la documentación procedimental, verificar los activos y riesgos de seguridad, y documentar el plan de continuidad del negocio y el plan de recuperación de desastres.

A continuación, se presentan los indicadores de implementación del MSPI basados en el instrumento de evaluación del MINTIC, como nueva herramienta de medición para iniciar con los procesos de autoevaluación y diagnostico a partir de la expedición de este plan.

Nro.	Dominio	Calificación actual	Calificación objetivo	Evaluación de efectividad de control
A.5	POLITICAS DE SEGURIDAD DE LA INFORMACIÓN	Instrumento adoptado	100	Optimizado
A.6	ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN	Instrumento adoptado	80	Optimizado
A.7	SEGURIDAD DE LOS RECURSOS HUMANOS	Instrumento adoptado	70	Optimizado
A.8	GESTIÓN DE ACTIVOS	Instrumento adoptado	70	Optimizado
A.9	CONTROL DE ACCESO	Instrumento adoptado	80	Optimizado
A.10	CRIPTOGRAFÍA	Instrumento adoptado	50	Optimizado
A.11	SEGURIDAD FÍSICA Y DEL ENTORNO	Instrumento adoptado	80	Optimizado
A.12	SEGURIDAD DE LAS OPERACIONES	Instrumento adoptado	80	Optimizado
A.13	SEGURIDAD DE LAS COMUNICACIONES	Instrumento adoptado	80	Optimizado
A.14	ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS	Instrumento adoptado	80	Optimizado
A.15	RELACIONES CON LOS PROVEEDORES	Instrumento adoptado	80	Optimizado
A.16	GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN	Instrumento adoptado	80	Optimizado
A.17	ASPECTOS DE SEGURIDAD DE LA INFORMACIÓN DE LA GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO	Instrumento adoptado	80	Optimizado
A.18	CUMPLIMIENTO	Instrumento adoptado	80	Optimizado
PROMEDIO EVALUACIÓN DE CONTROLES		N/A		

Actualmente, de acuerdo al modelo de madurez, la entidad se encuentra frente a la autoevaluación del estado actual de la entidad, en un nivel 3, denominado “definido”. Con este instrumento se busca formalizar y llegar al nivel “optimizado”.

9. DESARROLLO DE LA POLÍTICA.

La Alcaldía de Itagüí ha incorporado en su modelo de procesos el proceso de Sistemas de Información e Infraestructura Tecnológica a nivel estratégico. Esto permite garantizar de manera continua la seguridad y privacidad de la información, la seguridad digital y la continuidad de la operación de los servicios en el Municipio.

9.1. ESTRATEGIAS DE SEGURIDAD DIGITAL, COMO ELEMENTOS ARTICULADORES.

El Municipio de Itagüí, mediante la adopción e implementación del Modelo de Seguridad y Privacidad de la Información enmarcado en el Sistema de Gestión de Seguridad de la Información, se compromete a proteger, preservar y administrar la confidencialidad, integridad, disponibilidad, autenticidad, privacidad y no repudio de la información que circula en el mapa de operación por procesos. Esto se logra a través de una gestión integral de riesgos y la implementación de controles físicos y digitales para prevenir incidentes, garantizar la continuidad de la operación de los servicios y cumplir con los requisitos legales, reglamentarios y regulatorios.

El enfoque está orientado a la mejora continua y al alto desempeño del Sistema de Gestión de Seguridad de la Información, promoviendo el acceso, uso efectivo y apropiación masiva de las Tecnologías de la Información y las Comunicaciones.

9.2. 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. Esto incluye a todos sus funcionarios, contratistas, proveedores, operadores y entidades descentralizadas del orden municipal. También abarca a aquellas personas o terceros que, en el cumplimiento de sus funciones y las del Municipio de Itagüí, compartan, utilicen, recolecten, procesen, intercambien o consulten información relevante.

Asimismo, esta política se extiende a las entidades de control y otras entidades relacionadas que accedan, ya sea interna o externamente, a cualquier activo de información, sin importar su ubicación. Es importante destacar que esta política se aplica a toda la información creada, procesada o utilizada por el Municipio de Itagüí, sin importar el medio, formato, presentación o ubicación en la que se encuentre.

9.3. ESTRATEGIA DE SEGURIDAD DIGITAL.

La Alcaldía de Itagüí establecerá una estrategia de seguridad digital que integre principios, políticas, procedimientos, guías, manuales, formatos y lineamientos para la gestión de la seguridad de la información. Esta estrategia estará centrada en la implementación del Modelo de Seguridad y Privacidad de la Información (MSPI), así

como en la guía de gestión de riesgos de seguridad de la información y el procedimiento de gestión de incidentes que debe ser establecido.

Por lo tanto, la Entidad define las siguientes cinco estrategias específicas, que en conjunto conformarán una estrategia general de seguridad digital:

9.4. 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.
Concientización	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 roles	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.

9.5. 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 el Grupo de Políticas Digitales, 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, realizará el levantamiento de la Infraestructura Tecnológica Crítica de la Entidad.

3. El Grupo de Infraestructura Tecnológica, 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 el Grupo de Políticas Digitales, 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, 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 Infraestructura Tecnológica y la Oficina de Talento Humano, sensibilizarán 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 articularán 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.

9.6. PLAN DE FORTALECIMIENTO DE LAS CAPACIDADES INSTITUCIONALES RESPECTO A LA SEGURIDAD DE LA INFORMACIÓN.

La Alcaldía de Itagüí ha incorporado la Política de Seguridad y Privacidad de la Información como parte integral de su sistema de gestión en el Municipio. Con el objetivo de implementar y fortalecer esta política, se han diseñado una serie de ejecuciones dirigidas a avanzar en diversas actividades. Estos procesos están orientados a cumplir con las directrices establecidas por el Ministerio de Tecnologías de la Información y las Comunicaciones en relación con la adopción e implementación del Modelo de Seguridad y Privacidad de la Información (MSPI).

En consonancia con las directrices del modelo de seguridad y privacidad, así como con los requisitos del estándar NTC ISO 27001:2013, se aborda la identificación, evaluación, tratamiento y gestión de riesgos asociados a la seguridad de la información. Estos aspectos se consideran como contribuciones clave para las acciones a desarrollar en el marco del Modelo de Seguridad y Privacidad de la Información de la entidad.

Para fortalecer la implementación del modelo de seguridad y privacidad de la información en el Municipio de Itagüí, se propone el siguiente plan:

ESTRATEGIA / EJE	ACTIVIDADES	PRODUCTOS ESPERADOS
Liderazgo de seguridad de la información	1. Actualizar políticas de seguridad y privacidad de la información.	Políticas de Seguridad de la información actualizadas.
	2. Definición de Roles y Responsabilidades de Seguridad de la Información.	Matriz Roles y Responsabilidades en Seguridad de la Información.
	3. Revisión por la Dirección y por el comité municipal de gestión y desempeño y el comité institucional de gestión y desempeño del municipio de Itagüí.	Aprobación por parte del comité municipal de gestión y desempeño y el comité institucional de gestión y desempeño del municipio de Itagüí.

	4. Implementación estrategias de continuidad del negocio.	Estrategia talento Humano Estrategia Gestión Documental Estrategia T.I.
	5. Publicación y divulgación.	Publicar los planes adoptados y realizar la respectiva divulgación.
	6. Identificación de oportunidades de mejora acorde al seguimiento de la ejecución de los controles y de los planes.	Seguimiento y definición de oportunidades de mejora definidos por la Mesa Técnica de Gobierno Digital.
Gestión de riesgos	1. Identificar, valorar y clasificar riesgos asociados a continuidad del negocio.	Matriz de riesgos de continuidad del negocio.
	2. Seguimiento planes de tratamiento de riesgos de seguridad.	Informe seguimiento de riesgos.
Concientización	1. Establecer plan de comunicaciones	Documento plan de comunicaciones
	2. Campañas de sensibilización (Ciber martes Seguro)	Realizar 30 campañas y eventos de capacitación.
	3. Participación inducciones y reinducciones.	Acompañar los procesos de inducción y reinducción, desde el enfoque de esta política.
	4. Día de la ciberseguridad	Establecer un día institucional de la ciberseguridad, en donde se realicen actividades de concientización y promoción.
	5. Encuesta apropiación.	Validar los datos de las encuestas de percepción de los ejercicios de concientización.
Implementación de controles	1. Monitoreo seguridad.	Resultados de monitoreo SOC.
	2. Análisis de vulnerabilidades.	Informe de resultados.
	3. Controles de acceso.	Informe de resultados.
Gestión de incidentes	1. Reforzar conocimientos al personal en la gestión de incidentes de seguridad de la información	Sesiones de capacitación desarrolladas.
	2. Seguimiento y autoevaluación al registro de incidentes presentados.	Informe de seguimiento y exposición ante la Mesa Técnica de Gobierno Digital.
	3. Revisión, actualización y publicación cuando se	Documentos actualizados.

	requiera del procedimiento de incidentes de seguridad de la información basado en la norma	
	4. Apoyar la definición de los lineamientos, mecanismos y el alcance para la realización de pruebas de vulnerabilidades	Lineamientos y estrategias definidos por la Mesa Técnica de Gobierno Digital

9.7. MEJORAMIENTO CONTINUO.

La entidad consolidará los resultados obtenidos durante la fase de evaluación de desempeño con el fin de diseñar un plan integral de mejoramiento continuo en materia de seguridad y privacidad de la información. Este plan estará orientado a tomar las acciones necesarias para mitigar las debilidades identificadas en el proceso de evaluación.

Para este propósito, se establecerá y llevará a cabo un plan de mejora continúa basado en los resultados obtenidos durante la fase de evaluación del desempeño. Este plan abarcará:

1. Los resultados derivados de la ejecución del plan de seguimiento, evaluación y análisis del Sistema de Seguridad y Privacidad de la Información.

2. Los resultados obtenidos del plan de ejecución de auditorías y revisiones independientes al Sistema de Seguridad y Privacidad de la Información.

Al utilizar estos datos como insumos clave, la entidad estará en condiciones de realizar ajustes en los entregables, controles y procedimientos dentro del SSPI y su política asociada. Dichos insumos darán lugar a la elaboración de un plan integral de mejoramiento y un plan de comunicaciones para la mejora continua, los cuales serán revisados y aprobados por la mesa técnica de gobierno digital antes de ser presentados ante el comité municipal de gestión y desempeño, así como el comité institucional de gestión y desempeño de la entidad.

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 a 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).

10. CONTROL DE APROBACIONES:

PROYECTÓ	APROBÓ	SOCIALIZADO
JUAN ANDRÉS FERNÁNDEZ RESTREPO	SANTIAGO ECHAVARRÍA GALLEGO	COMITÉ INSTITUCIONAL DE GESTIÓN Y DESEMPEÑO
Contratista – Dirección Administrativa de las TIC.	Director Administrativo de las Tecnologías de la Información y las Comunicaciones TIC.	

11. CONTROL DE VERSIONES:

VERSIÓN	FECHA	DESCRIPCIÓN	PROYECTÓ	REVISÓ / APROBÓ
Versión 1	04-2024	Elaboración y aprobación del Plan.	Juan Andrés Fernández Restrepo	Santiago Echavarría Gallego
			Contratista – Dirección Administrativa de las TIC.	Director Administrativo de las TIC.
Versión 1.1	07-2024	Actualización identidad visual.	Juan Andrés Fernández Restrepo	Jerri Alejandro López Sánchez
			Contratista – Dirección Administrativa de las TIC.	Director Administrativo de las TIC.

ANEXO 1: ACTIVIDADES SEGUIMIENTO PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN
PLAN DE ACCIÓN

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

VIGENCIA: 2024

ACTIVIDAD	FUENTE DE VERIFICACIÓN	RESPONSABLES	CORRESPONSABLES	AVANCE DE EJECUCIÓN DE LAS ACTIVIDADES (EN % DE CUMPLIMIENTO)																									
				ENERO		FEBRERO		MARZO		SEGUIMIENTO PRIMER TRIMESTRE	ABRIL		MAYO		JUNIO		SEGUIMIENTO SEGUNDO TRIMESTRE	JULIO		AGOSTO		SEPTIEMBRE		SEGUIMIENTO TERCER TRIMESTRE	OCTUBRE		NOVIEMBRE		DICIEMBRE	
				P	E	P	E	P	E		P	E	P	E	P	E		P	E	P	E	P	E		P	E	P	E	P	E
Revisar y/o actualizar la información documentada asociada a las Políticas de Gobierno y Seguridad Digital.	Información documentada revisada y/o actualizada.	Director Administrativo de las TIC y Personal de Gobierno Digital.	Equipo de trabajo de la Dirección Administrativa de las TIC. Líder SIGI de las TIC.																		100%								
Socializar las Políticas de Gobierno y Seguridad Digital con la Administración Municipal.	Controles de asistencia.	Director Administrativo de las TIC y Personal de Gobierno Digital.	Jefes de las unidades administrativas y sus equipos de trabajo.										100%																
Elaborar y realizar el seguimiento al Plan de Acción de las Políticas de Gobierno y Seguridad Digital.	Plan de Acción de las Políticas Digitales.	Director Administrativo de las TIC. Líder SIGI de las TIC.	No aplica.					25%							25%						25%							25%	
Realizar la identificación, análisis y valoración de los riesgos de seguridad de la información.	Matriz de Riesgos.	Director Administrativo de las TIC y Personal de Gobierno Digital.	Equipo de trabajo de la Dirección Administrativa de las TIC. Líder SIGI de las TIC.										100%																
Realizar el monitoreo, seguimiento y control a los riesgos de seguridad de la información identificados.	Matriz de Riesgos.	Director Administrativo de las TIC y Personal de Gobierno Digital.	Equipo de trabajo de la Dirección Administrativa de las TIC. Líder SIGI de las TIC.												25%						50%							25%	
Administrar y gestionar los equipos de seguridad perimetral del Data Center.	Reportes técnicos del Data Center.	Director Administrativo de las TIC y Personal adscrito al Data Center.	No aplica.					25%							25%						25%							25%	
Brindar soporte y mantenimiento a la infraestructura tecnológica de la Entidad.	Registros del software de la Mesa de Servicios (GLPI).	Director Administrativo de las TIC.	Equipo de trabajo de la Dirección Administrativa de las TIC.	8%		8%		8%			9%		9%		9%			9%		8%		8%			8%		8%		8%	
Realizar la actualización del inventario de activos de información de la Entidad.	Inventario de activos.	Director Administrativo de las TIC y Personal de Gobierno Digital.	Equipo de trabajo de la Dirección Administrativa de las TIC.												50%													50%	
Realizar la autoevaluación del Formulario Único de Reporte de Avances de la Gestión (FURAG) asociado a las Políticas de Gobierno y Seguridad Digital.	Formulario de autoevaluación.	Director Administrativo de las TIC y Personal de Gobierno Digital.	Líder SIGI de las TIC.												100%														
Realizar la autoevaluación del Índice de Transparencia y Acceso a la Información (ITA).	Formulario de autoevaluación.	Director Administrativo de las TIC y Personal de Gobierno Digital.	Líder SIGI de las TIC.												100%														
Planificar y ejecutar el procedimiento de auditoría interna de las Políticas de Gobierno y Seguridad Digital.	Información documentada asociada al procedimiento de auditoría interna.	Director Administrativo de las TIC y Equipo de Auditoría Interna.	Líder SIGI de las TIC.																		100%								
Realizar el seguimiento al cumplimiento de los diferentes procesos y procedimientos de seguridad y privacidad de la información.	Información documentada asociada al Plan.	Director Administrativo de las TIC y Personal adscrito al Data Center.	Equipo de trabajo de la Dirección Administrativa de las TIC. Líder SIGI de las TIC.												50%													50%	