CONCEJO MUNICIPAL DE CARTAGO

PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

LUIS FERNANDO GIRALDO
Presidente

CARTAGO, VIGENCIA 2025

INTRODUCCION

La Estrategia de Gobierno en Línea, liderada por el Ministerio de Tecnologías de la Información y las Comunicaciones (MinTIC), busca maximizar el uso de las TIC para fortalecer la construcción de un Estado más participativo, eficiente y transparente.

En este marco, la planificación e implementación del Modelo de Seguridad y Privacidad de la Información (MSPI) en el Concejo Municipal de Cartago responde a las necesidades y objetivos institucionales, los requisitos de seguridad de la información, así como a los procesos misionales y la estructura organizacional de la Corporación Edilicia. Esta implementación garantiza que la protección de la información se alinee con las mejores prácticas y estándares, asegurando la confidencialidad, integridad y disponibilidad de los datos manejados por la entidad.

El Modelo de Seguridad y Privacidad de la Información (MSPI) tiene como objetivo garantizar la confidencialidad, integridad y disponibilidad de la información, asegurando la privacidad de los datos. Esto se logra mediante la implementación de un proceso de gestión del riesgo, que permite identificar, evaluar y mitigar posibles amenazas. De esta manera, el MSPI brinda confianza a las partes interesadas sobre la adecuada gestión de los riesgos asociados al manejo de la información.

El Decreto Único Reglamentario 1078 de 2015, del sector de Tecnologías de la Información y las Comunicaciones (TIC), establece el componente de Seguridad y Privacidad de la Información como parte integral de la Estrategia de Gobierno en Línea (GEL). Para el desarrollo de este componente, se ha elaborado un conjunto de documentos asociados al Modelo de Seguridad y Privacidad de la Información (MSPI), los cuales han sido utilizados por diversas entidades, tanto a nivel nacional como territorial, con el objetivo de mejorar sus estándares de seguridad de la información.

El MSPI es un modelo dinámico, que se actualiza periódicamente para mantenerse alineado con las buenas prácticas de seguridad y adaptarse a los cambios técnicos y normativos. Estas actualizaciones consideran la Ley de Protección de Datos Personales, la Ley de Transparencia y Acceso a la Información Pública, entre otras normativas relevantes para la gestión de la información.
Adicionalmente, el MSPI incorpora nuevos lineamientos que facilitan la adopción del protocolo IPv6 en el Estado Colombiano, garantizando así que las entidades públicas estén preparadas para enfrentar los retos tecnológicos actuales y futuros.

El Modelo de Seguridad y Privacidad de la Información (MSPI) está plenamente alineado con el Marco de Referencia de Arquitectura TI, asegurando su integración con las directrices tecnológicas y estratégicas del sector público. Además, el MSPI soporta de manera transversal los demás componentes de la Estrategia de Gobierno en Línea (GEL), incluyendo:

- TIC para Servicios, facilitando la prestación segura y confiable de servicios digitales a la ciudadanía.

- TIC para Gobierno Abierto, garantizando la protección de la información en los procesos de transparencia, participación y colaboración ciudadana.

- TIC para la Gestión, fortaleciendo la seguridad en la administración interna y operativa de las entidades públicas.

Esta integración asegura una gestión de la información segura, eficiente y coherente en todos los niveles de la administración pública.

El presente Modelo de Seguridad y Privacidad de la Información- MSPI tiene como objetivo facilitar la comprensión y el desarrollo de una política de privacidad dentro de la entidad. Esta política establecerá los criterios y directrices necesarios para garantizar la protección de la información y los datos, asegurando tanto la privacidad como la seguridad en su manejo. Además, el modelo abarca la protección de los procesos institucionales y de las personas vinculadas al tratamiento de dicha información, promoviendo una gestión responsable y alineada con las normativas vigentes.

Finalmente, a nivel metodológico, es fundamental destacar que el modelo incluye una serie de guías específicas para cada una de sus fases, lo que facilita su implementación de manera estructurada y eficiente. Estas guías están diseñadas para proporcionar a los destinatarios del modelo funcionarios, responsables de la seguridad de la información y demás partes interesadas, una visión clara sobre:

- Los objetivos y resultados esperados en cada fase del proceso.
- **Las actividades y procedimientos** necesarios para alcanzar dichos resultados.

- **Herramientas y mejores prácticas** que pueden aplicarse para asegurar la efectividad de las acciones.

- **Indicadores de seguimiento y evaluación** que permiten medir el progreso y la eficacia de las medidas implementadas.

De esta manera, el modelo no solo establece qué debe hacerse, sino también cómo hacerlo, asegurando que las políticas de seguridad y privacidad se desarrollen de manera coherente y alineada con los estándares nacionales e internacionales. Esta orientación metodológica contribuye a fortalecer la capacidad institucional para gestionar adecuadamente la seguridad de la información y garantizar el cumplimiento de las normativas vigentes.

1. OBJETIVO GENERAL

Establecer los lineamientos y directrices estratégicas para la implementación de políticas, procedimientos y controles que garanticen una gestión integral, eficiente y segura de la información en el Concejo Municipal de Cartago Valle. Estas políticas estarán orientadas a asegurar la confidencialidad, integridad y disponibilidad de los datos, así como a proteger la privacidad de la información, en cumplimiento con la normatividad vigente en materia de protección de datos personales, transparencia y acceso a la información pública.

Asimismo, este objetivo busca promover una cultura de seguridad digital dentro de la entidad, fomentando la adopción de buenas prácticas, tecnologías y metodologías de gestión del riesgo que permitan prevenir, detectar y responder eficazmente a incidentes de seguridad. De esta manera, se garantizará un manejo adecuado de la información, fortaleciendo la confianza de la ciudadanía y las partes interesadas en la gestión del Concejo Municipal.

1.2 OBJETIVOS ESPECIFICOS

- **Diseñar e implementar políticas y procedimientos:** orientados a la gestión integral de la seguridad de la información, asegurando su alineación con las normativas vigentes y las mejores prácticas en materia de protección de datos, ciberseguridad y privacidad. Estas políticas definirán las responsabilidades**, controles y mecanismos** necesarios para prevenir y responder a incidentes de seguridad dentro del Concejo Municipal de Cartago – Valle.

- **Identificar, evaluar y mitigar los riesgos:** asociados a la seguridad de la información, estableciendo estrategias de prevención, detección y respuesta ante

amenazas que puedan comprometer la integridad, confidencialidad, disponibilidad y privacidad de los datos gestionados por la entidad. Para ello, se adoptarán metodologías de gestión del riesgo, protocolos de actuación ante incidentes y medidas de seguridad adecuadas a la estructura y necesidades del Concejo.

- **Garantizar la protección de la información institucional**, tanto en medios físicos como digitales, mediante la implementación de controles de acceso, cifrado, autenticación, monitoreo y auditoría, asegurando que solo las personas autorizadas puedan acceder, modificar o utilizar los datos sensibles.

- **Promover una cultura de seguridad digital** dentro del Concejo Municipal, a través de la **capacitación y sensibilización** de los funcionarios y colaboradores en buenas prácticas de seguridad informática, manejo seguro de la información y cumplimiento de la normativa vigente en materia de privacidad y protección de datos.

- **Fortalecer la infraestructura tecnológica y los sistemas de seguridad** del Concejo Municipal de Cartago – Valle, mediante la adopción de herramientas y tecnologías avanzadas que permitan la protección contra **amenazas cibernéticas, ataques informáticos y brechas de seguridad**.

- **Establecer mecanismos de monitoreo, auditoría y mejora continua**, que permitan evaluar periódicamente el estado de la seguridad de la información, detectar vulnerabilidades y optimizar los controles implementados, garantizando una gestión efectiva y sostenible en el tiempo.

2. ALCANCE

El presente plan es aplicable a todos los procesos, procedimientos y actividades del Concejo Municipal de Cartago – Valle en los que se realice la recolección, procesamiento, almacenamiento, recuperación, intercambio y consulta de información. Su implementación abarca tanto la gestión de datos en medios físicos como digitales, garantizando la protección, integridad y disponibilidad de la información en el desarrollo de la misión institucional y el cumplimiento de sus objetivos estratégicos.

Este plan se extiende a funcionarios, contratistas, proveedores y cualquier persona o entidad que tenga acceso o realice tratamiento de la información dentro del Concejo Municipal. Asimismo, contempla la adopción de controles, normativas y

buenas prácticas en materia de seguridad y privacidad, alineadas con el Marco de Referencia de Arquitectura TI, la Ley de Protección de Datos Personales y demás regulaciones aplicables.

3. MARCO NORMATIVO

- . **Constitución Política de Colombia. Artículos 15, 20, 23 y 74.**
- **Resolución 500 de Marzo 10 de 2021 del Ministerio de tecnología de la Información y la Comunicación:** 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"

• **Ley 23 de 1982**. Sobre derechos de autor.

• **Ley 44 de 1993**. Por la cual se modifica y adiciona la Ley 23 de 2082 y se modifica la Ley 29 de 2044 y 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 regula el Derecho Fundamental de Petición y se sustituye un título del Código de Procedimiento Administrativo y de lo Contencioso Administrativo.

• **Ley 850 de 2003**. Por medio de la cual se reglamentan las veedurías ciudadanas.

• **Ley 962 de 2005**. Por la cual se dictan disposiciones sobre racionalización de trámites y procedimientos administrativos de los organismos y entidades del Estado y de los particulares que ejercen funciones públicas o prestan servicios públicos.

• **Ley 1221 del 2008**. Por la cual se establecen normas para promover y regular el Teletrabajo y se dictan otras disposiciones.

• **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.

• **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 1450 de 2011**. Por la cual se expide el Plan Nacional de Desarrollo, 2010-2014.

• **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 2088 de 2012**. Por la cual se regula el trabajo en casa y se dictan otras disposiciones.
• **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 1755 de 2015**. Por medio de la cual se regula el Derecho Fundamental de Petición y se sustituye un título del Código de Procedimiento Administrativo y de lo Contencioso Administrativo.

• **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.

• **Decreto 1078 de 2015** modificado por el Decreto 1008 de 2018 - Política de Gobierno Digital que contiene el Modelo de Seguridad y Privacidad - MSPI de MINTIC.

- **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. financiera, crediticia, comercial, de servicios y la proveniente de terceros países y se dictan otras disposiciones.

4. DEFINICIONES

Confidencialidad: propiedad de la información que la hace no disponible, es decir, divulgada a individuos, entidades o procesos no autorizados.

Disponibilidad: propiedad de ser accesible y utilizable a demanda por una entidad.

Estándar: Regla que especifica una acción o respuesta que se debe seguir a una situación dada. Los estándares son orientaciones obligatorias que buscan hacer cumplir las políticas. En este documento se habla de las Norma Técnica Colombiana ISO27001:2013 e ISO31000:2013.

Gestión del riesgo: proceso efectuado por la alta dirección de la entidad y por todo el personal para proporcionar a la administración un aseguramiento razonable con respecto al logro de los objetivos.

Incidente de seguridad de la información: Resultado de intentos intencionales o accidentales de romper las medidas de seguridad de la información impactando en la confidencialidad, integridad o disponibilidad de la información.

Información: Es un conjunto organizado de datos, que constituyen un mensaje sobre un determinado ente o fenómeno. Indicación o evento llevado al conocimiento de una persona o de un grupo. Es posible crearla, mantenerla, conservarla y transmitirla.

Integridad: propiedad de exactitud y completitud.

Inventario de activos: Lista de todos aquellos recursos (físicos, de información, software, documentos, servicios, personas, intangibles, etc.) dentro del alcance del SGSI, que tengan valor para la organización y necesiten por tanto ser protegidos de potenciales riesgos.

Sistema de Gestión de Seguridad de la Información: Parte del sistema de gestión general del Concejo, basada en un enfoque hacia los riesgos globales del negocio,

cuyos fines son establecer, implementar, operar, hacer seguimiento, revisar, mantener y mejorar la seguridad de la información.

Política de seguridad de información: Es el instrumento que adopta una entidad para definir las reglas de comportamiento aceptables en el uso y tratamiento de la información.

Riesgo: Es la posibilidad de que suceda algún evento que tendrá un impacto sobre los objetivos institucionales o de los procesos del Concejo. Se expresa en términos de probabilidad y consecuencias.

Riesgo de seguridad y privacidad: Potencial de que una amenaza determinada explote las vulnerabilidades de los activos o grupos de activos causando así daño a la organización. Se mide en términos de probabilidad y consecuencias.

5. RESPONSABLES

El **Concejo Municipal de Cartago – Valle** ha designado los siguientes responsables para garantizar la implementación, cumplimiento y mantenimiento de la Política de Seguridad y Privacidad de la Información:

1. **Presidente del Concejo Municipal de Cartago Valle**: Responsable de garantizar el cumplimiento de la política, velando por su correcta aplicación en la entidad.

2. **Funcionario delegado de las TIC**: Encargado de la formulación e implementación de la política, asegurando que se adopten los lineamientos y controles necesarios para su ejecución.

3. **Profesional universitario o asesor externo encargado de la gestión de TIC**: Responsable de desarrollar la implementación de la política, aplicando estrategias y acciones que permitan su adecuada ejecución en el Concejo Municipal.

4. **Funcionarios, contratistas y demás partes interesadas**: Tienen la responsabilidad de cumplir de manera obligatoria con la Política de Seguridad y Privacidad de la Información. En caso de incumplimiento, el Concejo Municipal se reserva el derecho de aplicar las medidas correspondientes según la normativa vigente.

6. POLITICAS

El Concejo Municipal de Cartago Valle se encarga de divulgar los objetivos y alcances de la seguridad de la información dentro de la entidad, asegurando que estos sean efectivos a través de la implementación de controles de seguridad. Estos controles tienen como propósito mantener, gestionar y mitigar los riesgos conforme a lo establecido en el Plan de Tratamiento de Riesgos. De esta manera, se garantiza la continuidad de los servicios y se disminuye la probabilidad de amenazas que puedan afectar los procesos internos, contribuyendo al cumplimiento eficiente de la prestación del servicio público.

- **Identificación, clasificación y valoración de activos de información:**

Cada proceso en el Concejo Municipal de Cartago Valle, bajo supervisión y conforme al inventario de activos de la entidad, debe actualizarse de manera constante. Este inventario incluirá la clasificación, valoración, ubicación y acceso de la información, así como otras características identificadas por la Alta Dirección. De este modo, se garantizará una administración eficiente de cada proceso, asegurando la disponibilidad, integridad y confidencialidad de la información en todo momento.

- **Seguridad de la información en el Talento Humano**

Todos los servidores públicos del Concejo Municipal de Cartago, independientemente de su tipo de vinculación laboral o contractual, el área en la que desempeñen sus funciones o el nivel de actividades que realicen, deben contar con un perfil de uso de los recursos de información, que incluye tanto el hardware como el software asociado a su rol.

Para ello, es esencial contar con un directorio completo y actualizado de los perfiles creados. Además, la responsabilidad de la custodia de cualquier documento o archivo generado dentro del Concejo, que haya sido usado o producido por algún funcionario o contratista que se retire o cambie de cargo, recae en la Secretaría General, los demás secretarios o el supervisor del contrato.

Es importante señalar que el proceso de cadena de custodia de la información debe formar parte integral de los procedimientos de terminación de la relación contractual o de cambio de cargo, asegurando que los documentos e información sean debidamente gestionados durante este proceso.

- **Usuarios invitados y servicios de acceso público.**

El acceso a los recursos de información institucional por parte de usuarios no registrados deberá ser autorizado únicamente por la Presidencia, y se limitará a la información institucional. Además, el servicio de internet al que puedan acceder debe estar protegido con una contraseña y contar con una restricción de acceso a sitios web no autorizados.

En caso de que los usuarios invitados no hayan completado el debido proceso de registro, no se les permitirá el acceso a cualquier otro tipo de recurso de información, aplicación o herramienta TIC.

- **Seguridad Física y del entorno**

Seguridad en los equipos:
Los servidores o equipos de cómputo que contengan información institucional deben estar ubicados en un ambiente seguro y protegido, cumpliendo, como mínimo, con los siguientes requisitos:

- Controles de acceso y seguridad física, que restrinjan el acceso no autorizado a los dispositivos y equipos.

- Sistemas eléctricos regulados, respaldados por fuentes de potencia ininterrumpida (UPS), para garantizar la continuidad operativa en caso de cortes de energía.

Toda información institucional en formato digital debe ser almacenada únicamente en los servidores y/o unidades extraíbles aprobados por la Secretaría General. Estos servidores y dispositivos deben estar adecuadamente protegidos y deben contar con mecanismos de control de acceso que aseguren que solo personas autorizadas tengan acceso a la información.

La infraestructura tecnológica debe contar con un mantenimiento y soporte adecuado para garantizar la operatividad continua tanto del hardware como del software. Es fundamental que las estaciones de trabajo sean operadas exclusivamente por los funcionarios de la Corporación Edilicia, quienes deben estar capacitados sobre el contenido de esta política y las responsabilidades personales que conlleva el uso y administración de la información institucional. Esta capacitación debe incluir el conocimiento de las mejores prácticas de seguridad de la información, el manejo adecuado de los recursos tecnológicos y las consecuencias de un manejo indebido de los datos.

En cuanto al manejo de copias de seguridad, los medios de almacenamiento que alojan estas copias deben ser conservados de manera segura y protegidos contra accesos no autorizados. Las copias de seguridad deben almacenarse en lugares físicamente seguros y, preferiblemente, en entornos distintos a los de producción para evitar pérdidas catastróficas. Además, deben seguirse las políticas y estándares establecidos en cuanto a la frecuencia de las copias de seguridad, los procedimientos de restauración de datos y la auditoría periódica de los procesos relacionados.

- **Administración de las comunicaciones y operaciones**

Reporte y revisión de incidentes de seguridad:
El personal vinculado al Concejo Municipal de Cartago Valle tiene la responsabilidad de reportar de manera eficiente y responsable cualquier presunta violación de seguridad que detecten. Estos reportes deben ser dirigidos a la Presidencia o, en casos especiales, cuando la situación lo amerite, podrán ser realizados directamente por la persona que detecte el incidente o la novedad.

Es fundamental que el procedimiento de reporte sea claro y accesible, permitiendo a los empleados y contratistas reportar incidentes de manera rápida y segura. El reporte debe incluir detalles clave sobre el incidente, como la hora de detección, la descripción del incidente, los recursos afectados, y cualquier acción preliminar tomada.
Además, se debe diseñar, mantener y difundir las normas, procesos y guías para el reporte y revisión de incidentes de seguridad. Esto incluye la elaboración de procedimientos escritos que aseguren la correcta operación de estas actividades. Los procedimientos deben detallar los siguientes pasos:

1. **Identificación y clasificación del incidente**: Cada incidente reportado debe ser clasificado según su gravedad y tipo (e.g., acceso no autorizado, pérdida de datos, malware). Esto ayudará a priorizar la respuesta.
2. **Notificación y escalamiento**: En casos de alta gravedad, como filtraciones de datos sensibles, se debe escalar el incidente inmediatamente a las autoridades pertinentes y tomar acciones inmediatas para mitigar el daño.

3. **Investigación y análisis**: El equipo responsable debe investigar la causa del incidente, analizando los registros, el comportamiento del sistema y los recursos afectados, para determinar el alcance y la naturaleza del problema.

4. **Remediación**: Una vez identificada la causa, se deben implementar acciones correctivas para resolver el problema, como la eliminación de malware, el fortalecimiento de las medidas de seguridad o la restauración de sistemas a partir de copias de seguridad.

5. **Seguimiento y reporte**: Después de la resolución, se debe hacer un seguimiento para verificar que el incidente no se repita y se deben elaborar informes detallados sobre el incidente, las acciones tomadas y las lecciones aprendidas.

6. **Revisión de políticas y medidas preventivas**: Como medida a largo plazo, se debe revisar y, si es necesario, ajustar las políticas de seguridad para prevenir futuros incidentes similares, así como mejorar la capacitación del personal en aspectos clave de seguridad.

Este proceso debe llevarse a cabo sin afectar el desarrollo normal de la prestación del servicio y asegurando la confiabilidad de la información en todo momento, manteniendo la continuidad operativa y el cumplimiento de las normativas vigentes.

- **Protección contra software malicioso y hacking**

Es fundamental proteger todos los sistemas de información mediante un enfoque integral que incluya controles humanos, físicos, técnicos y administrativos para evitar daños. Para ello, se elaborará y mantendrá un conjunto de políticas, normas, estándares y procedimientos que garanticen la mitigación de riesgos asociados a amenazas de software malicioso y técnicas de hacking que puedan comprometer la prestación del servicio.
Como medida de control básico, todas las estaciones de trabajo del Concejo Municipal deben estar protegidas con software antivirus que cuente con capacidad de actualización automática para asegurar que las firmas de virus estén siempre al día y que los sistemas estén protegidos frente a las amenazas emergentes. Además, el software antivirus debe incluir funcionalidades de detección en tiempo real para identificar y bloquear cualquier actividad sospechosa de forma inmediata.

Se debe implementar una política de actualización de software que asegure que todos los sistemas operativos, aplicaciones y herramientas de seguridad sean actualizados de forma periódica. Las actualizaciones de seguridad deben ser aplicadas de manera automática, siempre que sea posible, para garantizar que se aborden vulnerabilidades conocidas de manera oportuna. Asimismo, se deberán llevar a cabo pruebas de compatibilidad para evitar que las actualizaciones afecten el funcionamiento normal de los sistemas y servicios.

Para garantizar la efectividad de estas medidas, se implementará un sistema de monitoreo continuo que permita evaluar la actividad de los sistemas y detectar cualquier anomalía o vulnerabilidad en tiempo real. Este monitoreo incluirá la revisión periódica de los registros de eventos de seguridad y pruebas de penetración para asegurar que los sistemas se mantengan protegidos contra nuevas amenazas. Además, se deben realizar auditorías regulares para evaluar el cumplimiento de las políticas de seguridad y detectar posibles áreas de mejora.

Es esencial que todos los funcionarios del Concejo Municipal estén capacitados en seguridad informática. Se implementará un programa de formación continua sobre las mejores prácticas en ciberseguridad, incluyendo temas como el manejo seguro de contraseñas, el reconocimiento de phishing y otras amenazas, y el uso adecuado de herramientas de protección. Además, los funcionarios de TI deberán recibir formación especializada para mantenerse al día con las últimas tendencias en amenazas y tecnologías de protección.

- **Copias de Seguridad**

Toda información contenida en el inventario de activos de información o que sea relevante para un proceso debe estar respaldada mediante copias de seguridad. Estas copias deben tomarse siguiendo los procedimientos documentados y validados por el Sistema de Gestión Pública - MIPG.

El procedimiento de respaldo debe incluir actividades relacionadas con el almacenamiento, administración y custodia de las copias de seguridad, asegurando que estas se guarden en lugares seguros y que se lleve un control adecuado de los registros. Dentro de este procedimiento, se debe establecer la realización de auditorías aleatorias para garantizar el correcto funcionamiento de los procesos de copia de seguridad y asegurar que se mantengan alineados con los estándares establecidos.

Las auditorías de las copias de seguridad deben llevarse a cabo de manera periódica y no programada, con el objetivo de asegurar que se esté cumpliendo con los protocolos establecidos. Estas auditorías deben evaluar la integridad de los datos, verificar que las copias sean exactas y completas, y comprobar que los medios de almacenamiento estén funcionando correctamente.
Además, debe existir un procedimiento documentado que verifique la correcta restauración de los datos, lo que permitirá probar la efectividad de las copias de seguridad y garantizar que la información pueda ser recuperada en caso de un incidente.

Las auditorías también deben incluir pruebas de recuperación de datos en un entorno controlado para asegurar que no haya fallos durante el proceso de restauración.

Es importante tener en cuenta que la responsabilidad de crear copias de seguridad de archivos utilizados, custodiados o producidos por usuarios individuales recae exclusivamente en cada uno de los usuarios. Los usuarios deben ser conscientes de su responsabilidad en asegurar la actualización continua de las copias de seguridad de la información que manejan.

Los dueños de los activos de la información deben verificar regularmente la validez y accesibilidad de las copias de seguridad y asegurarse de que están almacenadas de acuerdo con los procedimientos establecidos. En caso de que los usuarios encuentren dificultades en la actualización o almacenamiento de sus copias, deberán informar inmediatamente a los responsables de la gestión de TI para que se tomen las acciones correctivas necesarias.

En cuanto al intercambio de información con entidades externas, cualquier petición o solicitud de información por parte de entes externos debe ser aprobada por la Alta Dirección. La Alta Dirección debe revisar cuidadosamente la solicitud para asegurarse de que la información solicitada sea relevante, esté completa y sea accesible conforme a las normas de confidencialidad y seguridad establecidas. Una vez aprobada la solicitud, la Alta Dirección designará a los responsables del manejo de esa información, quienes se encargarán de procesarla de acuerdo con los procedimientos internos y entregarla a la entidad solicitante.
El proceso de aprobación debe ser documentado y el registro de la solicitud debe ser almacenado de manera segura para garantizar la trazabilidad de la solicitud, permitiendo un seguimiento adecuado del uso y destino de la información institucional.
La solicitud deberá incluir detalles como el remitente, el asunto, la fecha y la naturaleza de la información solicitada, de forma que se pueda identificar claramente su origen y garantizar que no se viole ninguna normatividad vigente.

Además, toda información institucional debe ser manejada de acuerdo con la normatividad legal vigente, asegurando el cumplimiento de leyes como la protección de datos personales, la transparencia y el acceso a la información pública. Las solicitudes de entidades externas también deben cumplir con los protocolos de seguridad establecidos, asegurando que la información no se comparta con personas no autorizadas y que se mantenga la integridad y confidencialidad de los datos.

- **Instalación de Software**

Las instalaciones de software que se realicen sobre los sistemas operativos previamente instalados en el Concejo Municipal de Cartago Valle, deben contar con la aprobación expresa de la Alta Dirección. Esta aprobación debe basarse en una evaluación exhaustiva del software, que no solo contemple la compatibilidad con los sistemas existentes, sino también una revisión detallada de los aspectos de seguridad, eficiencia, y su adecuación al marco normativo de tecnologías de la información aplicable. Para ello, se deben seguir los procedimientos establecidos para la instalación de software, que incluyen la verificación de su origen legítimo, licencia válida, funcionalidad y que no represente ninguna amenaza a la seguridad de la información.

Los procedimientos de instalación deben también incluir una evaluación de riesgos que considere los impactos potenciales del software en los procesos internos, en la protección de datos personales y en la integridad de la infraestructura tecnológica. El procedimiento también debe establecer que el software solo puede ser instalado por personal capacitado en el área de gestión de TIC, siguiendo un protocolo que permita verificar la compatibilidad técnica con las aplicaciones existentes y asegurando que la instalación no afecte el rendimiento de los sistemas operativos ni de las estaciones de trabajo.
Es imperativo que la Alta Dirección asegure que el software instalado sea de fuentes confiables y aprobadas, evitando así la instalación de aplicaciones que puedan comprometer la seguridad, tales como software pirata o aplicaciones no verificadas. Esta política no solo asegura la legalidad del software, sino que también minimiza el riesgo de vulnerabilidades que puedan ser aprovechadas por ciberataques o malware.

El funcionario encargado de la gestión de las Tecnologías de la Información (TIC) en el Concejo Municipal tiene la responsabilidad inmediata de desinstalar cualquier software ilegal o no autorizado que sea detectado. La detección de software no autorizado debe ser considerada un incidente de seguridad, y debe ser registrada y gestionada a través de un sistema de gestión de incidentes. Este sistema debe estar diseñado para clasificar, priorizar y hacer un seguimiento de los incidentes, lo que permitirá una respuesta rápida y eficaz.

El proceso de investigación de incidentes debe incluir varias etapas. Primero, se debe llevar a cabo un análisis forense para determinar el origen y el alcance de la instalación del software no autorizado, lo que permitirá identificar cómo y cuándo fue instalado y por quién. Se debe analizar si este software ha causado algún daño

o afectación a los sistemas, si ha generado brechas en la seguridad de la información o si ha comprometido la confidencialidad de los datos institucionales.

El resultado de la investigación debe ser documentado detalladamente, y deben tomarse las acciones correctivas necesarias. Estas acciones pueden incluir la eliminación del software, la actualización de las medidas de seguridad, y, si fuera necesario, la capacitación adicional del personal para evitar que se repita la instalación de software no autorizado.

Adicionalmente, el funcionario encargado de las TIC debe mantener un inventario detallado y actualizado del software autorizado para su uso institucional. Este inventario debe ser revisado de manera periódica para garantizar que todos los programas que se están utilizando son legítimos y han sido debidamente aprobados por la Alta Dirección.
El inventario debe incluir detalles como el nombre del software, la versión, el tipo de licencia, los responsables de su instalación y uso, y cualquier otra información relevante que permita hacer un seguimiento adecuado del software autorizado. Además, el inventario debe estar disponible para auditorías internas y debe ser utilizado para realizar verificaciones periódicas de la legalidad del software instalado en los sistemas del Concejo Municipal.

- **Control de Claves y Nombres de Usuario**

Las claves de administrador de los diferentes sistemas deben ser conservadas por la Secretaría General y el funcionario encargado de la Gestión de las TIC. Estas claves deberán cambiarse en intervalos regulares y, de manera obligatoria, cada vez que se presente un cambio en el personal adscrito al cargo.
Adicionalmente, se debe elaborar, mantener y actualizar un procedimiento que defina claramente el uso, la complejidad y las buenas prácticas para la gestión segura de las claves de usuario.

Suspensión y Cancelación de Cuentas
Al finalizar la relación contractual o laboral de un funcionario con el Concejo Municipal de Cartago Valle, se deberá expedir un certificado de suspensión y/o cancelación de las cuentas asociadas al usuario en todos los sistemas de información donde estuviera activo, incluyendo correo electrónico y sistemas automatizados.
Se establecerá un tiempo prudencial para la posible renovación de la relación laboral. Si dicha renovación no se materializa al término de ese período, se procederá con la baja definitiva de las cuentas correspondientes.

- **Uso Adecuado de Internet**

Política de Gestión del Servicio de Internet
El Concejo Municipal de Cartago-Valle reconoce la importancia del servicio de Internet como una herramienta esencial para el desarrollo eficiente y seguro de las actividades institucionales. El acceso a este recurso permite optimizar procesos, facilitar la comunicación y garantizar la prestación efectiva de los servicios públicos. Por tal razón, la entidad se compromete a proporcionar los recursos necesarios para su disponibilidad, asegurando el acceso a los servidores públicos y a otras partes interesadas que lo requieran para el desempeño de sus funciones.

Para el cumplimiento de este objetivo, el proceso de Tecnologías de la Información y las Comunicaciones (TIC) deberá implementar las siguientes acciones:

1. **Asignación de recursos:**

   El proceso de TIC será responsable de gestionar, proveer y distribuir los recursos necesarios para la correcta implementación, administración y mantenimiento del servicio de Internet. Esta gestión se realizará garantizando su disponibilidad, estabilidad y seguridad, bajo las restricciones definidas según los perfiles de acceso establecidos. Se procurará la adquisición de tecnologías actualizadas que optimicen el rendimiento y la seguridad de la conexión.

2. **Continuidad del servicio:**
   Se deberá diseñar, documentar e implementar mecanismos que permitan garantizar la continuidad o el restablecimiento oportuno del servicio de Internet en caso de presentarse una contingencia interna. Para tal fin, se realizarán análisis de riesgos periódicos y se desarrollarán planes de contingencia que incluyan la definición de procedimientos de respuesta ante fallos y el establecimiento de mecanismos alternativos de conectividad.

3. **Monitoreo constante:**
   Se establecerá un monitoreo continuo de los canales de acceso a Internet con el objetivo de detectar, analizar y corregir de manera oportuna cualquier anormalidad que pueda afectar el funcionamiento del servicio. Este monitoreo incluirá la medición de indicadores clave de desempeño, como la velocidad de conexión, la disponibilidad del servicio y el consumo de ancho de banda, permitiendo así una gestión proactiva.

4. **Registro y control de accesos:**

El proceso de TIC deberá generar, almacenar y custodiar registros detallados sobre la navegación y los accesos realizados por los usuarios a través del servicio de Internet. Estos registros serán gestionados conforme a las disposiciones legales vigentes en materia de protección de datos y privacidad,
y se utilizarán para identificar posibles usos indebidos, garantizar el cumplimiento de las políticas internas y contribuir a la mejora continua del servicio.

5. **Sensibilización y formación:**
Se desarrollarán programas de sensibilización y capacitación dirigidos a los servidores públicos y demás usuarios autorizados, con el fin de promover el uso responsable, eficiente y seguro del servicio de Internet. Estas actividades incluirán lineamientos sobre el manejo adecuado de la información, la gestión segura de las credenciales de acceso y las buenas prácticas en el entorno digital.

Cumplimiento y Mejora Continua:
El Concejo Municipal de Cartago Valle, a través del proceso de TIC, establecerá mecanismos de auditoría y revisión periódica para evaluar el cumplimiento de esta política y realizar los ajustes necesarios que permitan su mejora continua. Asimismo, se mantendrá una actualización constante en las tecnologías y procedimientos utilizados, garantizando la eficiencia y seguridad del servicio en el marco de las necesidades institucionales y las disposiciones legales aplicables.

7. DESARROLLO DEL PLAN

7.1 Metodología de Implementación del Plan de Seguridad y Privacidad

La metodología de implementación del Plan de Seguridad y Privacidad del Concejo Municipal de Cartago-Valle se fundamenta en el ciclo PHVA (Planificar-Hacer-Verificar-Actuar) y en las directrices establecidas en el Modelo de Seguridad y Privacidad del Ministerio de Tecnologías de la Información y las Comunicaciones (MinTIC), según lo dispuesto en la Resolución 00500 del 21 de marzo de 2021. Esta metodología permite una gestión sistemática y continua de los riesgos asociados a la información, garantizando su confidencialidad, integridad, disponibilidad y privacidad.

1. Fase de Planificación (Planificar):

En esta fase se realiza un análisis exhaustivo del estado actual de la seguridad de la información, identificando activos críticos, posibles vulnerabilidades y amenazas potenciales. Se definen los objetivos, las estrategias y las acciones necesarias para mitigar riesgos, alineándolos con las necesidades institucionales y el marco normativo vigente. Adicionalmente, se elaboran políticas, procedimientos y planes de acción que orienten el proceso de implementación de las medidas de seguridad y privacidad.

2. Fase de Implementación (Hacer):
Durante esta etapa se ejecutan las acciones planificadas, aplicando las medidas técnicas, administrativas y operativas necesarias para proteger la información institucional. Esto incluye la configuración de mecanismos de control de acceso, la instalación de herramientas de seguridad, la capacitación del personal en buenas prácticas de gestión de la información y la implementación de procesos para la gestión segura de datos. Asimismo, se documentan las acciones realizadas para facilitar su seguimiento y evaluación posterior.

3. Fase de Verificación (Verificar):
En esta fase se evalúa la eficacia de las medidas implementadas a través de auditorías, revisiones y análisis de incidentes. Se miden los resultados obtenidos en comparación con los objetivos definidos y se identifican posibles desviaciones o fallas. Este proceso permite comprender el impacto de las acciones realizadas y determinar las mejoras necesarias para fortalecer el sistema de seguridad y privacidad de la información.

4. Fase de Mejora Continua (Actuar):
Finalmente, se toman las decisiones necesarias para corregir las deficiencias detectadas y optimizar los procesos de gestión de la seguridad y privacidad. Se ajustan las políticas, procedimientos y controles establecidos, incorporando lecciones aprendidas y mejores prácticas identificadas durante la fase de verificación. La mejora continua garantiza la adaptabilidad y resiliencia del sistema frente a nuevos riesgos y exigencias tecnológicas.

Compromiso Institucional:
El Concejo Municipal de Cartago Valle, reafirma su compromiso con la protección de la información institucional, adoptando las mejores prácticas en materia de seguridad y privacidad, conforme a la normativa aplicable y las recomendaciones de MinTIC. La aplicación rigurosa del ciclo PHVA permite una gestión efectiva de los riesgos, contribuyendo a la confianza de los ciudadanos y al fortalecimiento de la transparencia y eficiencia institucional.

Hasta la fecha, se han realizado las actividades de planificación, las cuales abarcan el análisis del contexto institucional, la definición de objetivos, la planeación estratégica, el soporte requerido y la evaluación del estado actual de la información.

En el marco de la implementación, se ha trabajado en la elaboración de procedimientos, guías y manuales, así como en el establecimiento de controles y la planificación operacional. Adicionalmente, se diseñó un plan de sensibilización para promover la cultura de seguridad de la información dentro de la entidad.

CUMPLIMIENTO DE LA IMPLEMENTACIÓN

El Concejo Municipal de Cartago-Valle en su modelo de seguridad y privacidad de la información se encuentra en la fase de implementación de acuerdo con el diagnóstico realizado en MIPG vigencia 2024

NIVEL DE MADUREZ

El modelo de seguridad y privacidad de la información, establecido por el Ministerio de Tecnologías de la Información, ofrece una guía para garantizar que las entidades públicas gestionen adecuadamente la información que poseen, protegiendo tanto la privacidad de los ciudadanos como la seguridad de los datos. En este contexto, el Concejo Municipal de Cartago, Valle, se encuentra en la fase inicial, es decir, en el nivel *incipiente* de implementación de este modelo.

El nivel *incipiente* se refiere a la etapa temprana en la que las acciones definidas en la fase de planeación aún no se han puesto en práctica de manera efectiva, pero se cuenta con una visión clara de las medidas que deben implementarse. Por lo tanto, el Concejo debe centrarse en ejecutar las acciones ya delineadas en esa etapa previa, lo que implica diseñar un modelo de privacidad acorde con los requisitos establecidos, asegurando que cumpla con las normativas legales mínimas, como la Ley Estatutaria de Protección de Datos Personales (Ley 1581 de 2012) y las disposiciones relacionadas con el manejo de información pública.

El proceso requiere que el Concejo también desarrolle y ponga en marcha una política de privacidad específica. Esta política será fundamental para la correcta gestión de la información, ya que establecerá procedimientos y protocolos claros sobre cómo se recoge, almacena, protege, utiliza y comparte la información dentro de la entidad. Adicionalmente, esta política debe contemplar la formación y sensibilización del personal encargado de la gestión de datos, asegurando que se actúe con la debida diligencia en el manejo de la información.

Implementar un modelo de privacidad robusto y cumplir con las regulaciones en vigor permitirá al Concejo no solo proteger los datos personales y confidenciales, sino también fortalecer la confianza de la ciudadanía en la administración pública, garantizando que se cumpla con los estándares más altos de seguridad y privacidad en la gestión de la información.

7.2 Mapa de Ruta Periodo 2025

No.	Actividad	Responsable	Producto o Resultado Esperado	Fecha Inicio	Fecha Final
1. Autodiagnóstico					
1.1	Realizar seguimiento de autodiagnóstico de evaluación de MSPI	Grupo de Apoyo	Informe de seguimiento al autodiagnóstico diligenciado	01/04/2025	30/06/2025
2. Activos de información					
2.1	Seguimiento a la actualización instrumentos de identificación de activos de información	Grupo de Apoyo	Informe de seguimientos a los Instrumentos de identificación de activos de información	01/04/2025	30/06/2025
2.2	Informe de Seguimiento a la actualización de Activos de información	Todos los Procesos Equipo de Apoyo MIPG	Avances de informes a las Matrices de activos	31/05/2025	30/06/2025
2.3	Verificar la Publicación Instrumentos de activos de información del Municipio	Grupo de Apoyo Equipo de Apoyo MIPG	Avances de Informes Matrices de activos en la página web	01/07/2025	5/07/2025

No.	Actividad	Responsable	Producto o Resultado Esperado	Fecha Inicio	Fecha Final
3. Riesgos de Seguridad y Privacidad de la Información					
3.1	Informe de actualización metodología de Riesgos de Seguridad y Privacidad	Equipo de Apoyo MIPG	Informe de Avance Matriz de riesgos	05/07/2025	30/12/2025
3.2	Informe detallado sobre la evaluación de riesgos de seguridad.	Equipo de Apoyo MIPG	Comunicación es internas / Correo electrónico	05/07/2025	30/12/2025
3.3	Informe de Identificación y Análisis	Todas las áreas y	Avances de la Matriz de riesgos	05/07/2025	30/12/2025

	de Riesgos Seguridad de la información	acompañamiento de Equipo MIPG			
3.4	Publicación de riesgos de seguridad de información	Equipo de Apoyo MIPG	Enlace de transparencia	31/07/2025	2/08/2025
4. Plan de Sensibilización Seguridad de la Información					
4.1	Actualización plan de sensibilización	Equipo de Apoyo	Matriz de sensibilización de seguridad de la información	1/11/2025	31/12/2025
4.2	Ejecución del plan de sensibilización	Equipo de Apoyo	Informe de ejecución	1/11/2025	31/12/2025

No.	Actividad	Responsable	Producto o Resultado Esperado	Fecha Inicio	Fecha Final
4.	**Seguimiento y Control del Plan de Seguridad y Privacidad de la Información**				
4.1	Realizar seguimiento y evaluación al Plan de seguridad y privacidad de la información en atención a los riesgos de seguridad y privacidad de la información identificados, analizados, valorados y priorizados sobre los activos de información bajo la responsabilidad de cada dependencia a nivel central	Equipo de Apoyo	Informe de Seguimiento y Auditoria	02/01/2026	31/01/2026

H C LUIS FERNANDO GIRALDO
Presidente

Elaboró: Contratista Asesor Concejo Municipal
Reviso: Ab. Jeisson A Rendon- Asesor Jurídico
Aprobó: Luis Fernando Giraldo- Presidente Mesa D.