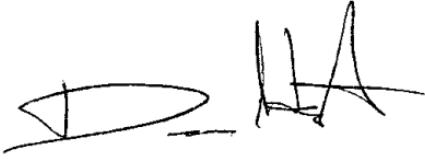




Tel. 07 1200000-3  
CAM Anganoy - los Rosales II  
Teléfono: +57 (602) 7244326 Ext: 1301  
Correo electrónico: [contactenos@pasto.gov.co](mailto:contactenos@pasto.gov.co)  
- Es su responsabilidad ecológica imprimir este documento -

Fecha	<b>Enero de 2026</b>		
Resumen	Este documento corresponde al Plan Estratégico de Tecnologías de la Información de la Alcaldía de Pasto – Nariño y tiene como propósito avanzar en la implementación del Sistema de Gestión de Seguridad de la Información – SGSI, este documento está basado en el producto tipo suministrado por MINTIC.		
Palabras clave	Plan, Tecnologías de la Información, Información, Datos, Sistemas, Infraestructura de TI, Servicios de TI, Gestión de TI		
Formato	PDF	Versión	009
Participantes	Mabel Alejandra Gonzalez Cisneros <b>Contratista</b>		
Aprobó	Lic. DARIO FERNANDO ALFARO FIGUEROA <b>Subsecretario de Sistemas de Información</b>		

## CONTROL DE CAMBIOS

No. Revisión	Descripción de la modificación	Fecha de aprobación	Versión Actualizada
1	Se realizan ajustes para la vigencia 2019	Ene-2019	2
2	Se realizan ajustes para la vigencia 2020	Ene-2020	3
3	Se realizan ajustes para la vigencia 2021	Ene-2021	4
4	Se realiza ajustes para la vigencia 2022	Ene-2022	5
5	Se realiza ajustes para la vigencia 2023	Ene-2023	6
6	Se realiza ajustes para la vigencia 2024	Ene-2024	7
7	Se realiza ajustes para la vigencia 2025	Ene-2025	8
8	Se realiza ajustes para la vigencia 2026	Ene-2026	9

APROBACIÓN COMITÉ MIPG

No. de acta	Fecha

NIT: 891280000-3  
CAM Anganoy - los Rosales II  
Teléfono: +57 (602) 7244326 Ext: 1301  
Correo electrónico: [contactenos@pasto.gov.co](mailto:contactenos@pasto.gov.co)  
- Es su responsabilidad ecológica imprimir este documento -

## CONTENIDO

	Pág.
1	2
2	3
3	6
4	9
4.1	9
5	10
6	11
7	14
7.1	14
8	16
9	19

## 1 INTRODUCCIÓN

La seguridad y privacidad de la información son pilares fundamentales para garantizar la confianza y credibilidad de las entidades públicas ante sus ciudadanos y las organizaciones con las que interactúan. Con el propósito de fortalecer nuestro sistema de gestión de la seguridad y privacidad de la información, y en cumplimiento de los lineamientos establecidos por el MINTIC, hemos diseñado este plan estratégico que define las acciones necesarias para alcanzar un nivel óptimo en estas áreas dentro de nuestra entidad.

Este plan estratégico incluye actividades clave para identificar riesgos, evaluar fortalezas y aprovechar oportunidades de mejora en nuestras prácticas de seguridad. Asimismo, establece metas y objetivos concretos a corto y mediano plazo, que permitirán mejorar continuamente nuestras capacidades.

Con la implementación de este plan, lograremos robustecer la protección de nuestra información, aumentar nuestra capacidad de respuesta ante incidentes de seguridad y reforzar la confianza de los ciudadanos en la gestión de la Alcaldía de Pasto.

En relación con la estrategia de seguridad digital, esta se encuentra inmersa dentro de la implementación del sistema de gestión de seguridad de la información.

## 2 MARCO LEGAL

- Constitución Política de Colombia. Artículos 15 y 20
- Ley 44 de 1993. Por la cual se modifica y adiciona la Ley 23 de 1982 y se modifica la Ley 29 de 1944.
- Decisión Andina 351 de 2015 – Comunidad Andina (Régimen Común Sobre Derecho De Autor Y Derechos Conexos).
- 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 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 1221 del 2008. Por la cual se establecen normas para promover y regular el Teletrabajo 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 de 2012. Por el cual se reglamenta parcialmente la Ley 1221 de 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 imparte 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 728 de 2017. Por el cual se adiciona el capítulo 2 al título 9 de la parte 2 del libro 2 del Decreto Único Reglamentario del sector TIC, Decreto 1078 de 2015, para fortalecer el modelo de Gobierno Digital en las entidades del orden nacional del Estado colombiano, a través de la implementación de zonas de acceso público a Internet inalámbrico.
- Decreto 1499 de 2017. Por medio del cual se modifica el Decreto 1083 de 2015, Decreto Único Reglamentario del Sector Función Pública, en lo relacionado con el Sistema de Gestión establecido en el artículo 133 de la Ley 1753 de 2015.
- Decreto 0317 del 24 de septiembre de 2018 por el cual se integra y se establece el reglamento de funcionamiento del comité institucional de gestión y desempeño de la Alcaldía de Pasto.
- Resolución 1519 de 2020, por la cual se definen los estándares y directrices para publicar la información señalada en la Ley 1712 del 2014 y se definen los requisitos en materia de acceso a la información pública, accesibilidad web, seguridad digital, y datos abiertos.
- Decreto 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 municipal 0496 de 2022, por el cual se deroga el decreto 0714 de 2016 y se adopta la política para el tratamiento de datos personales en el municipio de Pasto.

NIT: 891280000-3

CAM Anganoy - los Rosales II

Teléfono: +57 (602) 7244326 Ext: 1301

Correo electrónico: [contactenos@pasto.gov.co](mailto:contactenos@pasto.gov.co)

- Es su responsabilidad ecológica imprimir este documento -

- Resolución 00500 de marzo 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 02277 de junio de 2025 – MINTIC, Por la cual se actualiza el Anexo 1 de la Resolución 500 de 2021 y se derogan otras disposiciones relacionadas con la materia.

## FINICIONES

- Administración del riesgo: conjunto de elementos de control que al interrelacionarse brindan a la entidad la capacidad para emprender las acciones necesarias que le permitan el manejo de los eventos que puedan afectar negativamente el logro de los objetivos institucionales y protegerla de los efectos ocasionados por su ocurrencia.
- Activo de Información: en relación con la seguridad de la información, se refiere a cualquier información o elemento de valor para los procesos de la Organización.
- Análisis de riesgos: es un método sistemático de recopilación, evaluación, registro y difusión de información necesaria para formular recomendaciones orientadas a la adopción de una posición o medidas en respuesta a un peligro determinado.
- Amenaza: es la causa potencial de una situación de incidente y no deseada por la organización
- Causa: son todo aquello que se pueda considerar fuente generadora de eventos (riesgos). Las fuentes o agentes generadores son las personas, los métodos, las herramientas, el entorno, lo económico, los insumos o materiales entre otros.
- Confidencialidad: propiedad de la información de no ponerse a disposición o ser revelada a individuos, entidades o procesos no autorizados.
- Consecuencia: resultado de un evento que afecta los objetivos.
- Criterios del riesgo: términos de referencia frente a los cuales la importancia de un riesgo es evaluada.
- Control: medida que modifica el riesgo.
- Disponibilidad: propiedad de la información de estar accesible y utilizable cuando lo requiera una entidad autorizada.
- Evaluación de riesgos: proceso de comparación de los resultados del análisis del riesgo con los criterios del riesgo, para determinar si el riesgo, su magnitud o ambos son aceptables o tolerables.
- Evento: un incidente o situación, que ocurre en un lugar particular durante un intervalo de tiempo específico.
- Estimación del riesgo. proceso para asignar valores a la probabilidad y las consecuencias de un riesgo.
- Evitación del riesgo. decisión de no involucrarse en una situación de riesgo o tomar acción para retirarse de dicha situación.
- Factores de Riesgo: situaciones, manifestaciones o características medibles u observables asociadas a un proceso que generan la presencia de riesgo o tienden a aumentar la exposición, pueden ser internos o externos a la entidad.

- Gestión del riesgo: actividades coordinadas para dirigir y controlar una organización con respecto al riesgo, se compone de la evaluación y el tratamiento de riesgos.
- Identificación del riesgo. proceso para encontrar, enumerar y caracterizar los elementos de riesgo.
- Incidente de seguridad de la información: evento único o serie de eventos de seguridad de la información inesperados o no deseados que poseen una probabilidad significativa de comprometer las operaciones del negocio y amenazar la seguridad de la información (Confidencialidad, Integridad y Disponibilidad).
- Integridad: propiedad de la información relativa a su exactitud y completitud.
- Impacto. cambio adverso en el nivel de los objetivos del negocio logrados.
- Nivel de riesgo: magnitud de un riesgo o de una combinación de riesgos, expresada en términos de la combinación de las consecuencias y su posibilidad.
- Matriz de riesgos: instrumento utilizado para ubicar los riesgos en una determinada zona de riesgo según la calificación cualitativa de la probabilidad de ocurrencia y del impacto de un riesgo.
- Monitoreo: mesa de trabajo anual, la cual tiene como finalidad, revisar, actualizar o redefinir los riesgos de seguridad de la información en cada uno de los procesos, partiendo del resultado de los seguimientos y/o hallazgos de los entes de control o las diferentes auditorías de los sistemas integrados de gestión.
- Propietario del riesgo: persona o entidad con la responsabilidad de rendir cuentas y la autoridad para gestionar un riesgo.
- Proceso: conjunto de actividades interrelacionadas o que interactúan para transformar una entrada en salida.
- Riesgo Inherente: Es el nivel de riesgo propio de la actividad, sin tener en cuenta el efecto de los controles.
- Riesgo Residual: el riesgo que permanece tras el tratamiento del riesgo o nivel resultante del riesgo después de aplicar los controles.
- Riesgo: efecto de la incertidumbre sobre los objetivos.
- Riesgo en la seguridad de la información: potencial de que una amenaza determinada explote las vulnerabilidades de los activos o grupos de activos causando así daño a la organización.
- Reducción del riesgo: acciones que se toman para disminuir la probabilidad de las consecuencias negativas, o ambas, asociadas con un riesgo.
- Retención del riesgo. aceptación de la pérdida o ganancia proveniente de un riesgo particular
- Seguimiento: mesa de trabajo semestral, en el cual se revisa el cumplimiento del plan de acción, indicadores y metas de riesgo y se valida la aplicación de los controles de seguridad de la información sobre cada uno de los procesos.

- Tratamiento del Riesgo: proceso para modificar el riesgo" (Icontec Internacional, 2011).
- Valoración del Riesgo: proceso global de identificación del riesgo, análisis del riesgo y evaluación de los riesgos.
- Vulnerabilidad: es aquella debilidad de un activo o grupo de activos de información
- Seguridad de la información: preservación de la confidencialidad, integridad y disponibilidad de la información.

### 3 OBJETIVO GENERAL

Fortalecer la integridad, confidencialidad y disponibilidad de los activos de información de la entidad, para reducir los riesgos a los que está expuesta la organización hasta niveles aceptables, a partir de la implementación del Sistema de Gestión de Seguridad la Información.

#### 3.1 Objetivos específicos

- Dar continuidad a la implementación a la política general de seguridad de la información.
- Dar continuidad a la implementación de las políticas específicas de seguridad de la información.
- Dar continuidad a la implementación de la política de protección de datos personales.
- Dar continuidad a la implementación de la metodología de gestión de riesgos de seguridad de la información.

#### 4 ALCANCE

El Plan Estratégico de Seguridad de la Información al buscar la implementación del Sistema de Gestión de Seguridad de la Información, comparte el alcance definido dentro de la Política General de Seguridad de la Información, donde se indica que se tendrán en cuenta todos los procesos de la entidad.

NIT: 891280000-3  
CAM Anganoy - los Rosales II  
Teléfono: +57 (602) 7244326 Ext: 1301  
Correo electrónico: [contactenos@pasto.gov.co](mailto:contactenos@pasto.gov.co)  
- Es su responsabilidad ecológica imprimir este documento -

## 5 ESTADO ACTUAL

Acorde al instrumento de autodiagnóstico de avance de implementación del MSPI, el estado es el siguiente con corte a diciembre de 2025:

No.	Evaluación de Efectividad de controles			EVALUACIÓN DE EFECTIVIDAD DE CONTROL
	DOMINIO	Calificación Actual	Calificación Objetivo	
A.5	POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN	100	100	OPTIMIZADO
A.6	ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN	36	100	REPETIBLE
A.7	SEGURIDAD DE LOS RECURSOS HUMANOS	80	100	GESTIONADO
A.8	GESTIÓN DE ACTIVOS	49	100	EFFECTIVO
A.9	CONTROL DE ACCESO	10	100	INICIAL
A.10	CRPTOGRAFÍA	20	100	INICIAL
A.11	SEGURIDAD FÍSICA Y DEL ENTORNO	17	100	INICIAL
A.12	SEGURIDAD DE LAS OPERACIONES	11	100	INICIAL
A.13	SEGURIDAD DE LAS COMUNICACIONES	17	100	INICIAL
A.14	ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS	13	100	INICIAL
A.15	RELACIONES CON LOS PROVEEDORES	70	100	GESTIONADO
A.16	GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN	46	100	EFFECTIVO
A.17	ASPECTOS DE SEGURIDAD DE LA INFORMACIÓN DE LA GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO	44	100	EFFECTIVO
A.18	CUMPLIMIENTO	56	100	EFFECTIVO
<b>PROMEDIO EVALUACIÓN DE CONTROLES</b>		<b>41</b>	<b>100</b>	<b>EFFECTIVO</b>

Año	AVANCE PHVA		
	COMPONENTE	% de Avance Actual	% Avance Esperado
2024	Planificación	31%	40%
	Implementación	8%	20%
	Evaluación de desempeño	3%	20%
	Mejora continua	0%	20%
<b>TOTAL</b>		<b>42%</b>	<b>100%</b>



Matriz operativa PESI - 2025

Actividad/ Alternativa de Mejora	Producto	Meta	Porcentaje de avance
Actualizar la información de la entidad en el instrumento de evaluación del Modelo de Seguridad y Privacidad de la Información	Instrumento de evaluación del MSPI actualizado con la información de la entidad	Nivel de madurez del MSPI actualizado	100%
Formular y desarrollar un plan de acción para la implementación de las políticas específicas de seguridad de la información	Plan de acción para la implementación de las políticas específicas de seguridad de la información	Implementar al menos un 25% de las actividades propuestas en el plan de acción para la implementación de las políticas específicas de seguridad de la información	100%
Socializar la política de protección de datos personales con equipo de trabajo de seguridad de la información	Equipo de trabajo de seguridad de la información con conocimientos específicos en el Decreto 0496 de 2022	Socialización de la política de protección de datos al 100% DEL EQUIPO de trabajo de seguridad de la información	100%
Realizar intervenciones para la aplicación de la política de protección de datos personales	Informe de intervenciones de aplicación de la política de protección de datos personales realizadas	100% de casos que requieran intervención para la aplicación de la política de protección de datos personales atendidos	100%

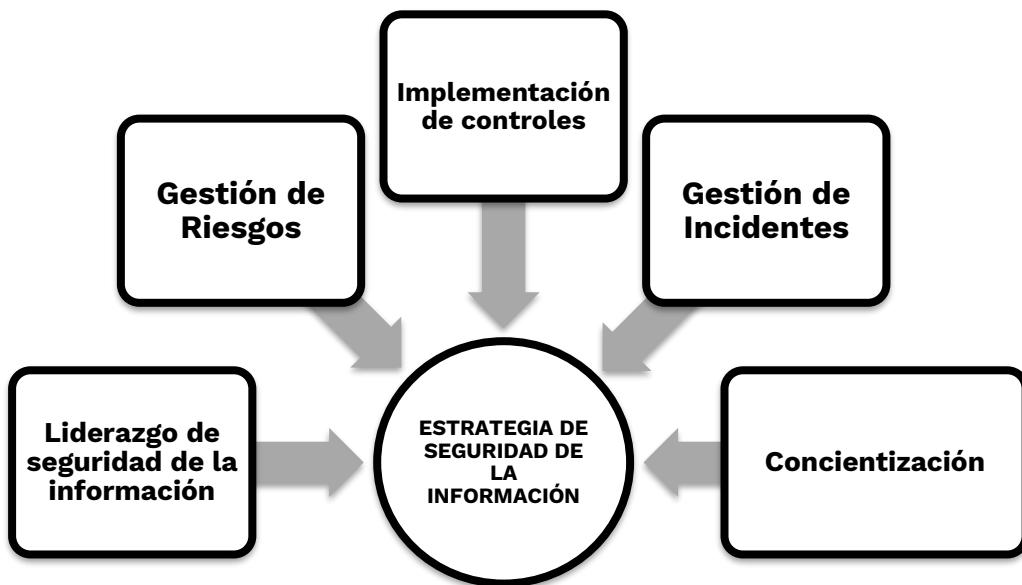


Actividad/ Alternativa de Mejora	Producto	Meta	Derecho aje de avance
Verificar la aplicación de la política de protección de datos personales en los formatos creados en el SGC	Depuración de formatos de 4 procesos priorizados del SGC para validación de la aplicación de la política de protección de datos personales	100% de los formatos de 4 procesos priorizados del SGC verificados en el cumplimiento de la política de protección de datos personales	100%
Actualizar el reporte de Registro Nacional de Bases de Datos	Registro Nacional de Bases de Datos actualizado con información de la vigencia 2024	100% De Registros de la entidad actualizados en la plataforma de RNBD con información de la vigencia 2024	1%
Mejorar la arquitectura de servicios de procesamiento, almacenamiento y base de datos en la entidad	Contratación de servicio en la nube	Al menos 1 sistema de información operando en la nube	100%

## 6 ESTRATEGIA DE SEGURIDAD DE LA INFORMACIÓN

La Alcaldía de Pasto establecerá una estrategia de seguridad de la información en la que se integren los principios, políticas, procedimientos, guías, manuales, formatos y lineamientos para la gestión de la seguridad de la información, teniendo como premisa que dicha estrategia gira entorno a la implementación del Modelo de Seguridad y Privacidad de la Información - MSPI, así como de la guía de gestión de riesgos de seguridad de la información y del procedimiento de gestión de incidentes que debe establecerse (Ver Resolución 500 de 2021).

Por tal motivo, la Alcaldía de Pasto define las siguientes 5 estrategias específicas, que permitirán establecer en su conjunto una estrategia general de seguridad de la información:



### 6.1 Descripción de las estrategias específicas (ejes)

A continuación, se describe el objetivo de cada una de las estrategias específicas a implementar, alineando las actividades a lo descrito dentro del MPSI y la resolución 500 de 2021:

ESTRATEGIA / EJE	DESCRIPCIÓN/OBJETIVO
Liderazgo de seguridad de la información	Asegurar que se establezca el Modelo de Seguridad y Privacidad de la Información (MSPI) a través de la aprobación de la política general y demás lineamientos que se definan buscando proteger la confidencialidad, integridad y disponibilidad de la información teniendo como pilar fundamental el compromiso de la alta dirección y de los líderes de las diferentes dependencias y/o procesos de la Entidad a través del establecimiento de los roles y responsabilidades en seguridad de la información.
Gestión de riesgos	Determinar los riesgos de seguridad de la información a través de la planificación y valoración que se defina buscando prevenir o reducir los efectos indeseados teniendo como pilar fundamental la implementación de controles de seguridad para el tratamiento de los riesgos.
Concientización	Fortalecer la construcción de la cultura organizacional con base en la seguridad de la información para que convierta en un hábito, promoviendo las políticas, procedimientos, normas, buenas prácticas y demás lineamientos, la transferencia de conocimiento, la asignación y divulgación de responsabilidades de todo el personal de la entidad en seguridad y privacidad de la información.
Implementación de controles	Planificar e implementar las acciones necesarias para lograr los objetivos de seguridad y privacidad de la información y mantener la confianza en la ejecución de los procesos de la Entidad, se pueden subdividir en controles tecnológicos y/o administrativos.
Gestión de incidentes	Garantizar una administración de incidentes de seguridad de la información con base en un enfoque de integración, análisis, comunicación de los eventos e incidentes y las debilidades de seguridad en pro de conocerlos y resolverlos para minimizar el impacto negativo de estos en la Entidad.



## 7 MATRIZ OPERATIVA

ACTIVIDADES DE GESTIÓN	QUÉ	CÓMO	QUIÉN	CUÁNDO (FECHA PREVISTA PARA INICIAR Y TERMINAR CADA TAREA)	EVIDENCIAS
	(ALTERNATIVAS DE MEJORA)	(MEJORAS/TAREAS A IMPLEMENTAR)	(RESPONSABLE DE CADA TAREA)		
Fortalecer la gestión de la seguridad de la información en la entidad	Dar continuidad a la implementación de la política general de seguridad de la información.	Actualizar las políticas de seguridad y privacidad de la información	Subsecretario de Sistemas de Información	01-feb-2026 - 11-dic-2026	(1) acto administrativo de actualización del manual de políticas de seguridad de la información
		Espacio de seguridad y privacidad de la información actualizado en portal web interno	Subsecretario de Sistemas de Información	01-feb-2026 - 11-dic-2026	(1) espacio de seguridad y privacidad de la información en portal web interno
		Actualizar matriz autodiagnóstico MSPI	Subsecretario de Sistemas de Información	01-feb-2026 - 11-dic-2026	(1) matriz autodiagnóstico MSPI actualizada

NIT: 891280000-3

CAM Anganoy - los Rosales II

Teléfono: +57 (602) 7244326 Ext: 1301

Correo electrónico: [contactenos@pasto.gov.co](mailto:contactenos@pasto.gov.co)

- Es su responsabilidad ecológica imprimir este documento -



ACTIVIDADES DE GESTIÓN	QUÉ	CÓMO	QUIÉN	CUÁNDO (FECHA PREVISTA PARA INICIAR Y TERMINAR CADA TAREA)	ALCALDÍA
	(ALTERNATIVAS DE MEJORA)	(MEJORAS/TAREAS A IMPLEMENTAR)	(RESPONSABLE DE CADA TAREA)		EVIDENCIAS
	Dar continuidad a la implementación de la metodología de gestión de riesgos de seguridad de la información.	Plan de tratamiento de riesgos de seguridad de la información	Subsecretario de Sistemas de Información	01-feb-2026 - 11-dic-2026	(1) plan de tratamiento de riesgos de seguridad de la información formulado que incluya al menos 10 procesos del sistema de gestión de calidad
	Dar continuidad a la implementación de la política de protección de datos personales.	Apoyo a la formalización de la actualización de la política de protección de datos personales	Subsecretario de Sistemas de Información	01-feb-2026 - 11-dic-2026	(1) acto administrativo de actualización de la política de protección de datos personales
		Realizar intervenciones para la aplicación de la política de protección de datos personales	Subsecretario de Sistemas de Información	01-feb-2026 - 11-dic-2026	(10) intervenciones de aplicación de la política de protección de datos personales



ACTIVIDADES DE GESTIÓN	QUÉ	CÓMO	QUIÉN	CUÁNDO (FECHA PREVISTA PARA INICIAR Y TERMINAR CADA TAREA)	ALCALDÍA
	(ALTERNATIVAS DE MEJORA)	(MEJORAS/TAREAS A IMPLEMENTAR)	(RESPONSABLE DE CADA TAREA)		EVIDENCIAS
		Actualizar el reporte de Registro Nacional de Bases de Datos	Subsecretario de Sistemas de Información	01-feb-2026 - 11-dic-2026	(1) Registro actualizados en plataforma RNBD
	Dar continuidad a la implementación de las políticas específicas de seguridad de la información.	Formular y aplicar matriz de seguimiento de implementación de política específicas de seguridad de la información	Subsecretario de Sistemas de Información	01-feb-2026 - 11-dic-2026	(1) matriz de seguimiento de implementación de políticas específicas de seguridad de la información formulada

Fuente: Alcaldía de Pasto.

## 8 ANÁLISIS PRESUPUESTAL

Proyecto	2026
Contratación servicio en la nube almacenamiento	\$90.000.000
Contratación licenciamiento de software antivirus	\$50.000.000
Contratación licenciamiento de software ofimático	\$70.000.000
Contratación licenciamiento de Windows 11	\$200.000.000

Nº Actividad	Estrategia / Eje	Actividad de Gestión	Producto	Evidencia
1	Liderazgo de seguridad de la información	Continuar con la política general y específicas de seguridad de la información.	Actualizar las políticas de seguridad y privacidad de la información	1 acto administrativo de actualización del manual de políticas de seguridad de la información
2	Liderazgo de seguridad de la información	Continuar con la política de protección de datos personales.	Actualizar la política de protección de datos personales	1 acto administrativo de actualización de la política de protección de datos personales
3	Gestión de riesgos	Continuar con la metodología de gestión de riesgos de seguridad de la información.	Implementar el Plan de tratamiento de riesgos de seguridad de la información	1 plan de tratamiento de riesgos de seguridad de la información formulado que incluya al menos 10 procesos del sistema de gestión de calidad
4	Concientización	Continuar con la política general de seguridad de la información.	Crear un espacio de seguridad y privacidad de la información actualizado en portal web interno	1 espacio de seguridad y privacidad de la información actualizado en portal web interno
5	Implementación de controles	Continuar con la metodología de gestión de riesgos de seguridad de la información.	Actualizar matriz autodiagnóstico MSPI	1 matriz autodiagnóstico MSPI actualizada
6	Implementación de controles	Continuar con la política de protección de datos personales.	Realizar intervenciones para la aplicación de la política de protección de datos personales Actualizar el reporte de Registro Nacional de Bases de Datos	Al menos 10 intervenciones de aplicación de la política de protección de datos personales Registros actualizados en plataforma RNBD
8	Implementación de controles	Continuar con las políticas específicas de seguridad de la información.	Formular y aplicar matriz de seguimiento de implementación de política específicas de seguridad de la información	1 matriz de seguimiento de implementación de políticas específicas de seguridad de la información formulada
9	Gestión de incidentes	Continuar con las políticas específicas de seguridad de la información.	Formular procedimiento de gestión de incidentes de seguridad de la información	1 procedimiento de gestión de incidentes de seguridad de la información formulado