



CONCEJO DE MEDELLÍN

**PLAN DE TRATAMIENTO DE RIEGOS DE SEGURIDAD Y PRIVACIDAD DE LA
INFORMACIÓN**

**UNIDAD DE INFORMÁTICA
CONCEJO DE MEDELLÍN**

ENERO 2021

CONTENIDO

PRESENTACIÓN	3
1. OBJETIVO GENERAL	4
2. OBJETIVOS ESPECÍFICOS:	4
3. ALCANCE	4
4. JUSTIFICACIÓN	4
5. POLÍTICA DE GESTIÓN DEL RIESGO DEL CONCEJO DE MEDELLÍN	5
6. DESARROLLO DEL PLAN	5
7. SEGUIMIENTO	6

PRESENTACIÓN

El Concejo de Medellín debe definir las acciones para gestionar los riesgos de seguridad de la información inaceptables e implantar los controles necesarios para proteger la misma a través de la implementación del plan de tratamiento de riesgos de seguridad de la información, en el cual se identifica el control a aplicar para llevar cada uno de los riesgos a un nivel aceptable para la Corporación.

Todo lo anterior se debe lograr en el marco de la normativa establecida por el Estado colombiano, CONPES 3854 de 2016, Modelo de Seguridad y Privacidad de 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, ISO 31000:2018 y la guía para la administración del riesgo y el diseño de controles en entidades públicas - Riesgos de gestión, corrupción y seguridad digital, emitida por el DAFP.

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

1. OBJETIVO GENERAL

Aplicar en el Concejo de Medellín las metodologías pertinentes para la gestión de los riesgos de seguridad y privacidad de la información que se identifiquen en el desarrollo del Sistema de Gestión Corporativo.

Lo anterior de conformidad con el Plan Estratégico de la Corporación 2020-2023 y el logro del objetivo estratégico: *“Desarrollar una cultura organizacional fundamentada en el ciclo de vida de la información”*, y en cumplimiento de la normativa legal aplicable.

2. OBJETIVOS ESPECÍFICOS:

- Definir y aplicar los lineamientos para el tratamiento integral de los riesgos de Seguridad y Privacidad de la Información, Seguridad Digital y Continuidad de la Operación de los servicios que el Concejo de Medellín pueda estar expuesto.
- Garantizar la protección, preservación, integridad, confidencialidad, disponibilidad y autenticidad de la información de la Corporación.
- Cumplir con los requisitos legales y reglamentarios pertinentes a la legislación colombiana.
- Fortalecer y apropiar conocimiento referente a la gestión de riesgos Seguridad y Privacidad de la información, Seguridad Digital y Continuidad de la Operación de los servicios del Concejo de Medellín.

3. ALCANCE

Aplica a todos los procesos del Sistema de Gestión Corporativo, servidores públicos, contratistas y partes interesadas, que participen o que tengan relación con la gestión de la información en el Concejo de Medellín.

4. JUSTIFICACIÓN

El Concejo de Medellín desde 2015 inició una serie de acciones dirigidas a fortalecer la seguridad y privacidad de la información, es así como resultado de un diagnóstico realizado se detectó la necesidad de fortalecer la plataforma tecnológica y contar con recurso humano competente que acompañara esta importante actividad.

A través de la contratación del servicio de mesa de ayuda se ha logrado avanzar en el propósito de contar con información íntegra, segura, confiable y disponible para su uso tanto por los usuarios internos como externos.

Es innegable que falta todavía mucho por implementar a la luz del MSPI, por lo tanto, este plan se orienta al inicio de acciones concretas en materia de gestión del riesgo de la información, teniendo como uno de los principales objetivos generar y mantener la cultura

de gestión del riesgo dentro de la Corporación desde la responsabilidad de los servidores públicos y demás actores que interactúan en el ciclo de vida de la información.

5. POLÍTICA DE GESTIÓN DEL RIESGO DEL CONCEJO DE MEDELLÍN

El Concejo de Medellín conocedor de la importancia de administrar los riesgos asociados a los objetivos estratégicos, procesos y proyectos relacionados con la operación de la Corporación, implementa su Sistema de Gestión de Riesgos como herramienta estratégica que permite anticipar y responder de manera oportuna y óptima a dichos riesgos, contribuir al cumplimiento de los objetivos y aprovechar al máximo los recursos destinados a planes, programas, y proyectos, siempre bajo las mejores condiciones de eficacia, eficiencia y efectividad.

6. DESARROLLO DEL PLAN

A continuación, se relacionan las actividades definidas para el presente plan:

Gestión	Actividad	Resultado	Responsable	Fecha	
				Inicio	Fin
Planificación	Establecer Contexto	Informe del Contexto Estratégico de la Corporación (Plan Estratégico, Caracterizaciones de los Procesos), con el análisis de factores internos y externos que pueden generar riesgos de seguridad y privacidad de la información.	Líder de Programa Unidad de Informática - Mesa de Ayuda	1/03/2021	31/03/2021
	Definir los criterios básicos para la gestión de los riesgos de seguridad y privacidad de la información	Documento con los criterios de evaluación del riesgo, criterios de impacto, criterios de aceptación; el alcance y los límites de gestión de los riesgos; y la política para el tratamiento de los riesgos.		1/04/2021	31/05/2021
	Definir el alcance y los límites para la gestión de los riesgos de seguridad y privacidad de la información				
	Definir el Plan de Tratamiento del Riesgo				
Implementación	Realizar el identificación, valoración y la incorporación de controles y el plan de acción para el tratamiento de los	Matriz de Riesgos de Seguridad y Privacidad de la Información.		1/06/2021	30/06/2021

Gestión	Actividad	Resultado	Responsable	Fecha	
				Inicio	Fin
	riesgos.				
Evaluación	Realizar monitoreo y revisión continua de los riesgos.	Plan de acción para el mejoramiento de la gestión de los riesgos de Seguridad y Privacidad de la Información.		1/07/2021	31/07/2021
Mejoramiento Continuo	Mantener y mejorar el Proceso de Gestión del Riesgo en la seguridad de la Información.	Implementación de acciones para el mejoramiento de la gestión de los riesgos de Seguridad y Privacidad de la Información.		1/08/2021	31/12/2021

7. SEGUIMIENTO

La Unidad de Informática realizará seguimiento trimestral a las acciones propuestas en el presente plan, presentará el avance en el Comité Institucional de Gestión y Desempeño, conforme al Calendario de Obligaciones Legales y Administrativas - COLA, de la Corporación.