Política de Seguridad Digital 2024-2027

(Versión 2)

Actualizada: Julio 2025

ALCALDÍA MUNICIPAL DE CHÍA
Carrera 7 N° 12-100
PBX: (601) 884 4444 Ext. 2300-2301
oficinatic @chia.gov.co
www.chia-cundinamarca.gov.co

TABLA DE CONTENIDO

1. INTRODUCCIÓN

El municipio de Chía, alineado con el creciente uso de las Tecnologías de la Información y las Comunicaciones (TICs) en Colombia, ha experimentado un notable avance en la integración digital en sus servicios sociales, económicos y educativos. Este fenómeno ha facilitado la interacción entre la población y la alcaldía, mejorando la accesibilidad y calidad de los servicios ofrecidos a través de plataformas digitales, como las Ventanillas Únicas Virtuales.

La adopción de TICs ha permitido a Chía desarrollar capacidades significativas para la formación de ciudadanos digitales. Estos avances han generado un incremento en la oferta de servicios y trámites digitales, optimizando la respuesta a las necesidades de la comunidad. Las plataformas digitales han simplificado la gestión de servicios, permitiendo una atención más eficiente y personalizada a las problemáticas de los ciudadanos.

Sin embargo, este progreso conlleva también una serie de riesgos en materia de seguridad digital que requieren atención inmediata y estrategias efectivas. La integridad de los datos de las entidades públicas y la información personal de la población que interactúa con estos servicios se ve constantemente amenazada por diversas vulnerabilidades. Los riesgos incluyen, pero no se limitan a, accesos no autorizados, ciberataques, pérdida de datos, y fraudes digitales, los cuales pueden comprometer la confidencialidad, integridad, disponibilidad, autenticidad y trazabilidad de la información.

Ante este escenario, es imperativo que el municipio de Chía ejecute la Política de Seguridad Digital garantizando un entorno digital seguro y confiable. Al abordar de manera proactiva los riesgos y establecer medidas de protección adecuadas, se podrá aprovechar plenamente las oportunidades que ofrecen las TICs, asegurando al mismo tiempo la integridad y privacidad de la información tanto de la entidad, como de los ciudadanos. Este esfuerzo contribuirá al desarrollo sostenible y a la confianza de la población en los servicios digitales, consolidando a Chía como un municipio líder en la transformación digital segura en Colombia.

1.1 Justificación actualización

La transformación digital del Estado exige garantizar entornos tecnológicos seguros, resilientes y confiables. La Alcaldía Municipal de Chía, en su compromiso con la modernización institucional y la protección de la información, ha identificado la necesidad de actualizar y fortalecer su Política de Seguridad Digital, alineándola con el Modelo de Seguridad y Privacidad de la Información (MSPI), versión ISO/IEC 27001:2022, y con los lineamientos del Ministerio de Tecnologías de la Información y las Comunicaciones (MINTIC).

Los resultados del diagnóstico FURAG, las recomendaciones técnicas, las vulnerabilidades en infraestructura, el aumento de riesgos cibernéticos, y las percepciones de funcionarios, contratistas y ciudadanos sobre la gestión de la seguridad digital, evidencian la necesidad de contar con una política integral, actualizada y ejecutable

1.2 Propósito

El primer propósito de la política de seguridad digital del municipio de Chía es establecer un marco integral que permita identificar, evaluar y mitigar los riesgos digitales que puedan comprometer la confianza de los ciudadanos y la calidad de los datos gestionados por las

Carrera 7 N° 12-100
PBX: (601) 884 4444 Ext. 2300-2301
oficinatic @chia.gov.co
www.chia-cundinamarca.gov.co

entidades públicas y la población. Esta política está orientada a contrarrestar cualquier amenaza cibernética y mitigar todo tipo de riesgo, alineándose con las directrices y recomendaciones establecidas en el CONPES 3854 de Seguridad Digital. Además, incorpora los aspectos relevantes del Decreto Nacional 1078 de 2015 y del Modelo de Privacidad y Seguridad de la Información (MSPI) expedido por el MinTIC, asegurando una protección robusta y efectiva de la información.

Este enfoque integral busca no solo proteger los datos y sistemas de información, sino también fomentar una cultura de seguridad digital entre los funcionarios públicos y la ciudadanía. Al hacerlo, se pretende asegurar un entorno digital seguro y confiable que fortalezca la interacción entre la población y las entidades gubernamentales, promoviendo la confianza y la participación activa en la transformación digital del municipio.

El segundo propósito de la Política de Seguridad Digital de la Alcaldía Municipal de Chía es establecer los lineamientos, principios y mecanismos necesarios para proteger la información institucional, los servicios digitales y la infraestructura tecnológica, frente a amenazas internas y externas que puedan comprometer la confidencialidad, integridad, disponibilidad y privacidad de los datos.

Mediante el logro de los dos propósitos anteriores buscamos promover una cultura institucional basada en la gestión del riesgo digital, la responsabilidad en el manejo de la información, la mejora continua de los controles de seguridad, y el uso ético y seguro de las Tecnologías de la Información y las Comunicaciones (TIC) por parte de servidores públicos, contratistas y terceros, proporcionando de esta manera servicios digitales, transparentes y seguros a la ciudadanía.

1.3 Políticas de gestión y desempeño con las que se articula

- Transparencia, acceso a la información pública y lucha contra la corrupción.
- Gobierno Digital.
- Seguridad de la información.
- Arquitectura empresarial

1.4 Estructura o elementos de la política

Los siguientes elementos forman una estructura integral para la Política de Seguridad Digital del Municipio de Chía, asegurando un enfoque completo y normativamente sustentado para la protección y gestión de la información digital.

1.4.1 Objetivo general y específicos

El objetivo general y los objetivos específicos planteados en la presente política, se encuentran alineados bajo los siguientes sustentos Normativos:

- CONPES 3854 de Seguridad Digital: Establece los lineamientos generales para la seguridad digital en Colombia, promoviendo la protección de la infraestructura y los datos.
- Decreto Nacional 1078 de 2015: Marco regulatorio para la gestión de la información y las comunicaciones en las entidades públicas.

Carrera 7 N° 12-100
PBX: (601) 884 4444 Ext. 2300-2301
oficinatic @chia.gov.co
www.chia-cundinamarca.gov.co

- ISO/IEC 27001:2022: Control de la seguridad de la información

1.4.2 Identificación, gestión y evaluación de riesgos

Se deben realizar diagnósticos continuos para identificar vulnerabilidades y evaluar riesgos asociados al uso de TICs.

Sustento Normativo:

- CONPES 3854 de Seguridad Digital: Incluye la identificación y gestión de riesgos como parte fundamental de la estrategia de seguridad digital.
- MSPI: Proporciona directrices para la identificación y tratamiento de riesgos de seguridad de la información.
- Norma NTC-ISO/IEC 27005: Metodología establecida en la política de administración de riesgos de seguridad de la información vigente en la entidad.

1.4.3 Protección de datos y privacidad de la información

Se deben implementar de medidas estrictas para asegurar la protección de los datos institucionales y personales contra ciberataques y brechas de seguridad, garantizando el uso legítimo y seguro de los datos personales, fomentando de esta manera confianza ciudadana en el uso de los servicios digitales.

Sustento Normativo:

- Decreto Nacional 1078 de 2015: Regula la protección de datos y la gestión de la información en las entidades públicas.
- Ley 1581 de 2012: Ley de Protección de Datos Personales en Colombia.

1.4.4 Capacitación y concientización

Promover la cultura de la seguridad digital a través de sensibilizaciones, formación y apropiación de buenas prácticas por parte de funcionarios, contratistas y ciudadanía, para lo cual, se debe elaborar e implementar programas de capacitación y concientización sobre seguridad digital con diferentes enfoques de acuerdo a la caracterización del público objetivo.

Sustento Normativo:

- CONPES 3854 de Seguridad Digital: Promueve la educación y la concientización en temas de seguridad digital.
- Decreto Nacional 1078 de 2015: Fomenta la formación y capacitación en TICs para mejorar la gestión de la información.

Carrera 7 N° 12-100
PBX: (601) 884 4444 Ext. 2300-2301
oficinatic @chia.gov.co
www.chia-cundinamarca.gov.co

1.4.5 Respuestas y gestión de incidentes

Adoptar los procedimientos claros y eficientes para la respuesta y gestión de incidentes de seguridad digital, implementados en la Alcaldía Municipal de Chía.

Sustento Normativo:

- MSPI y la Política de Seguridad de la Información: Proporciona un marco para la gestión de incidentes de seguridad de la información.
- CONPES 3854 de Seguridad Digital: Incluye lineamientos para la respuesta a incidentes y la recuperación ante desastres.

1.4.6 Actualización y adaptación tecnológica

Mantenerse al día con las últimas tendencias y tecnologías en ciberseguridad, adaptando políticas y procedimientos según sea necesario.

Sustento Normativo:

- CONPES 3854 de Seguridad Digital: Fomenta la actualización continua y la adopción de nuevas tecnologías para mejorar la seguridad digital.
- Decreto Nacional 1078 de 2015: Promueve la innovación y la mejora continua en la gestión de las TICs.

1.4.7 Cooperación interinstitucional

Colaboración entre diferentes niveles de gobierno y sectores, incluyendo alianzas con entidades especializadas en ciberseguridad.

Sustento Normativo:

- CONPES 3854 de Seguridad Digital: Resalta la importancia de la cooperación y coordinación entre entidades para fortalecer la seguridad digital.
- Decreto Nacional 1078 de 2015: Establece la necesidad de colaboración entre entidades públicas para una gestión eficiente de las TICs.

1.4.8 Monitoreo y evaluación continua

Seguir los mecanismos de monitoreo y evaluación continua de la eficacia de las medidas de seguridad implementadas.

Sustento Normativo:

- MSPI: Proporciona directrices para el monitoreo y evaluación de la seguridad de la información.

Carrera 7 N° 12-100
PBX: (601) 884 4444 Ext. 2300-2301
oficinatic @chia.gov.co
www.chia-cundinamarca.gov.co

- CONPES 3854 de Seguridad Digital: Incluye la evaluación continua como parte de la estrategia de seguridad digital.

1.5 Principios de la política de seguridad digital

- **Confidencialidad:** La información sensible o reservada será accesible únicamente por personas autorizadas, garantizando la protección frente a accesos indebidos.
- **Integridad:** Se garantizará que los datos no sean alterados de forma no autorizada, preservando su exactitud, coherencia y valor original.
- **Disponibilidad:** La información, los sistemas y los servicios digitales estarán accesibles cuando se necesiten, incluso ante eventos de contingencia.
- **Legalidad y Cumplimiento:** La política se rige por las leyes nacionales en materia de protección de datos, seguridad de la información, ciberseguridad y gobierno digital.
- **Responsabilidad:** Cada servidor, contratista o tercero que maneje información institucional asume el deber de protegerla y usarla conforme a las normas y políticas vigentes.
- **Prevención y Gestión del Riesgo:** Se prioriza la anticipación, evaluación y tratamiento de riesgos que puedan afectar la seguridad de los activos de información y tecnológicos.
- **Mejora Continua:** La política será revisada y actualizada de anualmente, incorporando lecciones aprendidas, nuevas amenazas y avances tecnológicos.
- **Transparencia y Confianza Digital:** Se promueve el uso ético y seguro de los datos, fortaleciendo la confianza de la ciudadanía en los servicios y plataformas digitales.
- **Interoperabilidad y Accesibilidad:** Las soluciones digitales deben ser seguras, pero también interoperables y accesibles para todos los ciudadanos, incluyendo personas con discapacidad.

1.6 Glosario

La mayoría de las definiciones se toman de la Política Nacional de Confianza y Seguridad Digital – CONPES 3995.

- **Activo de Información:** Es todo aquello que en la entidad es considerado importante o de alta validez para la misma ya que puede contener información importante como son en las Bases de Datos con usuarios, contraseñas, números de cuentas, etc.
- **Amenaza:** posible violación de la seguridad digital que tiene el potencial de ocurrir total o parcialmente en el entorno digital. Se caracteriza por la aparición de una situación donde uno o más actores (externos o internos) adelantan una o varias acciones con la capacidad de alterar una infraestructura física, un sistema de información o la integridad de la información en sí.
- **Ataque:** amenaza intencional que se concreta.
- **Confidencialidad:** La información no se pone a disposición ni se revela a individuos, entidades o procesos no autorizados.

Carrera 7 N° 12-100
PBX: (601) 884 4444 Ext. 2300-2301
oficinatic @chia.gov.co
www.chia-cundinamarca.gov.co

- **Ciberdefensa:** capacidad del Estado para prevenir y contrarrestar toda amenaza o incidente de naturaleza cibernética que afecten la sociedad, la soberanía nacional, la independencia, la integridad territorial, el orden constitucional y los intereses nacionales. La ciberdefensa implica el empleo de las capacidades militares ante amenazas cibernéticas, ataques cibernéticos o ante actos hostiles de naturaleza cibernética.
- **Ciberdelincuencia:** conjunto de acciones y actividades ilícitas que son cometidas total o parcialmente en el entorno digital, asociadas con el uso de las Tecnologías de la Información y las Comunicaciones o la utilización de un bien o servicio informático con el fin de causar daño, generar problemas o adelantar una agresión cibernética con el objetivo del propio beneficio o para desestabilizar la población, el territorio y la organización política del Estado.
- **Ciberdelito / Delito cibernético:** actividad delictiva o abusiva relacionada con los ordenadores y las redes de comunicaciones, bien porque se utilice el ordenador como herramienta del delito, bien porque sea el sistema informático (o sus datos) el objetivo del delito. (Ministerio de Defensa de Colombia)
- **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).
- **Ciberseguridad:** se entiende como la capacidad del Estado para minimizar el nivel de riesgo al que están expuestos sus ciudadanos, ante amenazas o incidentes de naturaleza cibernética, buscando la disponibilidad, integridad, autenticación, confidencialidad y no repudio de las interacciones digitales. La ciberseguridad tiene el fin de proteger a los usuarios y los activos de Estado en el Ciberespacio y comprende el conjunto de recursos, políticas, conceptos de seguridad, salvaguardas de seguridad, directrices, métodos de gestión del riesgo, acciones, investigación y desarrollo, formación, prácticas idóneas, seguros y tecnologías que pueden utilizarse para dicho fin.
- **Dato:** Es una representación simbólica (numérica, alfabética, algorítmica, espacial, etc.) de un atributo o variable cuantitativa o cualitativa.
- **Disponibilidad:** Acceso y utilización de la información y los sistemas de tratamiento de la misma por parte de los individuos, entidades o procesos autorizados cuando lo requieran.
- **Entorno digital:** ambiente, tanto físico como virtual sobre el cual se soportan las interacciones del futuro digital, tales como la economía digital.
- **Incidente:** cualquier evento adverso real o sospechado, intencionado o no intencionado, que puede cambiar el curso esperado de una actividad en el entorno digital.
- **Información:** Es un conjunto organizado de datos procesados, que constituyen un mensaje que cambia el estado de conocimiento del sujeto o sistema que recibe dicho mensaje.
- **Integridad:** Mantenimiento de la exactitud y completitud de la información y sus métodos de proceso.

Carrera 7 N° 12-100
PBX: (601) 884 4444 Ext. 2300-2301
oficinatic @chia.gov.co
www.chia-cundinamarca.gov.co

- **Riesgo:** es el efecto de incertidumbres sobre objetivos y puede resultar de eventos en donde las amenazas cibernéticas se combinan con vulnerabilidades generando consecuencias económicas.
- **Riesgo informático:** posibilidad de que una amenaza concreta pueda explotar una vulnerabilidad para causar una pérdida o daño en un activo de información. (MINTIC Guía No. 7 de 2016)
- **Seguridad digital:** es la situación de normalidad y de tranquilidad en el entorno digital (ciberespacio), derivada de la realización de los fines esenciales del Estado mediante la gestión del riesgo de seguridad digital; la implementación efectiva de medidas de ciberseguridad; y 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.
- **Vulnerabilidad:** es una debilidad, atributo o falta de control que permitiría o facilitaría la actuación de una amenaza contra información clasificada, los servicios y recursos que la soportan.

1.7 Normatividad

NORMATIVIDAD ASOCIADA
NORMAS NACIONALES
• Ley 1150 de 2007 • Ley 1341 de 2009 • Ley 1273 de 2009 • Ley 1474 de 2011 • Ley 1581 de 2012 • Ley 1712 de 2014 • Ley 2052 de 2020 • Resolución 3564 de 2015 • Resolución 2710 de 2017 • Resolución 1519 de 2020 • Resolución 1126 de 2021 • Resolución 500 de 2021 • Resolución 2239 de 2024 • Directiva No. 02 de abril de 2019 • Decreto 612 del 4 de abril de 2018 • Decreto 1413 de 2017 • Decreto 2693 de 2012 • Decreto 212 de 2014 • Decreto 1078 de 2015

Carrera 7 N° 12-100
PBX: (601) 884 4444 Ext. 2300-2301
oficinatic @chia.gov.co
www.chia-cundinamarca.gov.co

NORMATIVIDAD ASOCIADA
NORMAS NACIONALES
• Decreto 612 de 2018 • Decreto 2106 de 2019 • Decreto 620 de 2020 • Decreto 1692 de 2020 • Decreto 338 de 2022 • Acuerdo 03 de 2015 del AGN • CONPES 3995 • CONPES 3854
NORMAS TERRITORIALES
• Plan de Desarrollo Municipal 2024-2027 • MSPI de la Alcaldía Municipal de Chía
NORMAS INTERNACIONALES
• ISO 27001:2022 • ISO 27002:2022 • NTC-ISO/IEC 27005

2. ESTRATEGIA IMPLEMENTACIÓN POLÍTICA DE SEGURIDAD DIGITAL

2.1 Objetivo general

Implementar la Política de Seguridad Digital de la Alcaldía Municipal de Chía orientada a la identificación, gestión y mitigación de riesgos de seguridad digital, para la generación de confianza de los ciudadanos digitales en el municipio.

2.2 Objetivos específicos

- Capacitar a los funcionarios de la Alcaldía Municipal de Chía en buenas prácticas digitales.
- Desarrollar confianza digital a través de la mejora de la seguridad digital en la entidad.
- Fortalecer la capacidad de la Alcaldía Municipal de Chía en materia de prevención de riesgos digitales logrando mitigar incidentes de ciberseguridad, mediante la implementación de controles técnicos, procedimientos de respaldo y planes de recuperación y continuidad del negocio.
- Fortalecer la cultura organizacional fomentando la apropiación de las políticas establecidas en la Alcaldía Municipal de Chía.
- Establecer lineamientos técnicos y administrativos para la gestión de riesgos de seguridad digital, conforme al Modelo de Seguridad y Privacidad de la Información (MSPI) y la normativa nacional (ISO/IEC 27001:2022).

Carrera 7 N° 12-100
PBX: (601) 884 4444 Ext. 2300-2301
oficinatic @chia.gov.co
www.chia-cundinamarca.gov.co

- Proteger los activos de información institucionales mediante controles adecuados que salvaguarden su confidencialidad, integridad, disponibilidad y privacidad.
- Fortalecer la infraestructura tecnológica y los entornos digitales de la entidad, garantizando condiciones seguras para la operación de servicios ciudadanos digitales, trámites en línea y sistemas de información.
- Asegurar la trazabilidad y control del acceso a la información, instalaciones críticas, plataformas tecnológicas y componentes físicos y lógicos de la entidad.
- Implementar procesos seguros en la cadena de suministro tecnológica, validando la autenticidad, origen y calidad de los componentes y servicios TIC adquiridos.

2.3 Lineamientos

Los siguientes lineamientos, se establecen a través de la Política de Seguridad de Digital, aplicables a todas las áreas de la Alcaldía Municipal de Chía:

- La Oficina de Tecnologías de la Información y las Comunicaciones se encargará de definir, actualizar y socializar lineamientos sobre seguridad digital de manera anual, conforme a cambios tecnológicos, normativos o de contexto institucional.
- La Oficina de Tecnologías de la Información y las Comunicaciones, establecerá un plan anual de sensibilizaciones y/o capacitaciones obligatorias para servidores públicos y contratistas.
- La Oficina de Tecnologías de la Información y las Comunicaciones, haciendo uso del punto vive digital, promoverá la alfabetización digital ciudadana, especialmente en protección de datos y uso responsable de los servicios digitales.
- Todos los funcionarios, contratistas y otros que tengan relación con la administración y manejen información de la entidad, deben adoptar e implementar el Modelo de Seguridad y Privacidad de la Información (MSPI) versión ISO/IEC 27001:2022 como marco rector.
- Realizar control de acceso físico al nuevo edificio CAM mediante el reconocimiento facial y tarjetas electrónicas personalizadas, permitiendo la restricción de acceso por áreas o dependencias.
- Gestionar las 227 cámaras de video vigilancia ubicadas en el CAM, garantizando trazabilidad y privacidad de la información recolectada a través de este medio.
- Evitar la visibilidad o audibilidad desde el exterior de actividades con información confidencial.
- Está prohibido comer, beber o fumar en zonas de tratamiento de información.
- Las oficinas de Contratación y la Dirección de Función Pública, según corresponda, solicitarán la firma de acuerdos de confidencialidad al personal vinculado, a la administración municipal.
- Los buzones institucionales deben estar bajo responsabilidad del jefe de cada oficina o secretario; por lo tanto, habrá corresponsabilidad del uso compartido de credenciales, con

Carrera 7 N° 12-100
PBX: (601) 884 4444 Ext. 2300-2301
oficinatic @chia.gov.co
www.chia-cundinamarca.gov.co

el personal con acceso a dichos buzones, de manera que se debe llevar control en la entrega de las credenciales por parte del jefe de oficina o secretario.

- La administración municipal, liderará la asignación de los recursos necesarios requeridos para el mejoramiento de la infraestructura tecnológica e implementación de redundancia geográfica y alta disponibilidad en los activos de información catalogados como críticos.
- El área de Gestión Documental, deberá implementar los controles necesarios para que los archivos de gestión cuenten con los mecanismos de seguridad apropiados, de acuerdo con las Tablas de Retención Documental y Tablas de Control de Acceso, con el fin de proteger y conservar la confidencialidad, integridad y disponibilidad de la información física de la Alcaldía Municipal de Chía.
- La Oficina de Tecnologías de la Información y las Comunicaciones, liderará, implementará y actualizará el Plan de Continuidad de las TIC (Plan de Recuperación ante Desastres Tecnológicos) alineado a su vez con el BIA y el BCP.
- La Oficina de Tecnologías de la Información y las Comunicaciones debe designar un responsable de seguridad digital quien también es responsable de la seguridad de la información. La persona designada tendrá las siguientes responsabilidades frente a la seguridad digital de la entidad:
  - Definir el procedimiento para la identificación y valoración de Activos.
  - Realizar análisis de vulnerabilidades periódicos en: Portal web, sede electrónica e Infraestructura en la nube y on premise.
  - Adoptar o adecuar el procedimiento formal para la gestión de riesgos de seguridad digital (Identificación, Análisis, Evaluación y Tratamiento).
  - Asesorar y acompañar a la primera línea de defensa en la realización de la gestión de riesgos de seguridad digital y en la recomendación de controles para mitigar los riesgos.
  - Apoyar en el seguimiento a los planes de tratamiento de riesgo definidos.
  - Informar a la línea estratégica de Gobierno TI, sobre cualquier variación importante en los niveles o valoraciones de los riesgos de seguridad digital.
- De manera anual en la Alcaldía Municipal de Chía se deberá realizar la actualización y documentación de activos de información, se categorizará y se valorará cada activo según lo defina el responsable de seguridad digital.
- La identificación de activos de información se deberá realizar teniendo en cuenta los lineamientos vigentes establecidos por MINTIC, que permitan gestionar adecuadamente la seguridad y privacidad de sus activos de información, el cual debe contener mínimo lo siguiente:
  - Listar los activos por cada proceso.
  - Identificar el dueño o responsable de los activos.
  - Clasificar los activos.
  - Clasificar la información.
  - Determinar la criticidad del activo.
  - Identificar si existen infraestructuras cibernéticas.

Carrera 7 N° 12-100
PBX: (601) 884 4444 Ext. 2300-2301
oficinatic @chia.gov.co
www.chia-cundinamarca.gov.co

- Cada Secretario y/o Jefe de Oficina se encargará de asignar a un responsable en su equipo de trabajo, para hacer el seguimiento y cumplimiento de la política de seguridad digital en su dependencia.
- La Oficina de Tecnologías de la Información y las Comunicaciones verificará que todo desarrollo y plataforma digital propia, cumpla con los estándares de seguridad y protección de la información.
- La secretaría u oficina que ejecuten actividades de adquisición o licenciamiento de software tienen el deber solicitar el concepto técnico de la Oficina TIC, con el objetivo de seguir los lineamientos del licenciamiento, el número máximo de usuarios o recursos, la forma de instalación y los procedimientos para mantener las condiciones de licencia adecuadas.
- La secretaría u oficina que ejecuten actividades de desarrollo de software con entidades externas, tienen el deber solicitar asesoría a la Oficina TIC, en el proceso de contratación, con el fin de definir dentro de los compromisos contractuales, los lineamientos de desarrollo de software seguro, la entrega de la documentación relacionada, las bases de datos de propiedad de la Alcaldía y el código fuente.
- Se deben aplicar controles de acuerdo con la clasificación de la información salvaguardada y custodiada por cada uno de los funcionarios, minimizando impactos financieros, operativos o legales debido a un mal uso de esta.
- Toda información que adquiera la Alcaldía Municipal de Chía de manera externa deberá ser analizado con el antivirus institucional vigente.
- El uso de la información de cada equipo de la entidad será responsabilidad del funcionario asignado.
- Para el acceso a los servicios de red (Sistema de gestión de calidad, sistema de gestión documental, ventanilla única, correo electrónico, etc) se entrega usuario (Ej.: correo electrónico institucional) y contraseña, la cual debe ser cambiada por el usuario propietario del acceso y ser de uso exclusivo e intransferible. La confidencialidad de las contraseñas de acceso será de responsabilidad del funcionario.
- Cualquier funcionario y/o contratista que requiera capacitación en la administración del paquete de herramientas del correo institucional para temas de teletrabajo, deberá realizar la solicitud de manera formal a la Oficina de Tecnologías de la Información y las Comunicaciones.
- La Oficina de Tecnologías de la Información y las Comunicaciones será la encargada de hacer seguimiento a las aplicaciones instaladas en los equipos de cómputo de la entidad, verificando que cumplan con los estándares de uso, bajo licenciamiento.
- Se debe evitar la divulgación, modificación, retiro o destrucción no autorizada de información almacenada en los dispositivos móviles propios de la entidad.
- La Oficina TIC, documentará e implementará procedimientos de respaldo y restauración de información, software e imágenes.
- La Oficina TIC, realizará pruebas periódicas de recuperación de copias de seguridad, especialmente en aplicativos misionales.

Carrera 7 N° 12-100
PBX: (601) 884 4444 Ext. 2300-2301
oficinatic @chia.gov.co
www.chia-cundinamarca.gov.co

- Toda información de la entidad que se gestione de manera remota (teletrabajo) deberá ser salvaguardada en el drive del correo institucional.
- La herramienta recomendada para la realización de reuniones de manera virtual será la que contrate la Oficina TIC, dentro del paquete de correos institucional, según el tipo de licencias adquirido y asignado a cada usuario.
- Se debe minimizar el uso de dispositivos extraíbles dentro de la entidad para prevenir la infección de los equipos de cómputo de la entidad, aprovechando herramientas alternas como el almacenamiento en la nube del correo institucional.
- Todos los funcionarios y contratistas serán los responsables de salvaguardar información relevante de sus procesos para evitar accesos no autorizados, robo de información y realizar respaldos periódicos de la misma.
- Todos los funcionarios, contratistas y/o proveedores, deben realizar la entrega de la información trabajada en el desempeño de sus labores, o cumplimientos de compromisos contractuales al supervisor y/o a su jefe inmediato, según sea el caso.
- Todos los funcionarios y/o contratistas, deben tramitar ante la oficina TIC, liberación de la licencia de correo, para la emisión del respectivo paz y salvo, en el momento de su desvinculación de la entidad.
- Todos los funcionarios y contratistas de la entidad deberán reportar a la Oficina de Tecnologías de la Información y las Comunicaciones cualquier actividad que pueda atentar de manera directa o indirecta la integridad de la información, a su cargo.
- Todos los funcionarios y contratistas de la entidad deberán reportar a la Oficina de Tecnologías de la Información y las Comunicaciones cualquier actividad sobre mal uso de las herramientas TIC a su disposición, ya sea mal uso del internet para acceso a páginas web no permitidas, divulgación de correos de procedencia dudosa, entre otros casos que puedan afectar la seguridad digital de la entidad.
- La administración municipal, ubicará adecuadamente las instalaciones críticas para evitar el acceso del público, cuando sea aplicable, garantizando que los edificios sean discretos y dar una indicación mínima de su propósito, sin señales obvias, fuera o dentro del edificio.
- El comité de seguridad de la información de la Alcaldía Municipal de Chía, establecerá y comunicará el acuerdo de confidencialidad de la información, privacidad y tratamiento de datos personales, y aceptación de las políticas definidas para el sistema de seguridad de la información y buen uso de los activos de información mediante el cual se compromete a realizar un adecuado uso de estos.
- Los eventos de seguridad digital, reportados por los funcionarios y/o contratistas de la Alcaldía Municipal de Chía a la Oficina TIC, deberán ser atendidos, analizados, resueltos y documentados. Si el evento reportado es grave, debe ser informado y/o escalado a ColCERT y/o CSIRT, según corresponda.
- El comité de seguridad de la información de la Alcaldía Municipal de Chía, realizará seguimiento a los casos reportados como moderados y/o graves y trabajará en colaboración con las entidades nacionales ColCERT y/o CSIRT, hasta el cierre de la investigación, tomando las medidas pertinentes que de ella se deriven y socializando las lecciones aprendidas.

Carrera 7 N° 12-100
PBX: (601) 884 4444 Ext. 2300-2301
oficinatic @chia.gov.co
www.chia-cundinamarca.gov.co

2.4 Ámbito de aplicación

Para la implementación de la Política de Seguridad Digital en la Alcaldía Municipal de Chía, se establece el siguiente ámbito de aplicación:

2.4.1 Liderazgo y coordinación

La Oficina de Tecnologías de la Información y las Comunicaciones, será la líder responsable de la implementación, monitoreo, medición y seguimiento de la Política de Seguridad Digital y tendrá la autoridad para coordinar y supervisar todas las actividades relacionadas con la seguridad digital dentro del municipio.

2.4.2 Responsabilidad compartida

Todas las dependencias de la Alcaldía Municipal de Chía serán corresponsables de las acciones e información requeridas por la Oficina TIC. Cada dependencia deberá colaborar activamente proporcionando los datos necesarios y participando en las actividades de monitoreo y seguimiento establecidas por la política.

2.4.3 Aplicación general

La política será aplicable a todos los niveles de la administración municipal, incluyendo:

- Funcionarios y empleados públicos: Todos los empleados, independientemente de su nivel jerárquico, deben cumplir con las directrices y procedimientos establecidos en la política.
- Sistemas y plataformas tecnológicas: Todos los sistemas de información, plataformas digitales, aplicaciones, redes, servidores, dispositivos, servicios en la nube y bases de datos, utilizados por la Alcaldía estarán sujetos a las medidas de seguridad definidas en la política.
- Proveedores, pasantes y contratistas: Cualquier entidad externa que preste servicios o tenga acceso a los sistemas de información, plataformas digitales, redes, equipos tecnológicos o datos institucionales del municipio, deberá cumplir con los requisitos de seguridad digital establecidos por la Oficina TIC.
- Procesos críticos, estratégicos, misionales, de soporte y mejora continua: Cualquier proceso que involucre activos de información y plataformas TIC, incluyendo los servicios ciudadanos digitales, deben cumplir con los lineamientos de la política.
- Instalaciones físicas: Especialmente aquellas donde se almacena o trata información confidencial o crítica, en el edificio CAM y sedes alternas.

2.5 Ejecución de la política de seguridad digital

Es responsabilidad de todos los funcionarios, contratistas y/o proveedores, apropiar y seguir los lineamientos establecidos en la política de seguridad digital.

Carrera 7 N° 12-100
PBX: (601) 884 4444 Ext. 2300-2301
oficinatic @chia.gov.co
www.chia-cundinamarca.gov.co

La Alcaldía Municipal de Chía es responsable de liderar la implementación de la política a nivel territorial, en cabeza del representante legal y el equipo de trabajo del nivel directivo, de la entidad.

3. PLANEACIÓN DE LA POLÍTICA DE SEGURIDAD DIGITAL

La planeación de la Política de Seguridad Digital del Municipio de Chía se articulará con los instrumentos de planificación municipal para garantizar su integración efectiva en la administración pública, enfocada en proteger los activos de información institucional, fortalecer la confianza ciudadana en los servicios digitales, y promover una cultura organizacional orientada al uso seguro y responsable de las tecnologías de la información, dentro de un marco de gobernanza efectiva, colaboración interdependencias y optimización de los recursos disponibles.

Esta planeación se estructurará en tres niveles: el Plan de Desarrollo Municipal, el Plan Indicativo y el Plan de Acción.

3.1 Plan de desarrollo Municipal

El Plan de Desarrollo Municipal es el instrumento de planificación que orienta las acciones de la administración municipal durante un período de gobierno. Este plan establece la visión, programas, proyectos y metas de desarrollo asociados a los recursos públicos que se ejecutarán durante los cuatrienios de cada período de gobierno.

3.1.1 Incorporación de la política de seguridad digital:

Visión: La seguridad digital se integrará en la visión del desarrollo del municipio, enfatizando la importancia de un entorno digital seguro y confiable para la interacción ciudadana y la prestación de servicios públicos.

Programas y proyectos: Se desarrollarán programas y proyectos específicos en materia de seguridad digital, que incluirán la implementación de tecnologías avanzadas, el fortalecimiento de capacidades institucionales y la promoción de una cultura de seguridad digital entre los ciudadanos.

Metas de desarrollo: Se establecerán metas claras y medibles relacionadas con la protección de datos, la gestión de riesgos y la respuesta a incidentes de seguridad digital, en armonía con los lineamientos del Modelo de Seguridad y Privacidad de la Información (MSPI), la Política de Gobierno Digital del MINTIC y las necesidades específicas del contexto institucional y ciudadano.

3.2 Plan indicativo

El Plan Indicativo es un instrumento que permite resumir y organizar por anualidades los compromisos asumidos por el alcalde en el plan de desarrollo. En él se precisan los resultados y productos que se esperan alcanzar en cada vigencia y al terminar el período de gobierno.

Carrera 7 N° 12-100
PBX: (601) 884 4444 Ext. 2300-2301
oficinatic @chia.gov.co
www.chia-cundinamarca.gov.co

3.2.1 Incorporación de la política de seguridad digital:

Resultados y productos anuales: Se definirán resultados específicos que se esperan alcanzar anualmente, como la reducción de incidentes de seguridad, la capacitación de funcionarios y la implementación de nuevas medidas de protección de datos.

Indicadores de gestión: Se adoptarán e implementarán los indicadores de gestión definidos en el modelo de seguridad y privacidad de la información (MSPI), para medir el progreso y efectividad de las acciones de seguridad digital, asegurando que se cumplan los objetivos trazados en el Plan de Desarrollo Municipal.

3.3 Plan de acción

El Plan de Acción es un instrumento que sirve para que cada una de las dependencias oriente sus procesos, instrumentos y recursos disponibles (humanos, financieros, físicos, tecnológicos e institucionales) hacia el logro de sus objetivos y metas anuales de la administración.

3.3.1 Incorporación de la política de seguridad digital:

Orientación de procesos y recursos: Cada dependencia de la Alcaldía Municipal de Chía, integrará la política de seguridad digital en sus planes de acción anuales, asignando los recursos necesarios (humanos, financieros, tecnológicos) para implementar las medidas de seguridad.

Actividades específicas: Se detallarán las actividades específicas, responsables asignados y plazos de cumplimiento, incluyendo dentro estas las siguientes medidas:

- Sensibilización y formación del personal
- Implementación de controles básicos (copias de seguridad, contraseñas, accesos)
- Gestión de riesgos digitales y tratamiento de vulnerabilidades
- Fortalecimiento de la infraestructura tecnológica y los procesos críticos
- Revisión y fortalecimiento de la seguridad en la contratación TIC

Coordinación y monitoreo: Los secretarios y/o jefes de oficina de cada dependencia de la Alcaldía Municipal de Chía, coordinará y supervisará la ejecución de los planes de acción, asegurando una implementación coherente y efectiva de la política de seguridad digital.

3.3.2 Fortalecimiento Progresivo de Controles

Implementar medidas técnicas básicas de protección con ayuda de personal TIC existente y la infraestructura implementada en el CAM, mediante las cuales se logra avanzar en la reducción de brechas de seguridad, permitiendo la ejecución de las siguientes acciones:

Carrera 7 N° 12-100
PBX: (601) 884 4444 Ext. 2300-2301
oficinatic @chia.gov.co
www.chia-cundinamarca.gov.co

- Automatizar y verificar la realización de copias de seguridad en los sistemas críticos.
- Configurar doble autenticación en plataformas de sistemas de información o VPN.
- Establecer un formato de revisión mensual de accesos a plataformas y sistemas por dependencia.
- Implementar políticas de contraseñas seguras y gestión de buzones compartidos.

4. IMPLEMENTACIÓN DE LA POLÍTICA DE SEGURIDAD DIGITAL

Para cumplir con los objetivos de la política de seguridad digital en la Alcaldía Municipal de Chía se implementarán las siguientes líneas estratégicas:

4.1 Estructura administrativa y direccionamiento estratégico

4.1.1 Compromiso de la alta dirección

La alta dirección de la Alcaldía, encabezada por el alcalde, se comprometerá plenamente con la implementación y cumplimiento de la política de seguridad digital. Este compromiso incluye la asignación de recursos necesarios y la institucionalización formal de la política dentro de la estructura administrativa del municipio.

4.1.2 Direccionamiento estratégico

La Oficina TIC liderará la implementación de la política, con apoyo del Comité de Seguridad Digital, el cual será conformado por representantes de áreas estratégicas como Control Interno, Jurídica, Gestión Documental y Secretaría General. Este comité será responsable de hacer seguimiento al plan de acción, priorizar riesgos, promover la cultura de seguridad y presentar informes de avance a la alta dirección.

4.2 Fortalecimiento de capacidades

4.2.1 Capacitación y sensibilización

Se desarrollarán programas de capacitación continua y campañas de sensibilización dirigidas a todos los funcionarios municipales. Estos programas cubrirán el uso correcto de las TICs, la identificación y clasificación de riesgos de seguridad digital, y las estrategias para mitigar dichos riesgos.

Se desarrollarán campañas internas de concienciación sobre seguridad digital, programas de inducción y reinducción en la búsqueda de la adopción de la política de seguridad digital, promoviendo también la firma de acuerdos de confidencialidad por parte de funcionarios y contratistas.

Carrera 7 N° 12-100
PBX: (601) 884 4444 Ext. 2300-2301
oficinatic @chia.gov.co
www.chia-cundinamarca.gov.co

4.2.2 Desarrollo de competencias

Se fomentará el desarrollo de competencias específicas en ciberseguridad, tanto a nivel técnico como operativo, asegurando que el personal esté preparado para enfrentar y gestionar incidentes de seguridad digital de manera efectiva, mediante la implementación de buenas prácticas en el uso seguro de contraseñas, correo, dispositivos, etc.

4.3 Fortalecimiento tecnológico

Con la renovación tecnológica se ha logrado avanzar en el cumplimiento de las recomendaciones del FURAG, y en busca de que se continúe avanzando en esta línea se deberán realizar las siguientes acciones:

- Validar que productos y servicios TIC cumplan estándares de seguridad, informando sobre obsolescencias tecnológicas y necesidades de renovación tecnológica, cuya acción se encuentra alineada con la política de gobierno digital, la cual indica reemplazo mínimo cada 5 años.
- Realizar pruebas de respaldo a las copias de seguridad de la información de los aplicativos misionales, estratégicos, soporte y mejora, de manera programada para asegurar la disponibilidad de los datos en caso de ransomware, de manera coordinada con los responsables del proceso.
- Controlar las condiciones ambientales, como la temperatura y la humedad, para detectar condiciones que puedan afectar negativamente al funcionamiento de las instalaciones de tratamiento de la información.
- Aplicar protección contra rayos a todos los edificios e instalar filtros de protección contra rayos en todas las entradas de alimentación eléctrica y líneas de comunicaciones.
- Proteger los equipos que procesan información confidencial para minimizar el riesgo de fuga de información debido a la emanación electromagnética.
- Desactivar protocolos de red vulnerables.
- Obtener garantías de que los productos y componentes TIC suministrados, funcionan como se espera sin ningún tipo de características inesperadas o no deseadas.
- Implementar procesos que garanticen que los componentes de los proveedores son auténticos y no han sido alterados con respecto a su especificación.
- Implementar procesos específicos para la gestión de la información, el ciclo de vida, la disponibilidad y los riesgos de seguridad asociados a los sistemas de información.
- Garantizar que se instalan los parches aprobados y las actualizaciones de aplicaciones, de fuentes legítimas, más recientes para todo el software autorizado. Si es necesario realizar cambios, estos deben ser aprobados y documentados.
- Controlar las condiciones ambientales, como la temperatura y la humedad, para detectar condiciones que puedan afectar negativamente al funcionamiento de las instalaciones de tratamiento de la información.

Carrera 7 N° 12-100
PBX: (601) 884 4444 Ext. 2300-2301
oficinatic @chia.gov.co
www.chia-cundinamarca.gov.co

- Aplicar protección contra rayos a todos los edificios e instalar filtros de protección contra rayos en todas las entradas de alimentación eléctrica y líneas de comunicaciones.

4.4 Normativo y procedimental

4.4.1 Elaboración y actualización de procedimientos

Se elaborarán y/o actualizarán los procedimientos y la documentación necesaria para asegurar el cumplimiento normativo en temas de tratamiento de datos personales, transparencia y acceso a la información. Esto incluye la creación de políticas claras y procedimientos detallados que guíen la gestión de la seguridad digital.

4.4.2 Cumplimiento normativo

Se garantizará que todas las actividades y prácticas de seguridad digital cumplan con las leyes y regulaciones vigentes, así como con las mejores prácticas internacionales en materia de ciberseguridad.

5. HERRAMIENTAS DE IMPLEMENTACIÓN DE LA POLÍTICA DE SEGURIDAD DIGITAL

Para la correcta implementación de la política de seguridad digital, se tendrá como punto de partida la Política Nacional de Confianza y Seguridad Digital – CONPES 3995 la cual dispone los lineamientos iniciales para la gestión y mitigación de riesgos de seguridad digital en el territorio nacional, de igual manera se presentan las siguientes herramientas de complemento:

- Resultados FURAG 2021, 2022 y 2023
- Plataforma de seguimiento “Resultados de desempeño institucional territorio, vigencia 2022”
- CONPES 3995
- Modelo de Seguridad y Privacidad de la Información – MSPI 2023
- Política de administración de riesgos
- Política de seguridad de la información 2024-2027
- ISO 27001:2022 / ISO 27002:2022

6. SEGUIMIENTO Y MEDICIÓN DE LA POLÍTICA DE SEGURIDAD DIGITAL

6.1 Monitoreo y seguimiento

La oficina de control interno de la Alcaldía Municipal de Chía, en apoyo con la Oficina TIC, será responsable de:

- Monitorear el cumplimiento de las medidas de seguridad digital en todas las dependencias.
- Medir el impacto y la eficacia de las acciones implementadas para la mitigación de riesgos.

Carrera 7 N° 12-100
PBX: (601) 884 4444 Ext. 2300-2301
oficinatic @chia.gov.co
www.chia-cundinamarca.gov.co

- Realizar seguimientos periódicos para asegurar la continuidad y actualización de las prácticas de seguridad digital.

6.2 Medición:

El Modelo Integrado de Planeación y Gestión cuenta con una herramienta en línea, llamado Formulario Único Reporte de Avances de la Gestión - FURAG, a través del cual se capturan, monitorean y evalúan los avances sectoriales e institucionales en la implementación de las políticas de desarrollo administrativo de la vigencia anterior al reporte.

A nivel institucional, para implementar un sistema de medición efectivo para la política de seguridad digital del municipio de Chía, se utilizarán los siguientes componentes:

6.2.1 Indicadores clave de desempeño (KPIs)

Número de incidentes de seguridad reportados: Contar los incidentes de seguridad digital que se reportan mensualmente, a través de una herramienta de gestión de MDS.

Tiempo de respuesta a incidentes: Medir el tiempo promedio que se tarda en responder y resolver los incidentes de seguridad, a través de la herramienta de gestión MDS.

Porcentaje de cumplimiento de las capacitaciones: Monitorear el porcentaje de funcionarios que completan los programas de capacitación en seguridad digital, por medio de las planillas de asistencia.

6.2.2 Encuestas y cuestionarios

Realizar encuestas periódicas a los funcionarios para evaluar:

- Nivel de conocimiento en seguridad digital: Preguntar sobre prácticas seguras y políticas de la organización.
- Percepción de la efectividad de las medidas de seguridad: Obtener feedback sobre las medidas implementadas y su percepción de seguridad.

6.2.3 Registros y reportes Internos

Se utilizará un sistema de gestión de la MDS, en la cual se llevará el registro y documentación de:

- Requerimiento de seguridad: Detalle de las solicitudes realizadas de seguridad de la información (capacitaciones, orientación, información general)
- Incidentes de seguridad: Detalles de cada incidente, incluyendo causa, impacto y medidas correctivas.
- Problemas de seguridad: Trazabilidad, detalle, gestión, incluyendo causa, impacto, medidas correctivas y escalamientos realizados.

Carrera 7 N° 12-100
PBX: (601) 884 4444 Ext. 2300-2301
oficinatic @chia.gov.co
www.chia-cundinamarca.gov.co

6.2.4 Reuniones de seguimiento

El comité de seguridad de la información institucional, programará reuniones trimestrales, donde se revisen:

- Progreso de los KPIs: Analizar los datos recopilados y discutir cualquier desviación de los objetivos.
- Acciones correctivas: Identificar y planificar acciones para abordar problemas o áreas de mejora detectadas.

6.2.5 Revisión de documentación

El equipo de Gobierno TI de la Oficina TIC, realizará revisiones periódicas de los documentos clave, como procedimientos y políticas, para asegurar que estén actualizados y sean efectivos.

Elaboró	**Revisó**		**Aprobó**
Ing. Eliany Rocío Montejo Carrascal - Profesional especializado Fecha: Julio 26 /2024	Ing. Martha Yaneth Sánchez Herrera Ing. Gustavo Carvajal Millán Jefe de Oficina TIC Fecha: 06 de agosto 2024 / 18 de septiembre del 2024		Comité Institucional de Gestión y Desempeño Fecha: 01 de octubre de 2024
Control de cambios			
Versión	**Fecha**	**Actualizó**	**Revisó / Aprobó**
2	Julio / 2025	Ing. Eliany Rocío Montejo Carrascal - Profesional especializado	Ing. Gustavo Carvajal Millán Jefe de Oficina TIC

Carrera 7 N° 12-100
PBX: (601) 884 4444 Ext. 2300-2301
oficinatic @chia.gov.co
www.chia-cundinamarca.gov.co