CONCEJO MUNICIPAL DE CARTAGO

PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACION

PARA LA VIGENCIA 2024

Cartago, Vigencia 2024

INTRODUCCION

En el contexto del Concejo Municipal de Cartago, donde la gestión eficaz de la información es esencial para el funcionamiento transparente y efectivo de los servicios públicos, la seguridad y la privacidad de la información adquieren una importancia aún mayor. Con el compromiso de garantizar la integridad de los datos, preservar la confidencialidad de la información sensible y mantener la confianza de los ciudadanos, se debe embarcar en el diseño e implementación de un Plan de Seguridad y Privacidad de la Información adaptado a las necesidades y desafíos de la comunidad Cartagueña.

Este documento presenta un enfoque integral para fortalecer las defensas del Concejo Municipal contra las amenazas cibernéticas y los riesgos asociados con el manejo de la información pública y privada. Reconociendo la responsabilidad inherente de proteger los datos de los ciudadanos y salvaguardar los intereses de la administración local, el objetivo es establecer una estructura sólida de políticas, procedimientos y controles diseñados para garantizar la seguridad y la confidencialidad de la información.

A través de una evaluación exhaustiva de riesgos, la implementación de medidas de seguridad robustas y la capacitación continua del personal, se aspira a crear un entorno en el que la seguridad de la información sea una prioridad en cada faceta de las operaciones de la Corporación. Se reconoce que la seguridad y la privacidad de la información son fundamentales para mantener la confianza de los ciudadanos en la administración pública y garantizar la protección de sus derechos y datos.

En última instancia, este plan no solo busca proteger los activos de información del Concejo Municipal de Cartago, sino también promover una cultura de seguridad arraigada en la conciencia y el compromiso de cada miembro del equipo y de la comunidad en general. A través de la colaboración y el cumplimiento de las mejores prácticas de seguridad, se garantiza el fortalecimiento de las defensas y preservar la integridad y la confidencialidad de la información que le ha sido confiada.

PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACION

1. OBJETIVOS

El objetivo principal del Plan de Seguridad y Privacidad de la Información para el Concejo Municipal de Cartago es establecer una estructura integral y efectiva que garantice la protección de la información sensible y crítica gestionada por la Corporación. Este plan tiene como propósito fundamental:

Salvaguardar la confidencialidad, integridad y disponibilidad de la información: Implementar medidas de seguridad y controles adecuados para proteger los datos de los ciudadanos, los registros gubernamentales y otros activos de información contra amenazas internas y externas.

Cumplir con las regulaciones y normativas vigentes: Garantizar que el tratamiento de la información por parte del Concejo Municipal cumpla con las leyes y regulaciones de privacidad de datos pertinentes, así como con los estándares de seguridad establecidos por las autoridades competentes.

Mitigar riesgos y minimizar impactos: Identificar, evaluar y gestionar proactivamente los riesgos asociados con la seguridad y privacidad de la información para prevenir incidentes de seguridad, reducir la exposición a amenazas y minimizar los posibles impactos adversos en la organización y la comunidad.

Fomentar una cultura de seguridad de la información: Promover la conciencia y el compromiso de todo el personal del Concejo Municipal en materia de seguridad de la información mediante la capacitación, la sensibilización y la adopción de mejores prácticas en la gestión de la información.

Mejorar la resiliencia y la capacidad de respuesta: Establecer procedimientos claros y eficaces para la gestión de incidentes de seguridad, la respuesta a emergencias y la recuperación de datos, con el fin de minimizar el tiempo de inactividad y garantizar la continuidad de las operaciones en caso de incidentes.

En resumen, el objetivo primordial de este plan es garantizar la protección y el manejo seguro de la información gestionada por el Concejo Municipal de Cartago, fortaleciendo así la confianza de la comunidad en la institución y en la integridad de sus servicios públicos.

2. ALCANCE

El alcance del Plan de Seguridad y Privacidad de la Información para el Concejo Municipal de Cartago abarca todos los aspectos relacionados con la protección, gestión y manejo seguro de la información dentro de la Corporación. Este plan se aplica a todos los activos de información, procesos y recursos tecnológicos que son propiedad del Concejo Municipal, así como a aquellos que están bajo su responsabilidad, incluyendo, pero no limitándose a:

Datos de los ciudadanos: Información personal y confidencial de los ciudadanos, incluyendo datos de identificación, registros civiles, y cualquier otra información sensible gestionada por el Concejo Municipal en el ejercicio de sus funciones.

Registros gubernamentales: Documentación oficial, actas, resoluciones, contratos y otros registros gubernamentales que deben ser protegidos y mantenidos de acuerdo con las leyes y regulaciones aplicables.

Infraestructura tecnológica: Sistemas de información, redes, servidores, dispositivos de almacenamiento y cualquier otro componente de infraestructura tecnológica utilizado para el procesamiento, almacenamiento y transmisión de información dentro del ámbito del Concejo Municipal.

Personal y procesos: Actividades y prácticas relacionadas con el manejo de la información por parte del personal del Concejo Municipal, incluyendo políticas de acceso, procedimientos de seguridad, capacitación del personal y gestión de incidentes de seguridad.

El alcance de este plan se extiende a todas las áreas del Concejo Municipal de Cartago, así como a cualquier tercero o contratista que tenga acceso a los activos de información de la Corporación. Se espera que todos los empleados, contratistas y partes interesadas involucrados en el manejo de la información cumplan con las políticas, procedimientos y controles establecidos en este plan para garantizar la seguridad y la privacidad de la información en todas las etapas de su ciclo de vida.

3. MARCO NORMATIVO

Constitución Política de Colombia. Artículos 15, 209 y 269.

Ley 1581 de 201: Por la cual se dictan disposiciones generales para la protección de datos personales.

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 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.

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.

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 Único 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 1080 de 2015: Por medio del cual se expide el Decreto Único Reglamentario del Sector Cultura.

Decreto 1081 de 2015: Por medio del cual se expide el Decreto Reglamentario del Sector Presidencia.

Decreto 1083 de 2015: "Por medio del cual se expide el Decreto Único Reglamentario del Sector de Función Pública", el cual establece las políticas de Gestión y Desempeño Institucional, entre las que se encuentran las de "11. Gobierno Digital, antes Gobierno en Línea" y "12. Seguridad Digital".

CONPES 3854 de 2016: Política Nacional de Seguridad digital. 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 612 de 2018: Por el cual se fijan directrices para la integración de los planes institucionales y estratégicos al Plan de Acción por parte de las entidades del Estado.

Decreto 2106 de 2019: establece que las autoridades que realicen trámites, procesos y procedimientos por medios digitales, deberán disponer de una estrategia de seguridad digital siguiendo los lineamientos que emita el Ministerio de Tecnologías de la Información y las Comunicaciones.

Ley 1952 de 2019: Por medio de la cual se expide el código general disciplinario.

Resolución 500 de 2021: "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".

4. DEFINICIONES

El Modelo incluye la siguiente terminología para su comprensión:

• Acceso a la Información Pública: Derecho fundamental consistente en la facultad que tienen todas las personas de conocer sobre la existencia y acceso a la información pública en posesión o bajo control de sujetos obligados. (Ley 1712 de 2014, art 4).

• Activo: En relación con la seguridad de la información, se refiere a cualquier información o elemento relacionado con el tratamiento de ésta (sistemas, soportes, edificios, personas, etc.) que tenga valor para la organización. (ISO/IEC 27000).
• Activos de Información y recursos: Se refiere a elementos de hardware y de software de procesamiento, almacenamiento y comunicaciones, bases de datos y procesos, procedimientos y recursos humanos asociados con el manejo de los datos y la información misional, operativa y administrativa de cada entidad, órgano u organismo. (CONPES 3854 de 2016).

• Archivo: Conjunto de documentos, sea cual fuere su fecha, forma y soporte material, acumulados en un proceso natural por una persona o Entidad pública o privada, en el transcurso de su gestión, conservados respetando aquel orden para servir como testimonio e información a la persona o institución que los produce y a los ciudadanos, o como fuentes de la historia. También se puede entender como la institución que está al servicio de la gestión administrativa, la información, la investigación y la cultura. (Ley 594 de 2000, art 3).

• Amenazas: Causa potencial de un incidente no deseado, que puede provocar daños a un sistema o a la organización. (ISO/IEC 27000).

• Análisis de Riesgo: Proceso para comprender la naturaleza del riesgo y determinar el nivel de dicho riesgo. (ISO/IEC 27000).

• Auditoría: Proceso sistemático, independiente y documentado para obtener evidencias de auditoría y obviamente para determinar el grado en el que se cumplen los criterios de auditoría. (ISO/IEC 27000).

• Autorización: Consentimiento previo, expreso e informado del Titular para llevar a cabo el Tratamiento de datos personales (Ley 1581 de 2012, art 3).

• Bases de Datos Personales: Conjunto organizado de datos personales que sea objeto de Tratamiento (Ley 1581 de 2012, art 3).

• Ciberseguridad: Protección de activos de información, mediante el tratamiento de las amenazas que ponen en riesgo la información que se procesa, almacena y transporta mediante los sistemas de información que se encuentran interconectados.

• Ciberespacio: Es el ambiente tanto físico como virtual compuesto por computadores, sistemas computacionales, programas computacionales (software), redes de telecomunicaciones, datos e información que es utilizado para la interacción entre usuarios. (Resolución CRC 2258 de 2009).

• Control: Las políticas, los procedimientos, las prácticas y las estructuras organizativas concebidas para mantener los riesgos de seguridad de la información por debajo del nivel de riesgo asumido. Control es también utilizado como sinónimo de salvaguarda o contramedida. En una definición más simple, es una medida que modifica el riesgo.

• Datos Abiertos: Son todos aquellos datos primarios o sin procesar, que se encuentran en formatos estándar e interoperables que facilitan su acceso y reutilización, los cuales están bajo la custodia de las Entidades públicas o privadas que cumplen con funciones públicas y que son puestos a disposición de cualquier ciudadano, de forma libre y sin restricciones, con el fin de que terceros puedan reutilizarlos y crear servicios derivados de los mismos (Ley 1712 de 2014, art 6).

• Datos Personales: Cualquier información vinculada o que pueda asociarse a una o varias personas naturales determinadas o determinables. (Ley 1581 de 2012, art 3).

• Datos Personales Públicos: Es el dato que no sea semiprivado, privado o sensible. Son considerados datos públicos, entre otros, los datos relativos al estado civil de las personas, a su profesión u oficio y a su calidad de comerciante o de servidor público. Por su naturaleza, los datos públicos pueden estar contenidos, entre otros, en registros públicos, documentos públicos, gacetas y boletines oficiales y sentencias judiciales debidamente ejecutoriadas que no estén sometidas a reserva. (Decreto 1377 de 2013, art 3).

• Datos Personales Privados: Es el dato que por su naturaleza íntima o reservada sólo es relevante para el titular. (Ley 1581 de 2012, art 3 literal h).

- Datos Personales Mixtos: Para efectos de este documento es la información que contiene datos personales públicos junto con datos privados o sensibles.

- Datos Personales Sensibles: Se entiende por datos sensibles aquellos que afectan la intimidad del Titular o cuyo uso indebido puede generar su discriminación, tales como aquellos que revelen el origen racial o étnico, la orientación política, las convicciones religiosas o filosóficas, la pertenencia a sindicatos, organizaciones sociales, de derechos humanos o que promueva intereses de cualquier partido político o que garanticen los derechos y garantías de partidos políticos de oposición, así como los datos relativos a la salud, a la vida sexual, y los datos biométricos. (Decreto 1377 de 2013, art 3)

- Derecho a la Intimidad: Derecho fundamental cuyo núcleo esencial lo constituye la existencia y goce de una órbita reservada en cada persona, exenta de la intervención del poder del Estado o de las intromisiones arbitrarias de la sociedad, que le permite a dicho individuo el pleno desarrollo de su vida personal, espiritual y cultural (Jurisprudencia Corte Constitucional).

- 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. (ISO/IEC 27000).

- Información Pública Clasificada: Es aquella información que estando en poder o custodia de un sujeto obligado en su calidad de tal, 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, siempre que se trate de las circunstancias legítimas y necesarias y los derechos particulares o privados consagrados en el artículo 18 de la Ley 1712 de 2014. (Ley 1712 de 2014, art 6).

- Información Pública 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)

- Ley de Habeas Data: Se refiere a la Ley Estatutaria 1266 de 2008.

- Ley de Transparencia y Acceso a la Información Pública: Se refiere a la Ley Estatutaria 1712 de 2014.

- Mecanismos de protección de datos personales: Lo constituyen las distintas alternativas con que cuentan las Entidades destinatarias para ofrecer protección a los datos personales de los titulares tales como acceso controlado, anonimización o cifrado.

- 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) y según Norma NTC-ISO 22301 del 20 de noviembre de 2019, Seguridad y resiliencia. Sistema de gestión de continuidad del negocio. Requisitos. Se define en el numeral 3.4 como: Información documentada que

orienta a una organización para responder una interrupción y reanudar, recuperar y restaurar la oferta de productos y servicios de acuerdo con sus objetivos de continuidad del negocio.

- 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).

- Registro Nacional de Bases de Datos: Directorio público de las bases de datos sujetas a Tratamiento que operan en el país. (Ley 1581 de 2012, art 25).

- Responsabilidad Demostrada: Conducta desplegada por los responsables o Encargados del tratamiento de datos personales bajo la cual a petición de la Superintendencia de Industria y Comercio deben estar en capacidad de demostrarle a dicho organismo de control que han implementado medidas apropiadas y efectivas para cumplir lo establecido en la Ley 1581 de 2012 y sus normas reglamentarias.

- Responsable del Tratamiento de Datos: Persona natural o jurídica, pública o privada, que por sí misma o en asocio con otros, decida sobre la base de datos y/o el tratamiento de los datos. (Ley 1581 de 2012, art. 3).

- Riesgo: Posibilidad de que una amenaza concreta pueda explotar una vulnerabilidad para causar una pérdida o daño en un activo de información. Suele considerarse como una combinación de la probabilidad de un evento y sus consecuencias. (ISO/IEC 27000).

- Seguridad de la información: Preservación de la confidencialidad, integridad, y disponibilidad de la información en cualquier medio: impreso o digital. (ISO/IEC 27000).

- Seguridad digital: Preservación de la confidencialidad, integridad, y disponibilidad de la información que se encuentra en medios digitales.

- Titulares de la información: Personas naturales cuyos datos personales sean objeto de Tratamiento. (Ley 1581 de 2012, art 3)

- Tratamiento de Datos Personales: Cualquier operación o conjunto de operaciones sobre datos personales, tales como la recolección, almacenamiento, uso, circulación o supresión. (Ley 1581 de 2012, art 3).

- Trazabilidad: Cualidad que permite que todas las acciones realizadas sobre la información o un sistema de tratamiento de la información sean asociadas de modo inequívoco a un individuo o Entidad. (ISO/IEC 27000).

- Vulnerabilidad: Debilidad de un activo o control que puede ser explotada por una o más amenazas. (ISO/IEC 27000).

- Partes interesadas (Stakeholder): Persona u organización que puede afectar a, ser afectada por o percibirse a sí misma como afectada por una decisión o actividad.

5. TRASCENDENCIA DEL MODELO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

El Modelo de Seguridad y Privacidad de la Información (MSPI) se presenta como un marco estructurado que respalda el habilitador transversal de la Seguridad de la Información en el Concejo Municipal de Cartago. Este habilitador, según el Manual de Gobierno Digital, tiene como objetivo primordial que las entidades públicas, incluyendo el Concejo Municipal de Cartago, implementen lineamientos de seguridad de la información en todos sus procesos, trámites, servicios, sistemas de información e infraestructura. El propósito es preservar la confidencialidad, integridad, disponibilidad y privacidad de los datos.

El MSPI, que contempla 6 niveles de madurez, se convierte así en la base para la implementación de la seguridad de la información en el Concejo Municipal. Estos niveles de madurez han sido previamente determinados a través de la herramienta de diligenciamiento del instrumento de medición del MSPI de MinTIC.

Esta metodología describe los niveles de evaluación aplicados a la seguridad de la información y proporciona un marco claro para la mejora continua en este ámbito.

El Concejo Municipal de Cartago, al adoptar el MSPI como parte de su enfoque en seguridad de la información, se compromete a seguir estos niveles de madurez para fortalecer progresivamente sus controles de seguridad y privacidad. Esto implica una evaluación inicial de su estado actual de seguridad de la información, seguida de la implementación de medidas específicas para avanzar en los diferentes niveles de madurez.

A través del MSPI, el Concejo Municipal de Cartago podrá establecer una estructura sólida y coherente para la gestión de la seguridad de la información, garantizando así la protección adecuada de los datos de los ciudadanos y el cumplimiento de las regulaciones y normativas pertinentes en materia de seguridad y privacidad.

El Modelo de Seguridad y Privacidad de la Información - MSPI, contempla 6 niveles de madurez"; los niveles de madurez han sido determinados en la etapa previa a la actualización del presente documento a partir de la herramienta de diligenciamiento del instrumento de medición del MSPI de MinTIC, cuya metodología describe los niveles de evaluación aplicados a la seguridad de la información en el instrumento:

- Inexistente
- Inicial
- Repetible
- Efectivo
- Gestionado y;
- Optimizado

6. PLAN DE IMPLEMENTACIÓN DEL MODELO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

No.	DESCRIPCION DE LA ACTIVIDAD	RESPONSABLE	TIEMPO

No.	DESCRIPCION DE LA ACTIVIDAD	RESPONSABLE	TIEMPO
1	Identificar los riesgos de seguridad digital y Diseñar los controles de seguridad necesarios para garantizar la seguridad digital y la protección de los datos personales en el marco de los acuerdos de intercambio de información de la entidad con otros.	Secretaria General y Apoyo Tics.	2024-2027
2	Actualización del Diagnóstico del Modelo de Seguridad y Privacidad de la Información.	Secretaria General y Apoyo Tics.	2024-2027
3	Identificación, clasificación, valoración y asignación de responsables de Activos de Información (Software, Hardware, Redes y Telecomunicaciones, Servicios de Tecnologías de Información y de las Comunicaciones, Soportes, Servicios de Tecnologías de Información y de las Comunicaciones contratados)	Secretaria General y Apoyo Tics.	2024-2027
4	Identificación, valoración y tratamiento de riesgos de Seguridad Digital desde el Componente de Seguridad Informática.	Secretaria General y Apoyo Tics.	2024-2027
5	Gestión de Incidentes de Seguridad Informática	Secretaria General y Apoyo Tics.	2024-2027
6	Apropiación de la Seguridad Informática	Secretaria General y Apoyo Tics.	2024-2027
7	Implementación de Controles de Seguridad Informática	Secretaria General y Apoyo Tics.	2024-2027
8	Implementación de acciones para la continuidad de la seguridad informática, de la infraestructura y servicios de tecnologías de información.	Secretaria General y Apoyo Tics.	2024-2027
9	Definir lineamientos para la Seguridad Informática e infraestructura tecnológica de los servicios de tecnologías de información y comunicaciones, que la entidad adquiera en la Nube	Secretaria General y Apoyo Tics.	2024-2027
10	Documentar el manual de seguridad de la información para la protección de los datos personales en sistemas de información que realicen tratamiento de datos personales	Secretaria General y Apoyo Tics.	2024-2027