Política de Seguridad de la Información 2024-2027

(Versión 1)

Julio de 2024

ALCALDÍA MUNICIPAL DE CHÍA
-100
4444 Ext. 2300-2301
oficinatic @chia.gov.co
www.chia-cundinamarca.gov.co

TABLA DE CONTENIDO

1. INTRODUCCIÓN

En un mundo cada vez más digitalizado, la seguridad y privacidad de la información se convierten en pilares fundamentales para la confianza y el adecuado funcionamiento de las instituciones públicas. La Alcaldía Municipal de Chía, consciente de esta realidad y en cumplimiento del decreto 1008 de 2018, establece su compromiso con la protección rigurosa de sus activos informativos. Este decreto subroga el capítulo 1 del título 9 de la parte 2 del libro 2 del Decreto 1078 de 2015, reglamento único del sector de Tecnologías de la Información y las Comunicaciones, estableciendo así los lineamientos generales de la política de gobierno digital.

Reconociendo la importancia crítica de asegurar la integridad, confidencialidad, disponibilidad, autenticidad y trazabilidad de su información, la Alcaldía adopta la norma técnica NTC-ISO/IEC 27001:2022. Esta norma internacional proporciona un modelo efectivo para establecer, implementar, mantener y mejorar continuamente un sistema de gestión de seguridad de la información (SGSI). A través del habilitador de seguridad de la información de gobierno digital del Ministerio de Tecnologías de la Información y las Comunicaciones, la Alcaldía se compromete a desarrollar y ejecutar políticas y procedimientos que salvaguarden sus activos informativos, asegurando así la operatividad y el servicio efectivo a la ciudadanía.

Con esta política, la Alcaldía Municipal de Chía, no solo busca cumplir con los requerimientos legales y reglamentarios vigentes, sino que también se propone liderar por el ejemplo, en la gestión de la seguridad de la información, fortaleciendo la estructura organizacional y tecnológica para una Chía más segura y digital.

2. ALCANCE

La presente Política de Seguridad de la Información, es aplicable y obligatoria para todos los niveles y miembros de la estructura organizacional de la Alcaldía Municipal de Chía. Esto incluye, sin limitación, a todos los secretarios, directores, funcionarios y contratistas involucrados en cualquier proceso administrativo o técnico dentro de la Alcaldía.

2.1 Ámbitos de Aplicación:

2.1.1 Objetivo de aplicación

Estos lineamientos regulan las condiciones de los recursos TIC que proporciona la Alcaldía Municipal de Chía, estos recursos son susceptibles a ser atacados o vulnerados de forma deliberada o accidental con consecuencias que afectan negativamente a la entidad, estos recursos incluyen: Información, datos, software, servicios, comunicaciones y hardware.

La Alcaldía Municipal de Chía, como propietaria y administradora de los recursos TIC, precisará y garantizará los controles mínimos para una apropiada protección de dichos recursos.

Estos lineamientos servirán también para el uso de sistemas de información institucionales, red de comunicaciones cuando es utilizada por usuarios que no pertenecen a la 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

2.1.2 Ámbito subjetivo de la aplicación

Estos lineamientos se aplican para usuarios que utilizan los recursos TIC que dispone la Alcaldía Municipal de Chía. Se considera usuarios:

- **Funcionarios públicos:** Todos los empleados oficiales y/o de carrera administrativa, de la Alcaldía, independientemente de su rango o posición, están obligados a adherirse a los lineamientos establecidos en esta política.
- **Contratistas, consultores y proveedores:** Cualquier persona física o jurídica que tenga un contrato vigente con la Alcaldía para la prestación de servicios internos y/o externos o consultoría, debe cumplir con las normativas de seguridad de la información como condición de su contrato.
- **Directivos:** Incluye a secretarios y directores de departamento, quienes deben garantizar la implementación y cumplimiento de la política en sus respectivas áreas de influencia.

Los usuarios de los recursos TIC de la Alcaldía Municipal de Chía, tendrán derecho a:

- Recibir la capacitación o información oportuna para el empleo adecuado de los recursos TIC en función a sus actividades o necesidades.
- Ser proporcionados de información y soporte técnico sobre los incidentes de seguridad que pueden afectar a los recursos TIC de la Alcaldía Municipal de Chía, que fueron puestos a su disposición.
- Sus derechos de privacidad conforme a las políticas de seguridad de la información de la Alcaldía Municipal de Chía.
- Presentar sugerencias o quejas sobre los servicios y/o recursos TIC recibidos o utilizados.

Los usuarios de recursos TIC de propiedad de la Alcaldía Municipal de Chía, se regirán a los términos u condiciones de estos lineamientos.

Se suspenderá de forma inmediata el uso de los recursos TIC de la Alcaldía Municipal de Chía, si el responsable de la seguridad de la Oficina TIC, detecta comportamientos o manejo inadecuados de los mismos por parte de los usuarios de dichos recursos.

2.2 Procesos Involucrados:

La política abarca todos los procesos estratégicos, misionales y de apoyo que involucren el manejo, procesamiento, almacenamiento y transmisión de información en formatos electrónicos y físicos.

2.3 Infraestructura y Activos de Información:

Incluye todas las infraestructuras tecnológicas (hardware y software), redes de comunicaciones, bases de datos, documentos electrónicos y en papel, así como cualquier otro medio que contenga o gestione información propiedad de la Alcaldía o gestionada por ella.

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

2.4 Ubicaciones y Entornos:

El cumplimiento de esta política es requerido en todas las ubicaciones físicas y entornos virtuales donde se maneje información del municipio, incluyendo, pero no limitándose a, oficinas administrativas, centros de datos, plataformas en la nube y entornos de trabajo remoto.

Esta política se establece para proteger los activos de información contra todo riesgo de pérdida, mal uso, divulgación no autorizada o alteración, asegurando la continuidad de las operaciones y el cumplimiento de las obligaciones legales y reglamentarias pertinentes. Se espera que cada miembro de la entidad comprenda su responsabilidad en la protección de los activos de información y actúe en consecuencia.

3. DEFINICIONES

Activo: cualquier cosa que tiene valor para la organización, es decir, todo elemento que contenga información (hardware, información, software, servicios y recurso humano) y cuyo valor garantice el correcto funcionamiento de la entidad o dependencia.

Confidencialidad: Propiedad que determina que la información sólo esté disponible y sea revelada a individuos, entidades o procesos autorizados.

Disponibilidad: Propiedad de que la información sea accesible y utilizable por solicitud de una entidad autorizada, cuando ésta así lo requiera.

Integridad: Propiedad de salvaguardar la exactitud y estado completo de los activos.

Sistema de Gestión de Seguridad de la Información: Es el conjunto de manuales, procedimientos, controles y técnicas utilizadas para controlar y salvaguardar todos los activos que se manejan dentro de una entidad.

Controles: Medida que permite reducir o mitigar un riesgo.

Amenaza: causa potencial de un incidente no deseado que puede resultar en perjuicio de un sistema o la organización.

Autenticación: Proceso que tiene por objetivo asegurar la identificación de una persona o sistema.

Autenticidad: Busca asegurar la validez de la información en tiempo, forma y distribución. Así mismo, se garantiza el origen de la información, validando el emisor para evitar suplantación de identidades.

Ciberseguridad: Es el proceso de proteger los activos de información por medio del tratamiento de las amenazas a la información que es procesada, almacenada y/o transportada a través de sistemas de información interconectados.

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

Cifrado: Método que permite aumentar la seguridad de un mensaje o de un archivo mediante la codificación del contenido, de manera que sólo pueda leerlo la persona que cuente con la clave de cifrado adecuada para descodificarlo.

Criptografía: Práctica que consiste en proteger información mediante el uso de algoritmos codificados, hashes y firmas.

Acceso Lógico: restricción de acceso a los datos. Esto se logra mediante técnicas de ciberseguridad como identificación, autenticación y autorización

4. NORMATIVIDAD

NORMATIVIDAD ASOCIADA
NORMAS NACIONALES
• Constitución Política de Colombia 1991. Artículo 15. Reconoce como Derecho Fundamental el Habeas Data. • Ley 1273 de 2009, "Delitos Informáticos" protección de la información y los datos". • Ley 1581 de 2012, "Protección de Datos personales". • Decreto 1008 de 2018 ""Por el cual se establecen los lineamientos generales de la política de Gobierno Digital y se subroga el capítulo 1 del título 9 de la parte 2 del libro 2 del Decreto 1078 de 2015, Decreto Único Reglamentario del sector de Tecnologías de la Información y las Comunicaciones". • Decreto 1078 de 2015 "Por medio del cual se expide el Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones". • Resolución No. 001519 de 24 de agosto de 2020. • Resolución 2239 de 2024 • Ley 2052 de 25 agosto 2020. • Artículo 61 de la Constitución Política de Colombia. • Decisión Andina 351 de 1993. - Derechos de Autor. • Código Civil, Artículo 671. - PROPIEDAD INTELECTUAL. Las producciones del talento o del ingenio son una propiedad de sus autores. • Ley 23 de 1982. - Derechos de Autor. • Ley 44 de 1993. - Derechos de Autor. • CONPES 3995 DE 2020 - Política nacional de confianza y seguridad digital. • Resolución 500 de 2021 - Lineamientos y estándares para la estrategia de seguridad digital. • Decreto 338 de 2022 - Lineamientos generales para fortalecer la gobernanza de la seguridad digital.

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

5. POLÍTICA GENERAL DE SEGURIDAD DE LA INFORMACIÓN

La política de seguridad de la información para la Alcaldía Municipal de Chía, se debe apropiar como un marco normativo y operativo diseñado para proteger y manejar de manera efectiva los activos de información críticos de la Alcaldía. Este marco está orientado a preservar la confidencialidad, integridad, disponibilidad, autenticidad y trazabilidad de la información, en conformidad con la Resolución 500 del 2021 del Ministerio de Tecnologías de la Información y las Comunicaciones y la norma NTC-ISO-27001:2022.

Finalidad

Este lineamiento reglamenta la seguridad en la utilización de los recursos TIC que la Alcaldía Municipal de Chía, pone a disposición de su personal administrativo, operativo, contratista, proveedores y de los ciudadanos para garantizar las siguientes consideraciones:

- El desarrollo adecuado de las actividades del personal en función de sus responsabilidades.
- La protección de la información en los diferentes niveles de seguridad.
- La correcta protección de los datos personales de los que la Alcaldía Municipal de Chía, sea responsable.
- La adecuada y continua concienciación de los usuarios respecto a la seguridad de la información.

El cumplimiento de estos lineamientos, garantizan los siguientes aspectos:

- La seguridad y privacidad de los sistemas de información de la Alcaldía Municipal de Chía.
- El tratamiento y protección de los datos personales de sus funcionarios, contratistas y ciudadanos.
- Crea conciencia en funcionarios y contratistas sobre el uso responsable de los recursos TIC de la Alcaldía Municipal de Chía.
- Protege la información de la Alcaldía Municipal de Chía, en todos los niveles de ámbito de valor de la entidad (Confidencialidad, Disponibilidad, Integridad, Autenticidad y Trazabilidad).

5.1 Elementos Clave de la Política de Seguridad de la Información:

5.1.1 Confidencialidad, Integridad, Disponibilidad, Autenticidad y Trazabilidad:

La Alcaldía Municipal de Chía, se asegura de que la información es accesible solo para aquellos autorizados a accederla (confidencialidad), que la precisión y completitud de la información se mantiene (integridad), que los recursos informativos están disponibles

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

cuando son necesarios (disponibilidad), que la persona es quien dice ser (autenticidad), y el ciclo de vida de la información y/o datos en custodia de la entidad (trazabilidad).

5.1.2 Sistema de gestión de seguridad de la información (SGSI):

Implementación de un SGSI que siga las directrices de la norma NTC-ISO-27001:2022, proporcionando un proceso sistemático y estructurado para gestionar los riesgos de seguridad que afectan a la información y los activos relacionados.

5.1.3 Procesos y políticas:

Desarrollo e implementación de procesos y políticas de seguridad detalladas que regulen el acceso, uso, manejo y transferencia de información dentro y fuera de la Alcaldía. Esto incluye políticas de uso aceptable, clasificación de datos, gestión de incidentes, entre otros.

5.1.4 Evaluación de riesgos y controles:

Continua identificación y evaluación de riesgos para los activos de información y el establecimiento de controles adecuados para mitigar estos riesgos. Esto es vital para la protección contra amenazas internas y externas y para asegurar la resiliencia y la recuperación ante incidentes.

5.1.5 Compromiso con la protección según criticidad:

Priorización en la protección de activos de información basada en su criticidad para las operaciones Municipales y su impacto potencial en caso de compromiso, asegurando que los recursos más críticos reciban el más alto nivel de seguridad.

5.1.6 Minimización de impactos financieros y legales:

Al asegurar una protección efectiva de los activos de información, la Alcaldía se esfuerza por minimizar los impactos financieros y legales asociados con la pérdida de datos, violaciones de seguridad y fallas de conformidad.

5.1.7 Capacitación y concientización:

Desarrollo de programas de capacitación y sensibilización para todos los empleados y colaboradores sobre la importancia de la seguridad de la información y las prácticas correctas para su protección.

La Política de Seguridad de la Información de la Alcaldía Municipal de Chía es un componente esencial de la gobernanza y administración Municipal, asegurando no solo el cumplimiento de las normativas vigentes sino también promoviendo una cultura de seguridad que protege los intereses de la ciudadanía y la integridad de los procesos Municipales.

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

5.2 Objetivos

5.2.1 Definición de lineamientos para la privacidad de la información:

Objetivo: Establecer y clarificar los lineamientos fundamentales que regirán la privacidad de la información en la Alcaldía Municipal de Chía, asegurando que toda manipulación de datos personales y sensibles se realice en cumplimiento de las leyes de protección de datos aplicables, las mejores prácticas de privacidad y la normatividad establecida mediante la presente política.

5.2.2 Establecimiento de políticas de seguridad de la información:

Objetivo: Desarrollar y formalizar políticas robustas de seguridad de la información que protejan los activos de información críticos de la Alcaldía. Estas políticas estarán alineadas con el Modelo de Seguridad y Privacidad de la Información (MSPI), el Anexo A de la norma ISO/IEC 27001:2022, y cumplirán con todos los requisitos legales, contractuales y normativos vigentes.

5.2.3 Implementación y mejora continua del MSPI:

Objetivo: Implementar efectivamente y mantener actualizado el modelo de seguridad y privacidad de la información (MSPI) para fortalecer la confianza digital entre los ciudadanos y colaboradores. Este modelo será la base para garantizar el cumplimiento legal, promover una actitud ética y transparente, y estar en concordancia con la misión y visión de la Alcaldía Municipal de Chía.

5.3 Roles y responsabilidades

Las partes Interesadas (Funcionarios, Contratistas y Proveedores), deben cumplir con las políticas de seguridad y privacidad de la información y clausulas establecidas en el MSPI.

A continuación, se definen algunos roles y responsabilidades que se deben tener en cuenta en la implementación y seguimiento de la Política de Seguridad de la Información, Política de Seguridad Digital, Sistema de Gestión de Seguridad de la Información y el Modelo de Seguridad y Privacidad de la Información, el cual se encuentra en mayor detalle en el documento de “Gestión de roles y responsabilidades”

RECURSO HUMANO	FUNCIONARIOS RESPONSABLES	ROL	RESPONSABILIDADES
COMITÉ INSTITUCIONAL DE GESTIÓN Y DESEMPEÑO	Jefes de área(Secretarios, Directores, Jefes de Oficina)	Alta Dirección	Aprobación del MSPI, políticas relacionadas y de la Gestión de roles y responsabilidades. Apoyo implementación MSPI Gestión Estratégica

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

RECURSO HUMANO	FUNCIONARIOS RESPONSABLES	ROL	RESPONSABILIDADES
COMITÉ DE SEGURIDAD DE LA INFORMACIÓN	Control Interno Disciplinario, Área Jurídica, Planeación, Gestión de Calidad, Contratación, Oficina TIC, Oficina Asesora de Comunicación, Prensa y Protocolo.	Toma de decisiones.	Toma de decisiones frente a casos que atenten contra la seguridad de la Información
LÍDER DE TECNOLOGÍA	Jefe de Oficina TIC	Responsable MSPI.	Liderazgo y responsabilidad del MSPI Gestión estratégica y táctica
PARTES INTERESADAS.	Todas las Secretarías/dependencias de la administración Municipal	Cumplimiento MSPI.	Dar estricto cumplimiento a lo estipulado en el MSPI.
JEFATURA OFICINA TIC	Jefe de Oficina TIC	Gerente de proyectos TI	Revisión. ajustes y/o aprobación preliminar estrategias, políticas y procedimientos TI.
EQUIPO DE GOBIERNO TI	Líder de Gobierno TI	Liderar Estrategias TI	Realizar la gestión sobre la elaboración y/o actualización de las diferentes estrategias y políticas a implementar relacionadas con el sistema de seguridad de la información.
FUNCIONARIOS SOPORTE TÉCNICO	Mesa de ayuda	Apoyo operativo de las actividades requeridas del MSPI	Gestión operativa y apoyo al Oficial de Seguridad de la Información o quien haga sus veces y Especialista de Seguridad Informática.
ESPECIALISTA SEGURIDAD INFORMÁTICA	OPS o Funcionario de Planta Oficina TIC	Apoyo operativo de las actividades requeridas del MSPI	Gestión operativa y apoyo al Oficial de Seguridad de la Información o quien haga sus veces.

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

RECURSO HUMANO	FUNCIONARIOS RESPONSABLES	ROL	RESPONSABILIDADES
EQUIPO DE INFRAESTRUCTURA TECNOLÓGICA	OPS o Funcionario de planta Oficina TIC	Gestión de la transición y migración IPv4 a IPv6 Ejecución de actividades del MSPI	Implementar las estrategias de apropiación de los servicios tecnológicos.
EQUIPO DE DESARROLLO DE SISTEMAS DE INFORMACIÓN	Líder del área de desarrollo y OPS	Ejecución de actividades del MSPI	Implementar estrategias de seguridad en los sistemas de información desarrollados por la Oficina TIC

5.4 Política de uso de dispositivos móviles institucionales:

5.4.1 Modificación y gestión de software:

Los funcionarios y contratistas no están autorizados a modificar la configuración, ni instalar o desinstalar aplicaciones en los dispositivos móviles institucionales que se les asignen para el cumplimiento de sus funciones. La Oficina de Tecnologías de la Información y las Comunicaciones (TIC) es la única autorizada para gestionar la configuración y el software en estos dispositivos.

5.4.2 Configuración de correo electrónico institucional:

Todos los dispositivos móviles institucionales deben estar configurados con la cuenta de correo electrónico institucional proporcionada al personal, para asegurar una comunicación efectiva y segura dentro de la entidad.

5.4.3 Conexión a redes inalámbricas:

Está prohibido conectar los dispositivos móviles institucionales a redes inalámbricas públicas para evitar exposiciones a riesgos de seguridad.

5.4.4 Seguridad y bloqueo de pantalla:

Los dispositivos móviles deben estar protegidos con mecanismos de contraseña o bloqueo de pantalla para prevenir el acceso no autorizado cuando no estén en uso.

5.4.5 Uso de puertos USB en lugares públicos:

Se debe evitar conectar los dispositivos móviles institucionales a puertos USB de computadoras públicas, como las encontradas en hoteles, cafés internet, terminales y otros puntos de acceso público, para prevenir riesgos de seguridad como infecciones por malware.

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

5.4.6 Reporte de incidentes de seguridad:

Los funcionarios y contratistas deben reportar inmediatamente cualquier sospecha de infección por malware en dispositivos móviles institucionales al personal técnico de la entidad, para su análisis, evaluación y tratamiento adecuado.

5.4.7 Responsabilidad del usuario:

Cada funcionario y contratista es responsable del cuidado y buen uso de los dispositivos móviles asignados por la entidad, asegurando su correcta utilización en todo momento.

5.5 Política de seguridad de los recursos humanos:

5.5.1 Capacitación en seguridad y privacidad de la información:

Todos los servidores públicos y contratistas deben recibir formación adecuada sobre seguridad y privacidad de la información. Esta capacitación está diseñada para fortalecer la protección de datos personales y sensibles gestionados por la entidad.

5.5.2 Consecuencias del incumplimiento:

Cualquier incumplimiento o violación de las políticas de seguridad de la información por parte de los funcionarios o terceros implicará la aplicación de medidas disciplinarias según lo establecido en los procedimientos internos de investigación disciplinaria de la entidad.

5.5.3 Consentimiento para el tratamiento de información personal:

Antes de realizar el tratamiento de información personal de ciudadanos o servidores públicos, es obligatorio obtener el consentimiento por escrito del titular de los datos. Además, se debe mantener un registro adecuado de dicho consentimiento para garantizar la transparencia y la trazabilidad de las acciones.

5.5.4 Acuerdo de confidencialidad:

Todo el personal que labore en la entidad o preste servicios a la misma, deberá firmar un acuerdo de confidencialidad, tratamiento de datos personales y un documento de conocimiento 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.

5.5.5 Derecho de hábeas data:

Se garantizará en todo momento el pleno y efectivo ejercicio del derecho de hábeas data por parte de los titulares de la información. Esto incluye el derecho a conocer, actualizar y rectificar sus datos personales.

5.5.6 Notificación de violaciones de seguridad:

Es imperativo informar de manera inmediata cualquier violación de los lineamientos de seguridad que pueda representar un riesgo en la administración de la información. La

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

pronta notificación es crucial para la gestión efectiva de incidentes y la mitigación de posibles daños.

5.6 Política de compromiso de confidencialidad por parte de los funcionarios

La Dirección de Función Pública será responsable de asegurar que todos los funcionarios de la Alcaldía Municipal de Chía suscriban un compromiso de confidencialidad, no divulgación de información, aceptación y cumplimiento de los lineamientos establecidos en el sistema de seguridad de la información de la Alcaldía Municipal de Chía. Este compromiso incluye la protección de datos personales y cualquier otra información sensible manejada en el ejercicio de sus funciones. Además, la Dirección de Función Pública garantizará que todas las evidencias relacionadas con estos compromisos se almacenen de manera segura y conforme a las normativas institucionales de gestión de archivos.

5.7 Política de confidencialidad y seguridad para contratistas

5.7.1 Establecimiento de acuerdos de confidencialidad:

Antes de otorgar acceso a la información y a las instalaciones de la Alcaldía Municipal de Chía, es obligatorio que todo el personal contratado firme acuerdos y/o cláusulas de confidencialidad. Estos documentos aseguran el compromiso del contratista con la protección de la información a la que tendrá acceso durante la ejecución de sus servicios.

5.7.2 Aceptación de políticas de seguridad digital:

Además de los acuerdos de confidencialidad, los contratistas deberán firmar un documento de aceptación de las políticas de seguridad digital antes de que se les conceda acceso a la plataforma tecnológica de la Alcaldía Municipal de Chía. Este documento certifica que el contratista comprende y se compromete a cumplir con todas las normativas de seguridad digital establecidas por la entidad.

5.7.3 Garantía de cumplimiento:

La Alcaldía Municipal de Chía se asegurará de que todos los contratistas cumplan con los acuerdos de confidencialidad y las políticas de seguridad digital. Se realizarán revisiones y seguimientos periódicos para garantizar la adherencia continua a estos compromisos.

5.8 Política aplicable durante la ejecución del empleo

5.8.1 Fomento de la cultura de seguridad digital:

La alta dirección se compromete a proteger la información institucional fomentando una cultura robusta de seguridad digital y la gestión de riesgos. Este compromiso incluye asegurar la participación activa del personal en jornadas de capacitación y sensibilización. Estas actividades, lideradas por la Oficina de Tecnologías de la

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

Información y las Comunicaciones (TIC), son esenciales para la promulgación y comprensión de la política de seguridad de la información.

5.8.2 Protección de información confidencial:

Todos los funcionarios y el personal de prestación de servicios, deben ejercer el máximo cuidado para no divulgar información confidencial, especialmente en lugares públicos o en situaciones que puedan comprometer la seguridad o el buen nombre de la entidad.

5.8.3 Fortalecimiento de la cultura de seguridad:

Es primordial promover continuamente la cultura de seguridad digital entre los funcionarios y contratistas. Esto incluye el uso adecuado de la información para fortalecer la confianza con los ciudadanos y entre el personal interno.

5.8.4 Principios y lineamientos para la seguridad Digital:

Establecer y mantener principios claros y lineamientos para la promoción de la seguridad digital. Esto abarca actividades regulares de difusión, capacitación y concientización, dirigidas tanto a personal interno como a usuarios y ciudadanos externos.

5.8.5 Desarrollo y actualización de programas de capacitación:

Formular y coadyuvar en la ejecución y actualización constante del programa de capacitación y sensibilización en seguridad digital. Este programa debe incluir políticas, procedimientos y controles efectivos contra la ingeniería social para todos los funcionarios y contratistas.

5.8.6 Medidas administrativas por incumplimientos:

La Dirección de Función Pública, Control Interno disciplinario y/o supervisores de contratos y Contratación aplicarán, según corresponda, las medidas administrativas necesarias cuando se identifiquen violaciones o incumplimientos a las políticas de seguridad digital.

5.9 Política de gestión de transiciones laborales

Mediante esta política se busca garantizar que los procesos de desvinculación, reasignación de labores, licencias y vacaciones de funcionarios, se realicen de manera ordenada, controlada y segura, protegiendo la integridad y la seguridad de la información institucional.

5.9.1 Procedimientos de transición:

Realizar todos los procesos de desvinculación, licencias, vacaciones o cambios de labores conforme a los procedimientos establecidos, ejecutando los controles necesarios para asegurar una transición fluida y segura de responsabilidades sin comprometer la operatividad y la seguridad de la 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

5.9.2 Gestión de accesos y recursos informáticos:

Al momento de una desvinculación o cambio de labores, verificar los reportes correspondientes para proceder con la modificación o inhabilitación oportuna de los accesos a recursos informáticos, como usuarios de dominio y cuentas de correo electrónico institucional. Esta tarea será coordinada directamente con la Oficina de Tecnologías de la Información y Comunicaciones (TIC).

5.9.3 Responsabilidades de la oficina TIC:

La Oficina TIC tiene la responsabilidad de implementar las acciones necesarias para modificar o deshabilitar los accesos informáticos de los funcionarios que cambian de rol o se desvinculan, asegurando que todos los cambios se reflejen de forma efectiva y a tiempo para mantener la seguridad de la información.

5.9.4 Seguimiento:

Establecer mecanismos de seguimiento para evaluar la efectividad de los procesos de gestión de transiciones laborales y asegurar el cumplimiento de esta política.

5.10 Política gestión de activos de información

5.10.1 Identificación y clasificación de activos:

La Alcaldía Municipal de Chía se compromete a realizar una identificación sistemática y clasificación de todos los activos de información. Esta clasificación debe basarse en criterios de confidencialidad, integridad, disponibilidad, autenticidad y trazabilidad, considerando también los riesgos identificados y los requerimientos legales de retención.

5.10.2 Asignación de responsabilidades:

Cada activo de información debe tener un responsable designado, típicamente un líder de proceso, jefe de área o director, quien es encargado de asegurar un nivel adecuado de protección y de mantener actualizada la valoración del activo.

5.10.3 Protección de los activos de información:

Los propietarios de la información son responsables de garantizar que todos los activos de información reciban la protección adecuada. Esto incluye implementar medidas de seguridad apropiadas que reflejen el valor y la sensibilidad de la información contenida.

5.10.4 Gestión de cambios en los activos de información:

Es responsabilidad de cada líder de proceso, jefe de área o director identificar y reportar la aparición de nuevos activos de información, así como realizar actualizaciones periódicas en la valoración de estos activos.

5.10.5 Devolución de activos de información:

Al concluir una relación contractual, todos los servidores públicos y contratistas deben devolver o entregar los activos de información que estuvieron a su cargo, asegurando

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

que estos sean adecuadamente protegidos y restituidos a la entidad, teniendo en cuenta que, toda información sea física o digital generada, almacenada o transformada por los funcionarios, contratistas o proveedores de la entidad, utilizando los recursos dispuestos por la entidad para tal fin o en desempeño de sus labores o servicio contratado, son activos de información propiedad de la Alcaldía Municipal de Chía.

5.10.6 Responsabilidad sobre los activos de información:

Todos los activos deben tener un responsable específico que garantice la protección continua de la información y los datos almacenados, cumpliendo con las políticas y procedimientos establecidos por la Alcaldía.

5.11 Política de asignación de permisos y privilegios

Los usuarios utilizarán los recursos TIC de la Alcaldía Municipal de Chía, atribuyéndoles roles en base a las funciones que desempeñan, para ello existen dos tipos de permisos:

- Permisos de acceso al recurso: El usuario puede acceder al recurso y ejecutar funciones en base al rol asignado.
- Permiso de administrador del recurso: Con estos permisos el usuario, además de cumplir sus funciones, puede configurar, restaurar y comprobar el funcionamiento según el rol que ocupe.

En general, los usuarios que utilicen los recursos TIC de la Alcaldía Municipal de Chía, deberán regirse a estos lineamientos y disposiciones que le apliquen sobre los mismos.

Los privilegios otorgados a los usuarios que utilicen los recursos TIC de la Alcaldía Municipal de Chía, se determinarán en base a los siguientes criterios:

- La secretaría, oficina y/o dirección de la Alcaldía Municipal de Chía, a la que pertenece.
- Las funciones específicas que desempeñe dentro del equipo de trabajo al que pertenezca.
- Si las funciones que tenga asignadas en un momento determinado (Ej: reemplazo de vacaciones, licencias, encargos, etc.), requiere que el usuario solicite permisos de administrador de un activo de información, la duración de este permiso será temporal y mientras dure asume la total responsabilidad sobre este.

Los usuarios que tengan permisos de administrador sobre los recursos TIC, serán considerados responsables, del cumplimiento de lo dispuesto en los presentes lineamientos y deberán regirse también por las instrucciones específicas de uso del recurso, incluyendo:

- Gestión de seguridad, actualizaciones y parches de seguridad.
- Reportar incidentes de seguridad a las instancias pertinentes en un plazo máximo de 24 horas.

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

5.12 Política de control de acceso

5.12.1 Autorización y responsabilidad de acceso:

Todos los servidores públicos y contratistas con acceso a los sistemas de información o a la red informática institucional deberán disponer de una autorización única de acceso, que incluirá un identificador de usuario y contraseña. Cada persona será responsable de todas las acciones realizadas con el usuario que le ha sido asignado.

5.12.2 Acceso de entidades externas:

Cualquier entidad, empresa o personal externo que requiera acceso a información sensible o crítica, debe suscribir previamente acuerdos de confidencialidad o de no divulgación. Estos acuerdos son cruciales para garantizar la protección de la información y el cumplimiento de la normativa vigente.

5.12.3 Gestión de credenciales:

- Todo usuario de los recursos TIC y de sistemas de información de la Alcaldía Municipal de Chía, dispondrá de credenciales de acceso para su identificación.
- Las credenciales de acceso estarán compuestas de un usuario y contraseña.
- Las credenciales de acceso serán creadas dependiendo de los premisos y privilegios asignados al rol que ostenta el usuario.
- Las credenciales de acceso son de uso personal e intransferible. Es responsabilidad exclusiva del usuario gestionar y proteger las credenciales asignadas.
- Si un usuario deja de pertenecer a la de la Alcaldía Municipal de Chía, será dado de baja, conforme al proceso estipulado para el efecto.
- En base a los presentes lineamientos el usuario gestionará sus credenciales de acceso.
- Si las credenciales de acceso han sido utilizadas o manipuladas por personas no autorizadas, el usuario afectado pondrá la situación, en conocimiento de la Oficina TIC, de forma inmediata.
- El usuario debe bloquear o cerrar sesión cuando se ausente o deje de utilizar el recurso TIC

5.12.4 Autorización para la configuración de la red y equipos:

Solo el personal designado por la Oficina de Tecnologías de la Información y las Comunicaciones (TIC) está autorizado para configurar la red, así como para instalar software o hardware en los equipos y servidores de la infraestructura tecnológica.

5.12.5 Restricciones de acceso remoto y presencial:

Toda actividad que requiera acceso a los servidores, equipos o redes debe realizarse presencialmente en las instalaciones y por personal especializado. Las actividades de acceso remoto están prohibidas sin la debida autorización de la Oficina TIC.

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

5.12.6 Uso de cuentas de correo electrónico:

El uso de las cuentas de correo electrónico debe cumplir con los estándares de creación y utilización definidos en el procedimiento de correos electrónicos de la entidad. La Oficina TIC proporcionará contraseñas iniciales que los usuarios finales deben cambiar por contraseñas seguras e intransferibles.

5.12.7 Gestión de usuarios en sistemas de información:

La creación, edición y baja de usuarios en los sistemas de información en producción deben seguir un procedimiento estricto y formalizado para asegurar la integridad y la seguridad de los accesos.

5.13 Política de seguridad física y del entorno

5.13.1 Gestión de sesiones de usuarios:

Es obligatorio para todos los usuarios de aplicaciones y sistemas de información de la Alcaldía Municipal de Chía, cerrar sus sesiones al finalizar sus actividades. Las sesiones no deben quedar abiertas o desatendidas bajo ninguna circunstancia.

5.13.2 Protección de áreas seguras:

Las áreas seguras, que incluyen el datacenter, centros de cableado, áreas de archivo, y otros espacios críticos, deben estar equipadas con mecanismos de protección física y ambiental. Deberán implementarse controles de acceso rigurosos para asegurar la protección integral de la información.

5.13.3 Controles de acceso a áreas seguras:

El acceso a áreas seguras se controlará mediante sistemas de autenticación como claves, huellas dactilares, carnets institucionales o permisos especiales, según corresponda.

5.13.4 Mantenimiento de la seguridad en entradas:

Todas las entradas equipadas con sistemas de control de acceso deben permanecer cerradas. Es responsabilidad de todos los funcionarios, contratistas y terceros autorizados asegurarse de que las puertas no se dejen abiertas.

5.13.5 Delimitación de perímetros de seguridad:

Los perímetros de seguridad para áreas que manejan o generan información sensible deben estar claramente delimitados por barreras físicas. Estas pueden incluir puertas de acceso controlado y áreas de recepción atendidas por personal autorizado que controle el acceso físico.

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

5.13.6 Gestión de espacios de trabajo:

Los puestos de trabajo deben mantenerse limpios y libres de documentación sensible o clasificada fuera del horario laboral o durante ausencias prolongadas para prevenir el acceso no autorizado a la información.

5.13.7 Responsabilidad sobre equipos tecnológicos:

Los empleados deben asegurarse de bloquear, suspender o apagar todos los equipos tecnológicos como impresoras, computadoras y portátiles cuando no estén en uso. Al finalizar la jornada laboral, todas las aplicaciones deben ser cerradas y los equipos apagados.

5.13.8 Manejo de documentos sensibles:

Los documentos con información confidencial o clasificada deben ser retirados inmediatamente de las impresoras, fotocopiadoras, escáneres y/o faxes tras su uso para evitar pérdidas o robos de información.

5.14 Políticas de controles criptográficos

5.14.1 Conexiones seguras para acceso remoto:

El acceso remoto a la red y a los sistemas de información de la Alcaldía Municipal de Chía debe realizarse exclusivamente a través de conexiones seguras. Estas conexiones deben establecerse utilizando protocolos criptográficos robustos para garantizar la confidencialidad e integridad de la información transmitida desde redes externas.

5.14.2 Seguridad en sistemas de información y servicios tecnológicos:

Todos los sistemas de información y servicios tecnológicos de la Alcaldía Municipal de Chía, deben implementar parámetros de seguridad robustos, basados en usuarios, perfiles y roles. Estos parámetros serán aplicados rigurosamente en los procesos de autorización y autenticación para asegurar el acceso adecuado a los recursos informáticos.

5.14.3 Gestión de claves y usuarios para cifrado:

La asignación de claves y usuarios para el cifrado de información debe ser manejada mediante una solicitud formal dirigida a la Oficina de Tecnologías de la Información y las Comunicaciones (TIC). La solicitud debe justificar claramente la necesidad de dichas credenciales criptográficas.

5.14.4 Provisión de herramientas de encriptación:

La Oficina de TIC será responsable de proveer las herramientas de encriptación de datos necesarias. La asignación de estas herramientas se hará a los usuarios que lo requieran, previa presentación de una solicitud formal que explique el propósito y la necesidad del uso de la encriptación.

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

5.15 Políticas de seguridad en las operaciones

5.15.1 Generalidad

Para asegurar las operaciones realizadas en los recursos tecnológicos que soportan la operación de la entidad, la Alcaldía Municipal de Chía planea, gestiona, respalda y monitorea la infraestructura tecnológica. Esto se realiza con el fin de establecer los controles de seguridad necesarios para proteger la confidencialidad, integridad, disponibilidad, autenticidad y trazabilidad de la información, siguiendo los lineamientos establecidos en los procedimientos del SGSI (Sistema de Gestión de Seguridad de la Información).

5.15.2 Documentación y reducción de riesgos

La Oficina de Tecnologías de la Información y Comunicaciones (TIC) documenta los procesos operacionales de TIC con el objetivo de reducir los riesgos asociados con la ausencia de personal y posibles afectaciones en la infraestructura tecnológica.

5.15.3 Garantía de operaciones seguras

La Oficina TIC garantiza que las operaciones tecnológicas se realicen de manera correcta y segura, proporcionando protección dentro de las aplicaciones y sistemas de información.

5.15.4 Respaldo de información sensible

La Oficina TIC asegura el respaldo de la información sensible de las bases de datos mediante procesos seguros en el datacenter.

5.15.5 Actualizaciones y parches

El equipo de soporte técnico de la Oficina TIC, es responsable de aplicar los parches y actualizaciones del sistema operativo, software ofimático, antivirus y manejo de licencias.

5.16 Políticas de seguridad de las comunicaciones

La Oficina de Tecnologías de la Información y Comunicaciones (TIC) establecerá controles para el acceso lógico y la protección de las redes de la Alcaldía Municipal de Chía, con el fin de asegurar el cumplimiento de los acuerdos de niveles de servicios (ANS) establecidos para los servicios tecnológicos, los cuales serán acordados con la alta dirección.

5.16.1 Transferencia segura de información

La Alcaldía Municipal de Chía definirá procedimientos y lineamientos para la transferencia segura de información tanto interna como externamente, garantizando así la integridad y confidencialidad de la información.

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

5.16.2 Separación de redes virtuales

El proceso de TI implementa y mantiene la separación de las redes virtuales para garantizar la confidencialidad de la información en la red de telecomunicaciones de la Alcaldía Municipal de Chía.

5.16.3 Procedimientos de clasificación y manejo de información

Los servidores públicos y contratistas deben seguir las indicaciones del procedimiento de clasificación, etiquetado y manejo de la información de la administración Municipal de Chía para la transferencia de información, de acuerdo con la clasificación de la misma.

5.16.4 Correspondencia Virtual

En la Alcaldía Municipal de Chía, la correspondencia virtual se maneja mediante Corrycom y el correo institucional de cada dependencia de la administración Municipal de Chía.

5.16.5 Uso de Software y Aplicaciones Designadas

Existen software o aplicaciones designadas por la Contraloría o Procuraduría para la transferencia de información de diferentes dependencias de la administración Municipal de Chía. A los usuarios se les asigna un usuario y una contraseña para enviar informes y documentos de manera más eficiente y segura.

5.17 Política adquisición, desarrollo y mantenimiento de sistemas

La Alcaldía Municipal de Chía busca integrar la seguridad de la información en todo el ciclo de vida de los sistemas de información, así como en la adquisición de aquellos que presten servicios a la entidad.

5.17.1 Notificación y revisión de proyectos

Todas las dependencias de la entidad deben informar ante la oficina TIC, sobre sus proyectos de adquisición de sistemas de información. Con el fin de revisar los aspectos técnicos necesarios y otorgar concepto favorable para su desarrollo e implementación.

5.17.2 Requerimientos de seguridad en el software

La Alcaldía Municipal de Chía asegura que se diseñen e implementen los requerimientos de seguridad en el software, ya sea desarrollado internamente o adquirido. Esto incluye controles de autenticación y verificación de datos de entrada y salida.

5.17.3 Ambientes de desarrollo y pruebas seguros

La Alcaldía Municipal de Chía cuenta con un ambiente de desarrollo y pruebas en un entorno seguro. En su defecto, se exige al proveedor, mediante los contratos, que cuente con controles de seguridad de la información en sus ambientes.

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

5.17.4 Metodología de desarrollo seguro

La Alcaldía Municipal de Chía, aplica una metodología de desarrollo seguro de software, garantizando la protección de la información en todas las etapas del ciclo de vida del desarrollo de software.

5.18 Política de relaciones con los proveedores

La Alcaldía Municipal de Chía establecerá políticas y requisitos de seguridad de la información para mitigar los riesgos asociados a cada proceso de contratación, lo cual hace parte del manual de contratación de la entidad.

5.18.1 Acuerdos de confidencialidad

Antes de iniciar la ejecución de contratos con terceras partes, deberán suscribirse los respectivos acuerdos de confidencialidad. Estos acuerdos deben incluir cláusulas de confidencialidad y aspectos de seguridad de la información necesarios tanto durante como después del contrato.

5.18.2 Gestión de cambios con proveedores críticos

Cualquier cambio que se realice con un proveedor crítico de TI o de los procesos misionales debe aplicarse mediante el procedimiento de gestión de cambios establecido en la entidad.

5.18.3 Revisiones periódicas de cumplimiento

La Alcaldía Municipal de Chía realiza revisiones periódicas del cumplimiento de las políticas de seguridad y privacidad de la información por parte de los proveedores.

5.19 Política sobre el uso adecuado de internet

El internet es un recurso valioso para el desempeño de las labores de todos los funcionarios. Por lo tanto, se definen los siguientes lineamientos para su uso adecuado:

5.19.1 Restricciones de Acceso

- **Portales prohibidos:** El acceso a portales de juegos, pornografía, drogas, terrorismo, segregación racial, hacking, malware, software gratuito o ilegal, y cualquier otra página que vaya en contra de las leyes vigentes estará restringido.
- **Redes sociales:** El acceso a redes sociales como Facebook, WhatsApp, Instagram, Twitter, entre otras, estará limitado.
- **Nube e intercambio de información:** Se restringirá el acceso a portales de nube e intercambio de información masiva, exceptuando la nube corporativa o institucional.

5.19.2 Monitoreo de navegación

La Oficina TIC podrá verificar los registros de navegación (logs) cuando sea necesario para investigaciones o requerimientos específicos.

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

5.20 Política sobre el uso adecuado de correo electrónico:

Los buzones de correo asignados a los funcionarios, contratistas o terceros pertenecen a la Alcaldía Municipal de Chía; por lo tanto, su contenido también es propiedad de la entidad.

5.20.1 Uso institucional

El correo electrónico deberá emplearse exclusivamente para uso institucional y el desempeño de las funciones correspondientes a cada cargo.

5.20.2 Monitoreo de contenidos

La Oficina de Tecnología de la Información y Comunicaciones (TIC), podrá verificar el contenido de los buzones de correo electrónico cuando sea necesario para asegurar la continuidad del servicio o para investigaciones específicas.

5.21 Política de contraseñas seguras

Las claves de acceso al servicio de correo electrónico y/o sistemas de información no deben ser divulgadas a ninguna persona ni exhibidas en público. Para su gestión, se deben seguir los controles de protección de contraseñas definidos a continuación:

5.21.1 Cambio de contraseñas predeterminadas

Cualquier servicio, sistema de información, correo electrónico o equipo informático que tenga contraseñas por defecto configuradas por el proveedor o fabricante debe cambiarse por nuevas contraseñas personalizadas.

5.21.2 Confidencialidad y gestión de contraseñas

- **Personal e intransferible:** La contraseña asignada a un usuario es personal e intransferible. Los usuarios no deben divulgar, prestar, exhibir ni comunicar su contraseña de ninguna forma, ya sea escrita o verbal.
- **Soporte y mantenimiento:** Cuando se requiere la contraseña de usuario para labores de soporte o mantenimiento, el usuario debe digitarla personalmente. Al finalizar las actividades de soporte, se debe cambiar la contraseña por una nueva.

5.21.3 Frecuencia y requisitos de cambio de contraseña

- **Cambio regular:** Los usuarios deben cambiar sus contraseñas de acceso a servicios al menos cada dos meses.
- **Requisitos de seguridad:** Las contraseñas deben cumplir con los siguientes criterios:
  - **Dificultad:** Utilizar contraseñas que sean difíciles de deducir.
  - **No repetir:** No repetir contraseñas utilizadas en los últimos tres meses.

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

- **Evitar palabras obvias:** Evitar palabras comunes como nombres, fechas de cumpleaños, nombres de mascotas, nombres de hijos, etc.
- **Caracteres alfanuméricos y especiales:** Utilizar una combinación de caracteres alfanuméricos y especiales.
- **Contraseñas por frases:** Se recomienda usar la técnica de contraseñas por frases incluyendo alfanuméricos y caracteres especiales. Ejemplo: “Desde los 10 años me leo 20 libros al año”, contraseña: Dl10aml20la@
- **Diversidad de caracteres:** Usar caracteres diferentes que no sean consecutivos ni idénticos.
- **Diferente del usuario:** Usar contraseñas diferentes al nombre de usuario.
- **Memorizar:** Siempre memorizar la contraseña, no utilizar el recordatorio de contraseñas.

5.21.4 Prohibición de divulgación

Está expresamente prohibido divulgar contraseñas por cualquier medio.

5.22 Políticas de gestión de incidentes de seguridad

Todos los servidores públicos y contratistas deben conocer el método de reporte de eventos e incidentes de seguridad de la información.

5.22.2 reporte de incidentes

Cada vez que se detecte un evento, incidente o debilidad relacionada con la seguridad de la información, debe ser reportado a la Oficina TIC a través de cualquiera de los medios dispuestos para tal fin.

5.22.3 Procedimiento de actuación

La Alcaldía Municipal de Chía se asegurará de que todos los servidores públicos y contratistas conozcan y apliquen un procedimiento rápido y eficaz para actuar ante cualquier incidente de seguridad de la información. Este procedimiento, establecido en el sistema de gestión de la MDS, permite el registro de incidentes con sus pruebas y evidencias para analizar su origen y prevenir futuros incidentes.

5.22.4 Documentación de incidentes

La Oficina TIC debe documentar los incidentes de seguridad, incluyendo la clasificación del incidente (categoría y prioridad), los tiempos de respuesta, los responsables de atención según la clasificación, las líneas de atención y los indicadores de medición.

5.22.5 Tipificación de incidentes

La Oficina TIC debe establecer la tipificación de los incidentes de seguridad de la información, tales como:

- Phishing

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

- Malware
- Fuga de Información
- Defacement
- Otros

5.22.6 Obtención de evidencias

En la gestión de incidentes, cuando sea necesario obtener evidencia de un incidente, siempre se debe garantizar el cumplimiento de los requisitos legales aplicables o comunicarlo a un ente competente para que realice el debido proceso.

5.22.7 Registro de incidentes

La Alcaldía Municipal de Chía cuenta con un gestor de MDS en el cual se registran los incidentes de seguridad de la información reportados por los usuarios, atendidos por la Oficina TIC y/o escalados a los entes correspondientes.

5.23 Política de administración de riesgos

5.23.1 Objetivo

La política tiene como objetivo la identificación, clasificación y valoración de los riesgos digitales y de seguridad de la información en la Alcaldía Municipal de Chía, basándose en la política de gobierno digital y el modelo de seguridad y privacidad de la información.

5.23.2 Marco de referencia

Esta política está definida en la política de administración de riesgos de la Alcaldía Municipal de Chía, bajo la Resolución 4578 de 2019. Se deben seguir los lineamientos establecidos en dicha resolución, así como cualquier actualización y/o aprobación legalizada mediante actos administrativos.

5.23.3 Mejora continua

Se busca la mejora continua del sistema de gestión de seguridad de la información mediante un conjunto de reglas y directrices orientadas a garantizar la protección de los activos de información de la Alcaldía Municipal de Chía de manera contundente, eficiente y efectiva. Además, se implementarán las acciones necesarias para la evaluación, análisis y tratamiento de los riesgos, de acuerdo con la metodología adoptada por la administración.

5.23.4 Cumplimiento de requisitos

La administración Municipal de Chía, se compromete a cumplir con todos los requisitos legales, reglamentarios y contractuales pertinentes, con el fin de gestionar y reducir los riesgos a un nivel aceptable.

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

5.24 Políticas de cumplimiento

La Alcaldía Municipal de Chía, gestiona la seguridad de la información de tal forma que se dé cumplimiento adecuado a la legislación vigente. Para ello, analiza los requisitos legales aplicables a la información, incluyendo los derechos de propiedad intelectual, protección de datos personales, transparencia y del derecho de acceso a la información pública, según la normatividad vigente.

6. SENSIBILIZACIÓN Y COMUNICACIÓN EN SEGURIDAD DE LA INFORMACIÓN

6.1 Alcance

La Alcaldía Municipal de Chía, definirá un "Plan de Comunicación en Seguridad de la Información" a través de la oficina de comunicación interna y externa y la Oficina TIC, donde se planificará anualmente la manera en que se comunicarán recomendaciones de seguridad de la información por diferentes medios a todos sus funcionarios y contratistas, con el fin de socializar las políticas institucionales en seguridad de la información o las buenas prácticas en seguridad que se desean socializar para aumentar las capacidades de todas las áreas y procesos de la entidad. La creación de los contenidos se hará con apoyo del área de Gobierno TI de la oficina TIC y/o el enlace de Seguridad de la información.

6.2. Identificación de necesidades

Se debe realizar de manera anual análisis de necesidades de concienciación y formación en seguridad de la información, a todos los funcionarios, contratistas y proveedores de la organización, a través de aplicación de encuestas y procesos de ingeniería social, identificando de esta manera vulnerabilidades en la aplicación del conocimiento que se brinda a través de las campañas de sensibilización, con el objetivo de establecer planes de mejora de acuerdo con la realidad de la organización.

6.3 Objetivo General

Apropiar el conocimiento obtenido a través de las estrategias definidas en el presente programa de concienciación y formación en el sistema de gestión de seguridad de la información.

6.3.1 Objetivos específicos:

- Definir las estrategias de difusión para la comunicación del plan de concienciación y formación en seguridad de la información.
- Establecer los cursos de carácter obligatorio para todo el personal.
- Documentar y evidenciar la ejecución de las sensibilizaciones y formaciones en ciberseguridad.
- Sensibilizar a todo el personal, contratistas y proveedores sobre los riesgos en seguridad de la información, que se pueden presentar y afectan a todas las partes interesadas.

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

- Obtener nivel de apropiación de la política de seguridad de la información por parte del personal interno de la organización, de los contratistas y proveedores.
- Obtener aprobación de la alta dirección y asignación de recursos físicos y humanos.

6.4 Diseño del programa de concienciación y formación

A continuación, se relacionan los temarios que se tendrán en cuenta en el presente programa de concienciación y formación en seguridad de la información y los recursos humanos con los cuales se dará cumplimiento a dicho programa.

Temario	Recursos
Desarrollo de software seguro	Interno (Personal de Gobierno TI y/o de Desarrollo e innovación)
Énfasis Política de contraseñas seguras	Interno (Personal de Gobierno TI)
Sistema general de seguridad de la información (conceptos generales y políticas alineadas)	Interno (Personal de Gobierno TI)
Política de seguridad de la información	Interno (Personal de Gobierno TI)
Política de administración de riesgos en ciberseguridad	Interno (Personal de Gobierno TI)
Información práctica de amenazas informáticas (Virus informáticos, Malware, vulnerabilidades producidas por usuarios, denegación de servicios, ingeniería social, phishing)	Interno (Personal de Gobierno TI)
Responsabilidades con la organización del cumplimiento políticas relacionadas con el sistema de seguridad de la información y consecuencias legales por incumplimiento	Interno (Personal de Gobierno TI)
Uso adecuado de las herramientas Informáticas y gestión de incidentes	Interno (Personal de Gobierno TI y/o equipo de soporte TIC)

6.5 Desarrollo del plan de concienciación y formación

La elaboración del material de concienciación y/o formaciones realizadas por personal interno estará a cargo del área de Gobierno TI de la Oficina TIC, según sus competencias.

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

Las diferentes píldoras, posters, mailyng con boletines informativos sobre seguridad de la información y publicación en la intranet de la organización estarán a cargo de las dependencias de comunicaciones y de la Oficina TIC.

6.6 Mejoramiento del plan de concienciación y formación

De acuerdo con los resultados obtenidos a través de:

- Estadísticas de la mesa de servicios sobre los incidentes reportados en el presente año
- Las encuestas de apropiación del conocimiento
- La realización de actividades de ingeniería social

Se debe realizar de forma anual actualización, con enfoque a la mejora continua, el nuevo programa de concienciación y formación para el siguiente año.

En caso de presentarse incidentes repetitivos, se debe tramitar a través del proceso de gestión de cambios actualización al presente programa de concienciación y formación con el fin de dar solución al problema identificado.

7. AUDITORÍAS

Con el fin de garantizar el cumplimiento de los presentes lineamientos, se llevarán a cabo auditorías internas anuales.

El informe final será analizado por la Oficina de control interno y la Oficina TIC, para tomar medidas preventivas y/o correctivas sobre los puntos en los que la auditoría muestre como no exitoso, asegurando así una mejora continua en las políticas de seguridad de la información.

8. CULTURA DE LA SEGURIDAD DE LA INFORMACIÓN

La Alcaldía Municipal de Chía, a través de la Secretaría general, su dirección de función pública y oficina de Contratación, incluirá dentro de sus capacitaciones e inducciones las temáticas de seguridad de la información, con el objetivo de que cualquier funcionario y/o contratista que se vincule a la entidad tenga pleno conocimiento de las políticas de seguridad de seguridad de la información. El área de Gobierno TI de la oficina TIC y/o el enlace de Seguridad de la Información apoyará en dichas inducciones.

La entidad implementará las estrategias adecuadas para crear y fortalecer una cultura, cambio y apropiación de seguridad de la información, lo cual implica un cambio en el comportamiento de los colaboradores en relación a las políticas y directrices que deben cumplir. Esto debe generar la identificación de perfiles de conocimiento, público objetivo, temáticas identificadas para el año, y finalmente la medición de esta gestión.

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

9. SANCIONES

El comité de seguridad de la información, realizará el seguimiento de los casos que se llegasen a presentar de incumplimientos a las políticas de seguridad digital, seguridad de la información y al modelo de seguridad y privacidad de la información, realizando el debido proceso e informando según sea el caso, a las autoridades competentes, para lo cual se tendrá en cuenta la legislación vigente y en especial, la Ley 1273 de 2009, ley de delitos informáticos y sus actualizaciones.

La falta de conocimiento de los presentes lineamientos no libera al personal de la Alcaldía Municipal de Chía, de las responsabilidades establecidas en ellos, por el mal uso que hagan de los recursos de TIC o por el incumplimiento de los lineamientos aquí descritos.

- Se aplicarán sanciones de acuerdo con el Código Único Disciplinario.
- Pueden aplicarse sanciones de tipo penal según sea el caso y la gravedad de este, si así lo consideran los entes investigativos y judiciales correspondientes.
- La Oficina TIC y el comité de seguridad de la información, serán los encargados de recopilar y entregar a la Oficina de Control Disciplinario, las evidencias de incumplimiento de los lineamientos, informes de impactos, consecuencias y cualquier otro insumo requerido, para formalmente manejar la investigación, inicialmente a nivel interno; así mismo, la Oficina TIC, será la encargada de registrar y gestionar el Incidente de seguridad derivado con el incumplimiento de las políticas.

10. APROBACIÓN Y REVISIÓN DE LAS POLÍTICAS

Las políticas aquí definidas se harán efectivas a partir de su aprobación por el comité de gestión y desempeño y serán revisadas, con el fin de asegurar su vigencia y aplicabilidad dentro de la Alcaldía Municipal de Chía, de la siguiente manera:

- Anualmente,
- Cuando existan incidentes de seguridad de la información
- Cuando se produzcan cambios estructurales considerables.

Elaboró	Revisó	Aprobó
Ing. Eliany Rocío Montejo Carrascal - Profesional especializado Fecha: Julio 02 / 2024	Ing. Martha Yaneth Sánchez Herrera Ing. Gustavo Carvajal Millán Jefe de Oficina TIC Fecha: Julio 10/2024 / Septiembre 18/2024	Comité Institucional de Gestión y Desempeño Fecha: Octubre 01/2024

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