POLÍTICA SEGURIDAD DE LA INFORMACIÓN
ALCALDÍA MUNICIPAL DE CHÍA

OFICINA DE TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES

Versión 3: Actualización

Chía, Agosto 2022

Bibliografía: Caja de herramientas MinTic

CONTENIDO

Bibliografía: Caja de herramientas MinTic

1. INTRODUCCIÓN

La alcaldía municipal de Chía, dando cumplimiento al 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” y reconociendo la necesidad de proteger los activos de información de la alcaldía municipal de Chía, mediante un modelo de seguridad y privacidad de la información o sistema de gestión de seguridad de la información.

Teniendo en cuenta la norma técnica NTC-ISO/IEC 27001:2013 y el habilitador de seguridad de la información de gobierno digital del Ministerio de Tecnologías de la Información y la Comunicaciones, se debe establecer una política general de seguridad de la información, políticas y procedimientos de seguridad de la información para salvaguardar y proteger los activos en sus tres pilares: Confidencialidad, Integridad y Disponibilidad.

2. ALCANCE

Esta política deberá ser conocida, cumplida y aplicada a todos los secretarios, directores, funcionarios y contratistas de cada proceso de la alcaldía municipal de Chía.

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.

Bibliografía: Caja de herramientas MinTic

4. MARCO LEGAL

- 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
- 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 alcaldía municipal de Chía, de acuerdo a la resolución 500 del 2021, del Ministerio de Tecnologías de la Información y las Comunicaciones, establece que es necesario preservar la confidencialidad, integridad y disponibilidad de los activos de información de cada proceso de la alcaldía municipal de Chía, mediante la implementación de un sistema de gestión de seguridad de la información o modelo de seguridad y privacidad de la información, mediante procesos y políticas establecidas por la norma NTC-ISO-27001:2013.

La alcaldía municipal de Chía se compromete a proteger los activos de información de cada proceso, de acuerdo a su criticidad para minimizar los impactos financieros y legales.

La alcaldía municipal de Chía, se compromete a identificar y establecer controles para mitigar los diferentes riesgos que puedan afectar los activos de información y la continuidad de algún proceso de la alcaldía municipal de Chía.

5.1. OBJETIVOS

Definir los lineamientos para privacidad de la información de la Alcaldía Municipal de Chía.

Establecer las políticas en seguridad de la información necesarias para la protección de activos de información, las cuales se desarrollan alineadas con el MPSI el anexo A de la norma ISO/IEC 27001:2013, así como el cumplimiento de los requisitos legales, contractuales y normativos vigentes aplicables la Alcaldía Municipal de Chía.

Implementar y mejorar continuamente el Modelo de Seguridad y Privacidad de la Información (MSPI) como mecanismo para brindar a los ciudadanos y colaboradores confianza digital en torno al uso de los datos, al cumplimiento legal y mantener una actitud ética, transparente y en concordancia con a misión y la visión de la Entidad.

5.2. ROLES Y RESPONSABILIDADES

Comité Institucional de Gestión y Desempeño: Comunicar a los funcionarios, contratistas y/o particulares que participan en actividades de forma directa o indirecta con la entidad, la importancia de satisfacer los requisitos de seguridad digital.

Líderes de proceso: Identificar e inventariar los nuevos activos digitales de información y los riesgos cibernéticos asociados

Responsable de TI: Participar en la elaboración del cronograma de capacitación de seguridad en la entidad. Implementar las mejoras identificadas en la plataforma de seguridad que estén relacionadas con hardware, software, canales de comunicación de datos o Infraestructura TI.

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

5.3. POLÍTICA DE DISPOSITIVOS MÓVILES

Los funcionarios y contratistas no están autorizados a cambiar la configuración, ni la instalación/desinstalación de las aplicaciones móviles de los dispositivos institucionales que se les entregue como recurso para la ejecución de sus obligaciones o funciones.

La oficina de tecnologías de la información y las comunicaciones (TIC) es la única encargada de realizar la configuración y descarga de software de los dispositivos móviles institucionales.

El personal de la alcaldía municipal de chía tiene una cuenta de correo electrónico institucional y por tal motivo los dispositivos móviles deben ser configurados con esa cuenta para su uso.

Los dispositivos móviles no se podrán conectar a redes inalámbricas públicas.

Los dispositivos móviles deben contar con mecanismos de contraseña o bloqueo de pantalla cuando no estén en uso.

Los servidores públicos deben evitar conectar los dispositivos móviles institucionales a puertos USB de computadores públicos, hoteles o café internet, terminales y demás sitios de acceso público.

Los servidores públicos y contratistas deben notificar los dispositivos móviles institucionales con sospecha de infección por malware al personal técnico responsable de la entidad para el proceso de análisis, evaluación y tratamiento.

Cada uno de los funcionarios y/o contratistas de la alcaldía municipal de Chía es responsable del buen uso de los dispositivos móviles a su cargo.

5.4 POLÍTICA DE SEGURIDAD DE LOS RECURSOS HUMANOS

Todo servidor público y contratista debe recibir sensibilización en seguridad y privacidad de la información.

El incumplimiento o la violación de las políticas de seguridad de la información de la Entidad, por parte de los colaboradores o terceros se les aplicará lo establecido en el proceso de investigaciones disciplinarias.

En cualquier situación que se deba realizar el tratamiento de la información personal de algún ciudadano y/o servidor público, se deberá contar con el consentimiento por escrito al titular de los datos para realizar el ejercicio y tener un registro del mismo.

Se deberá garantizar al dueño de la información, en todo tiempo, el pleno y efectivo ejercicio del derecho de hábeas data.

Se deberá informar con prontitud cuando se presenten violaciones a los códigos de seguridad y existan riesgos en la administración de la información de los servidores públicos

5.5 POLÍTICA GESTIÓN DE ACTIVOS DE INFORMACIÓN

La alcaldía municipal de Chía realiza la identificación y clasificación de activos de información, así como la definición de la asignación de responsables.

Cada activo de información de la entidad debe tener un responsable que debe velar por su seguridad. Los propietarios de la información deben garantizar que todos los activos de información reciban un apropiado nivel de protección basado en su valor de confidencialidad, integridad, disponibilidad, riesgos identificados y/o requerimientos legales de retención.

Es responsabilidad del líder del proceso, jefe de área o director, la identificación y reporte de nuevos activos de información, así mismo mantener actualizada la valoración de estos.

Los servidores públicos y contratistas deben hacer la devolución de los activos de información asignados a su cargo una vez finalice la relación contractual con la entidad.

Todos los activos de información deben contar con un responsable, que asegure la protección de la información y los datos que son almacenados en cada uno de ellos.

5.6 POLÍTICA DE CONTROL DE ACCESO

Todos los servidores públicos y contratistas con acceso a un sistema de información o a la red informática institucional, dispondrán de una única autorización de acceso

compuesta de identificador de usuario y contraseña y serán responsables de las acciones realizadas por el usuario que les ha sido asignado.

Si una entidad, empresa o personal externo requiere acceso a la información sensible o crítica se deben suscribir acuerdos de confidencialidad o de no divulgación para salvaguardar la información, así como el cumplimiento de la normatividad vigente.

Las claves son de uso personal e intransferible y es responsabilidad del usuario el uso de las credenciales asignadas.

Sólo el personal designado por la Oficina de Tecnologías de la Información y las Comunicaciones está autorizado para configurar la red, instalar software o hardware en los equipos, servidores e infraestructura de tecnología de la Alcaldía Municipal de Chía.

Toda actividad que requiera acceder a los servidores, equipos o a las redes de la Alcaldía Municipal de Chía, se debe realizar en las instalaciones y con el personal especializado. No se debe realizar ninguna actividad de tipo remoto sin la debida autorización la Oficina de Tecnologías de la Información y las Comunicaciones.

El uso de las cuentas de correo electrónico debe cumplir con los estándares de creación y utilización de cuentas de usuario definidos en el procedimiento de correos electrónicos

La Oficina de Tecnologías de la Información y las Comunicaciones suministra a los usuarios las contraseñas de acceso a los servicios de red, servicios y sistemas de información que requiera para el desempeño de sus funciones laborales.

La creación y retiro de usuarios en los sistemas de información en producción debe seguir un procedimiento de creación, edición y estado de baja de usuarios.

5.7 POLÍTICA DE SEGURIDAD FÍSICA Y DEL ENTORNO

Para todos los usuarios de las aplicaciones y sistemas de información de la Alcaldía Municipal de Chía es obligatorio que las sesiones sean cerradas al finalizar las actividades y no deben quedar abiertas o desatendidas.

Las áreas seguras, dentro de las cuales se encuentran el Datacenter, centros de cableado, áreas de archivo, áreas de recepción y entrega de correspondencia, centros de datos físicos y digitales, áreas de procesamiento de información, entre

otros, deben contar con mecanismos de protección física y ambiental, y controles de acceso adecuados para la protección de la información.

Para el acceso a áreas seguras de la Administración Municipal se manejan accesos por medio de clave, huella, carnet institucional o permisos especiales según corresponda.

Todas las entradas que utilizan sistemas de control de acceso deben permanecer cerradas y es responsabilidad de todos los funcionarios, contratistas, colaboradores y terceros autorizados, como medida de seguridad, evitar que las puertas se dejen abiertas.

Los perímetros de seguridad para oficinas, recintos e instalaciones de la Administración Municipal que manejen o generen información sensible (bases de datos, archivos, almacenes, etc.) deben estar delimitados por una barrera, como una pared, puerta de acceso controlado por un dispositivo de autenticación o una oficina de recepción, atendida por personal de la Administración Municipal que controle el acceso físico a estas áreas.

Los puestos de trabajo de los funcionarios de la Administración Municipal deberán permanecer limpios y libres de documentación sensible y/o clasificada cuando se encuentren fuera de horario laboral o en ausencia prolongada del sitio, lo anterior con el fin de evitar accesos no autorizados a la información.

Las personas que trabajan o laboran en la Alcaldía Municipal de Chía, son responsables de bloquear, suspender o apagar los equipos tecnológicos (impresoras, equipos de cómputo, escáner y portátiles) cuando no estén en uso. Al finalizar actividades laborales, se deberán cerrar todas las aplicaciones y dejar los equipos respectivamente apagados

Los documentos con información confidencial o clasificada se deben retirar de la impresora, fotocopiadora, escáneres y/o fax para evitar la pérdida o robo de información de estos documentos.

5.8 POLÍTICAS DE CONTROLES CRIPTOGRÁFICOS

El acceso remoto a la red y a los sistemas de información de la Alcaldía Municipal de Chía, desde una red externa, se realizará a través de conexiones seguras.

Todo sistema de información o servicio tecnológico debe incluir parámetros de seguridad basado en usuarios, perfiles y roles, para ser aplicados en la autorización y autenticación según corresponda.

La asignación de claves y usuarios para el cifrado de información se debe realizar la solicitud formal a la Oficina de Tecnologías de la Información y las Comunicaciones justificando la necesidad.

La Oficina de Tecnologías de la Información y las Comunicaciones proveerá la herramienta de encriptación de datos a quien lo requiera, previa solicitud formal.

5.9 POLÍTICAS SEGURIDAD EN LAS OPERACIONES

La Oficina de Tecnologías de la información y Comunicaciones, documenta los procesos operacionales de TI, para reducir los riesgos asociados con la ausencia de personal y afectaciones en la infraestructura tecnológica.

La Oficina TIC, garantiza que las operaciones tecnológicas se realicen de manera correcta y se brinde seguridad dentro de las aplicaciones y/o sistemas de información.

La Oficina TIC, garantiza el respaldo de la información sensible de las Bases de datos, bajo procesos seguros en el Datacenter.

El equipo de soporte técnico de la Oficina TIC, es el encargado de aplicar los parches de actualizaciones del sistema operativo y ofimática.

5.10 POLÍTICAS SEGURIDAD DE LAS COMUNICACIONES

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.

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.

En la Alcaldía Municipal de Chía la correspondencia virtual se maneja mediante el correo institucional de cada dependencia de la Administración Municipal de Chía.

Existen software o aplicaciones que designan las Contralorías o Procuradurías para la transferencia de la información de diferentes dependencias de la Administración

Municipal de Chía donde se asignan un usuario y contraseña permitiendo enviar todo tipo de informes y documentos de manera más eficiente y segura.

5.11 Política Adquisición, Desarrollo y Mantenimiento de Sistemas

La Alcaldía Municipal de Chía busca que la seguridad de la información sea parte integral dentro del ciclo de vida de los sistemas de información y en la adquisición de aquellos que presten servicios a la entidad.

La Alcaldía Municipal de Chía asegura que se diseñe e implemente los requerimientos de seguridad de software, ya sea desarrollado o adquirido que incluya controles de autenticación y verificación de datos de entrada y salida.

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

La Alcaldía Municipal de Chía cuenta con una metodología de desarrollo seguro de software.

5.12 Política de Relaciones con los Proveedores

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

La Alcaldía Municipal de Chía realiza revisiones periódicas al cumplimiento de las políticas de seguridad y privacidad de la información a los proveedores.

5.13 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.

La Alcaldía Municipal de Chía debe asegurarse que todos los servidores públicos y contratistas conocen y aplican un procedimiento rápido y eficaz para actuar ante cualquier incidente en materia de seguridad de la información, para ello, tiene establecido en procedimiento de MDS, para el registro de incidentes con sus

pruebas y evidencias, para de esta manera estudiar su origen y evitar que ocurran en un futuro.

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

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

5.14 Política de administración de riesgos

La política tiene como objetivo la identificación, clasificación y valoración de los riesgos digitales o de seguridad de la información en la alcaldía municipal de Chía, basado en la política de gobierno digital y el modelo de seguridad y privacidad de la información.

Esta política se encuentra definida en la política administración de riesgos de la alcaldía Municipal de Chía bajo la Resolución 4578 de 2019 y se deben seguir los lineamientos definidos en esta, inclusive, cada vez que sea objeto de actualizaciones y/o aprobaciones, legalizadas mediante actos administrativos.

Establecer la mejora continua del sistema de gestión de seguridad de la información, a través de un conjunto de reglas y directrices orientadas a garantizar la protección de los activos de información de la Alcaldía Municipal de Chía, de una manera contundente, eficiente y efectiva, de la misma forma velar por tomar las acciones necesarias para la evaluación, análisis y tratamiento de los riesgos de acuerdo a la metodología adoptada por la Administración.

La Administración Municipal se compromete a cumplir con todos los requisitos legales, reglamentarios y contractuales que haya a lugar, con el fin de gestionar y reducir los riesgos a un nivel aceptable.

5.15 Política de contraseñas seguras

La clave de acceso al servicio de correo electrónico y/o sistemas de información, no debe ser divulgada a ninguna persona, exhibirse en público y para su gestión se debe seguir los controles de protección de contraseñas definidos a continuación:

Cualquier servicio, sistema de información, correo electrónico o equipo informático que tenga contraseñas por defecto configuradas por el proveedor o fabricante deben ser cambiadas por nuevas contraseñas.

La contraseña asignada a un usuario es personal e intransferible. Los usuarios no deben divulgar, prestar, exhibir, comunicar en forma escrita o verbal su contraseña. Cuando por labores de soporte o mantenimiento se requiere la contraseña de usuario, el usuario es quién debe digitarla y al final de las actividades de soporte se debe cambiar por una contraseña nueva.

Los usuarios deben cambiar mínimo cada dos meses sus contraseñas de acceso a servicios.

Adicionalmente las claves o contraseñas deben cumplir con lo siguiente:

- No utilice contraseñas que sean fáciles de deducir.
- Las contraseñas no pueden repetirse con las de los últimos 3 meses.
- Evite las palabras obvias. Ejemplos: Nombre, fecha de cumpleaños, nombre de la mascota, nombre de los hijos, entre otras.
- Utilice caracteres alfanuméricos y especiales.
- Recomendable 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@
- Procure usar caracteres diferentes, que no sean consecutivos o idénticos.
- Use contraseñas diferentes del usuario.
- Siempre procure memorizarla.

Está expresamente prohibido divulgar por cualquier medio las contraseñas.
De acuerdo con la Ley 1273 de 2009, ley de delitos informáticos: “Artículo 269 A. Acceso abusivo a un sistema informático. El que, sin autorización o por fuera de lo acordado, acceda en todo o en parte a un sistema informático protegido o no con una medida de seguridad, o se mantenga dentro del mismo en contra de la voluntad de quien tenga el legítimo derecho a excluirlo, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1000 salarios mínimos legales mensuales vigentes.”

Bibliografía: Caja de herramientas MinTic

5.16 Políticas de ciberseguridad

Inscripción de la Alcaldía Municipal de Chía, en las entidades nacionales ColCert y Csirt, para reportar incidentes de seguridad graves.

Asignar a un responsable de la seguridad digital,

Asignar un responsable de realizar monitoreos de seguridad a los servicios expuestos a través de internet, con el fin de evitar brechas de seguridad.

Realizar copias de seguridad periódicas de los servidores que manejan datos, de manera que haya disponibilidad de la última versión de datos.

5.17 Políticas de cumplimiento

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