ALCALDÍA MUNICIPAL DE CHÍA

DECRETO NÚMERO 545 DE 2024
(30 AGO 2024)

"POR EL CUAL SE CONFORMA EL COMITÉ DE SEGURIDAD DE LA INFORMACIÓN MUNICIPIO DE CHÍA Y SE DEFINEN SUS FUNCIONES"

EL ALCALDE DEL MUNICIPIO DE CHÍA - CUNDINAMARCA

En uso de sus facultades Constitucionales y Legales, especialmente las establecidas artículo 315 de la Constitución Política de Colombia, Ley 136 de 1994, modificada por la Ley 1551 de 2012, demás normas concordantes, y

CONSIDERANDO

Que los numerales 1, 3 y 10 del artículo 315 de la Constitución Política de Colombia, en su orden, consagran como atribuciones del Alcalde: 1. Cumplir y hacer cumplir la Constitución, la ley, los decretos del gobierno, las ordenanzas, y los acuerdos del concejo; 3. Dirigir la acción administrativa del municipio; asegurar el cumplimiento de las funciones y la prestación de los servicios a su cargo 10.- Las demás que la Constitución y la ley le señalen".

Que, conforme al principio de "masificación del gobierno en línea" hoy Gobierno Digital, consagrado en el numeral 8 del artículo 2 de la 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-,(...)", "(...) las entidades públicas deberán adoptar todas las medidas necesarias para garantizar el máximo aprovechamiento de las Tecnologías de la Información y las Comunicaciones (TIC) en el desarrollo de sus funciones (...)".

Que, en virtud del numeral 2 del artículo 17 de la Ley 1341 de 2009, el Ministerio de Tecnologías de la Información y las Comunicaciones tiene entre sus objetivos "(...) 2. Promover el uso y apropiación de las Tecnologías de la Información y las Comunicaciones entre los ciudadanos, las empresas, el Gobierno y demás instancias nacionales como soporte del desarrollo social, económico y político de la Nación"

Que, la Ley 1437 de 2011, "Por la cual se expide el Código de Procedimiento Administrativo y de lo Contencioso Administrativo", a través de su artículo 64 faculta al Gobierno Nacional para definir los estándares y protocolos que deberán cumplir las autoridades para incorporar en forma gradual los medios electrónicos en los procedimientos administrativos, entre los que se cuentan los relativos a la seguridad digital.

Que, el artículo 230 de la Ley 1450 de 2011, modificado por el artículo 148 de la Ley 1955 de 2019 señala que "Todas las entidades de la administración pública deberán adelantar las acciones que señale el Gobierno Nacional a través del Ministerio de Tecnologías de la información y las Comunicaciones para la implementación de la política de Gobierno Digital". Dentro de las acciones prioritarias se encuentra el cumplimiento de los lineamientos y estándares para el incremento de la confianza y la seguridad digital.

Que, con el objetivo de generar un proceso continuo de gestión de riesgos adaptable a nuevas tecnologías actuales y futuras, las autoridades deberán implementar tecnologías y seguridad cibernética que les permitan operar de una manera segura y generando confianza en los servicios ciudadanos ofrecidos.

Que el artículo 2.2.9.1.2.1. del Decreto 1078 de 2015, subrogado por el artículo 1 del Decreto 767 de 2022, determinó que uno de los habilitadores de la Política de Gobierno Digital es el de Seguridad y Privacidad de la Información, el cual busca que los sujetos obligados desarrollen capacidades a través de la implementación de los lineamientos de seguridad y privacidad de la información en todos sus procesos, trámites, servicios, sistemas de información, infraestructura y en general, en todos los activos de información, con el fin de preservar la confidencialidad, integridad, disponibilidad y privacidad de los datos. El artículo 2.2.22.2.1 del Decreto 1083 de 2015, 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".

Que en los términos del Decreto Nacional No. 1078 de 2015, "Por medio del cual se expide el Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones" en el Artículo 2.2.17.5.6, las entidades que manejen información pública, deberán propender por la seguridad de la información y la seguridad digital, así como de contar con una estrategia de seguridad y privacidad de la información, seguridad digital y continuidad de la prestación del servicio en la cual, deberán hacer periódicamente una evaluación del riesgo de seguridad digital que incluya una identificación de las mejoras a implementar en su Sistema de Administración del Riesgo Operativo. Para lo anterior, deben contar con normas, políticas, procedimientos, recursos técnicos, administrativos y humanos necesarios para gestionar efectivamente el riesgo. En ese sentido, deben adoptar los lineamientos para la gestión de la seguridad de la información y seguridad digital que emita el Ministerio de Tecnologías de la Información y las Comunicaciones.

Que los lineamientos generales para fortalecer la gobernanza de la seguridad digital, la identificación de infraestructuras críticas cibernéticas y servicios esenciales, la gestión de riesgos y la respuesta a incidentes de seguridad digital, en los términos del Decreto Nacional No. 1078 de 2015, deben ser acatados por las entidades que conforman la administración pública en los términos del artículo 39 de la ley 489 de 1998 y los particulares que cumplen funciones públicas o administrativas, quienes se denominan autoridades, de las cuales se puedes traer a colación las entre otras las siguientes;

(...) Las gobernaciones, las alcaldías, las secretarias de despacho y los departamentos administrativos son los organismos principales de la Administración en el correspondiente nivel territorial. Los demás les están adscritos o vinculados, cumplen sus funciones bajo su orientación, coordinación y control en los términos que señalen la ley, las ordenanzas y los acuerdos, según el caso. (...)

Que los objetivos generales del modelo de gobernanza de la seguridad digital, conforme con lo estableciendo en el Decreto Nacional 1078 de 2015, son el facilitar la participación, articulación e interacción de las múltiples partes interesadas para fortalecer las capacidades en la gestión de riesgos de seguridad digital y de esta manera lograr un abordaje integral que promueva el adecuado aprovechamiento de las oportunidades que ofrece el entorno digital, así como de establecerse dentro de los objetivos específicos los siguientes:

1. Fortalecer el liderazgo y orientación estratégica de la seguridad digital del país con un enfoque participativo y colaborativo.

2. Impulsar un enfoque integral para la gestión de riesgos de Seguridad digital.

3. Proveer mecanismos para coordinar la gestión y respuesta a incidentes de seguridad digital.

4. Promover la confianza para el intercambio de información y la gestión del conocimiento sobre seguridad digital en el país.

5. Impulsar la generación de capacidades de seguridad digital de las partes interesadas de manera eficiente y colaborativa.

Que el CONPES 3854 de 2016 señala que la Política Nacional de Seguridad Digital, tendrá como objetivos: (i) Establecer un marco institucional para la seguridad digital consistente, con un enfoque de gestión de riesgos, (ii) Crear las condiciones para que las partes interesadas gestionen el riesgo de seguridad digital en sus actividades socioeconómicas y se genere confianza en el uso del entorno digital, (iii) Fortalecer la seguridad de los individuos y del Estado en el entorno digital, a nivel nacional y transnacional , con un enfoque de gestión de riesgos, (iv) Fortalecer la defensa y soberanía nacional en el entorno digital, con un enfoque de gestión de riesgos, (v) Generar mecanismos permanentes y estratégicos para impulsar la cooperación, colaboración y asistencia en seguridad digital, a nivel nacional e internacional.

Que el citado CONPES define la seguridad digital como la situación de normalidad y de tranquilidad en el entorno digital (ciberespacio), derivada de la realización de los fines esenciales del Estado mediante (i) la gestión del riesgo de seguridad digital; (ii) la implementación efectiva de medidas de ciberseguridad; y (iii) el uso efectivo de las capacidades de ciberdefensa; que demanda la voluntad social y política de las múltiples partes interesadas y de los ciudadanos del país.

Que la Resolución No. 500 de 2021 del Ministerio de Tecnologías de la Información y las Comunicaciones, establece lineamientos generales para la implementación del Modelo de Seguridad y Privacidad de la Información - MSPI, la guía de gestión de riesgos de seguridad de la Información y el procedimiento para la gestión de los incidentes de seguridad digital, y, establece los lineamientos y estándares para la estrategia de seguridad digital, a los sujetos obligados señalados en el artículo 2.2.9.1.1.2 del Decreto Nacional No. 1078 de 2015.

Que el Ministerio de Tecnologías de la Información y las Comunicaciones, a través de la Resolución No 500 de 2021, artículo 5, establece que los sujetos obligados deben adoptar la estrategia de seguridad digital en la que se integren los principios, políticas, procedimientos, guías, manuales, formatos y lineamientos para la gestión de la seguridad de la información digital. Dicha estrategia se debe incluir en el Plan de Seguridad y Privacidad de la Información que se integra al Plan de Acción en los términos artículo 2.2.22.3.14. del capítulo 3 del Título 22 de la Parte 2 del Libro 2 del Decreto 1083 de 2015, Único Reglamentario del Sector de Función Pública, o la norma que la modifique, adicione, subrogue o derogue. Así como, adoptar el Modelo de Seguridad y Privacidad de la Información – MSPI señalado en el Anexo 1 de la misma resolución, como habilitador de la política de Gobierno Digital.

Que, a través de este instrumento, los encargados de seguridad pueden encontrar una guía para establecer la hoja de ruta para la implementación de la estrategia de

seguridad digital, de acuerdo con las características propias de cada entidad. Esto permite afianzar la seguridad digital como habilitador transversal para la protección de los activos de información por medio de los documentos y acciones generadas por los equipos técnicos.

Que el Modelo de Seguridad y Privacidad se ha diseñado como guía para que las entidades de gobierno puedan implementar gestión de la seguridad de la información en sus procesos, integrando actividades propias de la seguridad de la información y teniendo en cuenta la necesidad de fortalecer el aseguramiento de la infraestructura y los servicios TI, a través de guías y modelos de documentos editables, entre los que encontramos por ejemplo el Anexo 1 del Modelo de Seguridad y Privacidad de la Información manifiesta que se debe crear un Comité de Seguridad y se plantea un modelo del Decreto para la creación del comité.

Que de esta manera, se espera la implementación y compromiso de la alta dirección de las entidades públicas por medio de la creación de este comité, se establezcan procedimientos y herramientas que permitan monitorear a nivel técnico la infraestructura de TI, la implementación de procesos para la protección de la privacidad de la información, así como medidas para el desarrollo seguro de aplicaciones, y en general procesos de autenticación y controles con el fin de reaccionar a tiempo en caso de presentarse amenazas que comprometan la información tanto física como digital.

Que, en este contexto, estos lineamientos deben estar apropiados entre todos los servidores que componen los equipos de trabajo incluyendo terceros y colaboradores; así mismo, realizar labores de auditoría y mediciones periódicas para verificar la eficacia del sistema. Es importante recordar que la seguridad digital debe dar el marco para lograr mayor acceso a la información pública, y trámites y servicios ágiles a través de experiencias sencillas, satisfactorias y seguras.

Que conforme a las competencias de que trata el Decreto Municipal No. 040 de 2019, *Por el cual se establece el manual básico de la administración municipal de Chía y se adopta la estructura organizacional interna de la administración central del municipio de Chía*, la misión y objetivos de la Oficina de Tecnologías de Información y las Comunicaciones, es definir, formular, adoptar y promover las políticas, planes, programas y proyectos del Sector Tecnologías de la Información y las comunicaciones, que faciliten el acceso y uso de todos los habitantes del municipio y usuarios internos a la tecnologías de la información y las comunicaciones y coordinar su implementación, situación por la cual se adhiere a la ejecución de esta política y se procede con la creación del Comité de Seguridad Digital de la Alcaldía del Municipio de Chía.

Que, en mérito de lo expuesto,

DECRETA

Artículo 1°. Conformación del Comité de Seguridad de la Información. Créase el Comité de Seguridad de la Información de la Alcaldía del Municipio de Chía. El Comité estará integrado así:

1. El Alcalde del Municipio de Chía o su Delegado
2. El Secretario General o su Delegado
3. El Jefe de la Oficina de Tecnologías de la Información y las Comunicaciones TIC o su delegado.
4. El Secretario de Planeación o su Delegado.

5. Un Asesor del Despacho.
6. El Jefe de la Oficina Control Interno o su delegado.

Parágrafo.- El Comité podrá invitar a cada sesión, con voz y sin voto, a aquellas personas que considere necesarias por la naturaleza de los temas a tratar.

Artículo 2º. Objetivo del Comité de Seguridad de la Información. El Comité deberá asegurar que exista una dirección y apoyo gerencial para soportar la administración y desarrollo de iniciativas sobre seguridad de la información, a través de compromisos apropiados y uso de recursos adecuados en el organismo, así como de la formulación y mantenimiento de una política de seguridad de la información a través de todo el organismo.

Artículo 3°. Funciones del Comité. El Comité de Seguridad de la Información de la Alcaldía del Municipio de Chía tendrá dentro de sus funciones las siguientes:

1. Coordinar la implementación del Modelo de Seguridad y privacidad de la Información al interior de la entidad.
2. Revisar los diagnósticos del estado de la seguridad de la información la Alcaldía del Municipio de Chía.
3. Acompañar e impulsar el desarrollo de proyectos de seguridad.
4. Coordinar y dirigir acciones específicas que ayuden a proveer un ambiente seguro y establecer los recursos de información que sean consistentes con las metas y objetivos de la Alcaldía del Municipio de Chía.
5. Recomendar roles y responsabilidades específicos que se relacionen con la seguridad de la información.
6. Aprobar el uso de metodologías y procesos específicos para la seguridad de la información.
7. Participar en la formulación y evaluación de planes de acción para mitigar y/o eliminar riesgos.
8. Realizar revisiones periódicas del SGSI (por lo menos una vez al año) y según los resultados de esta revisión definir las acciones pertinentes.
9. Promover la difusión y sensibilización de la seguridad de la información dentro de la entidad.
10. Poner en conocimiento de la entidad, los documentos generados al interior del comité de seguridad de la información que impacten de manera transversal a la misma.
11. Las demás funciones inherentes a la naturaleza del Comité.

Parágrafo. Una vez conformado el Comité de Seguridad de la Información, este podrá expedir su reglamento, en el cual fijará el alcance de cada una de las funciones operativas señalas en el presente artículo.

Artículo 5°. Secretaria Técnica: La Secretaría Técnica del Comité será ejercida por el Jefe de la Oficina de Tecnologías de la Información y las Comunicaciones TIC.

Artículo 6°. Funciones de la Secretaría Técnica. Las funciones de la Secretaría Técnica serán las siguientes:

1. Elaborar las actas de las reuniones del Comité y verificar su formalización por parte de sus miembros.
2. Citar a los integrantes del Comité a las sesiones ordinarias o extraordinarias
3. Remitir oportunamente a los miembros la agenda de cada comité.
4. Llevar la custodia y archivo de las actas y demás documentos soporte.
5. Servir de interlocutor entre terceros y el Comité.

6. Realizar seguimiento a los compromisos y tareas pendientes del Comité.
7. Presentar los informes que requiera el Comité.
8. Las demás que le sean asignadas por el Comité.

Artículo 7°. Reuniones del Comité de Seguridad de la Información. El Comité de Seguridad de la Información – deberá reunirse trimestralmente, previa convocatoria del Secretario Técnico del Comité.

Artículo 8°. Sesiones Extraordinarias. Los miembros que conforman el Comité podrán ser citados a participar de sesiones extraordinarias de trabajo cuando sea necesario, de acuerdo con temas de riesgos, incidentes o afectaciones de continuidad dentro del Sistema de Gestión de Seguridad de la Información.

Artículo 9°. Vigencia y Derogatoria: La presente Resolución rige a partir de la fecha de su publicación y deroga todas aquellas disposiciones que le sean contrarias.

Dado en la Alcaldía Municipal de Chía, a los 30 AGO 2024

PUBLÍQUESE Y CÚMPLASE

LEONARDO DONOSO RUIZ
Alcalde Municipal

Proyectó: Luz Ángela Vargas Latorre – Contratista Profesional Oficina TIC
Revisó: Ing. Cristian Amezquita – Contratista Profesional Oficina TIC
Revisó y Aprobó: Gustavo Carvajal Millán - Jefe de Oficina de Tecnologías de la Información y las Comunicaciones TIC
Reviso: Julián Eusebio Arévalo Barrera –Profesional Especializado OAJ
Reviso: Luz Aurora Espinoza Tobar – Jefe Oficina Asesora Jurídica.