1. ALCANCE

Esta política aplica a toda la entidad, sus servidores públicos de planta, contratistas y terceros de la ALCALDÍA DE PASTO y la ciudadanía en general que tenga contacto con la entidad.

2. DEFINICIONES

- ACTIVO DE INFORMACIÓN: En relación con la privacidad de la información, se refiere al activo que contiene información pública que el sujeto obligado genere, obtenga, adquiera, transforme o controle en su calidad de tal.

- CONFIDENCIALIDAD: Propiedad que determina que la información sólo esté disponible y sea revelada a individuos, entidades o procesos autorizados.

- DISPONIBILIDAD: Propiedad de que la información sea accesible y utilizable por solicitud de una entidad autorizada, cuando ésta así lo requiera.

- INFORMACIÓN: Datos relacionados que tienen significado para la entidad. La información es un activo que, como otros activos importantes para la entidad, es esencial para las actividades de la entidad y, en consecuencia, necesita una protección adecuada. La definición dada por la ley 1712 del 2014, se refiere a un conjunto organizado de datos contenido en cualquier documento que los sujetos obligados generen, obtengan, adquieran, transformen o controlen.
- INTEGRIDAD: Propiedad de salvaguardar la exactitud y estado completo de los activos.

- POLÍTICA: Declaración de alto nivel que describe la posición de la entidad sobre un tema específico.

- SEGURIDAD DE LA INFORMACIÓN: Preservación de la confidencialidad, integridad, y disponibilidad de la información.

- SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN (SGSI): Conjunto de elementos interrelacionados o interactuantes (estructura organizativa, políticas, planificación de actividades, responsabilidades, procesos, procedimientos y recursos) que utiliza una organización para establecer una política y unos objetivos de seguridad de la información y alcanzar dichos objetivos, basándose en un enfoque de gestión y de mejora continua.

3. NIVELES DE APLICACIÓN DE LA POLÍTICA

1. PRIMER NIVEL: Definidas en el presente documento.
2. SEGUNDO NIVEL: Definidas en un documento cuyo nombre será: Manual de políticas de Seguridad de la Información de segundo nivel, este documento deberá ser formalizado en el sistema de gestión de calidad, en el proceso de Gestión de Tecnologías de la Información.

4. POLÍTICA

La ALCALDÍA DE PASTO, entendiendo la importancia de una adecuada gestión de la información, se ha comprometido con la implementación de un sistema de gestión de seguridad de la información buscando establecer un marco de confianza en el ejercicio de sus deberes con el Estado y los ciudadanos, todo enmarcado en el estricto cumplimiento de las leyes y en concordancia con la misión y visión de la entidad.

Para la ALCALDÍA DE PASTO, la protección de la información busca la disminución del impacto generado sobre sus activos, por los riesgos identificados de manera sistemática con objeto de mantener un nivel de exposición que permita responder por la integridad, confidencialidad y la disponibilidad de la misma, acorde con las necesidades de los diferentes grupos de interés identificados.

De acuerdo con lo anterior, esta política aplica a la Entidad según como se defina en el alcance, sus funcionarios, terceros, aprendices, practicantes, proveedores y la ciudadanía en general, teniendo en cuenta que los principios sobre los que se basa el desarrollo de las acciones o toma de decisiones alrededor del SGSI estarán determinados por las siguientes premisas:

- Minimizar el riesgo en las funciones más importantes de la entidad.
- Cumplir con los principios de seguridad de la información.
- Cumplir con los principios de la función administrativa.
- Mantener la confianza de sus clientes, socios y empleados.
- Apoyar la innovación tecnológica.
- Proteger los activos tecnológicos.
- Establecer las políticas, procedimientos e instructivos en materia de seguridad de la información.
- Fortalecer la cultura de seguridad de la información en los funcionarios, terceros, aprendices, practicantes y clientes de la ALCALDÍA DE PASTO.
- Garantizar la continuidad del negocio frente a incidentes.
- La ALCALCÍA DE PASTO ha decidido definir, implementar, operar y mejorar de forma continua un Sistema de Gestión de Seguridad de la Información, soportado en

lineamientos claros alineados a las necesidades de la entidad, y a los requerimientos regulatorios.

A continuación, se establecen las 12 políticas de seguridad que soportan el Sistema de Seguridad y Privacidad de la Información de la ALCALDÍA DE PASTO:

1. La ALCALDÍA DE PASTO ha decidido definir, implementar, operar y mejorar de forma continua un Modelo de Seguridad y Privacidad de la Información, soportado en lineamientos claros alineados a las necesidades de la entidad, y a los requerimientos regulatorios que le aplican a su naturaleza.
2. Las responsabilidades frente a la seguridad de la información serán definidas, compartidas, publicadas y aceptadas por cada uno de los empleados, contratistas o terceros.
3. La ALCALDÍA DE PASTO protegerá la información generada, procesada o resguardada por los procesos y activos de información que hacen parte de los mismos.
4. La ALCALDÍA DE PASTO protegerá la información creada, procesada, transmitida o resguardada por sus procesos, con el fin de minimizar impactos financieros, operativos o legales debido a un uso incorrecto de esta. Para ello es fundamental la aplicación de controles de acuerdo con la clasificación de la información de su propiedad o en custodia.
5. La ALCALDÍA DE PASTO protegerá su información de las amenazas originadas por parte del personal.
6. La ALCALDÍA DE PASTO protegerá las instalaciones de procesamiento y la infraestructura tecnológica que soporta sus procesos críticos.
7. La ALCALDÍA DE PASTO controlará la operación de sus procesos garantizando la seguridad de los recursos tecnológicos y las redes de datos.
8. La ALCALDÍA DE PASTO implementará control de acceso a la información, sistemas y recursos de red.
9. La ALCALDÍA DE PASTO garantizará que la seguridad sea parte integral del ciclo de vida de los sistemas de información.
10. La ALCALDÍA DE PASTO garantizará a través de una adecuada gestión de los eventos de seguridad y las debilidades asociadas con los sistemas de información una mejora efectiva de su modelo de seguridad.
11. La ALCALDÍA DE PASTO garantizará la disponibilidad de sus procesos y la continuidad de su operación basado en el impacto que pueden generar los eventos.
12. La ALCALDÍA DE PASTO garantizará el cumplimiento de las obligaciones legales, regulatorias y contractuales establecidas.

El incumplimiento a la política general de Seguridad y Privacidad de la Información o de las políticas de seguridad de la información de segundo nivel, traerá consigo, las consecuencias legales que apliquen a la normativa de la Entidad, incluyendo lo

establecido en las normas que competen al gobierno nacional y territorial en cuanto a seguridad y privacidad de la Información se refiere.

5. ROLES Y RESPONSABILIDADES

Considerando que la seguridad de la información es un tema transversal a la entidad, y que se hace necesario la participación de todas las áreas, se establecen los roles y responsabilidades del sistema de seguridad de la información, los cuales deben incluir responsables para:

5.1. Responsable de Seguridad de la Información para la entidad

El Responsable de Seguridad de la información será el líder del sistema y tendrá las siguientes responsabilidades:

- Aplicar conocimientos, habilidades, herramientas, y técnicas a las actividades propias de la seguridad de la información, de manera que cumpla o exceda las necesidades y expectativas de los interesados en el mismo.

- Identificar la brecha entre el Modelo de seguridad y privacidad de la información y la situación de la entidad.

- Generar el cronograma de la implementación del Modelo de Seguridad y privacidad de la información.

- Planear, implementar y hacer seguimiento a las tareas, fechas, costos y plan de trabajo de los objetivos específicos del cronograma definido.

- Gestionar el equipo de trabajo de seguridad de la información, definiendo roles, responsabilidades, entregables y tiempos.

- Coordinar las actividades diarias del equipo y proporcionar apoyo administrativo.

- Encarrilar las actividades del sistema hacia el cumplimiento de la implementación del Modelo de Seguridad y privacidad de la Información para la entidad.

- Realizar un seguimiento permanente a la ejecución de los planes de trabajo, monitoreando los riesgos del sistema para darle solución oportuna y escalar al Comité de seguridad en caso de ser necesario.

- Monitorear el estado del sistema de seguridad de la información en términos de calidad de los productos, tiempo y los costos.

- Trabajar de manera integrada con el grupo o áreas asignadas.

- Asegurar la calidad de los entregables y del sistema de seguridad de la información en su totalidad.

- Velar por el mantenimiento de la documentación del sistema de seguridad de la información, su custodia y protección.

- Contribuir al enriquecimiento del esquema de gestión del conocimiento sobre el sistema de seguridad de la información en cuanto a la documentación de las lecciones aprendidas.

- Liderar la programación de reuniones de seguimiento y velar por la actualización de los indicadores de gestión del sistema de seguridad de la información.

- Proponer la actualización de las políticas de seguridad de la información.

5.2. Equipo de trabajo

Teniendo en cuenta la naturaleza de la entidad, debe conformarse un equipo para el desarrollo del sistema de seguridad de la información al cual deben pertenecer miembros directivos, con el propósito de asegurar que toda la información más relevante de la entidad esté disponible oportunamente. De esta forma se busca asegurar que sea una iniciativa de carácter transversal a la entidad, y que no dependa exclusivamente de la oficina o área de TI, el equipo estará formado así:

- Al menos un representante de la Subsecretaría de Sistemas de Información.
- Al menos un representante de la Oficina de Control Interno.
- Al menos un representante de la Oficina de Planeación de Gestión Institucional.
- Al menos un representante del Sistema de Gestión de Calidad.
- Al menos un representante de la Oficina de Asesoría Jurídica.
- Al menos un representante de la Subsecretaría de Talento Humano.
- Al menos un representante de la Secretaría General.
- Al menos un representante del Departamento Administrativo de Contratación Pública.
- Representantes de las áreas que puedan apoyar en la implementación del sistema de seguridad de la información.

Responsabilidades del equipo del proyecto:

- Apoyar al líder de proyecto al interior de la entidad.
- Oficiar como consultores de primer nivel en cuanto a las dudas técnicas y de procedimiento que se puedan suscitar en el desarrollo del proyecto.

- Ayudar al líder de proyecto designado, en la gestión de proveedores de tecnología e infraestructura.
- Asistir a las reuniones de seguimiento o de cualquier otra naturaleza planeadas por el líder de proyecto.
- Las que considere el líder del proyecto o la instancia establecida como comité de seguridad de la información.
- Revisar y aprobar las políticas de seguridad de la información de segundo nivel.

5.3. Comité de Seguridad

Las funciones de este comité serán asumidas por el Comité Institucional de Gestión y Desempeño bajo las disposiciones establecidas para su funcionamiento y deberá asegurar que exista una dirección y apoyo gerencial para soportar la administración y desarrollo de iniciativas sobre seguridad de la información, a través de compromisos apropiados y uso de recursos adecuados en el organismo, así como de la formulación y mantenimiento de una política de seguridad de la información a través de todo el organismo, las temáticas a tratar en este comité son:

1. Revisar los diagnósticos del estado de la seguridad de la información en la Alcaldía de Pasto de la entidad.
2. Acompañar e impulsar el desarrollo de proyectos de seguridad.
3. Coordinar y dirigir acciones específicas que ayuden a proveer un ambiente seguro y establecer los recursos de información que sean consistentes con las metas y objetivos de la Alcaldía de Pasto.
4. Recomendar roles y responsabilidades específicos que se relacionen con la seguridad de la información.
5. Aprobar el uso de metodologías y procesos específicos para la seguridad de la información.
6. Participar en la formulación y evaluación de planes de acción para mitigar y/o eliminar riesgos.
7. Realizar revisiones periódicas del SGSI (por lo menos una vez al año) y según los resultados de esta revisión definir las acciones pertinentes.
8. Promover la difusión y sensibilización de la seguridad de la información dentro de la entidad.
9. Poner en conocimiento de la entidad, los documentos generados al interior del comité que impacten de manera transversal a la misma.
10. Revisar y aprobar la política de primer nivel de seguridad de la información.

6. NORMATIVIDAD

Norma	Concepto

Decreto 1078 de 2015	Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones.
Ley 1712 de 2014	Ley de transparencia y acceso a la información pública.
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.

7. CONTROL DE CAMBIOS

No. REVISIÓN	DESCRIPCIÓN DE LA MODIFICACIÓN	FECHA DE APROBACIÓN	VERSIÓN ACTUALIZADA

8. APROBACIÓN COMITÉ INSTITUCIONAL GESTIÓN Y DESEMPEÑO

No	No. Acta	Fecha
1	0009	05 de Julio de 2019

Revisó: JONNATHAN HUERTAS SALAS
Subsecretario de Sistemas de Información

Proyectó: EDUARDO HERNÁNDEZ ZAMBRANO
Técnico Administrativo