POLÍTICA SEGURIDAD DE LA INFORMACIÓN
ALCALDÍA MUNICIPAL DE CHÍA

OFICINA DE TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES

Versión 2: Actualización

Chía, Julio 2021

Cra. 11 No 11 - 29
PBX: 8844444 Ext. 2300
oficinatic@chia.gov.co
www.chia-cundinamarca.gov.co

CONTENIDO

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. OBJETIVO

Establecer la política general de la seguridad de la información, políticas y procedimientos de la seguridad de la información en la alcaldía municipal de Chía, basado en el decreto 1008 de 2018 del Ministerio de las Tecnologías de la Información y las Comunicaciones; y la norma NTC-ISO-27001:2013.

Establecer, implementar y monitorear el modelo de seguridad y privacidad de la información o sistema de gestión de seguridad de la información en la alcaldía municipal de Chía.

3. 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.

4. DEFINICIONES

Activo: cualquier cosa que tiene valor para la organización[1], 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.[2]

Disponibilidad: Propiedad de que la información sea accesible y utilizable por solicitud de una entidad autorizada, cuando ésta así lo requiera[3].

Integridad: Propiedad de salvaguardar la exactitud y estado completo de los activos.[4]

5. 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

[1] (ICONTEC, 2013)
[2] (ICONTEC, NTC ISO/IEC 27000:2013, 2013)
[3] (ICONTEC, NORMA TÉCNICA NTC-ISO/IEC 27001, 2013)
[4] (ICONTEC, NORMA TÉCNICA NTC-ISO/IEC 27001, 2013)

- Ley 44 de 1993. – Derechos de Autor

6. POLÍTICA GENERAL DE SEGURIDAD DE LA INFORMACIÓN

La alcaldía municipal de Chía, de acuerdo al decreto 1008 del 14 de junio de 2018 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.

7. POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN

7.1.Política de protección de datos y privacidad de la información

Definir los lineamientos para la protección de datos y privacidad de la información de datos personales de la Alcaldía Municipal de Chía.

La Alcaldía Municipal de Chía realizará procesos de recolección, almacenamiento, procesamiento, uso y transmisión (según corresponda) de datos personales, atendiendo de manera estricta los postulados de seguridad y confidencialidad postulados en la Ley 1581 de 2012 y el Decreto 1377 de 2013. Teniendo en cuenta lo postulado con anterioridad, se definieron los siguientes lineamientos:

- La Alcaldía Municipal de Chía reconoce que el único medio autorizado para el tratamiento de datos personales es el dueño de la información, de acuerdo a la Ley de protección de datos personales 1581 de 2012 y el decreto 1377 o la que la adicione, modifique o derogue.

- La Alcaldía Municipal de Chía se compromete a otorgar los recursos necesarios para garantizar los tres (3) pilares fundamentales de la seguridad como son la disponibilidad, integridad y confidencialidad de la información, con el fin de dar cumplimiento a los objetivos institucionales, la estrategia y misión de la entidad.

- 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.

- 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 Oficina de Tecnologías de Información y las Comunicaciones se compromete a velar por la aplicación y cumplimiento adecuado de la presente política de seguridad de la información y todas las que se deriven de ella, por parte de todos los funcionarios, contratistas, colaboradores y terceros de la Alcaldía Municipal de Chía.

- 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 conservar la información bajo condiciones de seguridad necesarias para impedir su adulteración, pérdida, consulta, uso o acceso no autorizado o fraudulento.

- En caso tal que la información obtenida contenga datos erróneos, se deberá notificar de inmediato y realizar las correcciones correspondientes en el menor tiempo posible.

- 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.

7.2.Política 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 la guía de administración de riesgos del Departamento Administrativo de la Función Pública – DAFP.

Esta política se encuentra definida en la **política administración de riesgos**

7.3.Política inventario de activos de información

Definir los lineamientos para la clasificación y valoración de activos de información en los procesos de la alcaldía municipal de Chía, basado en gobierno en gobierno digital.

Los lineamientos se encuentran definidos en la **Guía para el inventario, valoración y clasificación de los activos de información.**

7.4.Política de dispositivos móviles

Establecer los estándares para el uso y configuración de los dispositivos móviles suministrados por la alcaldía municipal de chía.

- 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.
- 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.
- El personal que cuente con dispositivos móviles de la alcaldía municipal de Chía no deben enviar documentos, audios, videos e imágenes con información reservada o clasificada.
- 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.
- En caso que el dispositivo móvil contenga información reservada o clasificada de la entidad esta información se deberá cifrar.
- El personal de la alcaldía municipal de chía es responsable del buen uso de los dispositivos móviles a su cargo.

7.5.Política pantalla y escritorio limpio

Establecer los estándares para prevenir el riesgo de acceso no autorizado, pérdida, robo o modificación de la información durante y después de horas laborales.

7.5.1. Pantalla limpia:

- Las personas que trabajan o laboran en la Alcaldía Municipal de Chía, deben bloquear, suspender o apagar los equipos tecnológicos (impresoras, equipos de cómputo, escáner y portátiles) cuando no estén en uso.
- La pantalla se debe conservar limpia, libre de información, que pueda ser utilizada por personas externas y sin autorización para su uso.
- El fondo de pantalla de los equipos de cómputo y portátiles de la Alcaldía Municipal de Chía es establecido por la Oficina de Tecnologías de la Información y las Comunicaciones.
- Cada equipo de cómputo y portátil que se encuentre en el dominio de la Alcaldía Municipal de Chía cuenta con un tiempo establecido para el bloqueo de la pantalla cuando no se encuentre en uso.
- Los equipos de cómputo o portátiles se pueden bloquear o suspender utilizando las teclas Windows + L, o las teclas CTRL + ALT + SUPR.
- Cada equipo de cómputo y portátil que se encuentre en el dominio de la Alcaldía Municipal de Chía cuenta con un sistema de autenticación por usuario y contraseña establecido por la Oficina de Tecnologías de la Información y las Comunicaciones.

7.5.2. Escritorio limpio:

- Las personas que trabajan o laboran en la Alcaldía Municipal de Chía, cuando se ausenten del puesto de trabajo o después del horario laboral deben guardar los documentos o medios de almacenamiento removibles (USB, CD, Discos duros o DVD) que contengan información confidencial o clasificada de la entidad en un gabinete o escritorio con llave.
- Los documentos o medios de almacenamiento removibles (USB, CD, Discos duros o DVD) que se encuentren sin uso o desatendidos se deben guardar.
- Los documentos con información confidencial o clasificada se deben retirar de la impresora, fotocopiadora, escáneres y/o fax.

- Evitar escribir o dejar a la vista las contraseñas de acceso a sistemas, aplicaciones o equipos de cómputo.

7.6.Política gestión de medios removibles

Definir las directrices para la gestión de medios removibles de la Alcaldía Municipal de Chía, cumpliendo con la preservación de la confidencialidad e integridad de la información.

- Como medida preventiva la Oficina de Tecnologías de la Información y las Comunicaciones ha decidido restringir el uso de medios removibles en los equipos de la Alcaldía Municipal de Chía, toda vez que realizado el análisis técnico se detectó como mayor amenaza de contagio de virus informático en los equipos de la Administración Municipal.

- Para habilitar los puertos USB en un equipo, se deberá justificar la solicitud por medio de un oficio al jefe de la Oficina TIC, dicho oficio deberá ser firmado por el Jefe de la Dependencia autorizando la solicitud.

- Para evitar el contagio de virus en los dispositivos de almacenamiento externos, se recomienda no hacer uso de ellos como único medio para reposar (proteger) información de la Administración Municipal.

- No es responsabilidad de la Oficina TIC salvar información en caso que los dispositivos de almacenamiento externo se hayan contagiado de virus o la información haya sido eliminada involuntariamente.

- Se recomienda no utilizar los archivos almacenados en estos dispositivos, para sobre escribir información en ellos, debido a que es un dispositivo que está expuesto a daños por su manipulación y factores externos.

- Como medio alternativo para salvaguardar información importante del funcionario, el correo institucional cuenta con Google Drive, una plataforma de almacenamiento en la nube que cuenta con una capacidad de 30 GB para guardar cualquier tipo de información.

- Toda la información etiquetada como CONFIDENCIAL o RESERVADA que sea almacenada en medios removibles y que se requiera de protección especial, debe cumplir con las directrices de seguridad emitidas por el Oficina de Tecnologías de la Información y las Comunicaciones, específicamente aquellas referentes al empleo de técnicas de cifrado.

- Los funcionarios son responsables en mantener asegurada la información, libre de software malicioso y verificando el escaneo de los dispositivos para verificar que estén libres de virus cada vez que se ingresen en algún equipo.

- Se debe hacer seguimiento a los medios de almacenamiento removibles como Discos Duros, Cintas, etc., con el fin de garantizar que la información sea transferida a otro medio antes de que esta quede inaccesible por deterioro o el desgaste que sufren a causa de su vida útil.

- Al momento en que los dispositivos removibles cumplan su ciclo de vida (ya no sean funcionales), se deberá retirar de la Administración Municipal y asegurar su des habilitación y/o destrucción pertinente.

- Como medida de seguridad se deberá promover el uso de DLP (Prevención de pérdida de datos) cuando se haga uso continuado de dispositivos removibles para el tratamiento de información de la Administración Municipal.

7.7.Política de acceso a redes y servicios en red.

Definir los lineamientos clave para el acceso a redes y servicios en red de la Alcaldía Municipal de Chía.

- 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.

- El acceso a red alámbrica de la Administración Municipal se realiza con una IP única asignada al funcionario.

- Las claves para el servicio de red inalámbrico están disponibles para los funcionarios y son publicadas en puntos clave de la Alcaldía Municipal de Chía para su acceso.

- Las claves para los servicios en red 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.

- 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.
- Toda actividad de red se controlará mediante una UTM Fortinet donde se realizará el proceso de filtrado web, control de aplicaciones y antivirus perimetral.
- Existe una red MPLS (autopista - red de datos) que permite interconectar diferentes áreas de red y las enruta de manera conjunta a internet. De igual manera por esta autopista va la red de telefonía. No se pierden los servicios locales en caso de caída de la autopista exceptuando lo que esté en la nube.
- Para el acceso a los servicios de red (corrycom, ventanilla única, etc) se entrega usuario (correo electrónico institucional) y contraseña.
- 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
- Existe una red de invitados (inalámbrica) habilitada para el acceso a todo público.
- En caso tal que otro usuario quisiera conectarse a una red interna de la Administración Municipal y no cuente con su IP, a la hora de que el sistema no reconozca el usuario (IP del equipo), automáticamente se apagará el puerto y tendrá que solicitar soporte para poder habilitarlo de nuevo.

7.8.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.”

7.9.Política control de acceso físico

Definir los lineamientos para el control de acceso físico en áreas seguras de la Alcaldía Municipal de Chía.

- 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.

- Cada dependencia es responsable de designar a funcionarios y/o contratistas con los permisos de acceso a zonas restringidas en su área, llevando el control y seguimiento de los mismos.

- 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.

- Las actividades de limpieza en las áreas seguras deben ser controladas y supervisadas por un funcionario o colaborador del proceso. El personal de limpieza se debe capacitar acerca de las precauciones mínimas a seguir durante el proceso de limpieza y se prohíbe el ingreso de maletas, bolsos u otros objetos que no sean propios de las tareas de aseo.

- Se deben realizar acciones para prevenir la pérdida, daño, robo o compromiso de activos de información y la interrupción de las operaciones de la organización; los equipos deben estar ubicados y protegidos para reducir los riesgos de amenazas, peligros del entorno y las posibilidades de acceso no autorizado, protegidos contra fallas de energía y otras interrupciones causadas por fallas en los servicios de suministro, el cableado de energía eléctrica y de telecomunicaciones que porta datos o brinda soporte a los servicios de información debe estar protegido contra interceptación, interferencia o daño.

Los lineamientos para el ingreso físico a instalaciones de la alcaldía municipal de Chía, se encuentran definidos en el **procedimiento ingresó instalaciones administración municipal - Diferentes sedes, circular 2 de 2019.**

7.10. Política seguridad en oficinas, recintos e instalaciones

Gestionar los lineamientos básicos para la seguridad en oficinas, recintos e instalaciones de la Alcaldía Municipal de Chía.

- Se debe establecer un control de acceso al público estricto para toda oficina, recinto e instalación clave (esta característica se define por el tipo de información y equipos tecnológicos con los que cuente cada área) para la Administración Municipal.

- Para toda oficina, recinto o instalación de la Administración Municipal que realicen actividades de procesamiento de información (manejo de información sensible) se deberán desarrollar estrategias para mostrar un indicio mínimo del propósito del área, con el fin de generar discreción en los procesos que se lleven a cabo y disminuir posibles intrusiones.

- Se debe tener un control estricto del directorio interno de extensiones de las oficinas de la Administración Municipal, es prioridad de los servidores públicos velar por mantener seguras las extensiones de áreas sensibles (Datacenter, oficinas que generan información de alta criticidad, entre otras).

- 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.[5]

- 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.[6]

- 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.[7]

---

[5] *Recurso de apoyo para la redacción de esta política:* https://www.mininterior.gov.co/sites/default/files/oip-2014-psi-especificas-4_seguridad_fisica.doc

[6] *Recurso de apoyo para la redacción de esta política:* https://www.mininterior.gov.co/sites/default/files/oip-2014-psi-especificas-4_seguridad_fisica.doc

[7] *Recurso de apoyo para la redacción de esta política:* https://www.mininterior.gov.co/sites/default/files/oip-2014-psi-especificas-4_seguridad_fisica.doc

7.11.Política gestión de incidentes de seguridad de la información

Gestionar de manera adecuada los eventos, incidentes y vulnerabilidades de seguridad de la información que se generen en la alcaldía municipal de Chía con el fin de prevenir y limitar el impacto de los mismos.

Los lineamientos para reportar incidentes se encuentran definidos en el **procedimiento para reportar incidentes de seguridad.**

7.12. Política instalación de software

Definir las directrices para la instalación de software en los equipos de la Alcaldía Municipal de Chía para su correcto funcionamiento.

- La Oficina de Tecnologías de la Información y las Comunicaciones deberá proporcionar el software que se requiera en los equipos de la Administración Municipal para el respectivo cumplimiento de las actividades laborales a desarrollar.
- Sólo personal capacitado y autorizado por la Oficina de Tecnologías de la Información y las Comunicaciones se encargará de la instalación, actualización y monitoreo de los software que estén instalados en los equipos de la Administración Municipal.
- Todo software que se instale en los equipos de la Administración Municipal deberán contar con su licencia correspondiente (exceptuando casos de software libre), así como es responsabilidad de la Oficina de Tecnologías de la Información y las Comunicaciones de mantener las licencias al día.
- Para el control de los programas que se instalen en los equipos de la Administración Municipal, la Oficina de Tecnologías de la Información y las Comunicaciones deberá monitorear cada equipo de cómputo con una herramienta especial para dicho proceso.
- Si alguna dependencia de la Administración Municipal solicita un software en específico para el funcionamiento de su área, se deberá realizar la solicitud formal al jefe de la Oficina de Tecnologías de la Información y las Comunicaciones a través de un oficio, donde especifique el software requerido (el pago de la respectiva licencia de software se hace por parte de la dependencia que lo solicita).

7.13.Política controles criptográficos

Definir las directrices para garantizar que la información reservada de la Alcaldía Municipal de Chía, sea almacenada, transmitida y recibida de manera segura cumpliendo con la preservación de la confidencialidad e integridad de la misma.

La Oficina de Tecnologías de la Información y las Comunicaciones debe proporcionar los mecanismos o herramientas necesarias para asegurar la protección de claves de acceso a la red de datos, los sistemas de información y servicios de la Administración Municipal.

- La Oficina de Tecnologías de la Información y las Comunicaciones es la encargada de verificar que todo sistema o aplicación que realice y/o permita la transmisión de información pública reservada o información pública clasificada, se realice mediante herramientas de cifrado de datos.
- La Oficina de Tecnologías de la Información y las Comunicaciones debe definir e implementar estándares para la aplicación de controles criptográficos.
- Los dispositivos móviles que manejen información pública reservada o información pública clasificada deberán contar con un sistema de cifrado para prevenir la afectación de esta información.
- 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.
- Se implementa un sistema de cifrado para los correos institucionales de los jefes de la Administración Municipal, quienes inicialmente realizan transmisión de información sensible a través de esta plataforma.
- La Oficina de Tecnologías de la Información y las Comunicaciones proveerá la herramienta de encriptación de datos a quien lo requiera, previa solicitud formal.

7.14.Política de transferencia de información

Garantizar que la información de la Alcaldía Municipal de Chía sea transferida terceros o las personas que la requieran cumpliendo una serie de acuerdos y lineamientos.

- Los controles de seguridad para la transferencia de información se deben seleccionar para mitigar los riesgos de pérdida de confidencialidad, integridad o disponibilidad de la 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.

- Los funcionarios públicos de la Administración Municipal que envíen todo tipo de documentación a entidades externas, se debe verificar previamente el envío, el nombre de los destinatarios de la información clasificada como pública reservada, con el fin de reducir la posibilidad de envío de este tipo de datos, a destinatarios no deseados.

- La Oficina de Tecnologías de información y Comunicaciones debe implementar las herramientas necesarias para asegurar la transferencia de información al interior y exterior de La Administración Municipal de Chía, contra interceptación, copiado, modificación, enrutador y destrucción.

- Cuando se envía documentación con información pública reservada o clasificada, la oficina de gestión documental de la Administración Municipal de Chía designa un funcionario profesional y responsable para llevar directamente la correspondencia a las diferentes entidades gubernamentales como la Contraloría, Procuraduría, gobernaciones entre otras, como evidencia del documento entregado, se relaciona la información en una planilla donde el funcionario que recibe la correspondencia firma la planilla y al oficio se le coloca un stickers donde aparece el número de radicado, fecha y todos los datos para que no haya ningún tipo de pérdida o modificación del mismo. Se adjunta imágenes de los formatos.

- Cuando se envía información a otras empresas públicas o privadas se hace mediante una empresa llamada 472 correo certificado, ellos se encargan de distribuir los documentos, como evidencia de entrega se coloca un sticker de color blanco destino y recibido de color azul en cada oficio, donde se estipula

toda la información correspondiente para evitar perdida de documento e información.

- 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.

- La correspondencia que ingresa a la Alcaldía Municipal de Chía, llega a la oficina de gestión documental y se maneja un consecutivo e informe donde se sube toda la documentación a la plataforma de Corrycom.

8. PROCEDIMIENTOS DE SEGURIDAD DE LA INFORMACIÓN

8.1. Procedimiento borrado seguro

La oficina de tecnologías de la información y las comunicaciones es la única dependencia encargada de aplicar y realizar el procedimiento de borrado seguro de la información a los medios tecnológicos (impresoras, teléfonos y equipos de cómputo), solo cuando el funcionario se retira de la alcaldía municipal de Chía, se traslada de dependencia o se realiza una modernización del medio tecnológico.

- El funcionario que cumpla con las siguientes causales de borrado seguro (se retira de la alcaldía municipal de Chía, se traslada de la dependencia o se realiza modernización del medio tecnológico) realiza la respectiva solicitud llamando a la oficina de tecnologías de la información y las comunicaciones (TIC).

- El técnico/ ingeniero de la oficina de TIC, genera el ticket de la solicitud y le indica al usuario que debe hacer llegar el medio tecnológico a la oficina TIC.

- El técnico/ingeniero recibe el medio tecnológico, verifica el estado del mismo y el usuario firma una autorización de formateo del equipo.

- Se realiza la copia de seguridad de la información del equipo de cómputo teniendo en cuenta lo siguiente:

  a. traslado o retiro de la entidad: El usuario debe realizar la copia de seguridad de la información y ser entregada a la oficina de control interno, teniendo en

cuenta el reglamento de la alcaldía municipal de Chía, si el usuario no realiza la copia de seguridad la oficina de control interno puede realizar la solicitud al técnico / ingeniero para realizar la copia de seguridad antes de realizar el borrado seguro.

b. Modernización de equipo de cómputo: El usuario realiza la copia de seguridad de la información y lo puede almacenar en el drive del correo institucional o en una unidad de almacenamiento externo provisional que le suministra el técnico/ingeniero.

- El técnico/ ingeniero realiza el formateo, eliminación de usuario y borrado seguro del medio tecnológico.

- Dependiendo de la dependencia donde se encuentra el medio tecnológico, se realiza la asignación del mismo a algún funcionario por orden del jefe o secretario de la dependencia.

- Si el jefe o secretario de la dependencia no desea realizar la asignación del medio tecnológico, este puede realizar la entrega a la oficina de almacén general.

8.2.Procedimiento para el uso de programas utilitarios privilegiados

Establecer los procedimientos para el uso de programas utilitarios privilegiados de la Alcaldía Municipal de Chía, con la capacidad de anular los controles de sistemas y de aplicaciones.

- La oficina de Tecnología de Información y Comunicaciones realiza la instalación de los programas utilitarios necesarios para el funcionamiento del equipo de cómputo al momento de entregar un equipo de computo.

- La Oficina de Tecnologías de la Información y las Comunicaciones debe revisar mensualmente las directrices para el uso de programas utilitarios con la capacidad de anular los controles de sistemas y de aplicaciones.

- La Oficina de Tecnologías de la Información y las Comunicaciones debe utilizar procedimientos de identificación, autenticación y autorización para los programas utilitarios que requieran los funcionarios para realizar trabajos específicos, así mismo, se llevará un control de los programas utilitarios instalados.

- La Oficina de Tecnologías de la Información y las Comunicaciones es la única autorizada para instalar, eliminar o modificar los programas utilitarios, si el funcionario instala algún programa de este tipo será eliminado.

- El funcionario que requiera la utilización de un programa utilitario deberá hacer la solicitud al jefe de la Oficina de Tecnologías de la Información y las Comunicaciones, enviando la información al correo institucional oficinatic@chia.gov.co, donde se realizará la viabilidad del programa.

8.3. Procedimiento propiedad intelectual, uso legal de software y productos informáticos.

Dar cumplimiento a los requisitos contractuales relacionados con los derechos de propiedad intelectual y el uso de productos de software patentados. Con fin de tener un mayor control y seguimiento de los programas y/o aplicaciones que reposan en cada equipo o servidor de la Alcaldía de Chía.

- Se establecen políticas a través del directorio activo, realizando control mediante la mesa de ayuda GLPI y el Dominio, permitiendo bloquear o dar acceso denegado para cualquier tipo de descarga de un aplicativo y/o software ilegal.

- Si se encuentra software ilegal o no cuenta con una licencia válida, se procede a la desinstalación del mismo mediante los procedimientos que realiza la oficina de Tecnologías de Información y Comunicaciones de la Alcaldía Municipal de Chía.

- Los Software que se adquieren en la Administración Municipal de Chía cuentan con licencias ilimitadas y no incumple con los derechos de propiedad intelectual.

- La Alcaldía Municipal de chía posee el inventario correspondiente y el software de verificación y control.

8.4. Procedimiento para la transferencia de medios físicos

Definir acciones que prevengan y eviten la divulgación, modificación, retiro o la destrucción no autorizada de la información almacenada en los medios suministrados por la Alcaldía municipal, cuidando por la disponibilidad y confidencialidad de la información.

- Mantener con las medidas de protección físicas y lógicas de los medios y equipos que permitan su monitoreo y correcto estado de funcionamiento, realizando los mantenimientos preventivos y correctivos que se requieran.

- Los sistemas de información, aplicaciones (software), el servicio de acceso a Internet, Intranet, medios de almacenamiento, cuentas de red, navegadores y equipos de cómputo que son propiedad de la Alcaldía, los cuales deben ser usados únicamente para el cumplimiento misional de la entidad.

- Realizar el procedimiento de borrado seguro en los equipos de cómputo y demás dispositivos, una vez el funcionario haya sido retirado de la Alcaldía.

- Restringir la copia de archivos en medios removibles de almacenamiento, deshabilitando la opción de escritura en dispositivos USB, unidades ópticas de grabación en los equipos de cómputo de la entidad. La autorización de uso de los medios removibles debe ser gestionada a través de la Oficina de Tecnologías de la Información y las Comunicaciones (TIC) y será objeto de auditorías de seguridad, apoyado en la prevención de pérdida de información de la Alcaldía.

- El intercambio de información de la Alcaldía con otras organizaciones o terceros debe estar controlado y se debe cumplir la legislación y normas vigentes que correspondan para mantener una adecuada protección de la información la Alcaldía, estableciendo acciones, procedimientos y controles de intercambio de información a través de medios físicos disponibles.

8.5.Lineamiento de seguridad de la información en el ciclo de vida de proyectos

Integrar diferentes métodos de gestión de proyectos en la Alcaldía municipal de Chía, para asegurar que los riesgos de seguridad de la información que se identifican y se tratan como parte de los diferentes proyectos desarrollados.

- Alinear los objetivos de los proyectos con los de seguridad y privacidad de la información de la entidad.

- Establecer y fijar responsabilidades en roles específicos para gestionar la seguridad de información en los proyectos, de acuerdo con los métodos definidos en la gestión de proyectos.

- Realizar la valoración de riesgos de seguridad en etapas iniciales de los proyectos desarrollados en los diferentes procesos de la alcaldía municipal de

Chía, con el propósito de identificar los controles necesarios para mitigar los riesgos.

- En las prácticas establecidas en gestión de riesgos de la cadena de suministro de Tecnologías de la Información y de las Comunicaciones (TIC) son apoyadas por prácticas generales de diseño de sistemas, de gestión de proyectos y de calidad que facilitan promover e integrar los lineamientos de seguridad de la información en la Alcaldía.

- Es conveniente que la Alcaldía municipal de Chía trabaje con proveedores que entiendan la cadena de suministro de TIC, así como las demás situaciones o eventos que tengan un impacto importante sobre los productos y servicios suministrados para la realización de los proyectos del municipio.

8.6.Procedimiento para el acceso de áreas de despacho y carga

Describir los accesos de áreas de despacho y de carga donde los funcionarios, contratistas y visitantes deben ingresar a las instalaciones de la Administración Municipal de Chía y asegurar solamente el ingreso de personal o visitantes autorizados a las diferentes dependencias al igual que en las áreas catalogadas como seguras.

- El acceso a las zonas de despacho y carga de la Alcaldía de Chía debe ser autorizado por la Administración del edificio o por solicitud directa del funcionario y/o jefe a cargo del área.

- Definir que el área de despacho y carga se debe diseñar de manera que los suministros se puedan cargar y descargar sin que el personal de despacho tenga acceso a otras partes de la edificación.

- Establecer que las puertas externas del área de despacho y carga se aseguran cuando las puertas internas están abiertas.

- Establecer que el material que ingresa se registra de acuerdo con los procedimientos de gestión de activos al entrar al sitio.

- Definir que los despachos entrantes y salientes están separados físicamente, en donde sea posible.

- Todo vehículo que ingrese a dejar o retirar elementos de la Entidad debe estar previamente autorizado por el personal encargado de dicha área.

- Definir que el material que ingresa se inspecciona y examina para determinar la presencia de explosivos, químicos u otros materiales peligrosos, antes de que se retiren del área de despacho y carga.

- La salida de bienes que sean propiedad de la Administración Municipal de Chía deben ser previamente autorizados, por el Jefe del Área a través de correo electrónico enviado por el nivel directivo del área donde pertenecen.

- Establecer que el material entrante se inspecciona para determinar evidencia de manipulación durante el viaje. Si se descubre esta manipulación, se debería reportar de inmediato al personal de seguridad.

8.7.Procedimiento para la restricción de instalación de software

Definir las directrices para las restricciones sobre la instalación se software de la Administración Municipal de Chía.

- Cuando algún funcionario de la Alcaldía Municipal de Chía realice un requerimiento para la instalación de un Software, la oficina TIC está en la obligación de evaluar la necesidad de adquisición de dicho software.

- Todo software que sea instalado en algún equipo de algún funcionario de la Administración Municipal de Chía, debe ser licenciado y aprobado por la oficina de Tecnología de Información y Comunicaciones.

- Cuando se realice la instalación de un software se deben tener en cuenta las características y/o capacidades de los equipos de cómputo.

- La oficina de Tecnología de Información y Comunicaciones debe tener un inventario del software licenciados e instalados en la Administración Municipal de Chía.

- Ningún software licenciado de la Alcaldía Municipal de Chía, bajo ninguna circunstancia debe proporcionarse a personas u organizaciones externas o usarse con fines de lucro.

8.8.Procedimiento para trabajo en áreas seguras

Definir los lineamientos para el trabajo en áreas seguras en las instalaciones y sedes de la Alcaldía Municipal de Chía.

La Alcaldía Municipal de Chía debe mantener áreas seguras de trabajo para la gestión, almacenamiento y procesamiento de la información en la Entidad. Teniendo en cuenta lo postulado con anterioridad, se definieron los siguientes lineamientos:

- Se deben definir perímetros de seguridad según las necesidades del área de trabajo y perfiles de los empleados que estén involucrados.
- Para áreas en donde se tenga custodia servidores, centros de cómputo y/o centros de cableado, se deberá realizar un monitoreo constante de variables como temperatura y humedad de las áreas de procesamiento de datos.
- La entidad debe designar y aplicar protección física para la prevención de desastres como: incendios, inundaciones, terremotos, explosiones, manifestaciones y otras formas de desastre natural o humano.
- Para áreas con centros de cómputo y/o cableado se debe velar por el ambiente adecuado para los activos informáticos, controlando temas de ventilación, iluminación, regulación de corriente, entre otros.
- Se debe tener un control de acceso físico a zonas que lo requieran, como pueden ser centros de bodegaje de archivos, activos físicos de sistemas de información, centros de datos, entre otros.
- Cuando un área que maneje información crítica de la Administración Municipal esté vacía o no se encuentre personal trabajando en estas áreas, se deberá mantener la zona con los recursos de seguridad correspondientes, como pueden ser, puertas cerradas con llave, bloqueos con único acceso a través de medios biométricos, cámaras activas y sensores de movimiento (alarmas) según se requiera.
- El uso de dispositivos de grabación y/o registro fotográfico tales como cámaras en dispositivos móviles están restringido en las áreas seguras de trabajo de la Administración Municipal, a menos que se cuente con una autorización para ello.
- Se debe evitar el trabajo no supervisado en las áreas seguras de la Administración Municipal, con el fin de proteger la integridad y seguridad de la información que se maneje en dicha área.
- La responsabilidad del ingreso a áreas denominadas como seguras será exclusiva del responsable de dicha área.
- Se deben usar los elementos de protección personal que el área segura requiera.

9. CUMPLIMIENTO

Todos los secretarios, directores, funcionarios y contratistas de la alcaldía municipal de Chía, debe cumplir con el 100% de la política.

10. REVISIÓN Y ACTUALIZACIÓN DE LA POLÍTICA

La oficina de tecnologías de la información y las comunicaciones actualizará la política general de seguridad de la información, políticas de seguridad de la información y los procedimientos de seguridad de la información, una vez al año con la aprobación de la alta dirección, teniendo en cuenta el monitoreo de los procesos y controles.

Cra. 11 No 11 - 29
PBX: 8844444 Ext. 2300
oficinatic@chia.gov.co
www.chia-cundinamarca.gov.co

PROCEDIMIENTO PARA REPORTAR INCIDENTES DE SEGURIDAD

Objetivo:

Gestionar de manera adecuada los eventos, incidentes y vulnerabilidades de seguridad de la información que se generen en la alcaldía municipal de Chía con el fin de prevenir y limitar el impacto de los mismos.

Aplicabilidad:

La política de procedimiento para reportar incidentes de seguridad aplica a la alta dirección, secretarios, jefes, funcionarios y contratistas de la Alcaldía Municipal de Chía.

Detalle:

- Cualquier incidente de seguridad de información que se presente en la Alcaldía Municipal de Chía se debe reportar de manera oportuna a la Oficina de Tecnologías de la Información y las Comunicaciones para tomar las medidas pertinentes frente al caso.
- Se deben recolectar las evidencias y documentar todos los incidentes de seguridad de la información.
- Se debe llevar un registro de todos los incidentes, vulnerabilidades y eventos reportados y su respectiva solución.
- Dependiendo del incidente de seguridad de la información que se esté tratando, la oficina de Tecnologías de la Información y las Comunicaciones es la única autorizada para contactar con las entidades de control pertinentes, descritas a continuación:

Nombre Entidad	**Contacto**	**Detalle**	**Cómo reportar un Incidente**
colCERT - Grupo de respuesta a emergencias	Ing. Wilson Arturo Prieto Hernández (cybersecurity Adviser) -Teléfono: (+57 1) 2959897 -Celular: (+57) 3107604463	El Grupo de Respuesta a Emergencias Cibernéticas de Colombia - colCERT, tiene como responsabilidad	Para reportar un incidente o vulnerabilidad deberá escribir directamente a: **Correo electrónico:** contacto@colcert.gov.co **Clave PGP/GPG:** FF433551

cibernéticas de Colombia	-E-mail: wprieto@colcert.gov.co -Twitter: @colCERT -Página Web: www.colcert.gov.co -Dirección: Avenida el Dorado Nro. 75 - 25 Barrio Modelia Edificio Central - Piso 2 - Bogotá D.C.	central la coordinación de la Ciberseguridad y Ciberdefensa Nacional, la cual estará enmarcada dentro del Proceso Misional de Gestión de la Seguridad y Defensa del Ministerio de Defensa Nacional. Su propósito principal será la coordinación de las acciones necesarias para la protección de la infraestructura crítica del Estado colombiano frente a emergencias de ciberseguridad que atenten o comprometan la seguridad y defensa nacional. La información presentada con anterioridad fue obtenida de la siguiente URL: *www.colcert.gov.co/?q=acerca-de* relacionada a la misión de colCERT.	1. Su información de contacto: -Nombre(s) y Apellido(s) -País -Zona Horaria -Número de Teléfono -Correo Electrónico -Nombre de la Entidad (si aplica) -Número de Teléfono de la Entidad (si aplica) -Número de móvil -Tipo de Organización (Gobierno, Privada u Operador de Infraestructura Crítica) -Tipo de Sector (primario, secundario o terciario) 2. Información del host(s) objetivo(s): -Nombres de los hosts y direcciones IPs -Función del sistema (web server, mail server, etc) -Sistema(s) operativo(s) -Aplicaciones involucradas en el incidente 3. Información del host origen: -Nombres de los hosts y direcciones IPs -Función del sistema (web server, mail server, etc) -Sistema(s) operativo(s) -Aplicaciones involucradas en el incidente 4. Información del Incidente: -Fecha y hora (Timestamp) -Zona horaria del incidente -Tipo de Incidente: *Escaneo de Host

			(ejemplo: Ping Sweep, Puerto(s), Servicio(s)) *Intento de Buffer Overflow *Login no autorizado *Otros intentos de intrusión 5. Descripción Adicional: Si desea enviar información de logs u otro tipo de información por favor utilizar nuestra llave pública que está publicada en el siguiente link: **Clave PGP/GPG:** FF433551 **Nota:** a vuelta de correo se le enviará un ticket asignado al incidente. La información presentada con anterioridad fue obtenida de la siguiente URL: *www.colcert.gov.co/?q=contenido/reportar-un-incidente*
Centro Cibernético Policial	Ficha de Contacto -Teléfono: (+57 1) 5159700 ext. 30427 -Correo Electrónico: caivirtual@correo.policia.gov.co -Dirección: Avenida el Dorado Nro. 75 - 25 Barrio Modelia	El Centro Cibernético Policial con base en la Ley 1274 de 2009 sobre Delitos Informáticos busca la prevención de ataques informáticos y la protección de la información y de los datos de la comunidad con un sistema de control y atención virtual habilitado las 24	En la URL www.caivirtual.policia.gov.co o la APP que también se encuentra en el anterior link se pueden reportar: -CiberIncidentes -Análisis de Malware -Reporte de delitos informáticos -Protección de Wanna Cry -CAI Virtual -Ciberseguridad -APPS -Mural Cibercrimen

		horas del día, los 7 días a la semana.	Para poder acceder a cualquiera de estos servicios que ofrece el Centro Cibernético Policial se debe realizar el respectivo registro en la página web o en su APP, lo que facilita el seguimiento a los casos.