Alcaldía de Itagüí

PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN 2024.

MUNICIPIO DE ITAGÜÍ.

DIEGO LEÓN TORRES SÁNCHEZ
Alcalde de Itagüí.

CONTENIDO:

1. INTRODUCCIÓN:

El plan de tratamiento de riesgos de Seguridad y Privacidad de la Información, Seguridad Digital y Continuidad de la Operación se fundamenta en una estrategia orientada hacia el desarrollo de una cultura preventiva. Esta cultura se centra en comprender el concepto de riesgo y su contexto, lo que permite la planificación de acciones destinadas a reducir el impacto negativo en la entidad en caso de que estos riesgos se materialicen. Además, el plan busca implementar estrategias para la identificación, análisis, tratamiento, evaluación y monitoreo de los riesgos de manera más objetiva. Esto implica revelar situaciones que podrían comprometer el cumplimiento de los objetivos establecidos en el entorno TIC para el Desarrollo Digital, incluyendo aspectos como ciudadanos y hogares empoderados en el Entorno Digital, Transformación Digital Sectorial y Territorial, así como la Inclusión Social Digital.

En Colombia, se está llevando a cabo la implementación de la política de gobierno digital, conforme a lo establecido por la Presidencia de la República y el Ministerio de Tecnologías de la Información y las Comunicaciones a través del Decreto 767 de 2022. Estas disposiciones se encuentran recopiladas en el Decreto Único Reglamentario del Sector TIC, 1078 de 2015, específicamente en el capítulo 1, título 9, parte 2, libro 2, siendo un instrumento clave para mejorar la gestión pública y la interacción entre el estado y los ciudadanos. Esta política se ha integrado con el Modelo Integrado de Planeación y Gestión, siendo una herramienta dinámica para alcanzar las metas de las políticas de desarrollo administrativo y su articulación con otras políticas esenciales para la gestión pública en Colombia.

El Manual de la política de Gobierno Digital expedido por el MinTIC establece que su propósito es objetivo de 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. Según el manual, la implementación de esta política se ha estructurado a través de un esquema que articula los elementos que la componen: gobernanza, innovación pública digital, habilitadores, líneas de acción, e iniciativas dinamizadoras, con el fin de lograr su objetivo. Dichos elementos deben desarrollarse por los actores involucrados para alcanzar los objetivos de la política.

El Artículo 2.2.9.1.2.1 del Decreto Nacional 1078 de 2015, subrogado por el artículo 1 del Decreto Nacional 767 de 2022, establece el desarrollo de la Política de Gobierno Digital a través de un esquema que integra varios elementos, incluyendo gobernanza, innovación pública digital, habilitadores, líneas de acción e iniciativas dinamizadoras, con el fin de alcanzar sus objetivos. Dentro de estos elementos, se destaca la Seguridad y Privacidad de la Información como un habilitador

fundamental. Según el numeral 3.2 de este artículo, los sujetos obligados deben fortalecer sus capacidades mediante la implementación de lineamientos de seguridad y privacidad en todos sus procesos, trámites, servicios, sistemas de información, infraestructura y activos de información, con el objetivo de preservar la confidencialidad, integridad, disponibilidad y privacidad de los datos.

El Modelo de Seguridad y Privacidad de la Información (MSPI), emitido por el Ministerio de Tecnologías de la Información y las Comunicaciones, destaca que la adopción de este modelo por parte de las entidades del estado contribuye a mantener la confidencialidad, integridad y disponibilidad de la información, respaldado por un proceso de gestión del riesgo que genera confianza entre las partes interesadas sobre la adecuada gestión de riesgos.

La adopción, implementación y evaluación de este modelo es una actividad obligatoria, como se establece en el artículo 2.2.9.1.3.2 del Decreto 767 de 2022. Es importante mencionar también que el Decreto Presidencial 612 de 2018, en su artículo 1, adiciona al Capítulo 3 del Título 22 de la Parte 2 del Libro 2 del Decreto Presidencial 1083 de 2015 un artículo 2.2.22.3.14, que integra los planes institucionales y estratégicos al Plan de Acción de las entidades del Estado. En este contexto, se establece la elaboración anual del "Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información" y del "Plan de Seguridad y Privacidad de la Información" como obligaciones para cada entidad.

La Resolución 0500 del 10 de marzo de 2021 emitida por el Ministerio de Tecnologías de la Información y las Comunicaciones establece lineamientos generales para la implementación del Modelo de Seguridad y Privacidad de la Información, la guía de gestión de riesgos de Seguridad de la Información, el procedimiento para la gestión de los incidentes de seguridad digital, y los estándares para la estrategia de seguridad digital. Esta resolución subraya la necesidad de que los sujetos obligados adopten medidas técnicas, administrativas y de talento humano para incorporar la seguridad digital en el Plan de Seguridad y Privacidad de la Información y mitigar los riesgos asociados con la protección, privacidad de la información e incidentes de seguridad digital.

El artículo 5 de la Resolución 0500 precisa la adopción de la estrategia de seguridad digital que integra principios, políticas, procedimientos, guías, manuales, formatos y lineamientos para la gestión de la seguridad de la información digital, incorporándola en el Plan de Seguridad y Privacidad de la Información, en concordancia con el artículo 2.22.22.3.14 del Decreto 1083 de 2015. En particular, el artículo 5, denominado "Estrategia de Seguridad Digital", en su numeral 2, enfatiza la necesidad de contar con un análisis y tratamiento de riesgos de seguridad digital e implementar controles para gestionarlos.

El anexo 1 de la Resolución detalla en su acápite "Planificación" la importancia de determinar las necesidades y objetivos de seguridad y privacidad de la información considerando el contexto interno y externo de la entidad. Esta fase incluye la definición del plan de valoración y tratamiento de riesgos, siendo el Plan de Tratamiento de Riesgos el documento clave para gestionar los riesgos de seguridad de la información y establecer los controles necesarios para protegerla, siguiendo los lineamientos del ISO/IEC 27000. El numeral 7.3.3 del anexo especifica que la entidad debe definir y aplicar un proceso de tratamiento de riesgos de la 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.

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 11.

La adopción e implementación del Modelo de Seguridad y Privacidad de la Información en las entidades públicas se sustenta en el estándar NTC ISO 27001:2013 y en principios regulatorios establecidos por el Gobierno Nacional, como la Ley 1712 de 2014 o la Ley 1581 de 2012. Este enfoque se basa en la implementación de un ciclo de identificación, valoración y tratamiento de riesgos de seguridad y privacidad de la información. Para respaldar este proceso, el Departamento Administrativo de la Función Pública ha emitido la guía para la administración del riesgo y el diseño de controles en entidades públicas, que sirve

como referencia para abordar los riesgos relacionados con la gestión, la corrupción y la seguridad de la información.

La adopción de prácticas de gestión de riesgos en las entidades públicas permite fortalecer la toma de decisiones en la implementación de controles conforme al plan de tratamientos definido. Estos referentes son fundamentales para la definición del plan de tratamiento de riesgos de seguridad y privacidad de la información en el Municipio de Itagüí, especialmente en lo que respecta a los activos de información que contribuyen al logro de los objetivos organizacionales.

Todo lo anterior se realiza en cumplimiento de la normativa establecida por el estado colombiano, incluyendo la CONPES 3854 de 2016, el Modelo de Seguridad y Privacidad de MINTIC, así como lo establecido en el decreto 1008 del 14 de junio de 2018 y la Resolución 500 de 2021. Estas normativas adoptan las buenas prácticas y los lineamientos de los estándares ISO 27001:2013, ISO 31000:2018, y la guía para la administración del riesgo y el diseño de controles en entidades públicas emitida por el DAFP, que aborda los riesgos de gestión, corrupción y seguridad digital.

En conclusión, la definición del Plan de Tratamiento de Riesgos tiene como objetivo establecer medidas para mitigar los riesgos identificados en el análisis, como la pérdida de confidencialidad, integridad y disponibilidad de los activos de información. Esto ayuda a prevenir situaciones que puedan afectar el cumplimiento de los objetivos de la Alcaldía de Itagüí, evitando así la incertidumbre.

El Plan de Tratamiento de Riesgos se estructura para evaluar las acciones necesarias para mitigar los riesgos en los procesos de la entidad. Estas acciones se organizan en actividades, donde se especifican las tareas, responsables y fechas de ejecución que se aplicarán durante la vigencia del plan.

Estas actividades se definen considerando la información del análisis de riesgos, las necesidades y el contexto de los procesos de la entidad en términos de seguridad y privacidad de la información. Esto proporciona las herramientas necesarias para identificar las características de los riesgos y definir los pasos a seguir para su ejecución.

En este contexto, se formula la actualización del Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información dentro del Municipio de Itagüí. Este proceso fue socializado y aprobado mediante el acta de la sesión 002-2024 del Comité Institucional de Gestión de Desempeño de la Administración de Itagüí.

2. OBJETIVO.

El objetivo general es realizar un seguimiento efectivo a los tratamientos de riesgos de Seguridad y Privacidad de la Información, así como identificar los riesgos de Continuidad de la Operación de TI de acuerdo con los contextos establecidos en la entidad. Se busca definir y aplicar lineamientos integrales para tratar los riesgos de Seguridad y Privacidad de la Información, Seguridad Digital y Continuidad de la Operación de los servicios (riesgos de interrupción) a los que el Municipio de Itagüí pueda estar expuesto. De esta manera, se pretende alcanzar los objetivos, la misión y la visión institucional, protegiendo y preservando la integridad, confidencialidad, disponibilidad, privacidad y autenticidad de la información.

Se plasma así mismo el objetivo específico de cumplir con los requisitos legales, reglamentarios, regulatorios y normas técnicas colombianas en seguridad y privacidad de la información, seguridad digital y protección de la información personal. Además, se busca gestionar los riesgos de Seguridad y Privacidad de la Información, Seguridad Digital y Continuidad de la Operación de los servicios (riesgos de interrupción) de acuerdo con los contextos establecidos en los procesos de la entidad. Asimismo, se pretende fortalecer y apropiar el conocimiento relacionado con la gestión de riesgos de Seguridad y Privacidad de la Información, Seguridad Digital y Continuidad de la Operación de los servicios (riesgos de interrupción) en la Alcaldía de Itagüí.

3. ALCANCE.

El objetivo es realizar una gestión eficiente de riesgos de Seguridad y Privacidad de la Información, Seguridad Digital y Continuidad de la Operación de los servicios (riesgos de interrupción) que permita integrar buenas prácticas en los procesos de la entidad. Esto contribuirá a la toma de decisiones y a prevenir incidentes que puedan afectar el logro de los objetivos establecidos. Además, se proporcionarán lineamientos para identificar, analizar, tratar, evaluar y monitorear los riesgos de seguridad y privacidad de la información en el Municipio de Itagüí.

El Plan de Tratamiento de Riesgos considerará especialmente aquellos riesgos clasificados en los niveles Moderado, Alto y Extremo, de acuerdo con los lineamientos establecidos por el Ministerio de las Tecnologías de la Información y las Comunicaciones MINTIC. Se aceptarán los riesgos que se encuentren en niveles inferiores a estos en la jerarquía de riesgos, según lo determinado por la entidad.

La gestión de riesgos se aplica a cualquier proceso de la Alcaldía de Itagüí mediante principios básicos y metodológicos para administrar los riesgos de seguridad de la información. Esto facilita el desarrollo de etapas como la identificación del contexto y del riesgo, el análisis, la evaluación, las opciones de tratamiento, así como las pautas para el seguimiento, monitoreo y evaluación de los riesgos.

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.

Amenaza: Es un ente o escenario interno o externo que puede hacer uso de una vulnerabilidad para generar un perjuicio o impacto negativo en la institución (materializar el riesgo).

Control o Medida: Medida que permite reducir o mitigar un riesgo.

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).

Impacto: Consecuencias que puede ocasionar a la organización la materialización del riesgo.

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.

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.

Riesgo: Efecto que se causa sobre los objetivos de las entidades, debido a eventos potenciales.

Riesgo de Seguridad de la Información: Posibilidad de que una amenaza concreta pueda explotar una vulnerabilidad para causar una pérdida o daño en un activo de información. Suele considerarse como una combinación de la probabilidad de un evento y sus consecuencias. (ISO/IEC 27000).

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

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).

SGSI: Sistema de Gestión de Seguridad de la Información.

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. 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 de la Información como parte integral de su sistema de gestión institucional. Para llevar a cabo su implementación y fortalecimiento, ha diseñado una serie de actividades destinadas 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 ha establecido este como un 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.

9. 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 e implicará 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”.

10. DESARROLLO DE LA POLÍTICA DE TRATAMIENTO DE RIESGOS.

El Municipio de Itagüí, a través de su Modelo Integrado de Gestión, se compromete a mantener una cultura de gestión del riesgo que permita fortalecer las medidas de prevención, monitoreo y seguimiento del control para mitigar posibles riesgos en las actividades desarrolladas por la Entidad asociadas con la responsabilidad de diseñar, adoptar, ejecutar y promover las políticas, planes, programas, iniciativas y proyectos que se relacionen con las tecnologías de la información y las comunicaciones TIC.

Esto se llevará a cabo mediante mecanismos, sistemas y controles que detecten integralmente hechos asociados con la estrategia, gestión, transparencia, ética, seguridad y privacidad de la información, seguridad digital, continuidad de la operación, riesgo fiscal, aspectos ambientales y de seguridad. Estos aspectos pueden afectar el cumplimiento de los objetivos institucionales, el máximo aprovechamiento de los recursos destinados y la atención a la ciudadanía.

Para ello, es necesario establecer los parámetros necesarios para una adecuada gestión de los Riesgos de Seguridad y Privacidad de la Información, Seguridad Digital y Continuidad de los servicios de la Alcaldía de Itagüí. Esto se logra procurando que no se materialicen, siguiendo los lineamientos establecidos en la Guía para la Administración del Riesgo y el Diseño de Controles en Entidades Públicas del Departamento Administrativo de la Función Pública DAFP.

El tratamiento de riesgos es la respuesta establecida por la primera línea de defensa, es decir, la unidad administrativa responsable del proceso junto con su equipo de trabajo, para mitigar los diferentes riesgos. El tratamiento o respuesta dada al riesgo se enmarca en las siguientes categorías, establecidas en la Guía para la Administración del Riesgo y el Diseño de Controles en Entidades Públicas del Departamento Administrativo de la Función Pública DAFP:

Aceptar el riesgo: Esta opción implica no adoptar ninguna medida que afecte la probabilidad o el impacto del riesgo. Por ejemplo, ningún riesgo en materia de TI critica es aceptado. La aceptación del riesgo puede ser viable en la entidad para los riesgos bajos, aunque también puede haber situaciones donde no se puedan aplicar controles y, por ende, se acepte el riesgo. En ambos casos, es crucial mantener un seguimiento continuo del riesgo.

Reducir el riesgo: En esta categoría se adoptan medidas para reducir la probabilidad o el impacto del riesgo, o ambos. Esto generalmente implica implementar controles adecuados, con una segregación de funciones apropiada. El tratamiento al riesgo adoptado debe lograr la reducción prevista sobre este.

Evitar el riesgo: Esta estrategia implica abandonar las actividades que generan el riesgo, es decir, no iniciar o no continuar con la actividad que lo provoca.

Compartir el riesgo: Aquí se reduce la probabilidad o el impacto del riesgo transfiriendo o compartiendo una parte de este. Por ejemplo, los riesgos de TI critica se pueden compartir, pero no se puede transferir su responsabilidad. Los principales métodos de compartir o transferir parte del riesgo son los seguros y la tercerización.

El enfoque orienta a la toma de decisiones oportunas y minimiza los efectos adversos al interior de la Entidad, con el fin de dar continuidad a la gestión

institucional y asegurar el cumplimiento de los compromisos con la ciudadanía itagüiseña.

La gestión de riesgos de Seguridad y Privacidad de la Información, Seguridad Digital y Continuidad de la Operación de los servicios permite al Municipio de Itagüí y a su administración municipal, llevar a cabo una identificación, análisis y tratamiento de los riesgos que podrían afectar el cumplimiento de los objetivos de sus procesos. Esto contribuye a la toma de decisiones y a la prevención de la materialización de dichos riesgos.

La administración de riesgos de Seguridad y Privacidad de la Información, Seguridad Digital y Continuidad de la Operación de los servicios se enfoca en identificar, analizar, valorar y tratar las amenazas y vulnerabilidades de los activos de información de la entidad, considerando su criticidad y la necesidad de protección. Las etapas presentes en la gestión de riesgos permiten alinearlas con los objetivos, estrategias y políticas institucionales, logrando un nivel de riesgo que la Alta Dirección pueda aceptar o asumir.

12.1. 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.

12.2. METODOLOGÍA.

GESTIÓN	ACTIVIDADES	EJECUCIONES	RESPONSABLE
Gestión de riesgos	Sensibilización.	Socialización de lineamientos y herramientas para la Gestión de Riesgos de Seguridad y privacidad de la Información y Seguridad Digital	Dirección Administrativa de las TIC.
	Identificación de Riesgos de Seguridad y Privacidad de la Información, Seguridad Digital y continuidad de la Operación.	Contexto, Identificación, Análisis y Evaluación de Riesgos - Seguridad y Privacidad de la Información y Seguridad Digital.	Dirección Administrativa de las TIC.
		Retroalimentación, revisión y verificación de los riesgos identificados	Dirección Administrativa de las TIC.
	Aceptación de riesgos identificados.	Aceptación, aprobación riesgos identificados y planes de tratamiento	Dirección Administrativa de las TIC.
	Seguimiento fase de tratamiento.	Seguimiento implementación de controles y planes de tratamiento de riesgos los identificados.	Dirección Administrativa de las TIC.
	Mejoramiento	Identificación de oportunidades de mejora acorde al seguimiento de la ejecución de los controles y de los planes de tratamiento.	Dirección Administrativa de las TIC.
		Revisión y/o actualización de lineamientos de Riesgos de Seguridad y privacidad de la información de acuerdo con las observaciones identificadas.	Dirección Administrativa de las TIC.
	Monitoreo y revisión.	Medición, presentación y reporte de indicadores	Dirección Administrativa de las TIC.

12.3. FLUJO METODOLÓGICO.

12.4. 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.

12.5. IDENTIFICACIÓN DEL RIESGO.

Para la identificación de riesgos de Seguridad y Privacidad de la Información, Seguridad Digital y Continuidad de la Operación de los Servicios de la administración municipal, es fundamental considerar varios aspectos, como la infraestructura física, las áreas de trabajo y el entorno en general. Cada proceso debe tener identificados los activos de información y reconocer las situaciones potenciales que podrían causar daño a la entidad, poniendo en riesgo el logro de sus objetivos.

La falta de apropiación en temas de seguridad de la información o la ausencia de controles pueden ser aprovechadas por amenazas, causando la materialización de un riesgo (incidente). Por lo tanto, es necesario identificar el atributo de los tres elementos del flujo metodológico (confidencialidad, integridad, disponibilidad), el dueño del riesgo (unidad administrativa responsable), el activo de información afectado, las amenazas, las vulnerabilidades y las consecuencias.

Para determinar los activos afectados, es crucial validarlos dentro de un inventario de activos de información, donde se establece la criticidad, la clasificación de la información y otros atributos importantes para el análisis del riesgo. La identificación de los activos de información se llevará a cabo según los lineamientos de la entidad.

12.6. VALORACIÓN DEL RIESGO.

La valoración de los riesgos de Seguridad y Privacidad de la Información, Seguridad Digital y Continuidad de la Operación de los Servicios de la administración municipal se llevará a cabo siguiendo la metodología para la administración de riesgos mencionada en la Guía emitida por el Departamento Administrativo de la Función Pública y que será adoptada por esta entidad territorial.

Se definirán controles en donde se identifiquen las variables a evaluar para su diseño adecuado, como la asignación de un responsable, la segregación y autoridad del responsable, el tipo de control (preventivo, detectivo o correctivo), la implementación (manual o automática), la periodicidad, el propósito, cómo se realiza la actividad de control, cómo se manejan las observaciones o desviaciones, y la evidencia de la ejecución del control. Además, se evalúa que cada control se ejecute de manera consistente para mitigar el riesgo. Esta valoración se realiza de acuerdo con las tablas y metodología establecidas en la Guía para la administración del riesgo y el diseño de controles en entidades públicas del Departamento Administrativo de la Función Pública DAFP.

12.7. 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.

11. 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 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).

12. 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.	

13. 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.

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

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 al tratamiento de riesgos de seguridad y privacidad de la información.	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 tratamiento de riesgos de seguridad y privacidad de la información.	Controles de asistencia.	Director Administrativo de las TIC. Líder SIGI de las TIC.	Jefes de las unidades administrativas y sus equipos de trabajo.															50%						50%					
Realizar la identificación de controles de seguridad para abordar los riesgos identificados, analizados, valorados y priorizados sobre los activos de información de la Entidad.	Matriz de Riesgos.	Director Administrativo de las TIC y Personal de Gobierno Digital.	Equipo de trabajo de cada unidad administrativa.												100%														
Identificar los recursos tecnológicos particulares autorizados (correos electrónicos, servicios de nube, sitios web, recursos compartidos, formularios de encuestas, etc.) para manejo de información institucional.	Información documentada asociada a la actividad.	Secretarios de Despacho, Subsecretarios, Directores, Subdirectores, Jefes de Oficina, otros Directivos.	Equipo de trabajo de cada unidad administrativa.												100%														
Realizar el seguimiento al uso de recursos tecnológicos particulares autorizados (correos electrónicos, servicios de nube, sitios web, recursos compartidos, formularios de encuestas, etc.) para manejo de información insitucional.	Información documentada asociada a la actividad.	Secretarios de Despacho, Subsecretarios, Directores, Subdirectores, Jefes de Oficina, otros Directivos.	Equipo de trabajo de cada unidad administrativa.												50%													50%	
Realizar la identificación, clasificación, tratamiento y divulgación de incidentes de seguridad de la información materializados, con el fin de aplicar acciones de mejoramiento (preventivas, correctivas, de corrección y de mejora).	Plan de Mejoramiento.	Director Administrativo de las TIC y Líder SIGI de las TIC.	Equipo de trabajo de la Dirección Administrativa de las TIC.												50%					25%							25%	
Realizar la puesta en funcionamiento y operación de los equipos del Data Center para implementar controles de seguridad de la información.	Informes técnicos del Data Center.	Director Administrativo de las TIC y Personal adscrito al Data Center.	Líder SIGI de las TIC.												50%										50%				
Realizar el mantenimiento y sostenimiento de los equipos de seguridad perimetral del Data Center.	Informes técnicos del Data Center.	Director Administrativo de las TIC y Personal adscrito al Data Center.	Líder SIGI de las TIC.					25%							25%					25%							25%	
Realizar el seguimiento a las actividades de identificación y operación de controles de seguridad de la información para abordar riesgos tecnológicos.	Información documentada asociada a la actividad.	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%				25%					25%							25%	