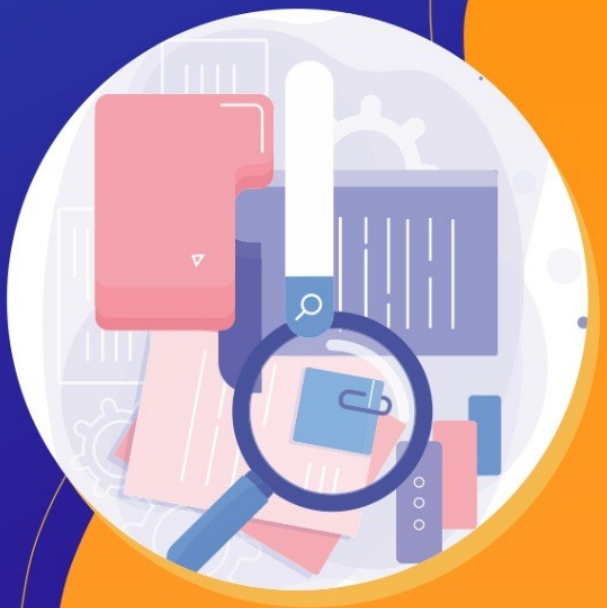
Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información



PASTO
LA GRAN CAPITAL
ALCALDÍA MUNICIPAL

ALCALDÍA DE PASTO

Fecha	**Enero de 2023**		
Resumen	Este documento corresponde al Plan Estratégico de Tecnologías de la Información y las Comunicaciones de la Alcaldía de Pasto – Nariño, se ha elaborado basado en el documento tipo del MINTIC denominado PETI Plus, cumpliendo con los lineamientos establecidos por esta entidad.		
Palabras clave	Plan, Tecnologías de la Información, Información, Datos, Sistemas, Infraestructura de TI, Servicios de TI, Gestión de Ti		
Formato	PDF	Versión	005
Aprobado por acta Comité MIPG No.			
Participantes	Ing. EDUARDO ANDRÉS HERNÁNDEZ ZAMBRANO **Contratista**		
	ANA MILENA RUALES BASANTE **Contratista**		
Aprobó	Ing. EDGAR EDUARDO ERAZO SEPÚLVEDA **Subsecretario de Sistemas de Información**		

CONTROL DE CAMBIOS

No. REVISIÓN	DESCRIPCIÓN DE LA MODIFICACIÓN	FECHA DE APROBACIÓN	VERSIÓN ACTUALIZADA
1	Se realizan ajustes para la vigencia 2019	Ene-2019	1
2	Se realizan ajustes para la vigencia 2020	Ene-2020	2
3	Se realizan ajustes para la vigencia 2021	Ene-2021	3
4	Se realiza ajustes para la vigencia 2022	Ene-2022	4

APROBACIÓN COMITÉ MIPG

NO. DE ACTA	FECHA
001	Enero-2023

ALCALDÍA DE PASTO

CONTENIDO

Pág.

1 INTRODUCCIÓN

Para la Alcaldía de Pasto, la seguridad y privacidad de la información, es un tema prioritario que debe ser gestionado conforme a las mejores prácticas de seguridad de la información y de acuerdo con la política de gobierno digital.

Para ello, la entidad ha decidido implementar el modelo de seguridad y privacidad de la información (MSPI), propuesto por el MINTIC y siguiendo la metodología de gestión de riesgos establecida por el DAFP, que involucra los riesgos de seguridad de la información. Con ello se espera que la entidad de manera incremental logre proteger la confidencialidad, integridad y disponibilidad de sus activos de información, además de la operatividad de la infraestructura tecnológica, permitiendo que los diferentes procesos de la entidad continúen su operación, en especial aquellos procesos misionales que trabajan de la mano de la comunidad.

2 MARCO NORMATIVO

- Constitución Política de Colombia. Artículo 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 (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 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 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 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 la 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.

3 GLOSARIO

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 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

Establecer las actividades que se deben desarrollar para reducir la probabilidad de la materialización de los riesgos de seguridad de la información, de la mano del Modelo de Seguridad y Privacidad de la Información propuesto por el MINTIC, la política de seguridad de la información, la política de protección de datos personales y la metodología de gestión de riesgos propuesta por el Departamento Administrativo de la Función Pública.

4.1 Objetivos Específicos

- Adoptar el modelo de seguridad de la información propuesto por el MINTIC.
- Adoptar la metodología de gestión de riesgos propuesta por el Departamento Administrativo de la Función Pública en lo que concierne a riesgos de seguridad y privacidad de la información.
- Fortalecer el uso y apropiación de la metodología de gestión de riesgos en los procesos de la entidad.

4.2 Alcance

El plan de tratamiento de riesgos aplica para todos los procesos del sistema de gestión de calidad de la entidad.

5 MATRIZ OPERATIVA

Actividad	Producto	Meta	Responsables	Fecha Inicio	Fecha Fin
Sensibilización de la metodología de Riesgos de seguridad de la Información	Presentación de la metodología de Riesgos de seguridad de la Información socializada, listados de asistencia y registro fotográfico	Una (1) socialización con equipo de trabajo de seguridad de la información	Subsecretario de Sistemas de Información	febrero-2023	abril-2023
Asesorar a los procesos para la aplicación de la metodología de gestión de riesgos se seguridad de la información	Cronograma de asesoría a procesos sobre aplicación de la metodología de gestión de riesgos de seguridad de la información	Veintidós (22) procesos del SGC asesorados en la metodología de gestión de riesgos de seguridad de la información	Subsecretario de Sistemas de Información, líderes de proceso	abril-2023	octubre-2023
Apoyar a los procesos en la identificación de activos de información	Formato de identificación de activos de información GTI-F-028 diligenciado	Al menos 5 procesos diligencian el formato GTI-F-028 en su aparte de identificación de activos	Subsecretario de Sistemas de Información, líderes de proceso	abril-2023	octubre-2023
Apoyar a los procesos en el establecimiento de la criticidad de los activos de información	Formato de identificación de activos de información GTI-F-028 diligenciado	Al menos 5 procesos diligencian el formato GTI-F-028 en su aparte de establecimiento de criticidad	Subsecretario de Sistemas de Información, líderes de proceso	abril-2023	octubre-2023
Realizar seguimiento a aplicación de metodología de gestión de riesgos en los procesos de la entidad	Matriz de riesgos institucional actualizada con riesgos de seguridad de la información	Al menos 5 procesos diligencian la matriz de riesgos incluyendo riesgos de seguridad de la información	Subsecretario de Sistemas de Información, líderes de proceso	octubre-2023	diciembre-2023

Fuente: Alcaldía de Pasto.