RESOLUCIÓN ADMINISTRATIVA 08
(29 de enero de 2026)

POR MEDIO DEL CUAL SE ADOPTA EL PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN DE LA PERSONERÍA MUNICIPAL DE SILVANIA CUNDINAMARCA

EL PERSONERO MUNICIPAL DE SILVANIA, CUNDINAMARCA

En uso de sus facultades Constitucionales, legales y en especial en las conferidas por la Ley 136 de 1994 y.

CONSIDERANDO

1. En el artículo 15 de la Constitución Política de Colombia se establece que “todas las personas tienen derecho a su intimidad personal y familiar y a su buen nombre, debiendo el Estado respetarlos y hacerlos respetar”

2. La Ley 1273 de 2009 crea un nuevo bien jurídico tutelado denominado "De la protección de la información y los datos", preservando integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones.

3. La Ley Estatutaria 1581 de 2012, tiene como objeto “(…) desarrollar el derecho constitucional que tienen todas las personas a conocer, actualizar y rectificar las informaciones que se hayan recogido sobre ellas en bases de datos o archivos, y los demás derechos, libertades y garantías constitucionales”, estableciendo, además, las disposiciones generales para la protección de datos personales.

4. La Ley Estatutaria 1712 de 2014, define en su Artículo 1, que “el objeto de la presente ley es regular el derecho de acceso a la información pública, los procedimientos para el ejercicio y garantía del derecho y las excepciones a la publicidad de información.”

5. En el marco del Decreto Nacional 2573 de 2014 establece los lineamientos generales de Gobierno en Línea e incorpora los requerimientos de la Ley 1581 de 2012 para la protección de datos personales y se diseñan en el marco de referencia a la norma ISO 27001 en cada uno de sus dominios.

6. El Decreto 1078 de 2015 dispone que las entidades que conforman la administración pública serán sujetos obligados para el cumplimiento de las políticas y los lineamientos de la Estrategia de Gobierno en Línea, estableciendo en su artículo 2.2.9.1.2.1 como uno de sus cuatro componentes, el de la Seguridad y privacidad de la Información, comprendido por las acciones transversales a los componentes de TIC para Servicios, TIC para el Gobierno Abierto y TIC para la Gestión, tendientes a proteger la información y sistemas de información, del acceso, divulgación, interrupción o destrucción no autorizada.

7. El Decreto 103 de 2015 reglamenta parcialmente la ley de transparencia y el derecho de acceso a la información pública

8. La Norma ISO 27001:2013 es la norma estándar para la seguridad de la información expedida por la Organización Internacional de Normalización.

9. Alineados con la política de Gobierno Digital y teniendo en cuenta que la Norma ISO 27001 es una norma emitida por la Organización Internacional de Normalización, que describe cómo gestionar la seguridad de la información en una organización, determina que la implementación del Sistema de Gestión de Seguridad de Información SGSI, se realice en el marco de dicha norma, sobre la cual se desarrolla la Política de Seguridad y Privacidad de la Información.

10. La Política de Seguridad y Privacidad de la Información, es la declaración donde se establece el compromiso y el enfoque de la Personería Municipal de SILVANIA Cundinamarca, respecto a la gestión de la seguridad y privacidad de la información, indicando las responsabilidades y la conducta aceptada para funcionarios, contratistas, proveedores y terceros que debido al cumplimiento de sus funciones u obligaciones tienen acceso a la información de la entidad.

11. De conformidad con el anterior marco jurídico, se hace necesario adoptar el Plan estratégico de tecnologías de la información y la comunicación-PETI para la vigencia 2026, el cual constituye el instrumento de planeación fundamental para adelantar la gestión del talento humano de la Personería Municipal de Silvania Cundinamarca.

RESUELVE

ARTÍCULO PRIMERO: Adoptar el Plan de tratamiento de riesgos de seguridad y privacidad de la información de la Personería Municipal de Silvania Cundinamarca.

ARTÍCULO SEGUNDO: El Plan de tratamiento de riesgos de seguridad y privacidad de la información será divulgado y socializado a todos los funcionarios de la Personería Municipal de Silvania Cundinamarca, y los programas y planes que lo conforman, se encontrarán disponibles para su consulta a través del portal institucional

ARTÍCULO TERCERO: La implementación y evaluación del Plan de tratamiento de riesgos de seguridad y privacidad de la información adoptado en la presente Resolución, será responsabilidad de la Personería Municipal de Silvania Cundinamarca y de su equipo de trabajo.

ARTÍCULO CUARTO: La presente resolución rige a partir de la fecha de su publicación y deroga cualquier disposición que sea la contraria.

PUBLÍQUESE, COMUNÍQUESE Y CÚMPLASE

Expedido en el despacho de la Personería Municipal de Silvania Cundinamarca, a los veintinueve (29) días del mes de enero del dos mil veintiséis (2026)

Diana Cordoba

DIANA MARGARITA CORDOBA PINZON
Personera Municipal

PERSONERÍA
DE SILVANIA

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

PERSONERÍA MUNICIPAL DE SILVANIA - CUNDINAMARCA
2026

DIANA MARGARITA CORDOBA PINZON
PERSONERA MUNICIPAL

INTRODUCCIÓN

El plan de tratamiento de riesgos de Seguridad y Privacidad de la información, Seguridad Digital y Continuidad de la Operación, se basa en una orientación estratégica que requiere el desarrollo de una cultura de carácter preventivo, de manera que, 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 las situaciones que pueden comprometer el cumplimiento de los objetivos trazados el Entorno TIC.

Es fundamental definir y establecer un plan para la Entidad en la que se establezcan los parámetros y protocolos para salvaguardar la información. Diariamente se genera información confidencial y a su vez de interés general, la cual debe tener un tratamiento especial en cada caso, para así garantizar su privacidad y adecuado tratamiento.

OBJETIVOS

OBJETIVO GENERAL

Formular, desarrollar y poner en práctica el Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información para la Personería Municipal de SILVANIA Cundinamarca, y que sirva de referencia en cuanto al tratamiento de información propia de la Entidad, así como de usuarios externos.

OBJETIVOS ESPECÍFICOS

1. Diagnosticar el estado de la Entidad en materia de Tratamiento de Riesgos de seguridad y privacidad de la información.

2. Aplicar las metodologías, mejores prácticas y recomendaciones dadas por la función pública y el MinTic para el Tratamiento de Riesgos de Seguridad y Privacidad de la Información

3. Fortalecer el sistema de gestión de riesgos de la Entidad incorporando controles y medidas de seguridad de la información que estén acordes al entorno operativo de la Entidad.

GLOSARIO

CONCEPTO	DEFINICIÓN
Activo	Cualquier elemento que tenga valor para la organización
Reducir/Mitigar	El riesgo se trata mediante la transferencia o la implementación de acciones que mitiguen su nivel. No necesariamente es un control adicional.
Análisis del riesgo	Se estima el riesgo con el fin de proporcionar bases que logre la evaluación y la naturaleza del riesgo.
Causa	Elemento específico que origina el evento
Contexto externo	Ambiente externo en el cual la organización busca alcanzar sus objetivos (tecnológico, legal, regional, etc.).
Controles:	Procesos, políticas y/o actividades que pueden modificar el riesgo.
Criterios de riesgos	Términos de referencia frente a los cuales se evaluará la importancia del riesgo.
Evaluación del Riesgo	Comparar los resultados del análisis de riesgo frente a los controles implementados, con el fin de determinar el riesgo final.
Evento	Posible ocurrencia de Incidente o amenaza de Seguridad de la

	Información.
Seguridad de la Información	Este principio busca crear condiciones de uso confiable en el entorno digital, mediante un enfoque basado en la gestión de riesgos, preservando la confidencialidad, integridad y disponibilidad de la información de las entidades del Estado, y de los servicios que prestan al ciudadano.
Vulnerabilidad	Es una falencia o debilidad que puede estar presente en la tecnología, las personas o en las políticas y procedimientos.
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 Entidad (materializar el riesgo).

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

Este documento se fundamenta conforme a los lineamientos arraigados por el Ministerio de las TIC y los estándares ISO 27001:2013, ISO 31000:2018, para establecer los principios e implementar un sistema de gestión de riesgos, cuyo objetivo es minimizar, gestionar y controlar cualquier tipo de riesgo teniendo en cuenta el origen, la causa y su grado de incidencia.

El Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información en la Personería Municipal de SILVANIA Cundinamarca, se llevó a cabo la expansión adecuada de diversas figuras importantes en el tema de plan de tratamiento del riesgo de la privacidad y seguridad de la información, ya que a través de ellos se pudo dar definición de algunas concepciones que se consideran de gran relevancia para mitigar los riesgos identificados en la entidad, este mismo busca ejecutar un proceso de gestión de los riesgos, adoptando medidas y acciones encaminadas a minimizar los mismos, preservando la confidencialidad, integridad y disponibilidad de la información.

Este asunto confiere en instaurar un estudio de caracterización de riesgos de forma preventiva para proceder a realizar un tratamiento y administración de estos.

POLITICAS DE GESTIÓN DEL RIESGO

1. Implementar la Política de Seguridad y Privacidad de la información.

2. Seguridad de la Información enfocada a los recursos humanos.

3. Revisión de los Controles de acceso.

4. Gestión de incidentes de Seguridad de la Información.

Para mitigar los riesgos, es fundamental que se destinen recursos humanos, tecnológicos, operativos y de presupuesto que permitan de una manera continua ejecutar esbozos de trabajo y acciones para mejorar las políticas de seguridad y privacidad existentes.

RIESGO

Es la posibilidad de sufrir daños o pérdidas.

La amenaza es un componente del riesgo y se puede considerar como: un agente de amenazas ya sea voluntario o involuntario, como identificar y explotar una vulnerabilidad, que ofrece un resultado inesperado y no deseado

La caracterización del riesgo consiente en conocer las ocurrencias que puedan surgir frente a las alteraciones en el funcionamiento de la entidad, y pueden complicar y afectar la confidencialidad, integridad y disponibilidad de la información.

El propósito fundamental de caracterizar el riesgo es determinar que puede ocurrir en el caso de tener una perdida potencial de información y que acciones tomar al comprender la causa y el dónde y por qué puede ocurrir el evento.

RIESGO	CAUSAS
Daño en los equipos tecnológicos.	Falta de mantenimiento.
	Uso inadecuado de las herramientas tecnológicas
Pérdida de la conexión.	Daños en el proveedor
	Daños de la redes de electricidad
Correos electrónicos no seguros.	Desconocimiento de los riesgos al acceder a correos falsos. - Instalación de programas espías.
	Fallas en los filtros de seguridad o mala configuración del servidor
Pérdida, Hurto o Evasión de Información.	Fallas en el proceso del respaldo de la información o restauración de la misma
	Fallas en los análisis y socialización

INDIVIDUALIZACIÓN DE LAS AMENAZAS

Las amenazas ocasionan daños a los activos como información, procesos y sistemas lo que produce el detrimento a cualquier entidad. Estas amenazas pueden ser fortuitas o voluntarias, por lo que pueden ser accidentales o deliberadas. Estas amenazas se deberían distinguir genéricamente.

TIPO	AMENAZA
Eventos naturales	Fenómenos Climáticos, polvo, corrosión
Daño físico	Pérdida del suministro de energía
Acciones no autorizadas	Uso no autorizado del equipo
	Corrupción de datos
	Procesamiento ilegal de datos
	Acceso forzado al sistema
	Copias ilegales de software y datos reservados
Pérdida de los servicios esenciales	Falla en equipos de comunicaciones
	Fallos en discos de datos
Compromiso de la información	Hurto de documentos
	Robo de equipos de computo
Fallas técnicas	Fallas en el diseño de software
	Faltas de mantenimiento

TRATAMIENTO DEL RIESGO

El Tratamiento del Riesgo de la Personería Municipal de SILVANIA Cundinamarca, debe distinguir las siguientes opciones para tratar los riesgos.

Evadir el riesgo

Esta opción de tratamiento busca eliminar la probabilidad de ocurrencia o el impacto del riesgo, tomar las medidas necesarias para prevenir la materialización del riesgo.

Es siempre la primera alternativa a considerar, se logra cuando al interior de los procesos se generan cambios sustanciales por mejoramiento, rediseño o eliminación, resultado de unos adecuados controles y acciones emprendidas.

Comprimir riesgos

Se efectúa cuando el riesgo se puede tratar internamente y puede llevarse a un nivel aceptable

Asumir el riesgo

Luego de que el riesgo ha sido reducido o transferido puede quedar un riesgo residual que se mantiene, en este caso, el jefe del proceso simplemente acepta la pérdida residual probable y elabora planes de contingencia para su manejo.

MODELO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN MSPI

Fundamentados en la guía del Ministerio de las Tecnologías de la Información y las Comunicaciones, el modelo de seguridad y privacidad de la información, contempla un ciclo de operación de cinco fases para realizar una gestión adecuada de los activos y los recursos de información en la Personería Municipal de SILVANIA Cundinamarca.

Este modelo de seguridad está encaminado a preservar la confidencialidad, integridad y disponibilidad de la información, lo que contribuye al cumplimiento del Plan Estratégico Institucional, la misión y la visión de la entidad.

Figura 1. Ciclo de Operación del Modelo de Seguridad y Privacidad de la Información

Fuente: https://www.mintic.gov.co/gestionti/615/articles-5482_Modelo_de_Seguridad_Privacidad.pdf

ACTIVIDADES POR FASES

PRIMERA FASE DE DIAGNOSTICO

ACTIVIDAD	PRODUCTO	FECHAS	
		INICIO	FIN

Determinar el estado actual de la gestión de seguridad y privacidad de la información al interior de la Entidad.	Diligenciamiento de la herramienta autodiagnóstico (MINTIC).	01-02-2026	20-02-2026
Determinar el nivel de madurez de los controles de seguridad de la información.	Diligenciamiento de la herramienta autodiagnóstico (MINTIC).	01-02-2026	30-01-2027
Identificar el avance de la Tecnológica y de la herramienta implementación del ciclo de la Información- autodiagnóstico operación al interior de la entidad.	Diligenciamiento de la herramienta autodiagnóstico (MINTIC).	01-02-2026	30-01-2027
Identificar el nivel de cumplimiento con la legislación vigente, relacionada con protección de datos personales.	Diligenciamiento de la herramienta autodiagnóstico (MINTIC).	01-02-2026	30-01-2027

SEGUNDA FASE DE PLANEACIÓN

ACTIVIDAD	PRODUCTO	FECHAS	
		INICIO	FIN
Realizar o actualizar la Política de Seguridad y Privacidad de la Información.	Documento con la Política de Seguridad de la Información, aprobado y socializado al interior de la Entidad.	01-01-2026	20-02-2026

TERCERA FASE DE IMPLEMENTACIÓN

ACTIVIDAD	PRODUCTO	FECHAS	
		INICIO	FIN
Metas para el cumplimiento de la Gestión.	Documento con la descripción de las metas de gestión de seguridad y privacidad de la información	01-02-2026	28-05-2026

CUARTA FASE DE EVALUACIÓN DE DESEMPEÑO

ACTIVIDAD	PRODUCTO	FECHAS	
		INICIO	FIN
Plan de revisión y seguimiento a la implementación del MSPI.	Documento con el plan de seguimiento y revisión del MSPI revisado y aprobado por el Personero Municipal.	01-12-2026	31-01-2027

QUINTA FASE DE MEJORA CONTINUA

ACTIVIDAD	PRODUCTO	FECHAS	
		INICIO	FIN
Plan de mejora continua	Resultados de la ejecución del Plan de Revisión y Seguimiento, a la Implementación del MSPI.	01-12-2026	31-01-2027
	Resultados del plan de ejecución y revisiones independientes al MSPI.	01-12-2026	31-01-2027

SEGUIMIENTO Y EVALUACIÓN

Se realiza seguimiento al plan de tratamiento de riesgos de seguridad y privacidad de la información de la Personería Municipal de Silvania Cundinamarca, para la vigencia 2026 será de manera anual.

Expedido en el despacho de la Personería Municipal de Silvania Cundinamarca, a los veintinueve (29) días del mes de enero del dos mil veintiséis (2026)

Diana Cordoba

DIANA MARGARITA CORDOBA PINZON
Personera Municipal