CONCEJO MUNICIPAL DE CARTAGO

PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACION PERIODO 2024 AL 2027

CARTAGO, VIGENCIA 2024

INTRODUCCION

La estrategia de Gobierno en Línea, liderada por el Ministerio TIC, tiene como objetivo, garantizar el máximo aprovechamiento de las tecnologías de la información y las comunicaciones, con el fin de contribuir con la construcción de un Estado más participativo, más eficiente y transparente. La planificación e implementación del Modelo de Seguridad y Privacidad de la Información – MSPI, en el Concejo está determinado por las necesidades y objetivos, los requisitos de seguridad, los procesos misionales y el tamaño y estructura de la Corporación Edilicia.

El Modelo de Seguridad y Privacidad de la Información – MSPI, conduce a la preservación de la confidencialidad, integridad, disponibilidad de la información, permitiendo garantizar la privacidad de los datos, mediante la aplicación de un proceso de gestión del riesgo, brindando confianza a las partes interesadas acerca de la adecuada gestión de riesgos.

A través del decreto único reglamentario 1078 de 2015, del sector de Tecnologías de Información y las Comunicaciones, se define el componente de seguridad y privacidad de la información, como parte integral de la estrategia GEL. Para el desarrollo del componente de Seguridad y Privacidad de la Información, se ha elaborado un conjunto de documentos asociados al Modelo de Seguridad y Privacidad de la Información, los cuales a lo largo de los últimos años, han sido utilizados por las diferentes entidades tanto del orden nacional como territorial, para mejorar sus estándares de seguridad de la información. El Modelo de Seguridad y Privacidad para estar acorde con las buenas prácticas de seguridad será actualizado periódicamente; así mismo recoge además de los cambios técnicos de la norma, legislación de la Ley de Protección de Datos Personales, Transparencia y Acceso a la Información Pública, entre otras, las cuales se deben tener en cuenta para la gestión de la información; de otro lado el MSPI especifica los nuevos lineamientos que permiten la adopción del protocolo IPv6 en el Estado Colombiano.

El Modelo de Seguridad y Privacidad de la Información se encuentra alineado con el Marco de Referencia de Arquitectura TI y soporta transversalmente los otros componentes de la Estrategia GEL: TIC para Servicios, TIC para Gobierno Abierto y TIC para Gestión.

El presente modelo pretende facilitar la comprensión del proceso de construcción de una política de privacidad por parte de la entidad, que permita fijar los criterios que seguirán para proteger la privacidad de la información y los datos, así como de los procesos y las personas vinculadas con dicha información.

Finalmente, a nivel metodológico es importante tener presente que se han incluido una serie de guías en cada una de las fases del modelo, para que los destinatarios del mismo tengan claridad de cuáles son los resultados a obtener y como desarrollarlos.

PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACION

1. OBJETIVOS

1.1 OBJETIVOS GENERALES

Establecer lineamientos para la implementación de políticas que garanticen la administración, manejo y control de la seguridad y privacidad de la información del Concejo Municipal de Cartago-Valle.

1.2 OBJETIVOS ESPECIFICOS

- Implementar políticas y procedimientos enfocados en la de seguridad de la información.

- Mitigar los riesgos asociados a la seguridad de la Información que afecten la integridad, confidencialidad, disponibilidad y privacidad de la Información del Concejo Municipal de Cartago – Valle.

2. ALCANCE

El presente plan aplica a los procesos definidos en el Concejo Municipal, donde haya recolección, procesamiento, almacenamiento, recuperación, intercambio y consulta de información, para el desarrollo de la misión institucional y cumplimiento de sus objetivos estratégicos.

3. MARCO NORMATIVO

Ley 527 de 1999 “por medio de 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 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”.

Decisión Andina 351 de 2015 “Régimen común sobre 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, el cual modificó el Decreto 1083 de 2015 – Modelo Integrado de Planeación y Gestión

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 tiene como responsables de la implementación, seguimiento y mantenimiento de la Política del Plan de Seguridad y Privacidad de la información lo siguiente:

- El presidente del Concejo Municipal de Cartago-Valle, quien velara por el cumplimiento de la Política de Seguridad y privacidad de la Información.

• El funcionario delegado de las TIC debe velar por la formulación e implementación de la Política de seguridad y privacidad de la información.

• El profesional Universitario o asesor externo encargado de la gestión de TICS será el encargado de desarrollar la implementación de la Política de seguridad y privacidad de la información.

• Todos los funcionarios y/o contratistas y demás partes interesadas del Concejo Municipal de Cartago -Valle, son responsables del cumplimiento obligatorio de la Política de seguridad y Privacidad de la Información y en caso de no cumplir se reserva el derecho de tomar las medidas correspondientes según el caso.

6. POLITICAS

El Concejo Municipal de Cartago-Valle, divulga los objetivos y alcances de la seguridad de la información dentro de la entidad, que son efectivos por medio de controles de seguridad, con el fin de mantener, gestionar y mitigar el riesgo como se estable en el Plan de Tratamiento de Riesgos, garantizando así la continuidad de los servicios y disminuyendo la probabilidad de amenazas que puedan afectar los procesos internos para el cumplimiento de la prestación del servicio.

• **Identificación, clasificación y valoración de activos de información:** Cada proceso, bajo supervisión y con base en el inventario de activos del Concejo Municipal de Cartago-Valle, siempre se debe estar actualizando en donde se incorpore la clasificación, valoración, ubicación y acceso de la información y demás características identificas por la Alta dirección permitiendo así la administración eficiente de cada proceso garantizando la disponibilidad, integridad y confidencialidad de dicha información.

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

Todos los servidores públicos del Concejo Municipal, independiente del tipo de vinculación laboral o contractual, o de los procesos al que pertenezca y del nivel de funciones o actividades que desempeñe deben contar con un perfil de uso de los recursos de información, incluyendo el hardware y software asociado.

Por ende, se debe contar con un directorio completo y actualizado de los perfiles creados. La responsabilidad de custodia de cualquier documento o archivo generado

dentro del Concejo Municipal, usado o producido por algún funcionario y/o contratista que se retira, o cambia de cargo, recae en la Secretaria General, demás secretarios o supervisor del contrato; Aclarando que el proceso de cadena de custodia de la información debe hacer parte integral de un procedimiento de terminación de la relación contractual o de cambio de cargo.

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

El acceso de usuarios no registrados solo debe estar autorizado por la Presidencia, de manera de información institucional, igualmente el servicio de internet al que puedan acceder debe estar protegido con una contraseña, contando con una restricción de sitios web no autorizados. Si los usuarios invitados no realizaron el debido proceso de registro, no se permitirá el acceso a cualquier otro tipo de recursos de información, aplicación y/o herramientas TIC.

- **Seguridad Física y del entorno**

Seguridad en los equipos: Los servidores o equipos de cómputo que contengan información institucional deben estar en un ambiente seguro y protegido por lo menos con:

- ✓ Controles de acceso y seguridad física.
- ✓ Sistemas eléctricos regulados y respaldados por fuentes de potencia ininterrumpida (UPS).

Además, toda información institucional en formato digital debe ser mantenida en los servidores y/o unidades extraíbles aprobados por la Secretaria General. También se debe asegurar que la infraestructura esté cubierta, con mantenimiento y soporte adecuados tanto para el hardware como para el software y las estaciones de trabajo deben ser operadas por funcionarios de la Corporación Edilicia el cual deben estar capacitados acerca del contenido de esta política y de las responsabilidades personales en el uso y administración de la información institucional. Se deben incluir los medios que alojan copias de seguridad el cual deben ser conservados de forma correcta de acuerdo con las políticas y estándares establecidos.

- **Administración de las comunicaciones y operaciones**

Reporte y revisión de incidentes de seguridad: El personal vinculado del Concejo Municipal de Cartago-Valle, debe realizar el reporte de una manera eficiente y con responsabilidad de las presuntas violaciones de seguridad detectadas y se deben

reportar a la presidencia o cuando la ocasión lo amerite si es un caso especial y podrá realizarse la directamente por la persona que encuentre el incidente o novedad.

Se debe diseñar, mantener y difundir las normas, procesos y guías para el reporte y revisión de incidentes de seguridad el cual se mantendrá procedimientos escritos para la operación de dichas actividades sin afectar el desarrollo normal de la prestación del servicio y asegurando la confiabilidad de la información.

- **Protección contra software malicioso y hacking.**

Se debe proteger todos los sistemas de información que involucre los controles humanos, físicos técnicos y administrativos para no incurrir en daños, se elaborará y mantendrá un conjunto de políticas, normas, estándares, procedimientos que garanticen la mitigación de riesgos asociados a amenazas de software malicioso y técnicas de hacking que pueda afectar la prestación del servicio. Como control básico, todas las estaciones de trabajo del Concejo Municipal deben estar protegidas por software antivirus con capacidad de actualización automática en cuanto a firmas de virus.

- **Copias de Seguridad**

Toda información que se encuentre contenida en el inventario de activos de información o que sea de interés para un proceso siempre debe estar ser respaldada con copias de seguridad tomadas de acuerdo con los procedimientos documentados y probados por el Sistema de Gestión Pública-MIPG.

El procedimiento debe incluir actividades de almacenamiento, administración y custodia de las copias de seguridad incluyendo lugares seguros y control de registros de dichas copias. Dentro del procedimiento debe quedar claro que se deben efectuar auditorías aleatorias que permitan determinar el correcto funcionamiento de los procesos de copia de seguridad.

Tener en cuenta que la creación de copias de seguridad de archivos usados, custodiados o producidos por usuarios individuales es responsabilidad exclusiva de dichos usuarios, es decir la responsabilidad de realizar las copias y mantenerlas actualizadas, recae directamente sobre cada dueño de los activos de la información de la Entidad.

- Intercambio de Información con Entidades Externas. Las peticiones o solicitudes de información por parte de entes externos deben ser aprobadas por la Alta dirección, y ser redireccionados a los responsables del manejo y custodia dicha información. Tener en cuenta que la información solicitada por parte de los entes externos debe ser realizada por un medio valido que permita el registro de la solicitud, donde se pueda identificar el remitente, el asunto y la fecha aclarando que toda información institucional debe ser manejada de acuerdo con la normatividad legal vigente.

- **Instalación de Software**

Todas las instalaciones de software que se realicen sobre sistemas operativos previamente instalados en el Concejo Municipal de Cartago-Valle, deben ser aprobadas por la Alta dirección, de acuerdo con los procedimientos establecidos para tal fin.

El funcionario encargado en la Gestión de las TIC debe desinstalar cualquier software ilegal y registrar este hecho como un incidente de seguridad para su respectiva investigación además debe tener un inventario del software autorizado para su uso institucional.

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

Las claves de administrador de los diferentes sistemas deben ser conservadas por la Secretaria General y el funcionario encargado en la Gestión de las TIC y deben ser cambiadas en intervalos regulares de tiempo y en todo caso cuando el personal adscrito al cargo cambie. Adicionalmente se debe elaborar, mantener y actualizar el procedimiento para la correcta definición, uso y complejidad de las claves de usuario.

Una vez se termine la relación contractual o laboral del personal con el Concejo Municipal de Cartago-Valle, se debe expedir un certificado de suspensión y/o cancelación de las cuentas creadas al respectivo usuario, en todos y cada uno de los sistemas de información en los cuales estuviera activo (correo electrónico, sistemas de información automatizados, entre otros); se determinara cualquier será el tiempo prudencial por la posible renovación de la relación contractual o laboral, o una vez transcurrido el tiempo se dará de baja las cuentas si no hay renovación ninguna.

- **Uso adecuado de Internet**

El Concejo Municipal de Cartago-Valle es consciente de la importancia del servicio de Internet como una herramienta fundamental para el desempeño de labores que proporcionará los recursos necesarios para asegurar su disponibilidad a los servidores públicos y demás partes de interés que así lo requieran.

a) El proceso de TIC debe proporcionar los recursos necesarios para la implementación, administración y mantenimiento requeridos para la prestación segura del servicio de Internet, bajo las restricciones de los perfiles de acceso establecidos.

b) El proceso de TIC debe diseñar e implementar mecanismos que permitan la continuidad o restablecimiento del servicio de Internet en caso de contingencia interna.

c) El proceso de TIC debe monitorear continuamente el canal o canales del servicio de Internet.

d) El proceso de TIC debe generar registros de la navegación y los accesos de los usuarios a Internet, así como establecer e implantar el monitoreo sobre la utilización del servicio de Internet.

7. DESARROLLO DEL PLAN

7.1 Metodología de implementación

La metodología de implementación del Plan de Seguridad y Privacidad para el Concejo está basada en el ciclo PHVA (Planificar-Hacer-Verificar-Actuar) y lo establecido en el Modelo de Seguridad y Privacidad del Ministerio de Tecnologías de la Información y las Comunicaciones - MinTIC:

A la fecha se realizaron las actividades de planificación que incluyen el contexto de la entidad, planeación, soporte, estado actual de la información.

En las actividades de implementación se incluyen la elaboración de una guía y planeación operacional de seguridad de la información.

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.

NIVEL DE MADUREZ

Según el modelo de seguridad y privacidad de la información establecido por el Ministerio de Tecnologías de Información el Concejo se encuentra en el nivel incipiente de implementación donde se deben ejecutar las acciones trazadas en la etapa previa de planeación de manera que la entidad diseñe un modelo de privacidad que le permita cumplir con los mínimos legales y generar una política de privacidad que le permita la correcta gestión de la información.

7.2 Mapa de Ruta Periodo 2024

No.	Actividad	Responsable	Producto o Resultado Esperado	Fecha Inicio	Fecha Final
1. Autodiagnóstico					
1.1	Realizar actualización de autodiagnóstico de evaluación de MSPI	Grupo de Apoyo	Autodiagnóstico diligenciado	04/01/2024	29/03/2024
2. Activos de información					
2.1	Actualización instrumentos de identificación de activos de información	Grupo de Apoyo	Instrumentos de identificación de activos de información	01/04/2024	31/05/2024
2.2	Actualización de Activos de información	Todos los Procesos Equipo de Apoyo MIPG	Matrices de activos	31/05/2024	30/06/2024
2.3	Publicación Instrumentos de activos de información del Municipio	Grupo de Apoyo Equipo de Apoyo MIPG	Matrices de activos en la página web	01/07/2024	5/07/2024