PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACION

Mesa Directiva

JHONY OSWALDO VELEZ QUINTERO
Presidente

JUAN DIEGO ALVAREZ UPEGUI
Vicepresidente Primero

PABLO ANDRES RESTREPO GARCES
Vicepresidente Segundo

DOLLY MARIA QUINTERO BETANCUR
Secretaria General

ENVIGADO-ANTIOQUIA
ENERO 2026

INTRODUCCIÓN

El presente Plan de Seguridad y Privacidad de La Información, da cuenta de una serie de tareas que el Concejo Municipal de Envigado realizará a fin de implementar la estrategia de gobierno digital alrededor del componente de seguridad y privacidad de la información, cuyo principal objetivo es proteger los derechos de los usuarios de la entidad y mejorar los niveles de confianza en los mismos a través de la identificación, valoración, tratamiento y mitigación de los riesgos de los sistemas de información.

OBJETIVO

Identificar, valorar, tratar y mitigar los riesgos de los sistemas de información con el fin de proteger los activos de información, el manejo de medios, el control de acceso y la gestión de los usuarios.

POLITICA GENERAL

El Concejo de Envigado, entendiendo la importancia de un adecuado manejo de la información, no solo ha definido el proceso “Gestión de la Información” dentro del procesos de la Corporación, sino que también se ha comprometido con la implementación del Modelo de Seguridad y Privacidad de la Información que promueve la estrategia de Gobierno Digital liderada por MINTIC; todo ello buscando establecer un marco de confianza en el ejercicio de sus deberes misionales, sus responsabilidades con el estado y también con los ciudadanos de Envigado; y por supuesto enmarcado en el estricto cumplimiento de las leyes en concordancia con la misión y visión de la entidad.

En el Concejo de Envigado, mediante la adopción e implementación del Modelo Integrado de Planeación y Gestión - MIPG, y específicamente del Modelo de Seguridad y Privacidad de la Información - MSPI, se protege, preserva y administra la confidencialidad, integridad, disponibilidad, autenticidad y no repudio de la información que circula en los procesos del Sistema de Gestión Corporativo, mediante una gestión integral de riesgos y la implementación de controles físicos y digitales, buscando la mitigación de incidentes y el cumplimiento a los requisitos legales y reglamentarios, orientados a la mejora continua y al mantenimiento de la privacidad y seguridad de la información. A su vez, se propende así por el acceso, uso efectivo y apropiación masiva de las TIC para el normal desarrollo del Debate Temático Público, a través de políticas y programas que favorezcan las expectativas de los grupos de valor, pero que también se mantengan alineadas con las iniciativas previstas dentro del Plan Estratégico de Tecnologías de Información – PETI.

MARCO LEGAL

Constitución Política de Colombia. Artículo 15.
Ley 44 de 1993: Por la cual se modifica y adiciona la Ley 23 de 1982 y se modifica la Ley 29 de 1944 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 expide la Ley General de Archivos.
Ley 850 de 2003: Por medio de la cual se reglamentan las veedurías ciudadanas
Ley 1266 de 2008: Por la cual se dictan las disposiciones generales del Habeas 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 1341 de 2009: Por la cual se definen principios y conceptos sobre la sociedad de la información y la organización de las tecnologías de la información y las comunicaciones – TIC, se crea la agencia Nacional de espectro y se dictan otras disposiciones.
Ley 1437 de 2011: Por la cual se expide el código de procedimiento administrativo y de lo contencioso administrativo.
Ley 1474 de 2011: Por la cual se dictan normas orientadas a fortalecer los mecanismos de prevención, investigación y sanción de actos de corrupción y la efectividad del control de la gestión pública.
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.
Ley 1915 de 2018: Por la cual se modifica la Ley 23 de 1982 y se establecen otras disposiciones en materia de derecho de autor y derechos conexos
Ley 1952 de 2019: Por medio de la cual se expide el código general disciplinario
Decreto 2609 de 2012: Por el cual se reglamenta el Título V de la Ley 594 de 2000, parcialmente los artículos 58 y 59 de la Ley 1437 de 2011 y se dictan otras disposiciones en materia de Gestión Documental para todas las Entidades del Estado.
Decreto 0884 del 2012: Por el cual se reglamenta parcialmente la Ley 1221 del 2008.
Decreto 1377 de 2013: Por el cual se reglamenta parcialmente la Ley 1581 de 2012.

Decreto 886 de 2014: Por el cual se reglamenta el Registro Nacional de Bases de Datos.
Decreto 103 de 2015: Por medio del cual se reglamenta parcialmente la Ley 1712 de 2014 y se dictan otras disposiciones.
Decreto 1074 de 2015: Por medio del cual se expide el Decreto Reglamentario del Sector Comercio, Industria y Turismo. Reglamenta parcialmente la Ley 1581 de 2012 e imparten instrucciones sobre el Registro Nacional de Bases de Datos. Artículos 25 y 26.
Decreto 1078 de 2015: Por medio del cual se expide el Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones.
Decreto 1080 de 2015: Por medio del cual se expide el Decreto Reglamentario del Sector Cultura.
Decreto 1081 de 2015: Por medio del cual se expide el Decreto Reglamentario del Sector Presidencia
Resolución 512 de 2019: Por la cual se adopta la Política General de Seguridad y Privacidad de la Información, Seguridad Digital y Continuidad de los servicios del Ministerio/Fondo de Tecnologías de la Información y las Comunicaciones y se definen lineamientos frente al uso y manejo de la información.
CONPES 3701 de 2011. Lineamientos de Política para Ciberseguridad y Ciberdefensa.
CONPES 3854 de 2016. Política Nacional de Seguridad digital.

ANÁLISIS DEL CONTEXTO ESTRATÉGICO	
DEBILIDADES	**OPORTUNIDADES**
● Usuarios no capacitados en el uso de herramientas tecnológicas ● Falta de uso y apropiación de los sistemas de información. ● Falta de continuidad en proyectos por cambios administrativos. ● Desarticulación de la información en los procesos. ● Falta de presupuesto ● Divulgación o tratamiento inapropiada de la información ● Nivel medio de cultura organizacional frente a la seguridad y privacidad de la información. ● Inadecuada estructura organizacional ● Falta gestión del conocimiento	● Apoyo por parte de la Alcaldía de Envigado en el fortalecimiento tecnológico y de seguridad. ● Soluciones tecnológicas que ofrece el mercado. ● Política de gobierno digital (MSPI) ● Fase de planificación del Modelo de Seguridad y Privacidad de la Información completada. ● Inicio de la etapa de implementación del modelo de Seguridad y Privacidad de la información ● MIPG (metodologías) ● Aplicación de cambios normativos

● Planeación institucional deficiente ● Falta de liderazgo en la gestión de la información al interior de los diferentes procesos y dependencias. ● Falta de control de acceso a los espacios destinados para los	

FASE DE DIAGNÓSTICO – ETAPAS PREVIAS A LA IMPLEMENTACIÓN

En esta fase se pretende identificar el estado actual de la organización con respecto a los requerimientos del Modelo de Seguridad y Privacidad de la Información.

Tabla 1 - Metas, Resultados e Instrumentos de la fase etapas previas a la implementación: En la fase de diagnóstico del MSPI se pretende alcanzar las siguientes metas:

• Determinar el estado actual de la gestión de seguridad y privacidad de la información al interior del Concejo Municipal de Envigado.
• Determinar el nivel de madurez de los controles de seguridad de la información.
• Identificar el avance de la implementación del ciclo de operación al interior de la entidad.
• Identificar el nivel de cumplimiento con la legislación vigente relacionada con protección de datos personales.
• Identificación del uso de buenas prácticas en ciberseguridad.

Para ello se recomienda utilizar los siguientes instrumentos: • Herramienta de diagnóstico.

• Instructivo para el diligenciamiento de la herramienta.
• Guía No 1 - Metodología de Pruebas de Efectividad. Para realizar dicha fase el Concejo Municipal de Envigado debe efectuar la recolección de la información con la ayuda de la herramienta de diagnóstico y la metodología de pruebas de efectividad.

Una vez se tenga el resultado del diagnóstico inicial y se haya determinado el nivel de madurez de la entidad se procede al desarrollo de la fase de Planificación.

Los resultados asociados a la fase de Diagnostico previas a la implementación deben ser revisados y socializados por las partes interesadas.

FASE DE PLANIFICACIÓN

Para el desarrollo de esta fase la entidad debe utilizar los resultados de la etapa anterior y proceder a elaborar el Plan de Seguridad y Privacidad de la Información alineado con el objetivo misional de la entidad, con el propósito de definir las acciones a implementar a nivel de seguridad y privacidad de la información, a través de una metodología de gestión del riesgo.

El alcance del MSPI permite a la Corporación definir los límites sobre los cuales se implementará la seguridad y privacidad.

Este enfoque es por procesos y debe extenderse a todo el Concejo Municipal de Envigado.

Para desarrollar el alcance y los límites del Modelo se deben tener en cuenta las siguientes recomendaciones:

Procesos que impactan directamente la consecución de objetivos misionales, procesos, servicios, sistemas de información, ubicaciones físicas, terceros relacionados, e interrelaciones del Modelo con otros procesos.

El contenido de la figura 3 fue tomado de la Norma ISO IEC 27001 Capítulos 4, 5, 6, 7, que permite orientar como se desarrolla la planificación del MSPI.

FASE DE IMPLEMENTACIÓN

Esta fase le permitirá al Concejo Municipal de Envigado, llevar a cabo la implementación de la planificación realizada en la fase anterior del MSPI.

El contenido de la figura 4 fue tomada de la Norma ISO IEC 27001 Capítulo 8, que permite orientar como se desarrolla la implementación del MSPI.

FASE DE EVALUACIÓN DE DESEMPEÑO

El proceso de seguimiento y monitoreo del MSPI se hace con base a los resultados que arrojan los indicadores de la seguridad de la información propuestos para verificación de la efectividad, la eficiencia y la eficacia de las acciones implementadas.

El contenido de la figura 5 fue tomada de la Norma ISO IEC 27001 Capítulo 9, que permite orientar como se desarrolla la evaluación de desempeño del MSPI. Plan de revisión y seguimiento a la implementación del MSPI.

En este aspecto, el Concejo Municipal de Envigado debe crear un plan que contemple las siguientes actividades:

• Revisión de la efectividad de los controles establecidos y su apoyo al cumplimiento de los objetivos de seguridad.
• Revisión de la evaluación de los niveles de riesgo y riesgo residual después de la aplicación de controles y medidas administrativas.
• Seguimiento a la programación y ejecución de las actividades de autorías internas y externas del MSPI.
• Seguimiento al alcance y a la implementación del MSPI.
• Seguimiento a los registros de acciones y eventos / incidentes que podrían tener impacto en la eficacia o desempeño de la seguridad de la información al interior de la entidad.
• Medición de los indicadores de gestión del MSPI
• Revisiones de acciones o planes de mejora (solo aplica en la segunda revisión del MSPI) Este plan deberá permitir la consolidación de indicadores periódicamente y su evaluación frente a las metas esperadas; deben ser medibles permitiendo analizar causas de desviación y su impacto en el cumplimiento de las metas y objetivos del MSPI.

FASE DE MEJORA CONTINUA

En esta fase el Concejo Municipal de Envigado debe consolidar los resultados obtenidos de la fase de evaluación de desempeño, para diseñar el plan de mejoramiento continuo de seguridad y privacidad de la información, tomando las acciones oportunas para mitigar las debilidades identificadas.

El contenido de la figura 6 fue tomada de la Norma ISO IEC 27001 Capítulo 10, que permite orientar como se desarrolla la fase de Mejoramiento Continuo del MSPI.

En esta fase es importante que la Corporación defina y ejecute el plan de mejora continua con base en los resultados de la fase de evaluación del desempeño.

Este plan incluye:

• Resultados de la ejecución del plan de seguimiento, evaluación y análisis para el MSPI.

• Resultados del plan de ejecución de auditorías y revisiones independientes al MSPI.

Utilizando los insumos anteriores, la Corporación puede efectuar los ajustes a los entregables, controles y procedimientos dentro del MSPI.

Estos insumos tendrán como resultado un plan de mejoramiento y un plan de comunicaciones de mejora continua, revisados y aprobados por la Alta Dirección de la entidad.

La revisión por la Alta Dirección hace referencia a las decisiones, cambios, prioridades etc. tomadas en sus comités y que impacten el MSPI.

PROTECCION DE DATOS PERSONALES

El Concejo Municipal de Envigado, pone en conocimiento la Política de Privacidad y Protección de Datos Personales en virtud de lo consagrado en la Ley 1581 de 2012 y su Decreto reglamentario 1377 de 2013, aplicado a todo dato personal que haya sido sido suministrado o que se suministre al CONCEJO MUNICIPAL DE ENVIGADO, teniendo en cuenta que la corporación, en su proceso de implementación del Sistema de Gestión de Seguridad de la Información bajo el marco de la norma ISO 27001, aplica y da cumplimiento a la normatividad vigente en materia de protección de datos de carácter personal.

Como parte del Sistema de Gestión basado en ISO 27001, desarrolló las políticas de seguridad tendientes a proteger los activos de información entre ello la protección de datos personales. Atendiendo la norma, el CONCEJO MUNICIPAL DE ENVIGADO en pro de mejorar su Sistema de Gestión de Seguridad de la Información, ha generado una política para aplicar al tratamiento y protección de datos de carácter personal. Los funcionarios y contratistas del CONCEJO MUNICIPAL DE ENVIGADO deben, observar, acatar y cumplir las órdenes e instrucciones de carácter legal que aplica la entidad respecto al manejo de los datos de carácter personal cuya divulgación o indebido uso pueda generar un perjuicio a los usuarios, en cumplimiento de los derechos contenidos en el artículo 15 de la Constitución Política de Colombia, ley 1266 de 2008, ley 1273 de 2009, ley 1581 de 2012, Decreto Reglamentario 1377 de 2013, y demás disposiciones complementarias.

INFORMACIÓN PERSONAL RECOLECTADA

La Información Personal que el CONCEJO MUNICIPAL DE ENVIGADO. Puede recolectar y someter a tratamiento es la siguiente:

• Nombre completo del titular de la información; • Identificación: • Fecha de nacimiento; • Domicilio; • Dirección para notificación; • Teléfonos de contacto; • Correo electrónico; • Identidad de género.

TRATAMIENTO DE DATOS PERSONALES DE MENORES DE EDAD - En aplicación de lo establecido en la normatividad vigente, el CONCEJO MUNICIPAL DE ENVIGADO procederá a efectuar el Tratamiento de la Información personal; de niños, niñas y adolescentes, respetando el interés superior de los mismos y asegurando, en todos los casos, el respeto de sus derechos fundamentales y garantías mínimas. - En todos los eventos en los que se requiera darle tratamiento a la información personal de menores de edad, el CONCEJO MUNICIPAL DE ENVIGADO obtendrá la autorización de sus representantes legales, que para este efecto son el padre y/o madre o tutor.

MANEJO DE LA INFORMACIÓN - CLASIFICACIÓN DE LA INFORMACIÓN

La información resultante de los procesos misionales y de apoyo de la entidad, se tratará conforme a los lineamientos y parámetros establecidos en el Manual de Gestión Documental de la entidad. Los activos informáticos asociados a cada sistema de información, serán identificados y clasificados por su tipo y uso siguiendo lo establecido en las tablas de retención documental vigentes, de acuerdo con los siguientes criterios:

a) Pública: Datos misionales y críticos.
b) Interna: Aplicativos, archivos de software, archivos de usuarios, herramientas y programas de desarrollo. Manuales, procedimientos internos, guías y formatos.
c) Confidencial: Bases de Datos, Documentación, procedimientos operativos, configuraciones.

ACTIVIDADES PARA LA IMPLEMENTACIÓN.

• Realizar diagnóstico.
• Comparar el objetivo con lo identificado
• Realizar inventario de activos de información (Software, bases de datos) con los líderes de cada proceso
• Realizar la valoración de los activos de información con los líderes de cada proceso y emitir el plan
• Socializar el plan
• Ejecución del plan
• Realizar seguimiento del plan

CUMPLIMIENO DE IMPLEMENTACIÓN.

De acuerdo con las fases mencionadas anteriormente, se describe a continuación los dominios que se deben desarrollar y los plazos de implementación de acuerdo a lo establecido por el Concejo Municipal de Envigado. • Implementar la Política de Seguridad de la información. • Aspectos organizativos de la seguridad de la información • Plan de tratamiento de riesgos de seguridad y privacidad de la información • Seguridad de la Información enfocada a los recursos humanos • Revisión de los Controles de acceso • Seguridad en las telecomunicaciones • Gestión de Incidentes de Seguridad de la Información • Aspectos de seguridad de la información en la gestión de continuidad del plan.