



ALCALDÍA
DE PASTO

**Política
Seguridad Digital**





ALCALDÍA
DE PASTO

Fecha	Enero de 2025		
Resumen	Este documento corresponde al plan de acción de la política de seguridad digital en el modelo integrado de planeación y gestión.		
Palabras clave	Seguridad, Seguridad Digital, Hardware, Software		
Formato	PDF	Versión	001
Participantes	Ing. EDUARDO ANDRÉS HERNÁNDEZ ZAMBRANO Contratista		
Aprobó	Lic. DARIO FERNANDO ALFARO FIGUEROA Subsecretario de Sistemas de Información		

CONTROL DE CAMBIOS

No. REVISIÓN	DESCRIPCIÓN DE LA MODIFICACIÓN	FECHA DE APROBACIÓN	VERSIÓN ACTUALIZADA
1	Se formula plan de acción para la vigencia 2025	Ene-2025	1

APROBACIÓN COMITÉ MIPG

NO. DE ACTA	FECHA



ALCALDÍA
DE PASTO

CONTENIDO

Pág.

1	1
2	2
3	4
4	6
4.1	6
5	7
6	8
7	9
8	10
9	11



ALCALDÍA
DE PASTO

1 INTRODUCCIÓN

En la actualidad, la transformación digital y el uso intensivo de tecnologías de la información y las comunicaciones (TIC) han incrementado la importancia de proteger los activos digitales de las organizaciones. La seguridad digital no solo es un requisito técnico, sino también un pilar fundamental para garantizar la continuidad operativa, la protección de la información y la confianza de los ciudadanos en los servicios ofrecidos.

Conscientes de los riesgos y amenazas que enfrentan las entidades públicas, este Plan de Acción de Seguridad Digital tiene como objetivo establecer un conjunto, actividades orientadas a fortalecer la capacidad de la organización para prevenir, detectar, mitigar y responder a incidentes de seguridad.

El presente documento se encuentra alineado con los requerimientos del DAFP en cuanto a la política de seguridad digital del modelo integrado de planeación y gestión.



ALCALDÍA
DE PASTO

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.
- 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.



3 DEFINICIONES

- 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 institución, (materializar el riesgo).
- Control o Medida: acciones o mecanismos definidos para prevenir o reducir el impacto de los eventos que ponen en riesgo, la adecuada ejecución de las actividades y tareas requeridas para el logro de objetivos de los procesos de una entidad.
- Encargado del Tratamiento de Datos: persona natural o jurídica, pública o privada, que por sí misma o en asocio con otros, realice el Tratamiento de datos personales por cuenta del responsable del Tratamiento. (Ley 1581 de 2012, art.3)
- Gestión de incidentes de seguridad de la información: procesos para detectar, reportar, evaluar, responder, tratar y aprender de los incidentes de seguridad de la información. (NTC/ISO:27000)
- Impacto: son las consecuencias que genera un riesgo una vez se materialice.
- Información Clasificada: es aquella información que estando en poder o custodia de un sujeto, pertenece al ámbito propio, particular y privado o semiprivado de una persona natural o jurídica, por lo que su acceso podrá ser negado o exceptuado de manera motivada y por escrito, siempre que se trate de las circunstancias legítimas y necesarias, y los derechos particulares o privados estipulados en el artículo 18 de la Ley 1712 de 2014, y su acceso pudiere causar un daño a ciertos derechos, contemplados en la misma ley.
- Información Reservada: es aquella información que estando en poder o custodia de un sujeto obligado en su calidad de tal, es exceptuada de acceso a la ciudadanía por daño a intereses públicos y bajo cumplimiento de la totalidad de los requisitos consagrados en el artículo 19 de la Ley 1712 de 2014. (Ley 1712 de 2014, art 6). □Integridad: garantía de la exactitud y completitud de la información de la información y los métodos de su procesamiento.
- Información: se refiere a toda comunicación o representación de conocimiento como datos, en cualquier forma, con inclusión de formas textuales, numéricas, gráficas, cartográficas, narrativas o audiovisuales, y en cualquier medio, ya sea magnético, en papel, en pantallas de computadoras, audiovisual u otro.
- Plan de continuidad del negocio: plan orientado a permitir la continuación de las principales funciones misionales o del negocio en el caso de un evento imprevisto que las ponga en peligro. (ISO/IEC 27000).
- Plan de tratamiento de riesgos: documento que define las acciones para gestionar los riesgos de seguridad de la información inaceptables e implantar los controles necesarios para proteger la misma. (ISO/IEC 27000).
- Privacidad: en el contexto de este documento, por privacidad se entiende el derecho que tienen todos los titulares de la información en relación con la información que involucre datos personales y la información clasificada que estos hayan entregado o esté en poder de la entidad en el marco de las funciones que a ella le compete realizar y que generan en las entidades



destinatarias del Manual de GEL, hoy gobierno digital, la correlativa obligación de proteger dicha información en observancia del marco legal vigente.

- Probabilidad: es la posibilidad de que la amenaza aproveche la vulnerabilidad para materializar el riesgo.
- Riesgo: es un escenario bajo el cual una amenaza puede explotar una vulnerabilidad generando un impacto negativo al negocio evitando cumplir con sus objetivos.
- Vulnerabilidad: es una falencia o debilidad que puede estar presente en la tecnología, las personas o en las políticas y procedimientos.



4 OBJETIVO GENERAL

Avanzar en la implementación de la política de seguridad digital liderada por MINTIC acorde a la normatividad vigente.

4.1 Objetivos Específicos

- Continuar con la implementación de lineamientos para copias de seguridad de información digital.
- Continuar con la instalación y uso del software antivirus.



ALCALDÍA
DE PASTO

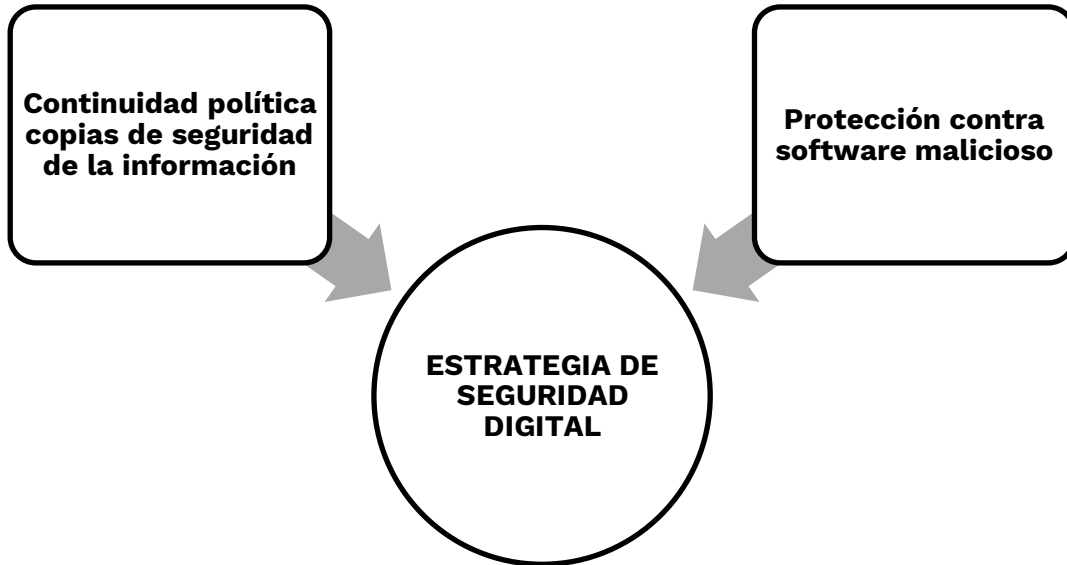
5 ALCANCE

Este plan aplica para la Subsecretaría de Sistemas de Información de la Alcaldía de Pasto y las demás dependencias involucradas en las actividades a desarrollar en el mismo.



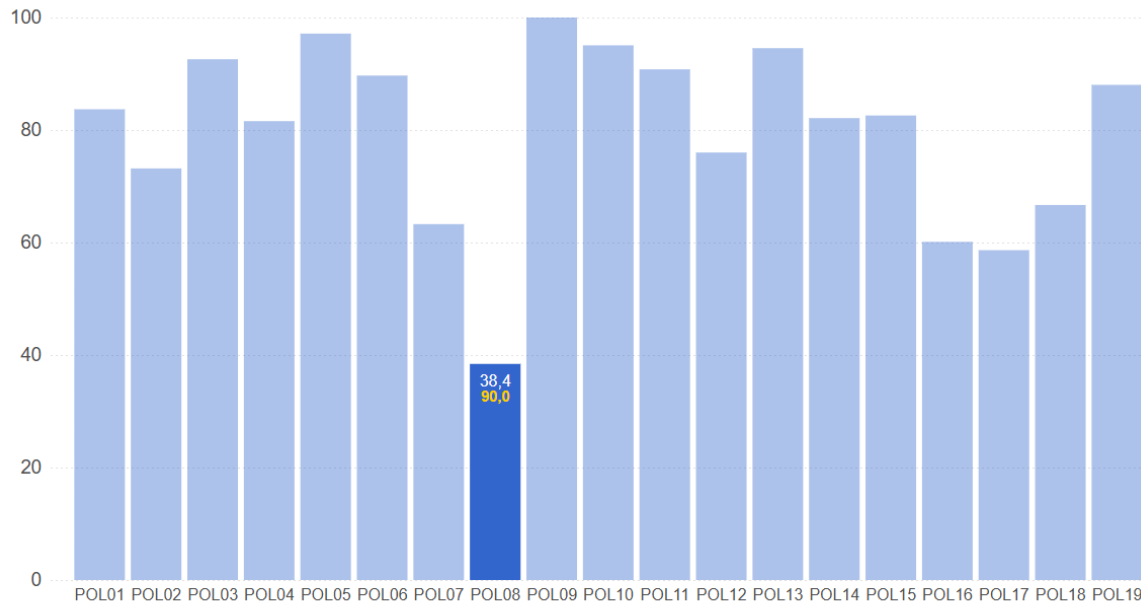
6 ESTRATEGIA DE SEGURIDAD DIGITAL

La estrategia de seguridad digital en la Alcaldía de Pasto, para la vigencia 2025 se fundamenta en las siguientes estrategias:



7 ANTECEDENTES Y RESULTADOS VIGENCIA 2023

III. Índices de las políticas de gestión y desempeño



Nota 1: La etiqueta de valores en amarillo, en cada columna, indica el valor máximo obtenido en la política específica consultada.

Nota 2: Con el fin de garantizar la calidad de los datos reportados, los líderes de política validaron la información reportada para una muestra de entidades; como resultado se identificaron algunas sobre las cuales se hace necesario adelantar una revisión más detallada a fin de confirmar los puntajes finales obtenidos.

Políticas

- POL01: Gestión estratégica del talento humano
- POL02: Integridad
- POL03: Planeación institucional
- POL04: Gestión presupuestal y eficiencia del gasto público
- POL05: Compras y contratación pública
- POL06: Fortalecimiento organizacional y simplificación de procesos
- POL07: Gobierno digital
- POL08: Seguridad digital**
- POL09: Defensa jurídica
- POL10: Mejora normativa
- POL11: Servicio al ciudadano
- POL12: Racionalización de trámites
- POL13: Participación ciudadana en la gestión pública
- POL14: Seguimiento y evaluación del desempeño institucional
- POL15: Transparencia, acceso a la información y lucha contra la corrupción
- POL16: Gestión documental
- POL17: Gestión información estadística
- POL18: Gestión del conocimiento
- POL19: Control interno



Fuente: <https://www1.funcionpublica.gov.co/web/mipg/resultados-medicion>

8 MATRIZ ESTRATEGIA DE SEGURIDAD DIGITAL

Estrategia / Eje	Objetivo específico asociado	Producto esperado	Meta	Fecha terminación	Responsable
Copias de seguridad de la información	Continuar con la implementación de lineamientos para copias de seguridad de información digital	Socializar lineamientos de copias de seguridad de sistemas de información	1 socialización realizada de lineamientos de copias de seguridad	31-jul-2025	Subsecretario de SSI
Copias de seguridad de la información	Continuar con la implementación de lineamientos para copias de seguridad de información digital	Realizar seguimiento a generación de copias de seguridad de sistemas de información	1 seguimiento realizado a generación de copias de seguridad	31-jul-2025	Subsecretario de SSI
Copias de seguridad de la información	Continuar con la implementación de lineamientos para copias de seguridad de información digital	Realizar prueba de restauración de copias de seguridad de forma aleatoria a un sistema de información	1 prueba de restauración de copia de seguridad realizada	30-dic-2025	Subsecretario de SSI
Copias de seguridad de la información	Continuar con la instalación y uso del software antivirus	Realizar monitoreo del uso del software antivirus gestionado desde la Subsecretaría de Sistemas de Información	1 informe de monitoreo de uso del software antivirus	31-jul-2025	Subsecretario de SSI

9 MATRIZ OPERATIVA

Acción de mejora a realizar	Tareas para cumplir la acción	Responsable de cada tarea	Fecha de inicio y fecha fin	Evidencias de ejecución de actividades	Evaluación de la eficacia de las acciones implementadas
Formular y ejecutar la matriz estratégica de seguridad digital de la Alcaldía de Pasto para la vigencia 2025.	P: Formulación matriz estratégica de seguridad digital para la vigencia 2025.	Subsecretario de Sistemas de Información	07-ene-2025 a 30-dic-2025	Matriz estratégica de seguridad digital formulada	Número de matrices estratégicas de seguridad digital de la información formuladas
	H: Ejecutar al menos un 95% de la matriz estratégica de seguridad digital para la vigencia 2025.	Subsecretario de Sistemas de Información	01-feb-2025 a 30-dic-2025	Registros de seguimiento a la ejecución de la matriz estratégica de seguridad digital	Número de actividades realizadas en la matriz estratégica de seguridad digital/ Total de actividades programadas
	V: Realizar verificaciones trimestrales al avance de la ejecución de la matriz estratégica de seguridad digital para la vigencia 2025.	Subsecretario de Sistemas de Información	04-abr-2025 a 30-dic-2025	Registros de seguimiento a la ejecución de la matriz estratégica de seguridad digital	Número de verificaciones trimestrales realizadas
	A: Requerir ajustes o acciones correctivas a las actividades programadas en la matriz estratégica de seguridad digital 2025 que presenten desviaciones significativas.	Subsecretario de Sistemas de Información	04-abr-2025 a 30-dic-2025	Ajustes realizados o acciones correctivas a la matriz estratégica de seguridad digital si hubiere lugar	Número de ajustes o acciones correctivas (Este valor puede ser igual a cero)

