

 <p>ALCALDÍA DE SANTIAGO DE CALI</p> <p>GESTION TECNOLÓGICA Y DE LA INFORMACION ADMINISTRACIÓN DE TECNOLOGÍAS DE INFORMACIÓN Y COMUNICACIÓN</p>	<p>SISTEMAS DE GESTIÓN Y CONTROL INTEGRADOS (SISTEDA, SGC y MECI)</p> <p>POLITICA DE SEGURIDAD DE LA INFORMACION</p>	MAGT04.04	
		VERSIÓN	2
		FECHA DE ENTRADA EN VIGENCIA	22/ago/2014

1. INTRODUCCIÓN

La Administración Central Municipal, adopto la Norma Técnica de Calidad de la Gestión Pública NTCGP-1000-2009, que conforme a la ley 872 de 2003, en el Artículo 3º., frente a la características del Sistema, este se desarrollará de manera integral, intrínseca, confiable, económica, técnica y particular en cada organización, y será de obligatorio cumplimiento por parte de todos los Servidores Públicos y/o Contratistas de la entidad y así garantizar en cada una de sus actuaciones la satisfacción de las necesidades de los usuarios, por lo cual se adoptaran otros Sistemas de Gestión, complementarios al quehacer de la entidad.

En la actualidad la información se ha reconocido como un activo valioso y a medida que los sistemas de información apoyan cada vez más los procesos de misión se requiere contar con estrategias de alto nivel que permitan el control y administración efectiva de los datos.

Consciente de sus necesidades actuales, la Administración Central del Municipio de Santiago de Cali implementará el Sistema de Gestión de Seguridad de la Información – SGSI, según lo indica la directriz presidencial de Gobierno en Línea (Manual 3.1 Componente 1 elementos transversales, actividad 4), como una herramienta de gestión que permite identificar y minimizar los riesgos a los cuales se expone la información, ayuda a la reducción de costos operativos y financieros, establece una cultura de seguridad y garantiza el cumplimiento de los requerimientos legales, contractuales, regulatorios vigentes.

La Administración Central del Municipio de Santiago de Cali, los sistemas y red de información enfrentan amenazas de seguridad que incluyen, entre muchas otras: el fraude por computadora, espionaje, sabotaje, vandalismo, fuego. Las posibilidades de daño y pérdida de información por causa de código malicioso, mal uso o ataques de denegación de servicio se hacen cada vez más comunes. Por esta razón se debe definir las políticas que permitan proteger el Sistema de Información.

La Política de Seguridad de la Información, es la declaración general que representa la posición de la Administración Central de Santiago de Cali con respecto a la protección de los activos de información (los Servidores Públicos y/o Contratistas, la información, los procesos, las tecnologías de información incluido el hardware y el software), a la

 <p>ALCALDÍA DE SANTIAGO DE CALI</p> <p>GESTION TECNOLÓGICA Y DE LA INFORMACION ADMINISTRACIÓN DE TECNOLOGÍAS DE INFORMACIÓN Y COMUNICACIÓN</p>	<p>SISTEMAS DE GESTIÓN Y CONTROL INTEGRADOS (SISTEDA, SGC y MECI)</p> <p>POLITICA DE SEGURIDAD DE LA INFORMACION</p>	MAGT04.04	
		VERSIÓN	2
		FECHA DE ENTRADA EN VIGENCIA	22/ago/2014

implementación del Sistema de Gestión de Seguridad de la Información y al apoyo, generación y publicación de sus políticas, procedimientos e instructivos.

2. OBJETIVO

Establecer la política de seguridad de la información y proveer una guía respecto a la Seguridad de los Sistemas de Información de la Administración Central del Municipio de Santiago de Cali.

3. ALCANCE

La Política de Seguridad de la Información aplica para todos los usuario(a)s internos en todos los niveles jerárquicos y usuarios externos de la Administración Central del Municipio de Santiago de Cali.

4. POLITICA DE SEGURIDAD DE LA INFORMACION

En la Administración Central Municipal de Santiago de Cali, la información es un activo fundamental para la prestación de sus servicios y la toma de decisiones eficientes, razón por la cual existe un compromiso expreso de protección de sus propiedades más significativas como parte de una estrategia orientada a la administración de riesgos y la consolidación de una cultura de seguridad; la Ley 87 de 1993, establece en artículo 4°, literal i) Establecimiento de sistemas modernos de información que faciliten la gestión y el control; por lo tanto, surge el deber de proteger y salvaguardar esta información.

La Política de Seguridad de la información de la Administración Central del Municipio de Santiago de Cali, busca evitar que las amenazas latentes en el entorno, puedan acceder, manipular o deteriorar la información producida por los procesos de la organización y disminuir la posible pérdida de información.

 <p>ALCALDÍA DE SANTIAGO DE CALI</p> <p>GESTION TECNOLÓGICA Y DE LA INFORMACION ADMINISTRACIÓN DE TECNOLOGÍAS DE INFORMACIÓN Y COMUNICACIÓN</p>	<p>SISTEMAS DE GESTIÓN Y CONTROL INTEGRADOS (SISTEDA, SGC y MECI)</p> <p>POLITICA DE SEGURIDAD DE LA INFORMACION</p>	MAGT04.04	
		VERSIÓN	2
		FECHA DE ENTRADA EN VIGENCIA	22/ago/2014

Esta política será revisada con regularidad como parte del proceso de revisión estratégica, o cuando se identifiquen cambios en la Entidad, su estructura, sus objetivos o alguna condición que afecte la política, para asegurar que sigue siendo adecuada y ajustada a los requerimientos identificados.

La Administración Central del Municipio de Santiago de Cali, para el cumplimiento de su misión, visión, objetivo estratégico y acorde a sus valores corporativos, establece la función de Seguridad de la Información en la Entidad, con el objetivo de:

- Implementar el Sistema de Gestión de Seguridad de la Información.
- Cumplir con los principios de confidencialidad, integridad y disponibilidad de la información.
- Cumplir con los principios de la función administrativa.
- Establecer las políticas, procedimientos e instructivos en materia de Seguridad de la Información.
- Fortalecer la cultura de seguridad de la información en los servidores públicos, practicantes, y usuarios de la Administración Central Municipal de Santiago de Cali
- Garantizar la continuidad del negocio frente a incidentes de Seguridad de la Información.
- Minimizar el riesgo en las funciones de la entidad.
- Apoyar la innovación tecnológica.
- Proteger los activos de información y tecnológicos.
- Mantener la confianza de sus usuarios y Servidores Públicos y/o Contratistas.

A continuación se establecen las políticas de seguridad que soportan el SGSI (Sistema de Gestión de Seguridad de la Información) de la Administración Central del Municipio Santiago de Cali:

1. 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.
2. Las responsabilidades frente a la seguridad de la información son definidas, compartidas, publicadas y aceptadas por cada uno de los empleados, proveedores y terceros.

 <p>ALCALDÍA DE SANTIAGO DE CALI</p> <p>GESTION TECNOLÓGICA Y DE LA INFORMACION ADMINISTRACIÓN DE TECNOLOGÍAS DE INFORMACIÓN Y COMUNICACIÓN</p>	<p>SISTEMAS DE GESTIÓN Y CONTROL INTEGRADOS (SISTEDA, SGC y MECI)</p> <p>POLITICA DE SEGURIDAD DE LA INFORMACION</p>	MAGT04.04	
		VERSIÓN	2
		FECHA DE ENTRADA EN VIGENCIA	22/ago/2014

3. Proteger la información creada, procesada o resguardada por los procesos estratégicos, misionales, de apoyo y control de la Entidad, su infraestructura tecnológica y activos de información del riesgo que se genera de los accesos otorgados a terceros (ej.: proveedores o clientes), o como resultado de un servicio interno en outsourcing.
4. Proteger la información creada, procesada, transmitida o resguardada por todos sus macroprocesos, con el fin de minimizar impactos financieros, operativos o legales debido a un uso incorrecto de esta, aplicando controles de acuerdo con la clasificación de la información de su propiedad o en custodia.
5. Establecer mecanismos de protección de su información contra las amenazas originadas por parte de cualquier tipo de personas.
6. Proteger las instalaciones de procesamiento y la infraestructura tecnológica que soporta sus procesos críticos.
7. Controlar la operación de sus macroprocesos garantizando la seguridad de los recursos tecnológicos y las redes de datos.
8. Implementar controles de acceso a la información, sistemas y recursos de red.
9. Garantizar que la seguridad sea parte integral del ciclo de vida de los sistemas de información.
10. Garantizar 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. Garantizar la disponibilidad de sus macroprocesos y la continuidad de su operación basado en el impacto que pueden generar los eventos.
12. Garantizar el cumplimiento de las obligaciones legales, regulatorias y contractuales establecidas.
13. Definir e implantar controles para proteger la información contra violaciones de autenticidad, accesos no autorizados, la pérdida de integridad y que garanticen la

 <p>ALCALDÍA DE SANTIAGO DE CALI</p> <p>GESTION TECNOLÓGICA Y DE LA INFORMACION ADMINISTRACIÓN DE TECNOLOGÍAS DE INFORMACIÓN Y COMUNICACIÓN</p>	<p>SISTEMAS DE GESTIÓN Y CONTROL INTEGRADOS (SISTEDA, SGC y MECI)</p> <p>POLITICA DE SEGURIDAD DE LA INFORMACION</p>	MAGT04.04	
		VERSIÓN	2
		FECHA DE ENTRADA EN VIGENCIA	22/ago/2014

disponibilidad requerida por los clientes y usuarios de los servicios ofrecidos por la Entidad.

La política de seguridad de la información será complementada por procedimientos, normas y guías específicas para orientar su implementación.

Es responsabilidad del equipo de gobierno asegurar el cumplimiento de las políticas de seguridad de la información al interior de sus dependencias.

5. POLITICA DE ADMINISTRACION DE LA SEGURIDAD DE LA INFORMACION

- La evaluación de riesgos de seguridad para los Recursos Informáticos en producción se debe ejecutar al menos una vez cada dos años. Todas las mejoras, actualizaciones, conversiones y cambios relativos asociados con estos recursos deben ser precedidos por una evaluación del riesgo.
- Cualquier brecha de seguridad o sospecha en la mala utilización en los Sistemas de Información o los recursos informáticos de cualquier nivel (local o corporativo) deberá ser comunicada por el Servidor Público o Contratista que la detecta, en forma inmediata y confidencial al Líder de Gobierno en Línea.
- Los Servidores Públicos o Contratistas que realicen las labores de administración del recurso informático son responsables por la implementación, permanencia y administración de los controles sobre los Recursos Computacionales. La implementación debe ser consistente con las prácticas establecidas por la Asesoría de Informática y Telemática.
- El Líder de Gobierno en Línea divulgará las políticas, estándares y procedimientos en materia de seguridad de la información, además efectuará el seguimiento al cumplimiento de las políticas de seguridad y reportará al Alcalde o a quien el ejecutivo delegue.