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

INSTITUTO MUNICIPAL DE CULTURA, RECREACIÓN Y DEPORTE DE ITAGÜÍ

SUBGERENCIA ADMINISTRATIVA Y FINANCIERA
AÑO 2025

INTRODUCCIÓN.

El Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información, Seguridad Digital y Continuidad de los Servicios del Instituto Municipal de Cultura, Recreación y Deporte de Itagüí, se basa en una orientación estratégica que requiere el desarrollo de una cultura de carácter preventivo, de manera que, al comprender el concepto de riesgo, así como el contexto, se planean acciones que reduzcan la afectación a la entidad en caso de materialización; adicional se busca desarrollar estrategias para la identificación, análisis, tratamiento, evaluación y monitoreo de dichos riesgos con mayor objetividad, dando a conocer aquellas situaciones que pueden comprometer el cumplimiento de los objetivos trazados en el entorno de las Tecnologías de la Información y las Comunicaciones (TIC). Lo anterior, dando cumplimiento a la normativa establecida por el estado colombiano, CONPES 3995 de 2020, Modelo de Seguridad y Privacidad del Ministerio de las Tecnologías de la Información y las Comunicaciones (MinTIC) y lo establecido en el Decreto 1008 de 14 de junio 2018, adoptando las buenas prácticas y los lineamientos de los estándares ISO 27001:2013.

DEFINICIONES Y TÉRMINOS.

Activo: En el contexto de seguridad digital, son elementos tales como aplicaciones de la organización, servicios web, redes, Hardware, información física o digital, recurso humano, entre otros, que utiliza la organización para funcionar en el entorno digital.

Apetito de riesgo: Es el nivel de riesgo que la entidad puede aceptar, relacionado con sus objetivos, el marco legal y las disposiciones de la Alta Dirección y del Órgano de Gobierno. El apetito de riesgo puede ser diferente para los distintos tipos de riesgos que la entidad debe o desea gestionar.

Causa: Todos aquellos factores internos y externos que solos o en combinación con otros, pueden producir la materialización de un riesgo.

Causa Inmediata: Circunstancias bajo las cuales se presenta el riesgo, pero no constituyen la causa principal o base para que se presente el riesgo.

Causa Raíz: Causa principal o básica, corresponde a las razones por la cuales se puede presentar el riesgo.

Confidencialidad: Propiedad de la información que la hace no disponible o sea divulgada a individuos, entidades o procesos no autorizados.

Consecuencia: Efectos o situaciones resultantes de la materialización del riesgo que impactan en el proceso, la entidad, sus grupos de valor y demás partes interesadas.

Control: Medida que permite reducir o mitigar un riesgo.

Disponibilidad: Propiedad de ser accesible y utilizable a demanda por una entidad.

Factores de Riesgo: Son las fuentes generadoras de riesgos.

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

Integridad: Propiedad de exactitud y completitud.

MIPG: Modelo Integrado de Planeación y Gestión

Nivel de riesgo: Es el valor que se determina a partir de combinar la probabilidad de ocurrencia de un evento potencialmente dañino y la magnitud del impacto que este evento traería sobre la capacidad institucional de alcanzar los objetivos. En general la fórmula del Nivel del Riesgo poder ser Probabilidad * Impacto, sin embargo, pueden relacionarse las variables a través de otras maneras diferentes a la multiplicación, por ejemplo, mediante una matriz de Probabilidad – Impacto.

Plan Anticorrupción y de Atención al Ciudadano: Plan que contempla la estrategia de lucha contra la corrupción que debe ser implementada por todas las entidades del orden nacional, departamental y municipal.

Probabilidad: Se entiende como la posibilidad de ocurrencia del riesgo. Estará asociada a la exposición al riesgo del proceso o actividad que se esté analizando. La probabilidad inherente será el número de veces que se pasa por el punto de riesgo en el periodo de 1 año.

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

Riesgo de Corrupción: Posibilidad de que, por acción u omisión, se use el poder para desviar la gestión de lo público hacia un beneficio privado.

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).

Riesgo Inherente: Nivel de riesgo propio de la actividad. El resultado de combinar la probabilidad con el impacto permite determinar el nivel del riesgo inherente, dentro de unas escalas de severidad.

Tolerancia del riesgo: Es el valor de la máxima desviación admisible del nivel de riesgo con respecto al valor del apetito de riesgo determinado por la entidad.

Vulnerabilidad: Representa la debilidad de un activo o de un control que puede ser explotada por una o más amenazas.

PLAN DE TRATAMIENTO DE RIESGOS.

Mediante la definición del Plan de Tratamiento de Riesgos, se busca mitigar los riesgos presentes en el análisis de riesgos (Pérdida de la Confidencialidad de los Activos, Pérdida de Integridad de los Activos y Pérdida de Disponibilidad de los Activos), evitando aquellas situaciones que impidan el logro de los objetivos del Instituto Municipal de Cultura, Recreación y Deporte de Itagüí.

El Plan de Tratamiento de Riesgos se define con el fin de evaluar las posibles acciones que se deben tomar para mitigar los riesgos existentes; estas acciones son organizadas en forma de medias de seguridad, y para cada una de ellas se define el nombre de la medida, objetivo, justificación, responsable de la medida y su prioridad.

OBJETIVOS.

- Definir y aplicar los lineamientos para tratar de manera integral los riesgos de seguridad y privacidad de la información, seguridad digital y continuidad de la operación de los servicios y de esta manera alcanzar los objetivos, la misión y la visión institucional, protegiendo y preservando la integridad, confidencialidad, disponibilidad y autenticidad de la información.

- Gestionar riesgos de seguridad y privacidad de la información, seguridad digital y continuidad de la operación de los servicios, de acuerdo con los contextos establecidos en la entidad.

- Fortalecer y apropiar conocimiento referente a la gestión de riesgos seguridad y privacidad de la información y seguridad digital

- Establecer una adecuada gestión mediante la identificación con acciones de control y respuestas oportunas que afecten el cumplimiento de la misión.

ALCANCE.

El Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información del Instituto Municipal de Cultura, Recreación y Deporte de Itagüí, es aplicable al Direccionamiento Estratégico de la Entidad, a los procesos, a los planes institucionales, a los proyectos y a las acciones ejecutadas por los servidores durante el ejercicio de sus funciones; dándoles el tratamiento necesario, con base en la metodología definida, para cada tipología de riesgos.

CLASIFICACIÓN DE LOS RIESGOS.

Riesgos de seguridad digital: Posibilidad de combinación de amenazas y vulnerabilidades en el entorno digital. Puede debilitar el logro de objetivos económicos y sociales, afectar la soberanía municipal, la integridad territorial y los intereses institucionales. Incluye aspectos relacionados con el ambiente físico, digital y las personas.

Riesgo estratégico: Se asocia con la forma en que se administra el Instituto Municipal de Cultura, Recreación y Deporte de Itagüí, enfocándose en asuntos globales relacionados con la misión y el cumplimiento de los objetivos estratégicos, la clara definición de políticas, diseño y conceptualización del Instituto.

Riesgo operativo: Comprende los riegos relacionados tanto con la parte operativa como técnica; incluye riesgos provenientes de las deficiencias en los sistemas de información, en la definición de los procesos, en la estructura de la entidad y en la desarticulación entre dependencias, lo cual conduce a ineficiencias, oportunidades de corrupción e incumplimiento de los compromisos institucionales.

Riesgos de tecnología: Se asocian con la capacidad de la entidad para que la tecnología disponible satisfaga las necesidades actuales y futuras del Instituto y soporten el cumplimiento de la misión.

Riesgos financieros: Se relacionan con el manejo de los recursos de la entidad, que incluyen: la ejecución presupuestal, la elaboración de los estados financieros, los pagos, manejos de excedentes de tesorería y el manejo sobre los bienes de cada entidad. De la eficiencia y transparencia en el manejo de los recursos, depende en gran parte el éxito o fracaso del Instituto.

Riesgos de cumplimiento: Se asocian con la capacidad de la entidad de cumplir con los requisitos legales, contractuales, de ética y, en general, con su compromiso con la comunidad.

Riesgos de corrupción: Posibilidad de que, por acción u omisión, se use el poder para desviar la gestión de lo público hacia un beneficio privado.

Riesgo de imagen o reputacional: Posibilidad de ocurrencia de un evento que afecte la imagen, buen nombre o reputación de una organización ante sus clientes y partes interesadas.

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)

POLÍTICA DE ADMINISTRACIÓN DE RIESGOS.

El Instituto Municipal de Cultura, Recreación y Deporte de Itagüí, conforme a su misión, establece que la administración de riesgos asociados a los procesos de la entidad tendrá un carácter prioritario y estratégico, fundamentada en el Modelo de Operación por Procesos, teniendo en cuenta el contexto estratégico de la entidad, la normatividad vigente aplicable y el Modelo Integrado de Planeación y Gestión (MIPG).

El Instituto, 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 del Instituto Municipal de Cultura, Recreación y Deporte 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).

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.

En virtud de lo anterior, la identificación, análisis, valoración, seguimiento y monitoreo de los riesgos, permite la reducción de vulnerabilidades ante las amenazas internas y externas o mejora las capacidades institucionales de respuesta a eventos identificados o inesperados que afecten al talento humano, la infraestructura tecnológica o los servicios esenciales de los que depende la entidad, enmarcado en el cumplimiento de los objetivos de los planes institucionales, de los procesos, de los proyectos y de las acciones ejecutadas por los servidores públicos y particulares que ejercen funciones públicas, durante el ejercicio de sus funciones y actividades, teniendo en cuenta los siguientes lineamientos:

Aplica para todos los niveles, áreas y procesos de la entidad e involucra el contexto, la identificación, valoración, tratamiento, monitoreo, revisión, comunicación, consulta y el análisis de los siguientes riesgos:

- Los riesgos de gestión de proceso, que puedan afectar el cumplimiento de la misión y objetivos institucionales.

- Los riesgos de posibles actos de corrupción, a través de la prevención de la ocurrencia de eventos en los que se use el poder para desviar la gestión de lo público hacia un beneficio privado.

- Los riesgos de seguridad digital, que puedan afectar la confidencialidad, integridad y disponibilidad de la información de los procesos de la entidad.

- Los riesgos que impiden la prestación normal de los servicios institucionales debido a eventos calificados como crisis

El tratamiento de riesgos es la respuesta establecida por la primera línea de defensa, es decir, por el líder o responsable del proceso junto con su equipo de trabajo, para la mitigación de los diferentes riesgos.

El tratamiento o respuesta dada al riesgo, se enmarca en las siguientes categorías:

- **Aceptar el riesgo:** No se adopta ninguna medida que afecte la probabilidad o el impacto del riesgo (tener en cuenta que ningún riesgo de corrupción es aceptado). La aceptación del riesgo

puede ser una opción viable en la entidad para los riesgos bajos, pero también pueden existir escenarios de riesgos a los que no se les puedan aplicar controles y, por ende, se acepta el riesgo. En ambos escenarios, debe existir un seguimiento continuo del riesgo.

- **Reducir el riesgo:** Se adoptan medidas para reducir la probabilidad o el impacto del riesgo, o ambos; por lo general, conlleva a la implementación de controles. Deben seleccionarse controles apropiados y con una adecuada segregación de funciones, de manera que el tratamiento al riesgo adoptado logre la reducción prevista sobre este.

- **Evitar el riesgo:** Se abandonan las actividades que dan lugar al riesgo, es decir, no iniciar o no continuar con la actividad que lo provoca.

- **Compartir el riesgo:** Se reduce la probabilidad o el impacto del riesgo transfiriendo o compartiendo una parte de este. Los riesgos de corrupción se pueden compartir, pero no se puede transferir su responsabilidad. Los dos principales métodos de compartir o transferir parte del riesgo son: seguros y tercerización.

La gestión de Riesgos de Seguridad y Privacidad de la Información, Seguridad Digital y Continuidad de la Operación de los Servicios, le permite al Instituto Municipal de Cultura, Recreación y Deporte de Itagüí realizar una identificación, análisis y tratamiento de los riesgos que puedan generar afectación al cumplimiento de los objetivos de sus procesos, contribuyendo en la toma de decisiones y en la prevención de la materialización de estos. La Administración de Riesgos de Seguridad y Privacidad de la Información se encuentra enfocada en identificar, analizar, valorar y tratar las amenazas y vulnerabilidades de los activos de información de la entidad, teniendo presente su criticidad y protección. Las etapas presentes en la gestión de riesgos, permiten alinearlas con los objetivos, estrategias y políticas corporativas, logrando un nivel de riesgo que pueda aceptar o asumir la alta dirección del Instituto.

METODOLOGÍA.

El Plan de Tratamiento de Riesgos contempla la definición de las actividades a desarrollar en aras de mitigar los riesgos sobre los activos. Estas actividades se estructuran de la siguiente manera, siguiendo las recomendaciones de la Guía de Gestión de Riesgos de Seguridad y Privacidad de la Información (MinTIC. 2016).

Gestión	Actividad	Tarea	Responsable	Fecha Inicio	Fecha Fin
Gestión de Riesgos	Actualización de lineamientos de riesgos	Actualizar política y metodología de gestión de riesgos	Control Interno de Gestión – Planeación	15/01/2025	31/12/2025
	Sensibilización	Socialización guía y herramienta, gestión de riesgos de seguridad y privacidad de la información, seguridad digital y continuidad de la operación	Control Interno de Gestión – Planeación	15/01/2025	31/12/2025
	Identificación de riesgos y seguridad de la información, seguridad digital y continuidad de la operación	Identificación, análisis y evaluación de riesgos y seguridad y privacidad de la información, seguridad digital y continuidad de la operación	Equipo de Planeación	15/01/2025	31/12/2025
		Realimentación, revisión y verificación de los riesgos identificados			
	Aceptación de riesgos identificados	Aceptación, aprobación de riesgos identificados y planes de tratamientos	Equipo de Planeación	15/01/2025	31/12/2025
	Publicación	Publicación matriz de riesgos	Equipo de Planeación	15/01/2025	31/12/2025
	Seguimiento fase de tratamiento	Seguimiento estado de planes de tratamientos de riesgos identificados y verificación de evidencias	Dirección TIC Convenio Marco – Planeación	15/01/2025	31/12/2025
	Evaluación de riesgos residuales	Evaluación de riesgos residuales	Equipo de Planeación	15/01/2025	31/12/2025
	Mejoramiento	Identificación de oportunidades de mejora acorde a los resultados obtenidos durante la evaluación de riesgos residuales	Equipo de Planeación	15/01/2025	31/12/2025
		Actualización guía de gestión de riesgos, seguridad de la información de acuerdo con los cambios solicitados			
	Monitoreo y revisión	Generación, presentación y reportes de indicadores	Equipo de Planeación	15/01/2025	31/12/2025

DESARROLLO METODOLÓGICO.

FASE 1: ANÁLISIS DE LA INFORMACIÓN.

En esta etapa, se evalúan los resultados de las entrevistas con los colaboradores del proceso de Tecnologías de la Información (TI) y se desarrollan las siguientes actividades:

- Aplicar las políticas de tratamiento de riesgos.
- Determinar los controles (se desprenden de las medidas) aplicados en MinTIC.
- Determinar los riesgos que van a ser incluidos en el Plan de Tratamiento de Riesgos.

FASE 2: DESARROLLO DE LOS PROYECTOS.

En esta fase se realizarán las actividades que permitan la estructuración de las medidas.

- Determinar el nombre de la medida.
- Definir los responsables de cada medida.
- Establecer el objetivo de cada medida.
- Elaborar la justificación de la medida.
- Definir las actividades a realizar para el desarrollo de la medida.

FASE 3: ANÁLISIS DE LOS PROYECTOS.

- Definición de los controles relacionados con cada medida.
- Validar los riesgos mitigados por cada medida.
- Análisis de la aplicabilidad de las medidas.
- Priorización de las medidas.

FASE 4: DEFINICIÓN DEL ORGANIGRAMA DE RESPONSABILIDAD

En esta fase se realizará un organigrama y se definirán responsabilidades respecto a la administración y gestión del riesgo, esta etapa deberá ser definida por el Instituto teniendo en cuenta su estructura organizacional para la gestión de riesgos.

- Identificación de las funciones del Instituto en materia de seguridad de la información.
- Definición del grupo de trabajo de gestión de riesgo por parte del Instituto.

- Definición de las funciones del grupo de trabajo referentes a la aplicación y gestión de las medidas.

FASE 5: CICLO DE VIDA DEL TRATAMIENTO DE RIESGOS.

Definir las actividades a realizar por cada uno de los elementos del ciclo de vida del Plan de Tratamiento de Riesgos.

Planear: Dentro de esta etapa se desarrollan las actividades definidas en la fase 1 de la metodología de tratamiento de riesgos.

Hacer: En este paso del ciclo de vida se desarrollarán las actividades enmarcadas en la fase 2 de la metodología del tratamiento de riesgos.

Verificar: En esta etapa se desarrollarán las actividades que permiten hacer seguimiento o auditorías a la ejecución de cada una de las medidas.

Actuar: Dentro de esta etapa se realizarán las mejoras teniendo en cuenta el seguimiento y los resultados de las auditorías de la ejecución de los proyectos.

Elabora: Asesor de Gerencia Profesional Universitario Sistema de Gestión de la Calidad	Revisa: Subgerente Administrativo y Financiero	Aprueba: Comité Institucional de Gestión y Desempeño