PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

PERIODO DE VIGENCIA DEL PLAN

Del 1 de enero al 31 de diciembre de 2026

Personería
Santiago de Cali

Dirección Financiera y Administrativa

Personería de Santiago de Cali NIT
805.003.895 - 9
CAM, Torre Alcaldía Piso 13
PBX (2) 6617999
atencionalciudadano@personeriacali.gov.co

Plan de Seguridad y Privacidad de la Información 2025

El Plan de Seguridad y Privacidad de la Información está basado en los lineamientos presentados en laguía de seguridad y privacidad de información del Ministerio de las Tecnologías de la Información y las Comunicaciones MINTIC.

El Plan Institucional de Seguridad y Privacidad de la Información se encuentra articulado con las políticas contenidas en el Modelo Integrado de Planeación y Gestión MIPG: ***Transparencia, Acceso a la Información Pública y Lucha contra la Corrupción, Gobierno Digital y Seguridad Digital.***

Contenido

1. MARCO NORMATIVO

Ley 44 de 1993. Por la cual se modifica y adiciona la Ley 23/1982 y se modifica la Ley 29/1944

Ley 527/1999. 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.

Ley 594 de 2000. Se expide la Ley General de Archivos.

Ley 1266 de 2008. Se dictan las disposiciones generales del Habeas 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.

Ley 1221 del 2008. Por la cual se establecen normas para promover y regular el Teletrabajo.

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

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 TICS.

Ley 1474 de 2011. Orientadas a fortalecer los mecanismos de prevención, investigación y sanción de actos de corrupción.

CONPES 3701 de 2011. Lineamientos de Política para Ciberseguridad y Ciberdefensa.

Ley 1581 de 2012. Disposiciones generales para la protección de datos personales.
Decreto 0884 del 2012. Reglamenta parcialmente la Ley 1221/2008.

Ley 1712 de 2014. Ley de Transparencia y del Derecho de Acceso a la Información Pública Nacional.

Decreto 103 de 2015. Reglamenta parcialmente la Ley 1712/2014.

Decreto 1078 de 2015. Expide el Decreto Único Reglamentario del Sector de las TIC.

CONPES 3854 de 2016. Política Nacional de Seguridad Digital.

Decreto 728 de 2017. Adiciona el capítulo 2 al título 9 de la parte 2 del libro 2 del Decreto Único Reglamentario del sector TIC, Decreto 1078/2015, para fortalecer el modelo de Gobierno Digital.

Decreto 1499 de 2017 Modifica el Dec.1083/2015, Decreto Único Reglamentario del Sector Función Pública, en lo relacionado con el Sistema de Gestión establecido en el art 133 de la Ley 1753/2015.

Ley 1915 de 2018. Por la cual se modifica la Ley 23/1982.

Decreto 1008 del 2018. 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 Dec.1078/2015, Decreto Único Reglamentario del sector de las TIC.

Ley 1978 de 2019. Se moderniza el sector de las TIC. Dec. 2609/2012. Por el cual se reglamenta el Título V de la Ley 594/2000, parcialmente los artículos 58 y 59 de la Ley 1437/2011

Decreto 2106 de 2019. Se dictan normas para simplificar, suprimir y reformar trámites, procesos y procedimientos innecesarios existentes en la administración pública.

Decreto 620 de 2020. por el cual se subroga el título 17 de la parte 2 del libro 2 del Dec.1078/2015, para reglamentarse parcialmente los artículos 53, 54, 60, 61 y 64 de la Ley 1437/2011, los literales e), j) y literal a) del parágrafo 2 del art. 45 de la Ley 1753/2015, el numeral 3 del art.147 de la Ley 1955/2019, y el art.9° de Dec. 2106/2019, estableciendo los lineamientos generales en el uso y operación de los servicios ciudadanos digitales.

CONPES 3905 de 2020. Política Nacional de Confianza y Seguridad Digital.

2. ORIENTACIÓN ESTRATÉGICA DE LA PERSONERIA

MISIÓN

La Personería Distrital de Santiago de Cali, como Agente del Ministerio Público, representa a la sociedad, protege y defiende los derechos humanos y el interés público ejerce control y vigilancia administrativa ante la Administración Distrital, promueve la participación ciudadana y los mecanismos alternativos de acceso a la justicia, actuando siempre dentro del marco constitucional y legal, garantizando la diversidad y la inclusión de todos los grupos poblacionales.

VISIÓN

Para el año 2028, la Personería Distrital de Santiago de Cali, será un órgano de control moderno, generador de confianza y credibilidad, reconocido por la efectividad de sus actuaciones y presencia permanente en el territorio.

POLÍTICA DE CALIDAD

La Personería Distrital de Santiago de Cali, como Agente del Ministerio Público y Ente de Control y Vigilancia, está comprometida en la mejora continua de procesos modernos e innovadores, a través de un capital humano idóneo, dispuesto a atender oportunamente nuevas dinámicas sociales, generando mayor impacto de satisfacción en el territorio; todo fundamentado en un Sistema de Gestión de Calidad que satisfaga eficientemente las necesidades de los(as) usuarios(as) y partes interesadas.

VALORES

Las conductas dentro y fuera de la entidad de servidores y contratistas vinculados a la Personería Distrital de Santiago de Cali, se orientan por los valores y principios de acción contenidos en el Código de Integridad del Servicio Público Colombiano, fijado en la Ley 2016 del 27 de febrero de 2020 y cumplen un carácter esencial para el cabal cumplimiento de la misión, visión y objetivos institucionales, así:

- **Honestidad**
- **Respeto**
- **Compromiso**
- **Diligencia**
- **Justicia**
- **Empatía**

3. OBJETIVO GENERAL

Adoptar un Sistema de Gestión de Seguridad de la Información (SGSI) bajo los parámetros establecidos en la norma técnica ISO 27001: 2022, para desarrollar controles de seguridad completos, que logren proteger los activos y realizar un mejoramiento continuo en la gestión de la seguridad, la información y el uso adecuado de los recursos en la Personería de Santiago de Cali.

3.1 Objetivos Específicos

a. Establecer la Política de Seguridad de la Información conforme a las reglas, pautas y procedimientos adoptados en la Personería Distrital de Santiago de Cali, garantizando que todos los activos y recursos de tecnología de la información se utilicen y gestionen de manera que protejan su confidencialidad, integridad y disponibilidad

b. Identificar los riesgos de seguridad y privacidad de la información, para establecer mecanismos de protección de datos asegurando confiabilidad, integridad y disponibilidad de la información.

c. Realizar un diagnóstico de los activos de información para minimizar los riesgos.

d. Tener políticas y prácticas de seguridad que logren guiar el comportamiento de los funcionarios y contratistas de la entidad, sobre la información generada y procesada en la entidad.

Articulación con el PETI

Articulación con el Plan Estratégico de Tecnologías de la Información y las Comunicaciones (PETI)

El Plan de Seguridad y Privacidad de la Información de la Personería Distrital de Santiago de Cali se constituye como un componente estratégico del Plan Estratégico de Tecnologías de la Información y las Comunicaciones (PETI), aportando al cumplimiento de los objetivos institucionales de Gobierno Digital, Seguridad Digital, sostenibilidad tecnológica y continuidad del negocio.

Las acciones definidas en este plan fortalecen la gestión integral de riesgos tecnológicos, la protección de los activos de información y la confianza en los servicios digitales institucionales, en coherencia con el Modelo Integrado de Planeación y Gestión (MIPG).

4. ALCANCE

Establecer esquemas para la implementación del Sistema de Gestión de Seguridad de la Información SGSI, con el propósito de proteger la información de la Personería de Santiago de Cali y garantizar laseguridad de los datos, minimizar riesgos, accesos no autorizados y preservar los activos de información.

5. TÉRMINOS Y DEFINICIONES

Activo: Es un recurso que tiene un valor específico para la entidad y debe ser protegido.

Análisis de riesgo: Uso metódico de la información para identificar fuentes y para evaluar el riesgo.

Administración de Riesgos: Es el proceso de identificación, control y minimización o eliminación a un costo aceptable de los riesgos de seguridad que podrían afectar a la información.

Auditabilidad: Define que todos los eventos de un sistema deben poder ser registrados para su control posterior.

Autenticidad: Busca asegurar la validez de la información en tiempo, forma y distribución. Asimismo, se garantiza el origen de la información, validando el emisor para evitar suplantación de identidades.

Antivirus: Software diseñado para la detección, prevención y eliminación de programas y archivos maliciosos o dañinos en equipos de cómputo y dispositivos.

Ciberseguridad: Procedimientos y herramientas que se implementan para proteger la información que se genera a través de equipos de cómputo, servidores, dispositivos móviles, redes y sistemas electrónicos.

Confidencialidad: Propiedad de la información por la que se garantiza que está accesible únicamente a personal autorizado.

Confiabilidad de la información. Es decir, que la información generada sea adecuada para sustentar la toma de decisiones y la ejecución de las misiones y funciones.

Control de acceso: Significa garantizar que el acceso a los activos esté autorizado y restringido, según los requisitos comerciales y de seguridad.

Criptografía: El procedimiento de transmitir datos y mensajes cifrados.

Disponibilidad: El proceso de asegurar que la información sea accesible para usuarios autorizados cuando ellos lo requieran.

Evento de seguridad: Una situación previamente desconocida que pueda ser relevante para la seguridad.

Encriptación: Codificación de los datos para evitar que los usuarios no autorizados los modifiquen. Solo los usuarios con acceso a una contraseña pueden descifrar y utilizar los datos.

Hacking Ético: Actividades encaminadas a realizar pruebas en redes y encontrar vulnerabilidades, para luego reportarlas y que se tomen medidas para evitar daños y alterar los datos.

Evaluación de Riesgos: Se entiende a las amenazas y vulnerabilidades relativas a la información y a las instalaciones de procesamiento de la misma. La probabilidad de que ocurra y su potencial impacto en la operatoria de la Personería de Santiago de Cali.

Información: Se refiere a toda comunicación o representación de conocimiento como datos, en cualquier forma, con inclusión de formas textuales, numéricas, graficas cartográficas, narrativas o audiovisuales, y en cualquier medio, ya sea magnético, en papel, en pantallas de computadoras, audiovisual u otros.

Incidente de seguridad: Un incidente de seguridad es un evento adverso en un sistema de computadoras, que compromete la confidencialidad de la información. Puede ser causada mediante la explotación de alguna vulnerabilidad o un intento o amenazas de romper los mecanismos de seguridad existentes.

Ingeniería Social: Método utilizado por los atacantes para engañar a los usuarios, con el fin de instarlos a que realicen una acción que normalmente producirá consecuencias negativas como pérdida de la información o descarga de virus.

Integridad: Propiedad que busca mantener los datos libres de modificaciones no autorizadas y asegurar que los datos del sistema no hayan sido alterados ni cancelados por personas, entidades no autorizadas y que el contenido de los mensajes recibidos es el correcto.

MSPI: (Modelo de Seguridad y Privacidad de la Información) Actividades, acciones y procesos para proteger el acceso, uso y divulgación del acceso a la información.

Seguridad de la información: Preservación de la confidencialidad, integridad y disponibilidad de la información.

SGSI: (Sistema de Gestión de Seguridad de la Información). Procesos y procedimientos para gestionar el acceso a la información encaminados a buscar confidencialidad, integridad y disponibilidad de los activos y minimizando los riesgos.

Sistema de Información: Conjunto de aplicaciones, servicios, activos de tecnología de la información u otros componentes de manejo de información.

Tecnología de la Información: Se refiere al hardware y software operado por la entidad.

Tratamiento del riesgo: Proceso de análisis e implementación de acciones de mejora que permitan gestionar el riesgo.

Vulnerabilidad: Debilidad de un activo o control que puede ser explotado por una o más amenazas.

6. PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

6.1 Política General

La Política de Seguridad y Privacidad de la Información está direccionada a gestionar los datos y la protección de los activos de información y los procesos, estableciendo políticas de seguridad y cumplimiento, suministrando los procedimientos y las pautas a los servidores públicos de la entidad, en la implementación del Sistema de Gestión de la Seguridad de la Información SGSI, bajo los parámetros establecidos en la norma técnica ISO 27001: 2022.

Para la implementación del SGSI se tienen en cuenta las siguientes premisas:

- Establecer políticas de seguridad y privacidad de la información.
- Proteger los activos de información.
- Evaluación de riesgos.
- Organización de la seguridad de la información.
- Adquisición, desarrollo y mantenimiento de los sistemas de información, tanto hardware como software.
- Mantener controles de seguridad en los servidores, equipos y dispositivos de la entidad.
- Implementar el sistema de gestión de seguridad de la información.
- Establecer reglas y procedimientos relacionados con el acceso a la información.
- Establecer políticas de seguridad física y controles de acceso.
- Garantizar la continuidad de los servicios que presta la entidad frente a incidentes de seguridad y vulneración.
- Fortalecer la cultura de los servidores públicos de la entidad, respecto a la seguridad y los activos de información.

Gestión de Incidentes de Seguridad de la Información

La Personería Distrital de Santiago de Cali establece un procedimiento formal para la gestión de incidentes de seguridad de la información, el cual comprende las siguientes etapas:

1. Detección y reporte del incidente.
2. Clasificación y evaluación del impacto.
3. Respuesta y contención.
4. Análisis de causa raíz.
5. Registro, cierre y lecciones aprendidas.

Todos los incidentes de seguridad serán documentados y reportados al Comité de Seguridad Digital para su seguimiento y mejora continua.

Continuidad del Negocio y Recuperación ante Desastres

La Personería Distrital de Santiago de Cali implementará medidas orientadas a garantizar la continuidad de los servicios críticos ante eventos que afecten la operación institucional, mediante:

- Plan de Continuidad del Negocio (BCP).
- Plan de Recuperación ante Desastres (DRP)
- Esquemas de respaldo periódico de la información.
- Pruebas periódicas de restauración y continuidad operativa.

Indicadores de Seguridad de la Información

Para medir la efectividad del Sistema de Gestión de Seguridad de la Información, se establecen los siguientes indicadores:

- Número de incidentes de seguridad reportados.
- Tiempo promedio de respuesta a incidentes.
- Porcentaje de controles de seguridad implementados.
- Porcentaje de servidores capacitados en seguridad de la información.
- Nivel de madurez del SGSI (Inicial, Gestionado, Optimizado

7. GESTIÓN DE RIESGOS

GESTIÓN	ACTIVIDADES	TAREAS	RESPONSABLE DE LAS TAREAS	FECHA DE PROGRAMACIÓN	
				FECHA INICIO	FECHA FIN
GESTIÓN DE RIESGOS	Actualización de lineamientos de Riesgos	Actualizar Política y Metodología	Equipo de Gestión de Riesgos	1/03/2026	31/03/2026
	Sensibilización	Socialización Guía de herramientas Gestión de Riesgos de Seguridad y privacidad de la información, Seguridad Digital y continuidad de Operación	Equipo de Gestión de Riesgos	1/05/2026	30/05/2026
	Identificación de Riesgos, Seguridad y Privacidad de la información, Seguridad Digital y continuidad de operación	Identificación, Análisis y Evaluación de Riesgos de Seguridad y Privacidad de la información Seguridad Digital Continuidad de Operación	Equipo de Gestión de Riesgos	1/06/2026	30/06/2026
		Revisión y verificación de los Riesgos Identificados	Equipo de Gestión de Riesgos	1/06/2026	30/06/2026
	Aceptación de Riesgos Identificación	Aceptación, Aprobación Riesgos Identificados y Planes de Tratamiento	Equipo de Gestión de Riesgos	1/07/2026	30/08/2026
	Publicación	Publicación de Matriz de Riesgos (en el Sistema de Matriz de Riesgos Personería de Santiago de Cali)	Equipo de Gestión de Riesgos	1/09/2026	30/09/2026
	Seguimiento fase de tratamiento	Seguimiento Estado planes de tratamientos de riesgos identificados y verificados de evidencias	Equipo de Gestión de Riesgos	1/10/2026	30/10/2026
	Evaluación de Riesgos Residuales	Evaluación de Riesgos Residuales	Equipo de Gestión de Riesgos	15//10/2026	30/10/2026
	Mejoramiento	Identificación de oportunidades de mejora acorde a los resultados obtenidos durante la evaluación de los riesgos residuales	Equipo de Gestión de Riesgos	1/11/2026	30/11/2026
	Monitoreo y revisión	Generación, Presentación y reportes de indicadores	Equipo de Gestión de Riesgos	1/12/2026	30/12/2026

Gestión Tecnológica y de la Información
Líder del Proceso
Líder Política de Gobierno y Seguridad Digital
Oficina Asesora de Planeación-Revisión Técnica

Personería
Santiago de Cali

Ley de Transparencia y Acceso a la Información

www.personeriacali.gov.co.