Política de Seguridad de la Información 2024-2027

Alcaldía Municipal de Chía

(Versión 3)

Actualizada: Mayo de 2026

TABLA DE CONTENIDO

1. INTRODUCCIÓN

En el contexto actual de transformación digital, la información se constituye en uno de los activos más estratégicos para la gestión pública, la prestación de servicios a la ciudadanía, la toma de decisiones institucionales y el cumplimiento de los fines misionales de la alcaldía municipal de Chía. Por esta razón, la seguridad y privacidad de la información deben gestionarse de manera integral, preventiva y continua, garantizando la protección de los datos, los sistemas de información, la infraestructura tecnológica, los servicios digitales y los recursos TIC utilizados por funcionarios, contratistas, proveedores, terceros y ciudadanos.

La alcaldía municipal de Chía, consciente de los riesgos asociados al uso de tecnologías de la información, tales como accesos no autorizados, fuga de información, pérdida de disponibilidad, uso indebido de privilegios, amenazas cibernéticas, errores humanos, ingeniería social, tratamiento inadecuado de datos personales y afectaciones a la continuidad operativa, adopta la presente Política de Seguridad de la Información como marco institucional para preservar la confidencialidad, integridad, disponibilidad, autenticidad y trazabilidad de la información.

Esta política se encuentra alineada con la Política de Gobierno Digital, el Modelo de Seguridad y Privacidad de la Información (MSPI), el Modelo de Gestión y Gobierno TI (MGGTI), la normatividad vigente en materia de protección de datos personales, delitos informáticos, transparencia y acceso a la información pública, así como con los estándares internacionales ISO/IEC 27001:2022 e ISO/IEC 27002, los cuales orientan la implementación, operación, mantenimiento y mejora continua del Sistema de Gestión de Seguridad de la Información (SGSI).

En este sentido, la presente política establece lineamientos para la gestión de activos de información, control de accesos, uso adecuado de recursos tecnológicos, administración de privilegios, seguridad en operaciones, comunicaciones, desarrollo de sistemas, relaciones con terceros, monitoreo tecnológico, uso de herramientas digitales, continuidad, gestión de incidentes, protección de datos personales, videovigilancia, control biométrico y demás aspectos necesarios para fortalecer la seguridad digital institucional.

Asimismo, reconoce que la seguridad de la información no es responsabilidad exclusiva de la Oficina TIC, sino una responsabilidad compartida entre la alta dirección, las dependencias, los líderes de proceso, los funcionarios, contratistas y proveedores que acceden o gestionan información institucional. Por ello, promueve una cultura de cumplimiento, prevención, reporte oportuno, uso responsable de la tecnología, protección de la privacidad y mejora continua.

Con esta política, la alcaldía municipal de Chía reafirma su compromiso con la gestión segura, ética, transparente y responsable de la información, fortaleciendo la confianza institucional, la protección de los derechos de los titulares de la información, la continuidad de los servicios tecnológicos y la consolidación de una administración pública más segura, eficiente y orientada al ciudadano.

2. ALCANCE

La presente Política de Seguridad de la Información, aplica a todos los procesos, personas, tecnologías, datos y sistemas de información involucrados en la gestión pública de la alcaldía municipal de Chía, incluyendo:

- Funcionarios de planta y provisionales
- Contratistas, proveedores, pasantes y terceros que accedan a información institucional
- Infraestructura tecnológica (equipos, redes, servidores, sistemas)
- Plataformas, aplicativos y servicios digitales institucionales
- Información generada, procesada, almacenada o transmitida por la entidad

Es de cumplimiento obligatorio para todas las secretarías, dependencias y niveles jerárquicos de la administración municipal.

2.1 Ámbitos de aplicación:

2.1.1 Objetivo de aplicación

Establecer lineamientos que regulen las condiciones de seguridad informática, de los recursos TIC, que proporciona la alcaldía municipal de Chía, ya que estos 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.

Proporcionar las directrices que 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.

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, directores de departamento y jefes de oficina, 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.

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.

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.

Trazabilidad: mantener registros de acciones y accesos.

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.

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.
- Garantizar que todos los funcionarios, contratistas y proveedores asuman responsabilidad sobre la protección de la información en función de sus roles.
- Formalizar roles y responsabilidades del modelo de seguridad y privacidad de la información (MSPI).
- 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 cuando son necesarios (disponibilidad), que la persona es quien dice ser (autenticidad), y del 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.

5.2 Objetivos

5.2.1 Objetivo general

Establecer, implementar y mantener un marco estratégico de seguridad de la información que permita proteger los activos de información de la alcaldía municipal de Chía, frente a amenazas internas y externas, garantizando la confidencialidad, integridad, disponibilidad, autenticidad y trazabilidad de la información, apoyando la prestación segura y continua de los servicios institucionales a la ciudadanía y el cumplimiento de las obligaciones legales y misionales de la entidad.

5.2.2 Objetivos específicos

5.2.2.1 Definición de lineamientos para la privacidad de la información

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 de la información y la normatividad establecida mediante la presente política.
Dar cumplimiento a la legislación nacional e internacional vigente en materia de protección de datos personales, delitos informáticos, habeas data, propiedad intelectual y Gobierno Digital.

5.2.2.2 Establecimiento de políticas de seguridad de la información

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.
Identificar, evaluar, controlar y mitigar los riesgos asociados al uso de tecnologías de la información y comunicaciones, mediante procedimientos documentados y mejoras continuas.

5.2.2.3 Implementación y mejora continua del MSPI

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.
Definir y formalizar los compromisos de las áreas, funcionarios, contratistas y terceros en la protección de la información, alineados con el modelo de seguridad y privacidad de la información (MSPI).

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 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	Secretarios, Directores y Jefes de Oficina	Alta dirección	Aprobación del MSPI, políticas relacionadas y la gestión de roles y responsabilidades. Apoyo implementación MSPI, garantizando los recursos necesarios (presupuesto, personal y herramientas). Fomentar una cultura de apropiación de la seguridad de la información y el cumplimiento normativo.

RECURSO HUMANO	FUNCIONARIOS RESPONSABLES	ROL	RESPONSABILIDADES
COMITÉ DE SEGURIDAD DE LA INFORMACIÓN	Control Interno Disciplinario, Oficina Asesora Jurídica, Sec de Planeación, Sec General, Oficina de 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. Dar respuestas a entes de control (ColCERT, CSIRT).
JEFATURA OFICINA TIC	Jefe de Oficina TIC	Responsable MSPI.	Liderazgo y responsabilidad del MSPI, gestión estratégica y táctica. Aprobar requerimientos de cifrado, segmentación de red y control de acceso.
		Gerente de proyectos TI	Revisión. ajustes y/o aprobación preliminar de 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. Mantener actualizada la matriz de riesgos informáticos, con medidas preventivas, correctivas y/o de contingencia, alineadas a la norma ISO 27002:2022
EQUIPO DE SOPORTE TÉCNICO	Mesa de ayuda	Apoyo operativo de las actividades requeridas del MSPI	Gestión operativa y apoyo al especialista de seguridad informática. Proveer soporte de seguridad informática de primer y segundo nivel. Clasificar, escalar y documentar incidentes y requerimientos de seguridad informática. Realizar seguimiento a los incidentes de

RECURSO HUMANO	FUNCIONARIOS RESPONSABLES	ROL	RESPONSABILIDADES
			seguridad y mantener registros en GLPI.
ESPECIALISTA SEGURIDAD INFORMÁTICA	OPS o funcionario de carrera administrativa de la Oficina TIC	Apoyo operativo de las actividades requeridas del MSPI	Apoyar la planificación, análisis y respuesta ante incidentes. Configurar y mantener elementos de seguridad (IPS, UTM, antivirus, IDS). Verificar cumplimiento del MSPI. Coordinar con entes de control y equipos técnicos, las gestiones requeridas sobre incidentes de seguridad informática.
EQUIPO DE INFRAESTRUCTURA TECNOLÓGICA	OPS o funcionario de carrera administrativa de la Oficina TIC	Gestión de implementación IPv6 Ejecución de actividades del MSPI y de las políticas de seguridad digital de la información	Implementar las estrategias y lineamientos definidos en las políticas de seguridad digital y de la información, relacionados con infraestructura tecnológica, entre ellos: Administrar redes, servidores, VPN, firewalls, dispositivos institucionales. Activar cifrado, borrado remoto, segmentación y control de accesos. Gestionar cuentas de usuario, cambios de configuración y planes de contingencias
EQUIPO DE DESARROLLO DE SISTEMAS DE INFORMACIÓN	Líder del área de desarrollo y OPS	Ejecución de actividades del MSPI	Implementar estrategias y lineamientos de seguridad en los sistemas de información desarrollados por la Oficina TIC. Implementar entornos separados (desarrollo,

RECURSO HUMANO	FUNCIONARIOS RESPONSABLES	ROL	RESPONSABILIDADES
			prueba, producción). Aplicar controles sobre roles, perfiles y código fuente. Impartir capacitaciones sobre desarrollo seguro. Monitorear repositorios, versiones y vulnerabilidades en el código
PARTES INTERESADAS.	Todas las Secretarías/direcciones y oficinas de la administración municipal	Cumplimiento MSPI, políticas de seguridad digital y de la información	Cumplir con las políticas y procedimientos de seguridad. Garantizar la veracidad y reserva de la información. Notificar incidentes, accesos irregulares o errores. Hacer uso adecuado de los activos informáticos y recursos tecnológicos. Participar en capacitaciones y actividades de concientización
	Funcionarios con acceso privilegiado	Cumplimiento MSPI, políticas de seguridad digital y de la información	Administrar bases de datos, servidores y sistemas críticos. Mantener la integridad, confidencialidad y disponibilidad de la información. No acceder a datos sin autorización. Proteger sus credenciales y reportar incidentes de inmediato.

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.

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 a través de la mesa de servicios de la oficina TIC, 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/o 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 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 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/o la oficina de 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.

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 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 de Chía.

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 tres 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.
- **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.

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.

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, aplicando la autenticación multifactor, en las herramientas tecnológicas que así lo permitan.
- 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 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.

Garantizar que los accesos a los sistemas de información son eliminados cuando alguien no necesita acceder a la información y a otros activos asociados, en particular garantizando que los funcionarios que han renunciado al cargo o finalizado su vinculación contractual son eliminados en el momento oportuno.

Modificar los accesos a los sistemas de información, de los usuarios que hayan cambiado de rol o de trabajo.

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.
Se deben 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.
Se deben aplicar mecanismos de 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.
Ubicar adecuadamente las instalaciones críticas para evitar el acceso del público, cuando sea aplicable, garantizar que los edificios sean discretos y dar una indicación mínima de su propósito, sin señales obvias, fuera o dentro del edificio, identificando la presencia de actividades de procesamiento de 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, reconocimiento facial, tarjetas de acceso, 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.
Configurar las funciones para evitar que la información confidencial o las actividades sean visibles y audibles desde el exterior.

No tener directorios, orientaciones telefónicas internas y mapas accesibles en línea que identifiquen ubicaciones de instalaciones de procesamiento de información confidencial fácilmente disponibles para cualquier persona no autorizada.

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.

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.
Está prohibido comer, beber y fumar cerca de los equipos de cómputo y de las instalaciones de tratamiento de la información.

5.13.8 Protección de equipos informáticos

Se deben proteger los equipos que procesan información confidencial para minimizar el riesgo de fuga de información debido a la emanación electromagnética.

5.13.9 Seguridad en redes

- Mantener la documentación actualizada, incluidos los diagramas de red y los archivos de configuración.
- Restringir protocolos vulnerables, ya identificados.
- Realizar supervisión y auditoría permanente del tráfico, accesos, configuración y uso de recursos.
- Diseñar e implementar infraestructura redundante y geográficamente distribuida, con componentes activos o de respaldo automáticos, según criticidad.
- Restringir el acceso a sitios web que contengan información ilegal o que se sepa que contienen virus o material de phishing, bloqueando la dirección IP o el dominio del sitio web en cuestión.

5.13.10 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.

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 el MSPI (Modelo de Seguridad y Privacidad 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.

Se debe garantizar que se instalan los parches aprobados y las actualizaciones de aplicaciones más recientes para todo el software autorizado. Si es necesario realizar cambios, estos deben ser aprobados y documentados

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.

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:

- Separación de los entornos de desarrollo, prueba y producción.
- Definir y documentar los requisitos de seguridad en la fase de especificación y diseño.
- Definir y documentar los puntos de revisión de seguridad en proyectos de desarrollo
- Documentar las pruebas de sistema y seguridad tales como pruebas de regresión, escaneo de código y pruebas de penetración
- Gestión de versiones segura
- Crear repositorios seguros de código fuente y la configuración

- Identificar requisitos de licencia y las alternativas para asegurar soluciones efectivas evitando futuros problemas de licenciamiento
- Documentar los 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 debe contar con un ambiente de desarrollo y pruebas en un entorno seguro y exigir a los proveedores, mediante los contratos, que cuenten con controles de seguridad de la información en sus ambientes de desarrollo.

5.17.4 Metodología de desarrollo seguro

La alcaldía municipal de Chía, aplicará una metodología de desarrollo de software seguro, buscando garantizar la protección de la información en todas las etapas del ciclo de vida del desarrollo de software, para ello elaborará y publicará en el sistema de gestión de calidad (kawak), un procedimiento que incluya los ítems relacionados en los requerimientos de seguridad de software (5.17.2), adicionando la capacidad que deben tener los desarrolladores para prevenir, encontrar y corregir vulnerabilidades.

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.

5.20 Política para la asignación y uso adecuado de correo electrónico

Con el fin de garantizar el uso eficiente, seguro y sostenible de los recursos tecnológicos institucionales, la alcaldía municipal de Chía establece los siguientes lineamientos para la administración, asignación y uso de cuentas de correo electrónico institucional, teniendo en cuenta la disponibilidad limitada de licenciamiento y la necesidad de priorizar el acceso a usuarios que gestionan información crítica, estratégica o sensible de la entidad.

5.20.1 Principios de asignación

La asignación de cuentas institucionales deberá realizarse bajo criterios de:

- Necesidad funcional.
- Criticidad de la información.
- Rol institucional.
- Riesgo asociado.
- Disponibilidad presupuestal.
- Prioridad operativa.

La asignación de una cuenta institucional no constituye un derecho automático derivado de la vinculación contractual o laboral.

5.20.2 Priorización de licencias

Debido a la disponibilidad limitada de licencias institucionales, la Oficina TIC priorizará la asignación de cuentas de correo electrónico institucional a usuarios que:

- Administren información sensible o reservada.
- Gestionen procesos misionales.
- Manejen datos personales.
- Requieran acceso a sistemas institucionales integrados.
- Ejerzan funciones directivas.
- Realicen actividades de atención ciudadana,
- Requieran interoperabilidad con plataformas oficiales del Estado.

5.20.3 Clasificación de Usuarios

La Oficina TIC podrá clasificar los usuarios en categorías de acceso, tales como:

- Usuarios prioritarios: Usuarios con acceso completo a correo institucional y herramientas colaborativas, debido a la criticidad de sus funciones.
- Usuarios operativos o temporales: Usuarios que, conforme a análisis de necesidad y disponibilidad, podrán:

    - Compartir buzones funcionales.
    - Utilizar cuentas genéricas de la dependencia.
    - Acceder únicamente a plataformas específicas.
    - Utilizar mecanismos alternativos autorizados de comunicación institucional.

5.20.4 Buzones de correo institucionales

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.

5.20.5 Responsabilidad del usuario

Todo usuario con acceso a correo institucional deberá:

- Utilizarlo exclusivamente para fines institucionales.
- Proteger sus credenciales.
- Evitar compartir accesos abiertos.
- Reportar incidentes de seguridad.
- Cumplir las políticas institucionales de seguridad de la información.

5.20.6 Monitoreo de contenidos

La Oficina de Tecnología de la Información y Comunicaciones (TIC), podrá verificar el contenido de los buzones de correo electrónico cuando sean solicitados de manera formal, con su respectiva justificación documentada, por entes de control, para investigaciones específicas.

5.20.7 Uso de cuentas genéricas o funcionales

Cuando la disponibilidad de licencias no permita asignación individual, podrán utilizarse cuentas funcionales asociadas a:

- Secretarias, direcciones u Oficinas.
- Areas.
- Procesos.
- Ventanillas.
- Servicios institucionales.

El jefe de oficina, director, secretario y/o la persona a la que este delegue, será responsable de:

- Controlar accesos.
- Custodiar credenciales.
- Actualizar permisos.
- Garantizar trazabilidad de uso.

5.20.8 Restricción de uso de correos personales

La información institucional clasificada como:

- Reservada.
- Confidencial.
- Sensible.
- Estratégica.
- Relacionada con datos personales.

No deberá ser gestionada mediante cuentas personales no autorizadas.

Excepcionalmente, y ante limitaciones operativas o presupuestales, la Oficina TIC podrá definir mecanismos transitorios controlados, siempre que:

- Exista autorización formal,
- Se implementen medidas de seguridad,
- Se minimicen riesgos de fuga o pérdida de información.

5.20.9 Administración y control

La Oficina TIC será responsable de:

- Administrar las licencias disponibles.
- Definir criterios técnicos de asignación.
- Realizar revisiones periódicas de uso.
- Deshabilitar cuentas inactivas.
- Optimizar recursos de licenciamiento.
- Priorizar necesidades institucionales conforme al riesgo y criticidad.

5.20.10 Finalización de accesos

Cuando termine la relación contractual o laboral:

- Los accesos deberán revocarse oportunamente.
- Las cuentas deberán bloquearse o eliminarse.
- La información institucional deberá preservarse conforme a las políticas de gestión documental y continuidad operativa.

5.20.11 Medidas de seguridad obligatorias

Las cuentas institucionales deberán cumplir controles mínimos de seguridad, incluyendo:

- Contraseñas robustas.
- Autenticación multifactor (cuando aplique).
- Monitoreo de accesos.
- Protección antiphishing.
- Trazabilidad de eventos de seguridad.

5.21 Política de gestión de identidad

- Un nombre de usuario específico sólo debe estar vinculado a una única persona para poder responsabilizarla de las acciones realizadas con ese usuario específico.
- Los nombres de usuarios asignados a múltiples personas (por ejemplo, usuarios compartidos) sólo deben estar permitidos cuando son necesarios por razones operativas y deben estar aprobadas por el jefe del área y documentada.
- La información secreta de autenticación utilizada en el contexto de nombres de usuarios vinculados a múltiples funcionarios y/o contratistas, se comparte únicamente con personas autorizadas.

5.22 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:

5.22.1 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.

5.22.2 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.

5.22.3 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.
  - **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.

5.22.4 Prohibición de divulgación

Está expresamente prohibido divulgar contraseñas por cualquier medio.

5.23 Política para la realización de pruebas de penetración y evaluaciones de seguridad digital

Con el fin de fortalecer la seguridad de la información, identificar vulnerabilidades y validar la efectividad de los controles de seguridad implementados, la Alcaldía Municipal de Chía podrá realizar pruebas de penetración, análisis de vulnerabilidades y ejercicios controlados de evaluación de seguridad sobre su infraestructura tecnológica, sistemas de información, redes y plataformas institucionales.

Estas actividades deberán desarrollarse bajo principios de legalidad, trazabilidad, proporcionalidad, confidencialidad y control de privilegios, para cuya documentación se podrá hacer uso del formato TIC-FT-10-V1 Control de cambios desarrollos tecnológicos.

5.23.1 Autorización formal

Toda prueba de penetración o evaluación ofensiva deberá contar previamente con:

- Autorización formal de la Oficina TIC.
- Validación del responsable de Seguridad de la Información.
- Definición de alcance.
- Cronograma.
- Responsables.
- Activos involucrados.
- Plan de contingencia asociado.

Las pruebas sobre activos críticos podrán requerir aprobación adicional del Comité de Seguridad de la Información o instancia equivalente.

5.23.2 Alcance controlado

Las pruebas deberán limitarse exclusivamente a:

- Sistemas autorizados,
- Rangos IP definidos.
- Aplicaciones incluidas en el alcance.
- Recursos tecnológicos previamente aprobados.

Se prohíbe extender actividades sobre activos no autorizados o ajenos al alcance definido.

5.23.3 Comunicación y coordinación

Las dependencias o usuarios potencialmente impactados deberán ser informados previamente sobre:

- La realización de las pruebas.
- Posibles afectaciones operativas.
- Ventanas de ejecución.
- Canales de soporte.

5.23.4 Uso controlado de privilegios

El personal encargado de las pruebas únicamente podrá utilizar los accesos y privilegios estrictamente necesarios para la ejecución de las actividades autorizadas.

Se prohíbe expresamente:

- Acceder a información no relacionada con la prueba.
- Extraer bases de datos o información sensible sin autorización.
- Mantener accesos persistentes.
- Alterar evidencia.
- Utilizar hallazgos para fines distintos al proceso autorizado.
- Realizar actividades no contempladas en el alcance aprobado.

5.23.5 Trazabilidad, registro y gestión de hallazgos

Toda actividad realizada durante las pruebas deberá quedar registrada mediante un informe que permitan identificar:

- Responsable de la actividad.
- Fecha y hora.
- Herramientas utilizadas.
- Sistemas intervenidos.
- Acciones ejecutadas.
- Hallazgos identificados.

La información recopilada deberá manejarse como confidencial.

Los resultados de las pruebas deberán documentarse formalmente, incluyendo:

- Vulnerabilidad identificada.
- Nivel de criticidad.
- Evidencia técnica.
- Impacto.
- Recomendación.
- Responsable de remediación.
- Tiempo estimado de corrección.

Los hallazgos deberán gestionarse conforme al procedimiento institucional de gestión de incidentes de seguridad.

5.23.6 Protección de la continuidad operativa

Las pruebas deberán ejecutarse minimizando riesgos sobre la operación institucional y evitando afectaciones innecesarias sobre:

- Disponibilidad de servicios.
- Integridad de la información.
- Continuidad operativa.
- Atención al ciudadano.
- Plataformas misionales.

No se permitirá la ejecución de ataques destructivos, denegaciones de servicio no autorizadas o pruebas que comprometan la estabilidad institucional.

5.23.7 Confidencialidad

Toda persona que participe en pruebas de penetración deberá cumplir acuerdos y/o cláusulas de confidencialidad y garantizar reserva sobre:

- Vulnerabilidades encontradas.
- Configuraciones internas.
- Credenciales.
- Evidencias técnicas.
- Información sensible obtenida durante el proceso.

5.23.7 Incumplimiento a los lineamientos establecidos

El uso indebido de herramientas ofensivas, privilegios administrativos o información obtenida durante las pruebas será considerado una violación grave a la política de seguridad de la información y podrá generar:

- Revocatoria inmediata de accesos.
- Investigaciones disciplinarias.
- Terminación contractual.
- Reporte a entes de control.
- Acciones legales aplicables.

5.24 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.

5.24.1 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.

5.24.2 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.

5.23.3 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.

5.24.4 Tipificación de incidentes

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

- Phishing
- Malware
- Fuga de Información
- Defacement
- Otros

5.24.5 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.

5.24.6 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.

5.24.7 Escalamiento de incidentes de alta complejidad a ColCERT y CSIRT PONAL

Cuando un incidente de seguridad de la información sea clasificado como de **alta complejidad**, la Oficina TIC deberá activar el procedimiento de escalamiento técnico correspondiente, con el fin de garantizar una respuesta oportuna, especializada y coordinada con las instancias nacionales competentes en materia de ciberseguridad.

Para efectos de la presente política, se entenderán como incidentes de alta complejidad aquellos que puedan comprometer de forma significativa la confidencialidad, integridad, disponibilidad, autenticidad o trazabilidad de la información institucional, afectar servicios críticos, comprometer infraestructura tecnológica estratégica o superar la capacidad de respuesta ordinaria de la Oficina TIC.

5.24.7.1 Criterios para clasificar un incidente como de alta complejidad

Se considerarán incidentes de alta complejidad, entre otros, los siguientes:

- Compromiso de servidores, bases de datos, sistemas misionales o infraestructura crítica.
- Ataques de ransomware, malware avanzado o persistencia maliciosa.
- Fuga, exposición o pérdida de información institucional, confidencial, reservada o datos personales.
- Acceso no autorizado a cuentas privilegiadas, consolas administrativas, servidores, firewalls, VPN o sistemas críticos.
- Alteración, destrucción o modificación no autorizada de información institucional.
- Defacement o alteración no autorizada de portales web institucionales.
- Ataques de denegación de servicio que afecten la disponibilidad de servicios institucionales.
- Explotación de vulnerabilidades críticas en sistemas, aplicaciones, redes o servicios expuestos.
- Incidentes que involucren múltiples dependencias, proveedores, terceros o entidades externas.

- Incidentes que puedan afectar la continuidad operativa, la atención ciudadana o la confianza institucional.

5.24.7.2. Escalamiento técnico a ColCERT

Cuando el incidente sea de alta complejidad técnica, afecte la infraestructura tecnológica institucional o requiera acompañamiento especializado en ciberseguridad, los ingenieros de tercer nivel de la Oficina TIC deberán reportar el caso a ColCERT, a través de los canales oficiales vigentes definidos para tal fin.

Para estos efectos, se entenderá por ingenieros de tercer nivel el personal tecnico de la Oficina TIC o contratado por la entidad que tenga competencias en infraestructura, seguridad informática, redes, servidores, continuidad tecnológica o respuesta avanzada ante incidentes.

El reporte a ColCERT deberá realizarse una vez se cuente con información mínima del incidente, sin retrasar las acciones de contención inicial, e incluir como mínimo:

- Fecha y hora de detección.
- Descripción general del incidente.
- Activos afectados.
- Nivel de criticidad.
- Impacto preliminar.
- Acciones de contención realizadas.
- Evidencias técnicas disponibles.
- Responsable institucional de contacto.
- Necesidad de acompañamiento técnico o coordinación externa.

5.24.7.3 Escalamiento a CSIRT de la Policía Nacional

Cuando durante el análisis del incidente se identifiquen elementos que permitan presumir la posible configuración de un delito informático, el caso deberá ser escalado al CSIRT de la Policía Nacional, a través de los canales oficiales vigentes.

Se deberán considerar como posibles delitos informáticos, entre otros:

- Acceso abusivo a sistemas informáticos.
- Daño informático.
- Interceptación no autorizada de datos.
- Violación de datos personales.
- Uso de software malicioso.
- Suplantación digital.
- Hurto por medios informáticos.
- Transferencia no consentida de activos.
- Sabotaje o alteración de sistemas institucionales.
- Obtención, comercialización o divulgación no autorizada de información.

El escalamiento a CSIRT PONAL deberá realizarse sin perjuicio de las actuaciones que correspondan ante la oficina asesora jurídica, control interno disciplinario, el ordenador del gasto o autoridades competentes, según la naturaleza del caso.

5.24.7.4 Responsables del escalamiento

El escalamiento técnico o institucional deberá ser coordinado por:

- La Jefatura de la Oficina TIC.
- Los ingenieros de tercer nivel responsables del análisis técnico.

- El Comité de Seguridad de la Información, cuando el nivel de criticidad lo requiera.

Los ingenieros de tercer nivel deberán documentar técnicamente el incidente y suministrar los insumos requeridos para el reporte ante ColCERT o CSIRT PONAL.

5.24.7.5 Cadena de custodia y preservación de evidencias

Cuando un incidente sea escalado a ColCERT, CSIRT PONAL o cualquier autoridad competente, la Oficina TIC deberá preservar la evidencia técnica disponible, evitando alteraciones, eliminación o manipulación indebida de la información.

La evidencia podrá incluir:

- Logs de sistemas, servidores, firewalls, VPN, correo electrónico o aplicaciones.
- Capturas de pantalla.
- Direcciones IP, dominios, hashes o indicadores de compromiso.
- Correos electrónicos sospechosos.
- Registros de acceso.
- Reportes del antivirus, EDR, IDS, IPS, SIEM u otras herramientas.
- Actas o informes técnicos de atención.

Toda evidencia deberá ser tratada como información confidencial y utilizada únicamente para fines de análisis, contención, investigación, reporte y mejora de controles.

5.24.7.6 Tiempos de escalamiento

Una vez clasificado el incidente como de alta complejidad, la Oficina TIC deberá realizar el escalamiento en el menor tiempo posible, priorizando la contención, preservación de evidencias y continuidad operativa.

Como criterio institucional:

- Los incidentes críticos deberán escalarse de forma inmediata.
- Los incidentes altos deberán escalarse dentro de la misma jornada laboral.
- Los incidentes con posible delito informático deberán escalarse tan pronto se identifiquen indicios razonables.

5.24.7.7 Registro y cierre del incidente

Todo incidente escalado a ColCERT o CSIRT PONAL deberá quedar registrado en la mesa de servicios GLPI, incluyendo:

- Número de caso o radicado interno.
- Clasificación del incidente.
- Entidad externa a la que fue escalado.
- Fecha y hora del reporte.
- Responsable del reporte.
- Evidencias entregadas.
- Recomendaciones recibidas.
- Acciones de contención, erradicación y recuperación.
- Lecciones aprendidas.
- Plan de mejora o controles correctivos.

El cierre del incidente deberá realizarse únicamente cuando se hayan documentado las acciones ejecutadas, los riesgos residuales y las medidas de prevención de recurrencia.

5.24.8 Mejora continua

Los incidentes escalados a ColCERT o CSIRT PONAL deberán ser analizados posteriormente por la Oficina TIC y el Comité de Seguridad de la Información, con el fin de:

- Identificar causas raíz.
- Actualizar controles de seguridad.
- Fortalecer procedimientos de respuesta.
- Ajustar reglas de monitoreo.
- Actualizar la matriz de riesgos.
- Definir acciones de capacitación o sensibilización.
- Reducir la probabilidad de recurrencia.

5.25 Política para el monitoreo tecnológico y el uso de accesos privilegiados

La alcaldía municipal de Chía, reconoce la necesidad de implementar mecanismos de monitoreo tecnológico, administración remota y supervisión de eventos de seguridad, con el fin de garantizar la disponibilidad, integridad, confidencialidad y trazabilidad de la información institucional. No obstante, dichas actividades deberán ejecutarse bajo principios de legalidad, proporcionalidad, transparencia y mínimo privilegio, evitando cualquier uso indebido de herramientas administrativas o accesos privilegiados.

5.25.1 Transparencia del monitoreo

La entidad deberá informar a funcionarios, contratistas y terceros autorizados sobre:

- La existencia de mecanismos institucionales de monitoreo.
- Las actividades susceptibles de registro.
- Las herramientas tecnológicas utilizadas para administración y soporte.
- Las finalidades relacionadas con seguridad, soporte técnico, continuidad operativa y cumplimiento normativo.

5.25.2 Uso autorizado de herramientas administrativas

Las herramientas de administración remota, monitoreo, soporte o supervisión, únicamente podrán ser utilizadas por personal autorizado de la Oficina TIC o terceros debidamente habilitados. Toda actividad deberá estar relacionada con:

- Soporte técnico.
- Administración de infraestructura.
- Gestión de incidentes.
- Mantenimiento.
- Monitoreo de seguridad.
- Actividades formalmente autorizadas.

5.25.3 Restricción de actividades no autorizadas

Se prohíbe expresamente:

- Realizar monitoreo oculto no autorizado.

- Acceder a información sin justificación funcional.
- Utilizar herramientas administrativas para fines personales.
- Consultar archivos ajenos sin necesidad técnica.
- Activar conexiones remotas sin autorización institucional.
- Utilizar credenciales de otros usuarios.
- Extraer información institucional sin autorización.
- Realizar cualquier actividad que vulnere la privacidad, confidencialidad o integridad de la información.

5.25.4 Principio de mínimo privilegio

Los privilegios administrativos deberán asignarse únicamente conforme a las funciones requeridas y durante el tiempo estrictamente necesario.

Los accesos privilegiados deberán:

- Estar documentados.
- Ser trazables.
- Contar con mecanismos de control.
- Estar sujetos a revisión periódica.

5.25.5 Trazabilidad y registro del monitoreo

Toda actividad administrativa o privilegiada deberá generar registros que permitan identificar:

- Usuario administrador.
- Fecha y hora.
- Sistema o equipo intervenido.
- Actividad realizada.
- Herramienta utilizada.
- Evidencia técnica asociada.

5.25.6 Acceso remoto a equipos institucionales

Las conexiones remotas realizadas sobre equipos institucionales deberán efectuarse únicamente para actividades autorizadas de soporte o administración tecnológica.

Siempre el usuario final deberá:

- Conocer la existencia de la sesión remota.
- Identificar al personal que realiza la conexión.
- Ser informado del propósito de la intervención.

5.25.7 Supervisión de usuarios privilegiados

La Oficina TIC deberá implementar mecanismos de supervisión, auditoría y control sobre las cuentas con privilegios elevados, con el fin de prevenir abuso de accesos, modificaciones no autorizadas o uso indebido de herramientas administrativas.

5.25.8 Reporte de posibles irregularidades

Todo funcionario, contratista o tercero podrá reportar posibles irregularidades relacionadas con accesos no autorizados, abuso de privilegios o actividades sospechosas, a través de los canales institucionales definidos para gestión de incidentes de seguridad de la información.

5.25.8 Incumplimiento lineamientos establecidos

El uso indebido de privilegios administrativos o herramientas de monitoreo será considerado una violación grave a la Política de Seguridad de la Información y podrá dar lugar a:

- Revocatoria inmediata de accesos.
- Investigaciones disciplinarias.
- Acciones contractuales.
- Reporte a entes de control.
- Demás medidas legales aplicables.

5.26 Política para el uso de equipos portátiles personales o de terceros en la red institucional

Con el fin de proteger la infraestructura tecnológica, la información institucional y los servicios digitales de la alcaldía municipal de Chía, se establecen los siguientes lineamientos para el uso de equipos portátiles personales o de terceros que requieran conectividad o interacción con la red institucional.

El acceso de equipos personales o de terceros a la red institucional no constituye un derecho automático y estará sujeto a:

- Validación técnica.
- Necesidad funcional.
- Disponibilidad tecnológica.
- Evaluación de riesgos realizada por la Oficina TIC.

5.26.1 Registro y autorización

Todo equipo portátil externo que requiera acceso a la red institucional deberá:

- Estar previamente autorizado por la Oficina TIC.
- Registrarse en inventario o control de acceso.
- Identificar usuario responsable.
- Registrar dirección MAC o identificador técnico cuando aplique.
- Contar con validación previa de seguridad.

5.26.2 Requisitos mínimos de seguridad

Los equipos externos deberán cumplir, como mínimo, con:

- Sistema operativo soportado y actualizado.
- Antivirus activo y actualizado.
- Firewall habilitado.
- Bloqueo automático de sesión.
- Contraseñas robustas.
- Cifrado de disco cuando aplique.
- Ausencia de software no autorizado o potencialmente malicioso.

La Oficina TIC podrá negar el acceso a equipos que representen riesgo para la infraestructura institucional.

5.26.3 Restricción de acceso

Los equipos externos únicamente podrán acceder a:

- Servicios autorizados.
- Redes segmentadas.
- Plataformas requeridas para el desarrollo contractual.
- Recursos previamente definidos por la Oficina TIC.

5.26.4 Segmentación de red

La Oficina TIC deberá implementar mecanismos de segmentación y control que permitan aislar los equipos externos de:

- Servidores críticos,
- Bases de datos institucionales,
- Infraestructura sensible,
- Sistemas misionales,
- Demás activos críticos de información.

5.26.5 Instalación de software institucional

La Oficina TIC podrá requerir la instalación de controles mínimos de seguridad en equipos externos, tales como:

- Agentes antivirus.
- Herramientas de monitoreo.
- VPN institucional.
- Controles de acceso.
- Mecanismos de autenticación.

La instalación deberá limitarse exclusivamente a controles relacionados con la seguridad institucional y el acceso autorizado.

5.26.6 Uso de dispositivos externos

No se permitirá el uso de:

- Software no licenciado.
- Herramientas de hacking no autorizadas.
- Dispositivos USB.
- Redes no seguras.
- Aplicaciones que comprometan la seguridad institucional.

5.26.7 Responsabilidad del usuario

El usuario responsable del equipo externo deberá:

- Custodiar adecuadamente el dispositivo.
- Proteger credenciales institucionales.
- Evitar compartir accesos.
- Reportar incidentes de seguridad.
- Permitir validaciones técnicas autorizadas.
- Cumplir la Política de Seguridad de la Información.

5.26.8 Revocatoria de acceso a la red institucional

La Oficina TIC podrá suspender o bloquear inmediatamente el acceso de equipos externos cuando:

- Se detecten riesgos de seguridad.
- Exista incumplimiento de la política.
- Se identifique software malicioso.
- Finalice la relación contractual.
- Se comprometa la integridad de la infraestructura institucional.

5.26.9 Restricción de soporte técnico sobre equipos personales

La Oficina de Tecnologías de la Información y las Comunicaciones – TIC no prestará sobre equipos de propiedad de contratistas, funcionarios o terceros, servicios de:

- Mantenimiento preventivo.
- Mantenimiento correctivo.
- Reparación física.
- Actualización de hardware.
- Instalación de componentes.
- Formateo.
- Recuperación de información personal.
- Instalación de software personal.
- Ni soporte técnico particular.

La gestión de soporte de la Oficina TIC se limitará exclusivamente a:

- Activos tecnológicos institucionales.
- Plataformas oficiales.
- Servicios autorizados.
- Configuraciones requeridas para acceso seguro a recursos institucionales.

5.26.10 Restricción de recepción y custodia de equipos personales

La Oficina TIC no recibirá en custodia equipos personales de contratistas o funcionarios para procesos de reparación, mantenimiento o almacenamiento.

La entidad no asumirá responsabilidad, sobre equipos particulares, por:

- Pérdida de información.
- Daño físico.
- Pérdida de componentes.
- Alteraciones de configuración.
- Incompatibilidades.
- Ni fallas de funcionamiento.

5.26.11 Verificación de software licenciado

La Oficina TIC no será responsable de validar integralmente el licenciamiento del software instalado en equipos personales o de terceros. No obstante, cuando un equipo requiera acceso a la infraestructura institucional, la Oficina TIC podrá realizar validaciones básicas orientadas exclusivamente a verificar:

- Que el sistema operativo se encuentre activo.
- Que no existan indicios evidentes de software ilegal o alterado.
- Que el equipo no represente riesgo de seguridad.
- Que cuente con herramientas mínimas de protección requeridas.

La validación de licenciamiento no constituirá certificación legal, auditoría de software ni aprobación integral del estado del equipo.

5.26.12 Responsabilidad sobre equipos personales

Todo contratista, funcionario o tercero que utilice equipos personales dentro de la entidad será responsable de:

- Mantenimiento del equipo,
- Legalidad del software instalado,
- Respaldo de información,
- Funcionamiento del dispositivo,
- Cumplimiento de obligaciones legales relacionadas con propiedad intelectual y licenciamiento.

5.26.13 Prevención de riesgos institucionales

Con el fin de prevenir:

- Pérdida de activos,
- Conflictos internos,
- Uso indebido de recursos públicos,
- Contaminación de responsabilidad institucional,
- Riesgos disciplinarios o de seguridad,

la Oficina TIC deberá abstenerse de intervenir físicamente equipos particulares salvo actividades estrictamente necesarias para habilitar acceso institucional autorizado.

5.27 Política para sistemas de videovigilancia, control biométrico y protección de la privacidad

Con el fin de garantizar la seguridad física, la protección de los activos institucionales, el control de acceso a las instalaciones y la prevención de incidentes de seguridad, la alcaldía municipal de Chía podrá implementar mecanismos tecnológicos de videovigilancia y control biométrico en sus sedes administrativas.

La implementación y operación de dichos mecanismos deberá realizarse bajo principios de legalidad, proporcionalidad, transparencia, necesidad, protección de datos personales y respeto por la dignidad, privacidad y derechos de funcionarios, contratistas, ciudadanos y terceros.

Los presentes lineamientos se encuentran alineados con:

- Ley 1581 de 2012: Por la cual se dictan disposiciones generales para la protección de datos personales
- Ley 1266 de 2008: Por la cual se dictan las disposiciones generales del hábeas data
- Principios constitucionales de intimidad y habeas data
- ISO/IEC 27001:2022
- ISO/IEC 27701

5.27.1 Finalidad de los sistemas de videovigilancia y control biométrico

Los sistemas de videovigilancia y control biométrico únicamente podrán utilizarse para:

- Control de acceso físico.
- Protección de personas y activos.
- Seguridad institucional.
- Prevención de incidentes.
- Control perimetral.
- Investigación de eventos de seguridad.

En ningún caso dichos mecanismos podrán implementarse con fines de:

- Persecución laboral,
- Vigilancia arbitraria,
- Control desproporcionado del comportamiento,
- Monitoreo indebido de conversaciones privadas,
- Hostigamiento,
- Discriminación,
- Afectación de derechos fundamentales.

5.27.2 Transparencia y comunicación

La entidad deberá informar de manera clara y visible sobre la existencia de:

- Cámaras de videovigilancia.

- Sistemas biométricos.
- Grabación de imágenes.
- Controles de acceso.
- Finalidades del tratamiento de datos.

La información deberá comunicarse mediante:

- Avisos visibles.
- Políticas institucionales.
- Comunicaciones internas.
- Mecanismos de divulgación institucional.

5.27.3 Restricción sobre grabación de audio

Los sistemas de videovigilancia institucional deberán priorizar la captura de video con fines de seguridad física. La grabación de audio únicamente podrá realizarse cuando:

- Exista justificación técnica o legal,
- Se encuentre autorizada institucionalmente,
- Se informe previamente a los titulares de la información.

No se permitirá la utilización de mecanismos ocultos de grabación de conversaciones ni interceptación de comunicaciones sin autorización legal competente.

5.27.4 Ubicación de cámaras

Las cámaras deberán instalarse únicamente en áreas relacionadas con seguridad institucional y control operativo. Se prohíbe la instalación de cámaras en:

- Baños.
- Vestidores.
- Áreas de descanso privadas.
- Espacios que comprometan la intimidad personal.
- Lugares donde exista expectativa razonable de privacidad.

Las cámaras ubicadas cerca de zonas sensibles deberán orientarse exclusivamente a accesos, pasillos o áreas de circulación general.

5.27.5 Proporcionalidad del monitoreo

La implementación de sistemas de vigilancia deberá responder a análisis de riesgo, necesidad y proporcionalidad, evitando monitoreo excesivo o invasivo frente a las actividades laborales ordinarias.

La videovigilancia no deberá utilizarse como mecanismo permanente de supervisión individualizada del desempeño laboral.

5.27.6 Protección de datos biométricos

Los datos biométricos recolectados mediante sistemas de reconocimiento facial o control de acceso tendrán carácter sensible y deberán tratarse conforme a:

- Principios de confidencialidad.
- Acceso restringido.
- Finalidad específica.
- Minimización.
- Protección reforzada.

La información biométrica únicamente podrá utilizarse para control de acceso y seguridad física institucional.

5.27.7 Acceso a grabaciones y registros

El acceso a grabaciones, imágenes, registros biométricos, logs de acceso, y material audiovisual, deberá limitarse exclusivamente a personal autorizado.

Toda consulta deberá:

- Quedar registrada.
- Justificar finalidad.
- Generar trazabilidad.
- Cumplir procedimientos definidos por la entidad.

5.27.8 Restricción de uso de grabaciones

Las grabaciones y registros obtenidos no podrán:

- Divulgarse sin autorización.
- Compartirse informalmente.
- Utilizarse con fines personales.
- Editarse indebidamente.
- Utilizarse para intimidación.
- Ni emplearse para actividades ajenas a la seguridad institucional.

5.27.9 Reporte de inconformidades o posibles abusos

Funcionarios, contratistas y terceros, a través de los canales institucionales establecidos para seguridad de la información y control interno, podrán reportar posibles irregularidades relacionadas con:

- Uso indebido de cámaras.
- Acceso no autorizado a grabaciones.
- Monitoreo desproporcionado.
- Utilización indebida de información biométrica.
- Posibles afectaciones a la privacidad.

5.27.10 Responsabilidad Administrativa

Los administradores de sistemas de videovigilancia y control biométrico deberán:

- Custodiar adecuadamente la información,
- Restringir accesos,
- Garantizar trazabilidad,
- Proteger credenciales,
- Cumplir las políticas institucionales de seguridad y privacidad.

5.28 Política para la creación y uso de conexiones VPN institucionales

Con el fin de garantizar el acceso remoto seguro a los recursos tecnológicos de la Alcaldía Municipal de Chía, se establecen los siguientes lineamientos para la creación, administración y uso de conexiones VPN (Virtual Private Network), orientados a proteger la confidencialidad, integridad y disponibilidad de la información institucional.

El acceso mediante VPN no constituye un derecho automático y deberá otorgarse únicamente cuando:

- Exista necesidad funcional.
- Se justifique técnicamente.
- El acceso remoto sea indispensable para el cumplimiento de funciones.
- Se cuente con aprobación formal de la Oficina TIC.

5.28.1 Solicitud y aprobación

Toda creación de acceso VPN deberá:

- Solicitarse formalmente.
- Justificar necesidad operativa.
- Definir alcance de acceso.
- Identificar usuario responsable.
- Establecer tiempo de vigencia.
- Contar con aprobación de la Oficina TIC y/o el jefe inmediato.

5.28.2 Principio de mínimo privilegio

Los accesos VPN deberán limitarse exclusivamente a:

- Sistemas requeridos.
- Servicios autorizados.
- Recursos necesarios para las funciones del usuario.

No se permitirá acceso irrestricto a la infraestructura interna institucional.

5.28.3 Requisitos técnicos de seguridad

Todo equipo autorizado para conexión VPN deberá cumplir como mínimo con:

- Sistema operativo soportado y actualizado.
- Antivirus activo y actualizado.

- Firewall habilitado.
- Mecanismos de autenticación segura.
- Bloqueo automático de sesión.

La Oficina TIC podrá negar o revocar accesos cuando el equipo represente riesgo para la entidad.

5.28.4 Autenticación

Las conexiones VPN deberán implementar mecanismos de autenticación robusta, incluyendo:

- Credenciales institucionales.
- Autenticación multifactor (MFA) cuando técnicamente sea posible.
- Certificados digitales.
- Mecanismos equivalentes definidos por la Oficina TIC.

5.28.5 Restricción de equipos compartidos o públicos

No se permitirá el acceso VPN desde:

- Equipos públicos.
- Cafés internet.
- Dispositivos compartidos no controlados.
- Equipos comprometidos.
- Dispositivos que no cumplan requisitos mínimos de seguridad.

5.28.6 Trazabilidad y monitoreo

Toda conexión VPN deberá generar registros de auditoría que permitan identificar:

- Usuario conectado.
- Fecha y hora.
- Dirección IP.
- Duración de sesión.
- Recursos accedidos.
- Eventos de seguridad asociados.

La Oficina TIC podrá monitorear conexiones VPN con fines de:

- Seguridad.
- Auditoría.
- Prevención de incidentes.
- Protección de activos institucionales.

5.28.7 Responsabilidad del usuario

Las conexiones VPN únicamente podrán utilizarse para fines institucionales.

Se prohíbe:

- Compartir credenciales.
- Utilizar VPN para actividades personales no autorizadas.

- Transferir información institucional a servicios externos no autorizados.
- Instalar herramientas no aprobadas.
- Realizar actividades que comprometan la seguridad institucional.

5.28.8 Restricción de uso

Las conexiones VPN únicamente podrán utilizarse para fines institucionales.

Se prohíbe:

- Compartir credenciales.
- Utilizar VPN para actividades personales no autorizadas.
- Transferir información institucional a servicios externos no autorizados.
- Instalar herramientas no aprobadas.
- Realizar actividades que comprometan la seguridad institucional.

5.28.9 Vigencia y revocatoria

Los accesos VPN deberán revisarse periódicamente y revocarse cuando:

- Finalice la relación contractual o laboral.
- Cambien las funciones del usuario.
- Exista inactividad prolongada.
- Se identifiquen riesgos de seguridad.
- Desaparezca la necesidad operativa.

5.28.10 Vigencia y revocatoria

Los accesos VPN deberán revisarse periódicamente y revocarse cuando:

- Finalice la relación contractual o laboral.
- Cambien las funciones del usuario.
- Exista inactividad prolongada.
- Se identifiquen riesgos de seguridad.
- Desaparezca la necesidad operativa.

5.28.11 Conexiones de terceros

Los proveedores o terceros que requieran acceso VPN deberán:

- Firmar acuerdos de confidencialidad.
- Cumplir requisitos de seguridad institucional.
- Utilizar accesos individuales.
- Limitarse exclusivamente a los recursos autorizados.

5.29 Política para la gestión de información sensible en espacios compartidos

La información institucional clasificada como reservada, confidencial o sensible no deberá ser visualizada, discutida o manipulada en espacios abiertos, zonas de circulación o áreas compartidas donde pueda ser observada por personas no autorizadas.

Los funcionarios y contratistas deberán adoptar medidas razonables para evitar exposición involuntaria de información institucional en pasillos, ascensores, salas de espera, espacios de atención, cafeterías, reuniones informales o entornos virtuales compartidos.

5.30 Política para la seguridad en reuniones virtuales

Las reuniones virtuales institucionales deberán implementar medidas básicas de seguridad, incluyendo:

- Control de participantes.
- Uso de enlaces autorizados.
- Validación de asistentes.
- Protección de grabaciones.
- Restricción de acceso no autorizado.

5.31 Política para el uso responsable de inteligencia artificial y herramientas generativas

La utilización de herramientas de inteligencia artificial generativa deberá realizarse de manera responsable, segura y alineada con los principios de confidencialidad, protección de datos y seguridad de la información.

Los funcionarios y contratistas podrán utilizar herramientas de inteligencia artificial como apoyo para elaboración de documentos, análisis de información, automatización de tareas, asistencia técnica, apoyo metodológico y fortalecimiento de procesos institucionales, siempre que:

- No se compartan credenciales,
- No se divulgue información clasificada o reservada,
- No se incorporen datos personales sensibles sin autorización,
- Se minimice la exposición de información institucional,
- Los resultados sean revisados y validados por el usuario responsable.

5.31.1 Restricciones

No deberá ingresarse en plataformas públicas de inteligencia artificial:

- Bases de datos institucionales completas.
- Información reservada.
- Vulnerabilidades críticas.
- Configuraciones sensibles.
- Información protegida por reserva legal.
- Ni datos personales sensibles sin autorización institucional.

5.32 Política de administración de riesgos

5.32.1 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.

5.32.2 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.

5.32.3 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.

5.32.4 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.

5.33 Política de cumplimiento

Esta política busca asegurar que funcionarios, contratistas, proveedores, terceros y demás usuarios de los recursos TIC conozcan, acepten, apliquen y cumplan las disposiciones de seguridad de la información, con el fin de proteger la confidencialidad, integridad, disponibilidad, autenticidad y trazabilidad de la información institucional.

5.33.1 Principios de cumplimiento

El cumplimiento de la Política de Seguridad de la Información se regirá por los siguientes principios:

- **Legalidad:** toda actuación deberá ajustarse a la constitución, la ley, los actos administrativos, la normatividad de protección de datos y las políticas institucionales.
- **Responsabilidad:** cada usuario será responsable del uso adecuado de la información y los recursos tecnológicos asignados.
- **Confidencialidad:** la información institucional solo podrá ser conocida, utilizada o divulgada por personas autorizadas.
- **Integridad:** la información deberá conservarse exacta, completa y protegida contra modificaciones no autorizadas.
- **Disponibilidad:** los activos de información deberán estar disponibles para los usuarios autorizados cuando se requieran.
- **Trazabilidad:** las actuaciones sobre activos de información y recursos TIC deberán poder ser verificadas mediante registros, evidencias o controles.
- **Mínimo privilegio:** los accesos deberán limitarse estrictamente a lo requerido para el cumplimiento de funciones u obligaciones contractuales.

- **Transparencia:** los usuarios deberán conocer las reglas, controles y condiciones aplicables al uso de los recursos tecnológicos institucionales.
- **Proporcionalidad:** las medidas de control y seguimiento deberán ser adecuadas al riesgo identificado.

5.33.2 Obligación de conocimiento, aceptación y aplicación

Todos los funcionarios, contratistas, proveedores y terceros que accedan a información o recursos tecnológicos institucionales deberán conocer, aceptar y cumplir la Política de Seguridad de la Información y sus lineamientos complementarios.

El desconocimiento de la política no exime a los usuarios de las responsabilidades derivadas de su incumplimiento.

5.33.3 Responsabilidad individual y compartida

La seguridad de la información es una responsabilidad compartida entre la alta dirección, la Oficina TIC, líderes de proceso, funcionarios, contratistas y terceros.

Cada usuario será responsable de:

- Proteger sus credenciales.
- Usar adecuadamente los recursos tecnológicos.
- No divulgar información institucional sin autorización.
- Reportar incidentes, riesgos o accesos sospechosos.
- Cumplir los controles definidos por la entidad.
- Abstenerse de realizar acciones no autorizadas sobre sistemas, equipos o información.
- Participar en actividades de capacitación y sensibilización.
- Respetar la privacidad y derechos de otros usuarios.

5.33.4 Cumplimiento por parte de secretarios, directores y jefes de oficina

Los secretarios, directores y jefes de oficina deberán promover y verificar el cumplimiento de la política de seguridad de la información dentro de sus dependencias o equipos de trabajo.

En particular deberán:

- Facilitar la participación de su personal en actividades de capacitación.
- Reportar oportunamente cambios de vinculación, retiro, traslado o modificación de funciones.
- Solicitar formalmente la creación, modificación o retiro de accesos.
- Velar porque los contratistas cumplan los lineamientos de seguridad.
- Coordinar con la Oficina TIC la atención de riesgos o incidentes.
- Evitar prácticas informales que puedan comprometer la seguridad de la información.

5.33.5 Cumplimiento por parte de contratistas y proveedores

Todo contratista o proveedor que tenga acceso a información, instalaciones, sistemas o recursos tecnológicos de la alcaldía municipal de Chía deberá cumplir la política de seguridad de la información como condición para el desarrollo de sus obligaciones contractuales.

Los contratos, órdenes de prestación de servicios o documentos equivalentes deberán contemplar, cuando aplique:

- Obligación de confidencialidad.
- Cumplimiento de políticas de seguridad.
- Protección de datos personales.
- Restricciones sobre uso de información institucional.
- Devolución o eliminación segura de información al finalizar la relación contractual.
- Prohibición de uso no autorizado de sistemas, credenciales o recursos TIC.
- Responsabilidad por incumplimientos de seguridad atribuibles al contratista o proveedor.

5.33.6 Gestión de incumplimientos

Cuando se identifique un posible incumplimiento de la política de seguridad de la información, la entidad deberá:

- Registrar el evento o situación identificada.
- Analizar los hechos y evidencias disponibles.
- Determinar el nivel de riesgo o afectación.
- Definir si corresponde a incidente de seguridad, incumplimiento administrativo, contractual o disciplinario.
- Implementar medidas de contención o corrección.
- Escalar el caso a la instancia competente cuando corresponda.
- Documentar las acciones realizadas.
- Generar acciones de mejora para evitar recurrencia.

La gestión de incumplimientos deberá realizarse respetando el debido proceso, la proporcionalidad y las competencias de cada dependencia.

5.33.7 Medidas preventivas y correctivas

Frente a incumplimientos o riesgos identificados, la entidad podrá adoptar medidas preventivas o correctivas, tales como:

- Reinducción o capacitación obligatoria.
- Advertencia formal.
- Restricción temporal de accesos.
- Revocatoria de privilegios.
- Bloqueo de cuentas.
- Retiro de equipos no autorizados de la red.
- Ajustes de configuración.
- Actualización de procedimientos.
- Fortalecimiento de controles.
- Reporte a contratación y/o al ordenador del gasto.
- Escalamiento a control interno disciplinario o instancia competente.

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 comunicaciones internas y externas, lideradas por 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.
- 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

Temario	Recursos
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 Infraestructura Informática)
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 Soporte Técnico)

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 de cada una de las áreas de la Oficina TIC, según sus competencias.

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 la Oficina asesora 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.

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 aĺicarám acciones contractuales.
- 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 al ordenador del gasto y/o 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

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
3	Mayo / 2026 Agosto / 2026	Ing. Eliany Rocío Montejo Carrascal - Profesional especializado	Ing. Gustavo Carvajal Millán - jefe de Oficina TIC Comité de gestión y desempeño