PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACION

2021

GERMÁN MOGOLLÓN DONOSO
Alcalde

TABLA DE CONTENIDO

PAG

1. INTRODUCCION

Los niveles de seguridad y la exigencia de la misma se han expandido exponencialmente en los últimos años por el avance tan drástico de la tecnología, dado a esto la protección de la información y bloqueo de intrusos son el objetivo a lograr para que la información y la estructura informática de la organización sea segura.

Los sistemas de almacenamiento de la información se expanden continuamente interconectando bases de dato, usuarios y demás, esto ha dado lugar a la aparición de nuevos problemas “amenazas” en los sistemas computarizados, al expandirse la cobertura del mismo modo se expande la vulnerabilidad de la misma.

Las Administración Municipal ha dado prioridad y pie de fuerza para incentivar y mejorar el resguardo de la información de los proveedores y de las propias compañías, además del uso de adecuado de las tecnologías y hacen recomendación para aprovechar sus ventajas y minimizar los riesgos.

El presente plan surge para convertirse en una herramienta con la cual se da conocimiento del uso de la información y la necesidad de conservar la privacidad de la misma de aquellos ajenos del ente territorial, el buen uso de los equipos la recuperación de la información en el menor tiempo.

La **Política de Seguridad y Privacidad de la Información** es la declaración general que representa la posición de la administración Municipal con respecto a la protección de los activos de información (los empleados, contratistas, terceros. la información, los procesos, las tecnologías de información incluido el hardware y

el software), que soportan los procesos y apoyan la implementación del Sistema de Gestión de Seguridad de la Información, por medio de la generación y publicación de sus políticas, procedimientos e instructivos, así como de la asignación de responsabilidades generales y específicas para la gestión de la seguridad de la información.

La Alcaldía Municipal del Carmen de Apicalá (Tolima), para asegurar la dirección estratégica establece la compatibilidad de la política de seguridad de la información y los objetivos de seguridad de la información, estos últimos correspondientes a:

- *Minimizar el riesgo de los procesos misionales de la entidad.*
- *Cumplir con los principios de seguridad de la información.*
- *Cumplir con los principios de la función administrativa.*
- *Mantener la confianza de los empleados, contratistas y terceros.*
- *Apoyar la innovación tecnológica.*
- *Implementar el sistema de gestión de seguridad de la información.*
- *Proteger los activos de información.*
- *Establecer las políticas, procedimientos e instructivos en materia de seguridad de la información.*
- *Fortalecer la cultura de seguridad de la información en los empleados, terceros, y proveedores del ente territorial*
- *Garantizar la continuidad del negocio frente a incidentes.*

2. ALCANCE

La aplicación del manual de políticas de seguridad de la Alcaldía Municipal del Carmen de Apicalá (Tolima), aplica a todo el personal que hagan uso de equipos y herramientas informáticas o estén conectados en la red interna de trabajo o manipulen información que está ligada con la base de datos central de la entidad, esta política de seguridad requiere de un gran compromiso por parte de todos los funcionarios de la institución, la capacidad para detectar anomalías y fallas generando una política cambiante y evolutiva.

3. RIESGOS NFORMÁTICOS

La ISO 27001 (Organización Internacional de Estandarización) define el riesgo informático como: "La posibilidad que una amenaza se materialice, utilizando vulnerabilidad existente en un activo o grupos de activos, generándose así pérdidas o daños."

En una entidad, los riesgos informáticos, son latentes día a día y pueden afectar gravemente la seguridad y la estabilidad de los sistemas de información, estos pueden presentarse en diversas áreas como lo ilustra la siguiente tabla.

Riesgos externos	Riesgos internos
Caída de la conexión a internet	Caída inesperada de algunos servicios del servidor, cambios bruscos en el fluido eléctrico de la institución
Errores en el suministro de la información.	Errores al utilizarlos recursos informáticos
Error en soporte técnico echo por terceros	Error en el diligenciamiento de la información de los usuarios dentro de la red de la institución
Eventos naturales que afecten la infraestructura de la institución afectando las redes y equipos informáticos.	Mal manejo de los equipos. Descargar software no autorizado Visitar sitios con contenido explicito

4. POLITICAS DE SEGURIDAD

Son las reglas y procedimientos que regulan la forma en que una organización mitiga los riesgos y busca establecer los estándares de seguridad a ser seguidos por todos los involucrados en el uso y mantenimiento de las herramientas tecnológicas.

Se consideran como el primer paso para aumentar la conciencia de seguridad de la información, están orientadas hacia la formación de buenos hábitos.

5. CLASIFICACIÓN DE LAS POLÍTICAS DE SEGURIDAD

Para efectos de comprensión y estructuración de este documento, la Administración Municipal ha clasificado las políticas de seguridad en los siguientes grupos:

Equipos: Todo lo relacionado con el hardware, su uso y cuidado.
Usuarios: Concerniente a las personas que utilizan los recursos informáticos de la institución.
Software: los recursos lógicos tales como programas, aplicativos y demás.
Redes e Internet: las medidas que se deben tomar a la hora de utilizar los recursos de telecomunicación.
Datos e Información: Políticas que regulan la manipulación, transporte y almacenamiento de la información de la entidad.

5.1. POLITICA DE SEGURIDAD DE EQUIPOS.

La ley 734 de 2002 en su artículo 48, considera una falta gravísima lo siguiente: **"Artículo 48. Faltas gravísimas. Son faltas gravísimas las siguientes: Causar daño a los equipos estatales de informática, alterar, falsificar, introducir, borrar, ocultar o desaparecer información en cualquiera de los sistemas de información oficial contenida en ellos o en los que se almacene o guarde la misma, o permitir el acceso a ella a personas no autorizadas."**

los equipos de cómputo son el centro más fundamental de gran parte de las organizaciones y para la administración Municipal no es ajeno esta herramienta, ya que allí se almacena y se gestiona la información, la función del funcionario de sistemas de información es velar que los equipos funcionen adecuadamente y establecer medidas preventivas y correctivas.

En caso de robo, incendio, desastres naturales, fallas eléctricas y cualquier otro factor que atente contra la infraestructura de la red y la informática se dan a comprender las siguientes políticas:

- Todo equipo de cómputo, periférico o accesorio que esté o sea conectado a la Red de la Administración sea propiedad o no de la institución debe de sujetarse a las normas y procedimientos de instalación establecidos por la oficina de Sistemas de Información, de lo contrario no le será permitido conectar su equipo o dispositivo.
- El administrador o responsable del seguimiento de los equipos tendrá registro de todos los equipos que son propiedad del Ente territorial, si se requiere hacer un traslado de un computador, periférico o accesorio, debe contar con el consentimiento del responsable directo de cada secretaria.
- Cualquier equipo, periférico o accesorio de propiedad del Ente territorial, que necesite ser retirado de la institución tendrá que ser autorizado por el administrador de almacén, visto bueno de gerencia y visto bueno del administrador de sistemas.
- Todo equipo de la institución debe estar ubicado en el área que cumpla con los requerimientos de: seguridad física, condiciones ambientales adecuada, seguridad y estabilidad en la parte eléctrica.
- Todos los equipos de cómputos, periféricos y demás deben estar lejos de los siguientes factores principales: la luz directa del sol y la humedad, filtraciones, fallas eléctricas, instrumentos que emitan campos magnéticos u radiación.
- Todos los equipos o periféricos pertenecientes a las redes habilitadas por la Administración Municipal deberán contar con el dispositivo de protección eléctrica ya sea un estabilizador o una UPS, que resguarde los equipos ante un cambio repentino en la corriente eléctrica.
- Los usuarios responsables de los equipos en cada dependencia deberán dar cumplimiento con las normas y estándares de instalación con las que fue entregado el equipo, y deberán pedir aprobación de actualización o instalación de cualquier software, reubicación del equipo, reasignación, y todo aquello que implique cambios respecto a su instalación, asignación, función y misión original.
- La protección física y la limpieza externa de los equipos corresponde al funcionario de sistemas al que se le asigne la tarea, y la custodia y cuidado

en el sitio de trabajo le corresponde al funcionario que lo manipula y quien debe notificar las eventualidades, tales como daños, pérdidas y demás en el menor tiempo posible.

- Está totalmente prohibido el consumo o ubicación de alimentos cerca de los equipos e impresoras, así como pegar distintivos, calcomanías y demás. En caso que ocurra un incidente producido por el derrame de algún tipo de alimentos sobre un equipo, periférico o accesorio, este debe apagarse y desconectarse de inmediato e informar oportunamente para realizar por el personal responsable el diagnóstico del equipo y evaluara el daño y notificara al Secretario General y de Gobierno. Además, el funcionario se hace cargo de la reparación del equipo u daño de impresoras por mal uso.
- Los equipos de cómputo del ente territorial, no deben ser alterados ni mejorados (cambios de procesador, adición de memoria o tarjetas) bajo ninguna causa. Está totalmente prohibido a los usuarios destapar o desarmar los equipos o impresoras bajo cualquier motivo, sin exclusión.
- No se puede dar mantenimiento o soporte técnico a nivel de hardware a un equipo de cómputo que no es propiedad de la Administración Municipal.
- El personal designado para el mantenimiento en coordinación con el Secretario General y de Gobierno son los únicos autorizados para manejar, mantener y velar por la integridad y seguridad de los servidores centrales de la institución, a su vez de mantener las claves de estos.
- El servidor central debe estar ubicado en un lugar exclusivo, sin acceso de personas ajenas a la oficina de Sistemas de Información, y con las condiciones adecuadas de espacio, temperatura, iluminación, entre otras.
- La adquisición de nueva infraestructura de procesamiento de la información (hardware, software, aplicaciones e instalaciones físicas) o la actualización de la existente, deberá ser autorizada por Secretario General y de Gobierno.
- Todo equipo que sea asignado a un funcionario o contratista, deberá ser entregado al responsable de este, en las mismas condiciones en que lo

recibió, como parte de las actividades definidas en la terminación del contrato o cambio de cargo

- Todo funcionario debe firmar un acta de entrega de los equipos, verificar las condiciones del equipo y en esas mismas condiciones debe ser entregados al administrador de almacén.
- Todos los empleados y contratistas deben apagar y dejar desconectados los equipos y periféricos al culminar la jornada laboral.

5.2. POLÍTICA DE SEGURIDAD EN USUARIOS

Los usuarios son las personas que utilizan la estructura tecnológica de la Institución, ya sean equipos, recursos de red o gestión de la información, se debe establecer normas que buscan reducir los riesgos a la información o infraestructura informática, estas normas incluyen, restricciones, autorizaciones, denegaciones, perfiles de usuario, protocolos y todo lo necesario que permita un buen nivel de seguridad informática.

Todos los funcionarios y contratistas del ente territorial, deberán cumplir con estos requerimientos de seguridad de la Información. Igualmente, durante el proceso de vinculación deberán recibir inducción sobre lo establecido en este documento y sobre la responsabilidad del cumplimiento de las políticas, procedimientos y estándares definidos por la entidad, la información almacenada en los equipos de cómputo deberá ser protegida en su integridad, confidencialidad y disponibilidad. No es permitido divulgar, alterar, borrar, eliminar información sin la debida autorización.

Toda información en formato electrónico o impreso de la entidad debe estar debidamente identificada mediante rótulos o etiquetas, lo que permitirá su identificación y clasificación. Con esto se alimenta el inventario y clasificación de los archivos de información.

Las claves o los permisos de acceso que les sean asignados a los funcionarios y/o contratista, son responsabilidad exclusiva de cada uno de ellos y no deben utilizar la identificación o contraseña de otro usuario, excepto cuando los funcionarios de Sistemas la soliciten para la reparación o el mantenimiento de algún servicio o equipo.
Los permisos a usuarios son personales e intransferibles y serán acordes a las funciones que desempeñen y no deberán tener permisos adicionales a estos. Estos permisos se conceden a solicitud escrita del administrador de sistemas.

Los usuarios deben renovar periódicamente su clave de acceso al sistema; está totalmente prohibido: el intento o violación de los controles de seguridad establecidos; el uso sin autorización de los activos informáticos; El uso no autorizado o impropio de la conexión al Sistema; el uso indebido de las contraseñas, firmas, o dispositivos de autenticación e identificación; acceder a servicios informáticos utilizando cuentas, claves, contraseñas de otros usuarios. Aún con la autorización expresa del usuario propietario de la misma

El usuario será el directo responsable de cualquier daño producido por medidas o decisiones mal tomadas, mantenimientos, reparaciones o instalaciones realizados por él que no fueran informadas.

Los usuarios son responsables de todas las actividades llevadas a cabo con su código de usuario, si detectan actividades irregulares con su código, tienen que solicitar una auditoría al Secretario General y de Gobierno quien de forma coordinada se encargará de dar soporte e informar al usuario la actividad completa en el período y módulos solicitados y de igual manera informara qué medidas se deben tomar al respecto. (Investigación preliminar, cambio de usuario, proceso disciplinario).

Informar cualquier anomalía, aparición de virus o programas sospechosos e intentos de intromisión y no intente distribuir este tipo de información interna o externamente.

Está prohibido intentar sobrepasar los controles de los sistemas, o tratar de saltar los bloqueos de acceso a internet (cambio de dirección IP, cambio de nombre de equipo, etc.) o introducir intencionalmente software malintencionado que impida el normal funcionamiento de los sistemas.

Todo funcionario que utilice los recursos informáticos, tiene la responsabilidad de velar por su integridad, confidencialidad y disponibilidad de la información que Maneje, especialmente si dicha información es crítica.

No se permitirá el almacenamiento y/o procesamiento de información propiedad Municipio en equipos o dispositivos de propiedad de los funcionarios o contratistas. Todos los contratistas y funcionarios deben firmar una cláusula de confidencialidad, que permita a la entidad proteger la información.

5.3. POLITICA DE SEGURDAD DE SOFTWARE

En los equipos de cómputo de la Administración Municipal no se permite la instalación de software que no cuente con el licenciamiento apropiado. Está prohibido el uso de aplicaciones ilegales y el uso de “Cracs”, “Keygens” y demás aplicativos.

Está totalmente prohibido la instalación de juegos, programas de mensajería o aplicativos que no estén relacionados con las labores institucionales que se realizan en la entidad.

Con el propósito de proteger la integridad de los equipos y sistemas informáticos y de telecomunicaciones, es obligatorio que todos y cada uno de estos dispongan de software de seguridad (antivirus, filtros de contenido web, controles de acceso, entre otros). Equipo que no cuente con estos aplicativos de seguridad, no puede conectarse a la red de la institución.

La adquisición y actualización de software para los equipos de cómputo y de telecomunicaciones se llevará a cabo de acuerdo al calendario y requerimientos que sean propuestos y a la disponibilidad presupuestal con el que se cuente.

Es obligación de todos los usuarios que manejen información masiva y/o crítica, solicitar respaldo sobre la generación copias de seguridad ya que se considera como un activo de la institución que debe preservarse; las copias de respaldo a la información generada por el personal y los recursos informáticos de la institución deben estar resguardados en sitios debidamente adecuados para tal fin.

5.4. POLITICAS DE SEGURIDAD DE LA RED E INTERNET

Se prohíbe utilizar la red y los equipos del Ente Territorial, para cualquier actividad que sea lucrativa o comercial de carácter individual, privado o para negocio particular.

Para garantizar la seguridad de la información y el equipo informático, se establecerá por el personal designado por la Secretaria General y de Gobierno los filtros y medidas para regular el acceso a contenidos en el cumplimiento de esta normatividad:

Se prohíbe:

- Utilizar los servicios de comunicación, incluyendo el correo electrónico o cualquier otro recurso, para intimidar o insultar a otras personas, o interferir con el trabajo de los demás.
- Utilizar los recursos del Municipio, para el acceso no autorizado a redes y sistemas remotos.
- Provocar deliberadamente el mal funcionamiento de computadoras, estaciones o terminales periféricos de redes y sistemas, mediante técnicas, comandos o programas a través de la red.

- Monopolizar los recursos en perjuicio de otros usuarios, incluyendo: el envío de mensajes masivamente a todos los usuarios de la red, iniciación y facilitaciones de cadenas, creación de procesos innecesarios, generar impresiones en masa, uso de recursos de impresión no autorizado.
- Poner información en la red que infrinja el derecho a la intimidad de los demás funcionarios y/o contratistas.
- Utilizar los servicios de la red para la descarga, uso, intercambio y/o instalación de juegos, música, películas, imágenes protectoras o fondos de pantalla, software de libre distribución, información y/o productos que de alguna manera atenten contra la propiedad intelectual de sus actores o que contenga archivos ejecutables.
- El intercambio no autorizado de información de propiedad del Municipio del Carmen de Apicalá (Tolima).
- Utilizar los servicios para acceder a páginas de radio o TV en línea, descargar archivos de música o video, visitar sitios de pornografía, ocio, entre otros que estén fuera de las funciones del usuario.
- Los servicios bancarios vía web solamente podrán ser utilizados por la Secretaria de Hacienda y Tesorería únicamente en el equipo que este tenga asignado.
- El acceso a la red interna, se permitirá siempre y cuando se cumpla con los requisitos de seguridad necesarios.
- Cualquier alteración del tráfico entrante o saliente a través de los dispositivos de acceso a la red, será motivo de verificación y tendrá como resultado directo la realización de una auditoría de seguridad y un reporte de los hallazgos a la oficina De Control Interno para que se tomen las medidas pertinentes.
- Los mensajes y la información contenida en los buzones de correo son de propiedad de Municipio, los buzones no deberán contener mensajes con más de un año de antigüedad. Pero se debe dejar un histórico del registro de los mensajes. Todos los mensajes enviados deben respetar los formatos de imagen del ente territorial por el Sistema de Gestión Documental y conservar todas las normas de legalidad de los documentos.

5.5. POLITICAS DE SEGURIDAD DE DATOS E INFORMACIÓN

La información es en uno de los elementos más importantes dentro de una organización. La seguridad informática debe evitar que usuarios externos y no autorizados puedan acceder a ella sin autorización, de lo contrario la entidad corre el riesgo de que la información sea utilizada maliciosamente para obtener ventajas de ella o que sea manipulada, ocasionando datos errados o incompletos, el objetivo de esta política es la de asegurar el acceso a la información en el momento oportuno.

Toda información de relevancia debe contar con copia de seguridad y un tiempo de retención determinado, por lo cual, la información no se debe guardar indefinidamente en un archivo activo ocupando espacio innecesario de almacenamiento, el usuario debe establecer cuándo su información pasará a ser inactiva.