ALCALDÍA DE TULUÁ

MODELO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

2023

Tabla de contenido

INTRODUCCIÓN

Este documento describe las políticas y normas de seguridad de la información definidas por la Alcaldía de Tuluá, teniendo en cuenta que la información es reconocido como un activo valioso y a medidaque los sistemas de información a poyan cada vez más los procesos de misión crítica se requierecontar con estrategi as de alto nivel que permitan el control y administración efectiva de los datos.

El asegurar la información es uno de los requisitos fundamentales para preservar la confidencialidad, integridad y disponibilidad de la información, y por otra, determina los procesos, procedimientos y controles que se deben aplicar conforme a la legislación colombiana y a las necesidades y objetivos estratégicos de la Alcaldía de Tuluá.

Para lograr este objetivo, las políticas aquí definidas brindan las herramientas necesarias para que los funcionarios, contratistas y terceros que hacen parte del Sistema de Gestión de Seguridad de la Información (SGSI en adelante) de la Alcaldía de Tuluá, puedan adoptar los controles requeridos para asegurar la información, gestionar con eficiencia los riesgos de seguridad y mejorar continuamente el SGSI; para la elaboración del mismo, se toman como base las leyes y demás regulaciones aplicables, la norma ISO 27001:2013

Las políticas incluidas en este manual se constituyen como parte fundamental del sistema de gestión de seguridad de la información de la Alcaldía de Tuluá y se convierten en la base para la implantación de los controles, procedimientos y estándares definidos

Esta política será revisada con regularidad como parte del proceso de revisión estratégica, o cuando se identifiquen cambios en la Entidad, su estructura, sus objetivos o alguna condición que afecte la política, para asegurar que sigue siendo adecuada y ajustada a los requerimientos identificados.

En la actual y cambiante sociedad de la información, toda entidad pública o privada debe lograr una adecuada articulación entre el SGSI y las políticas de seguridad de la información, ello solo es posible a través de la integración de políticas, procedimientos, sistemas de información y controles con un fin común: gestionar de manera pertinente y eficaz los riesgos, de tal forma que las partes interesadas obtengan un alto nivel de seguridad y confianza. Se entiende, por lo tanto, que las políticas deben ser plenamente conocidas y cumplidas por los funcionarios, contratistas y terceras partes que tienen acceso a los activos de información y a los sistemas de procesamiento de información de la Alcaldía de Tuluá.

En este sentido, es indispensable que sus esfuerzos y capacidades se concentren en lograr los fines primordiales de las políticas, como son:

- Generar controles para proteger los activos de información;
- Crear conciencia en los usuarios acerca del uso responsable de las tecnologías de la información y comunicaciones
- Realizar una gestión de riesgos adecuada que permita minimizar el impacto frente a un eventual caso de materialización.

1. DEFINICIONES

- **Activo:** en relación con la seguridad de la información, se refiere a cualquier información o elemento relacionado con el tratamiento de la misma (sistemas, soportes, edificios, personas, etc.) que tenga valor para la organización.

- **Anonimización del dato:** eliminar o sustituir algunos nombres de personas (físicas o jurídicas); direcciones y demás información de contacto, como números identificativos, apodos o cargo.

- **Autenticidad**: busca asegurar la validez de la información en tiempo, forma y distribución. Asimismo, se garantiza el origen de la información, validando el emisor para evitar suplantación de identidades.

- **Confidencialidad:** propiedad de la información de no ponerse a disposición o ser revelada a individuos, entidades o procesos no autorizados.

- **Datos abiertos:** son datos primarios o sin procesar puestos a disposición de cualquier ciudadano, con el fin de que terceros puedan reutilizarlos y crear servicios derivados de los mismos.

- **Datos personales sensibles:** se entiende por datos sensibles aquellos que afectan la intimidad del Titular o cuyo uso indebido puede generar su discriminación, tales como aquellos que revelen el origen racial o étnico, la orientación política, las convicciones religiosas o filosóficas, la pertenencia a sindicatos, organizaciones sociales, de derechos humanos o que promueva intereses de cualquier partido político o que garanticen los derechos y garantías de partidos políticos de oposición así como los datos relativos a la salud, a la vida sexual y los datos biométricos.

- **Dato privado**: es el dato que por su naturaleza íntima o reservada sólo es relevante para el titular.

- **Dato público:** es el dato calificado como tal según los mandatos de la ley o de la Constitución Política y todos aquellos que no sean semiprivados o privados, de conformidad con la presente ley. Son públicos, entre otros, los datos contenidos en documentos públicos, sentencias judiciales debidamente ejecutoriadas que no estén sometidos a reserva y los relativos al estado civil de las personas.

- **Dato semiprivado:** es el dato que no tiene naturaleza íntima, reservada, ni pública y cuyo conocimiento o divulgación puede interesar no sólo a su titular sino a cierto sector o grupo de personas o a la sociedad en general, como el dato financiero y crediticio de actividad comercial o de servicios.

- **Disponibilidad:** propiedad de la información de estar accesible y utilizable cuando lo requiera una entidad autorizada.

- **Habeas data:** derecho a acceder a la información personal que se encuentre en archivos o bases de datos; implica la posibilidad de ser informado acerca de los datos registrados sobre sí mismo y la facultad de corregirlos.

- **Integridad:** la propiedad de salvaguardar la exactitud y complejidad de la información.

- **Inventario de activos:** lista de todos aquellos recursos (físicos, de información, *software*, documentos, servicios, personas, intangibles, etc.) dentro del alcance del SGSI, que tengan valor para la organización y necesiten por tanto ser protegidos de potenciales riesgos. (ISO 27000.es, 2012)

- **No repudio**: servicio de seguridad que previene que un emisor niegue haber remitido un mensaje (cuando realmente lo ha emitido) y que un receptor niegue su recepción (cuando realmente lo ha recibido). (ISO-7498-2).

- **Parte interesada (*Stakeholder*):** persona u organización que puede afectar a, ser afectada por o percibirse a sí misma como afectada por una decisión o actividad.

- **Plan de continuidad del negocio**: plan orientado a permitir la continuidad de las principales funciones misionales o del negocio en el caso de un evento imprevisto que las ponga en peligro.

- **Propietario de activo de información:** identifica a un individuo, un cargo, proceso o grupo de trabajo designado por la entidad, que tiene la responsabilidad de definir los controles, el desarrollo, el mantenimiento, el uso y la seguridad de los activos de información asignados.

- **Responsable del tratamiento:** persona natural o jurídica. Pública o privada. Que por sí misma o en asocio con otros, decida sobre la base de datos y/o el Tratamiento de los datos.

2. NORMATIVIDAD

El sistema de Gestión de Seguridad de la información de la Alcaldía de Tuluá, se ciñe a la normatividad legal vigente colombiana, tal como se describe a continuación:

LEGISLACIÓN

Ley 527/99	Por medio de la cual se define y se reglamenta el acceso y el uso de los mensajes de datos	El mensaje de datos es "*La información generada, enviada, recibida, almacenada o comunicada por medios electrónicos, ópticos o similares, como pudieran ser, entre otros, el Intercambio Electrónico de Datos, Internet, el correo electrónico, el telegrama, el télex o el telefax*".
Ley 594/00	Por medio de la cual se dicta la Ley General de Archivo y se dictan otras disposiciones	La presente ley "*tiene por objeto establecer las reglas y principios generales que regulan la función archivística del Estado". Y "comprende a la administración pública en sus diferentes niveles, las entidades privadas que cumplen funciones públicas y los demás organismos regulados por la presente ley*".
La Ley 850/03 establece en su artículo 9º	Principio de Transparencia	"*A fin de garantizar el ejercicio de los derechos, deberes, instrumentos y procedimientos consagrados en esta ley, la gestión del Estado y de las veedurías deberán asegurar el libre acceso de todas las personas a la información y documentación relativa a las actividades de interés colectivo de conformidad con lo dispuesto en esta ley y en las normas vigentes sobre la materia*".

Ley 1266/08	Por la cual se dictan disposiciones generales del hábeas data y se regula el manejo de la información contenida en bases de datos personales, en especial la financiera, crediticia, comercial, de servicios y la proveniente de terceros países.	Se regula el manejo de la información para "*todos los datos de información personal registrados en un banco de datos, sean estos administrados por entidades de naturaleza pública o privada*".
Ley 1221 de 2008	Por la cual se establecen normas para promover y regular el Teletrabajo y se dictan otras disposiciones	La presente ley tiene por objeto promover y regular el Teletrabajo como un instrumento de generación de empleo y autoempleo mediante la utilización de tecnologías de la información y las telecomunicaciones (TIC).
Ley 1273/09	Por medio de la cual se crea un nuevo bien jurídico tutelado denominado "*de la protección de la información y de los datos*" y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones.	"*De los atentados contra la confidencialidad, la integridad y la disponibilidad de los datos y de los sistemas informáticos*".
CONPES 3701 de 2011	Lineamientos de política para ciberseguridad y Ciberdefensa	Busca generar lineamientos de política en ciberseguridad y ciberdefensa encaminados a desarrollar una estrategia nacional que contrarreste el incremento de las amenazas informáticas que afectan significativamente al país.

Resolución 2886 de 2012	Por la cual se definen las entidades que harán parte de la Red Nacional de Fomento al Teletrabajo y se dictan otras disposiciones.	Resolución del Ministerio de Trabajo define "*las entidades que harán parte de la Red Nacional de Fomento al Teletrabajo, las actividades que compete desarrollar y su funcionamiento*".
Ley 1581/12	Por medio de la cual se dictan disposiciones generales para la Protección de Datos Personales *En la recolección, tratamiento y circulación de datos.*	Hace referencia, en particular, al artículo 15 de la Constitución Nacional, según el cual "*todas las personas tienen derecho a su intimidad personal y familiar y a su buen nombre, y el Estado debe respetarlos y hacerlos respetar. De igual modo, tienen derecho a conocer, actualizar y rectificar las informaciones que se hayan recogido sobre ellas en bancos de datos y en archivos de entidades públicas y privadas. En la recolección, tratamiento y circulación de datos.*

3. POLÍTICA GENERAL DE SEGURIDAD DE LA INFORMACIÓN

LA ALCALDIA DE TULUÁ, entendiendo la importancia de una adecuada gestión de la información, se ha comprometido con la implementación de un sistema de gestión de seguridad de la información buscando establecer un marco de confianza en el ejercicio de sus deberes con el Estado y los ciudadanos, todo enmarcado en el estricto cumplimiento de las leyes y en concordancia con la misión y visión de la entidad.

Para la **ALCALDÍA DE TULUÁ** la protección de la información busca la disminución del impacto generado sobre sus activos, por los riesgos identificados de manera sistemática con objeto de mantener un nivel de exposición que permita responder por la integridad, confidencialidad y la disponibilidad de la misma, acorde con las necesidades de los diferentes grupos de interés identificados.

De acuerdo con lo anterior, esta política aplica a la Entidad según como se defina en el alcance, sus funcionarios, terceros, aprendices, practicantes, proveedores y la ciudadanía en general, teniendo en cuenta que los principios sobre los que se basa el desarrollo de las acciones o toma de decisiones alrededor del SGSI estarán determinadas por las siguientes premisas:

La Alcaldía De Tuluá, para asegurar la dirección estratégica de la Entidad, 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 funcionarios, 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 funcionarios, terceros, aprendices, practicantes y clientes de la Alcaldía de Tuluá

- Garantizar la continuidad del negocio frente a incidentes.

4. COMPROMISO DE LA DIRECCION

La alta dirección de la **ALCALDÍA DE TULUÁ**, aprueba esta Política de Seguridad de la Información como muestra de su compromiso y apoyo en el diseño e implementación de políticas eficientes que garanticen la seguridad de la información de la entidad. La Alta Dirección de la entidad demuestran su compromiso a través de:

- La revisión y aprobación de las Políticas de Seguridad de la Información contenidas en este documento.
- La promoción activa de una cultura de seguridad.
- Facilitar la divulgación de este manual a todos los funcionarios de la entidad.
- El aseguramiento de los recursos adecuados para implementar y mantener las políticas de seguridad de la información.
- La verificación del cumplimiento de las políticas aquí mencionadas.

5. OBJETIVO

Definir los lineamientos generales en los para preservar y proteger la confidencialidad, integridad, disponibilidad y privacidad de los activos de la información que orientan los procesos de la Alcaldía de Tuluá, tendientes a proteger la información, los sistemas de información, de acceso, uso, divulgación, interrupción o destrucción no autorizada.

6. ALCANCE Y APLICABILIDAD

Las políticas de seguridad de la información cubren todos los aspectos administrativos y de control que deben ser cumplidos por los directivos, funcionarios, contratistas y terceros que laboren o tengan relación con la Alcaldía de Tuluá, para conseguir un adecuado nivel de protección de las características de seguridad y calidad de la información relacionada.

7. NIVEL DE CUMPLIMIENTO

Todas las personas cubiertas por el alcance y aplicabilidad deberán dar cumplimiento un 100% de la política.

8. POLÍTICAS DE LA ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN

La Alcaldía de Tuluá, establecerá un esquema de seguridad de la información en donde existan roles y responsabilidades definidos que consideren actividades de administración, operación y gestión de la seguridad de la información.

Deberes de la ALTA DIRECCION

❖La Alta Dirección debe definir y establecer los roles y responsabilidades relacionados con la seguridad de la información en niveles directivo y operativo.

❖ La Alta Dirección debe definir y establecer el procedimiento de contacto con las autoridades en caso de ser requerido, así como los responsables para establecer dicho contacto.

❖ La Alta Dirección debe revisar y aprobar las Políticas de Seguridad de la Información contenidas en este documento.

❖ La Alta Dirección debe promover activamente una cultura de seguridad de la información en el instituto.

❖ La Alta Dirección debe facilitar la divulgación de las Políticas de Seguridad de la Información a todos los funcionarios de la entidad y al personal provisto por terceras partes.

❖ La Alta Dirección y (el área responsable del SGSI) deben asignar los recursos, la infraestructura física y el personal necesario para la gestión de la seguridad de la información de la Entidad.

Deberes COMITÉ DE SEGURIDAD DE LA INFORMACION

❖ El Comité de Seguridad de la Información debe actualizar y presentar ante la Alta Dirección las Políticas de Seguridad de la Información, la metodología para el análisis de riesgos de seguridad y la metodología para la clasificación de la información, según lo considere pertinente.

❖ El Comité de Seguridad de la Información debe analizar los incidentes de seguridad que le son escalados y activar el procedimiento de contacto con las autoridades, cuando lo estime necesario.

❖El Comité de Seguridad de la Información debe verificar el cumplimiento de las políticas de seguridad de la información aquí mencionadas.

Deberes de la OFICINA DE CONTROL INTERNO

❖ La Oficina de Control Interno debe planear y ejecutar las auditorías internas al Sistema de Gestión de Seguridad de la Información de la Alcaldía de Tuluá a fin de determinar si las políticas, procesos, procedimientos y controles establecidos están conformes con los requerimientos institucionales, requerimientos de seguridad y regulaciones aplicables.

❖ La Oficina de Control Interno debe ejecutar revisiones totales o parciales de los procesos o áreas que hacen parte del alcance del Sistema de Gestión de Seguridad de la Información, con el fin de verificar la eficacia de las acciones correctivas cuando sean identificadas no conformidades.

❖ La Oficina de Control Interno debe informar a las áreas responsables los hallazgos de las auditorías.

Deberes del DEPARTAMENTO ADMINISTRATIVO DE LAS TIC

❖ La Departamento Administrativo de las TIC, debe asignar las funciones, roles y responsabilidades, a sus funcionarios para la operación y administración de la plataforma tecnológica de la Entidad. Dichas funciones, roles y responsabilidades deben encontrarse documentadas y apropiadamente segregadas.

Todos los Usuarios

❖ Los funcionarios, contratistas y personal provisto por terceras partes que realicen labores en o para la ALCALDÍA DE TULUÁ, tienen la responsabilidad de cumplir con las políticas, normas, procedimientos y estándares referentes a la seguridad de la información.

9. Responsabilidades asignadas

La Política de Seguridad de la Información es de aplicación obligatoria para todo el personal de la ALCALDÍA DE TULUÁ, independiente del tipo de vinculación, el área o dependencia a la cual se encuentre adscrito y el nivel del cargo o funciones que desempeñe.

El ALCALDE DEL MUNICIPIO DE TULUÁ, aprueba esta Política y es responsable de la aprobación y adopción de las actualizaciones.

El Comité de Seguridad de la Información de la entidad es responsable de revisar, proyectar y proponer a la administración Municipal en cabeza del Alcalde, para su aprobación, el documento de la Política de Seguridad de la Información, las funciones generales en materia de seguridad de la información y la estructuración, recomendación, seguimiento y mejora continua del Sistema de Gestión de Seguridad de Información de la ALCALDÍA DE TULUÁ. Es responsabilidad de dicho comité definir las estrategias de capacitación en materia de seguridad de la información al interior de la Administración Municipal.

El Coordinador del Comité de Seguridad de la Información será el responsable de coordinar las acciones del Comité de Seguridad de la Información y de impulsar la socialización, implementación, seguimiento y control de la política.

Los propietarios de activos de la información, son responsables de la clasificación, mantenimiento, actualización y valoración de la misma; así como de documentar y mantener actualizada la clasificación efectuada, definiendo el perfil de los usuarios, y el nivel de permisos de acceso a la información de acuerdo a sus cargos, funciones y competencias. Tienen la responsabilidad de mantener de forma integral, confidencial y disponible el activo de información mientras que es desarrollado, producido, mantenido y utilizado.

Quien ejerza el cargo de Secretario (a) de Desarrollo Institucional, deberá notificar a todo el personal que se vincule con la ALCALDÍA DE TULUÁ, el detalle de las obligaciones respecto al cumplimiento de la Política de Seguridad de la Información y de todos los estándares, procesos, procedimientos, prácticas, guías y lineamientos que surjan del Sistema de Gestión de la Seguridad de la Información. De igual forma, será responsable de la notificación y socialización de la presente Política y de los cambios o actualizaciones que en ella se produzcan a todo el personal, a través de la suscripción de los acuerdos de Confidencialidad y de labores de capacitación continua en materia de seguridad según los lineamientos establecidos por el Comité de Seguridad de la Información de la Entidad.
Los profesionales universitarios y equipo de trabajo del Departamento Administrativo de las TIC, en coordinación con la Secretaría DE Desarrollo Institucional deben seguir los lineamientos de la presente política y cumplir los requerimientos que en materia de seguridad informática se establezcan para la

operación, administración, comunicación y mantenimiento de los sistemas de información e infraestructura tecnológica de la Entidad.

La Oficina de Archivo de la Alcaldía, en colaboración con el Departamento Administrativo de las TIC, determinara el inventario de activos de información y recursos tecnológicos de los cuales son propietarios o custodios, el cual será revisado y avalado por el Almacén, en responsabilidad de los respectivos líderes.

Quien ejerza el cargo de Secretario de la Oficina Asesora Jurídica en el área de Contratación verificará que los contratos, convenios u otra documentación de la entidad con servidores públicos y con terceros incluyan los lineamientos de la Política de Seguridad de la Información de la Entidad.

Los usuarios de la información y de los sistemas utilizados para su procesamiento son responsables de conocer y cumplir la Política de Seguridad de la Información vigente.
La Oficina de Control Interno de la Gestión, es responsable de realizar seguimiento y control periódico sobre información contenida en documentos, sistemas de información y/o actividades vinculadas con la gestión de activos de información. Es responsabilidad de esta área informar sobre el cumplimiento de los lineamientos y medidas de seguridad de la información establecidas por esta Política, y normas adicionales vigentes.

El incumplimiento a la política de Seguridad y Privacidad de la Información, traerá consigo, las consecuencias legales que apliquen a la normativa de la Entidad, incluyendo lo establecido en las normas que competen al Gobierno nacional y territorial en cuanto a Seguridad y Privacidad de la Información se refiere.

10. POLITICAS DE PROTECCIÓN FRENTE A SOFTWARE

10.1COMPONENTES DE SOFTWARE

10.2 Software y Licencias

- Todas las aplicaciones manejadas en la entidad, deben ser clasificadas de acuerdo a su prioridad, como Alta, Media o Baja. Para las aplicaciones con prioridad Alta se debe contar con una copia actualizada y su respectiva documentación técnica en un sitio externo al Departamento Administrativo de Informática.

- Todas las aplicaciones software de la entidad, están protegidas por derechos de autor y requieren licencia de uso, por lo cual está prohibido realizar copias o usar dicho software para fines personales.

- Ningún usuario puede instalar software adicional en los equipos de cómputo de la administración municipal, sin la autorización del Departamento Administrativo de Informática.

- Los usuarios deben advertir y comunicar inmediatamente los síntomas de los posibles problemas que ocurran con el software al Departamento Administrativo de informática.

- Los computadores que contengan software malicioso, deben ser en lo posible aislados de la red, hasta que el problema se haya resuelto.

- Los usuarios no deben desinstalar software por ningún motivo, incluso si éste presenta anomalías. La desinstalación, instalación, restauración o recuperación del sistema debe ser realizada única y exclusivamente por personal autorizado del Departamento Administrativo de informática.

10.3 - Software Antivirus

- Se debe actualizar periódicamente el software de detección de virus y examinar los equipos de cómputo y medios de almacenamiento informático según la frecuencia establecida por el Departamento Administrativo de Informática.

- Cada usuario es responsable de verificar que no exista software malicioso, en los archivos ó información proveniente de redes externas (Internet). Este procedimiento debe realizarse haciendo uso del software antivirus proporcionado por el Departamento Administrativo de Informática.

11. POLÍTICAS DE HARDWARE

11.1- Componentes de Hardware

11.2 - Ubicación y protección de equipos

- El Departamento Administrativo de Informática deberá entregar a cada funcionario un documento que especifique la configuración actual de equipo que tiene a su cargo (Hoja de Vida del Equipo). El funcionario será responsable de velar por la seguridad e integridad del mismo.

- La configuración de hardware de los equipos de cómputo, no debe ser alterada ni mejorada por los funcionarios de la entidad, dicha labor es exclusiva del Departamento Administrativo de Informática.

- Ningún usuario está autorizado para abrir o manipular el interior de los equipos de cómputo ni sus dispositivos de entrada y salida.

- Los equipos de cómputo propiedad de la entidad, deben estar reportados en un inventario que incluya información de sus características, configuración y ubicación.

- Ningún equipo de cómputo, incluyendo computadores, servidores, elementos de red e impresoras, debe ser trasladado o reubicado sin la aprobación del

Departamento Administrativo de Informática.

- Los equipos propiedad de la entidad (impresoras, equipos de cómputo, portátiles, etc.) no deben retirarse de las instalaciones físicas por ninguno de los funcionaros, a menos que esté previamente autorizado.

- Los usuarios que hayan sido autorizados para retirar de manera temporal los equipos de la entidad, (impresoras, equipos de cómputo, portátiles, etc.) deben cumplir las políticas establecidas en este documento.

- Los equipos del centro de datos, incluyendo los componentes que apoyan los diferentes sistemas de información, deben estar conectados en lo posible a varias fuentes de alimentación continua (UPS).

11.3 Mantenimiento Preventivo y Correctivo

- Debe realizarse mantenimiento preventivo a todos los equipos de cómputo de la administración municipal, de acuerdo al cronograma establecido por el Departamento Administrativo de Informática y según lo establecido en el Instructivo de Mantenimiento Preventivo, IN-230 04. De tal forma que el riesgo a fallas se mantenga en una probabilidad de ocurrencia baja.

- Los funcionarios deben reportar al Departamento Administrativo de Informática, sobre daños al equipo que se encuentra a su cargo.

- Los funcionarios no podrán intervenir en la reparación de los equipos de cómputo. El Departamento Administrativo de Informática debe proporcionar personal interno o externo para la solución del problema reportado.

11.4 Dispositivos portátiles de almacenamiento.

- Los dispositivos portátiles de almacenamiento (como memorias y discos duros USB) deben ser analizados por el software antivirus, antes de utilizarlos como medio de almacenamiento en los equipos de cómputo de la entidad.

- Los usuarios que permitan el uso de dispositivos portátiles de almacenamiento en su equipo de cómputo, son responsables de la información que se almacene en ellos y de velar por la información sensible de la entidad.

11.5 Uso de Equipos e Impresoras

- Los usuarios deben abstenerse de usar objetos con propiedades magnéticas (como imanes) cerca de los equipos de cómputo y dispositivos de almacenamiento, ya que pueden provocar la pérdida de los datos en ellos

almacenados.

- Como medida de prevención, los usuarios deben abstenerse de usar grapadoras ó saca ganchos cerca de la impresora y teclado, ya que se pueden incrustar internamente obstruyendo sus piezas, provocando daños irreparables.

- Los usuarios deben conservar en buen estado las herramientas informáticas que les han sido asignadas para llevar a cabo sus funciones laborales. Son responsables entonces de mantener limpia la parte externa de los equipos de cómputo como pantalla, teclado, mouse y torre.

- Los usuarios no deben colocar cerca o encima del monitor ni de la CPU dispositivos telefónicos, celulares, reproductores de CD, radios u otro tipo de dispositivos electrónicos.

- Los usuarios no deben retirar el papel de las impresoras de forma manual ó con fuerza cuando se encuentre encendida.

12. POLÍTICAS DE GESTIÓN DE ACTIVOS DE INFORMACIÓN

12.1 POLITICA DE RESPONSABILIDAD POR LOS ACTIVOS

LA ALCALDÍA DE TULUÁ, como propietario de la información física así como de la información generada, procesada, almacenada y transmitida con su plataforma tecnológica, otorgará responsabilidad a las áreas sobre sus activos de información, asegurando el cumplimiento de las directrices que regulen el uso adecuado de la misma.

La información, archivos físicos, los sistemas, los servicios y los equipos (ej. estaciones de trabajo, equipos portátiles, impresoras, redes, Internet, correo electrónico, herramientas de acceso remoto, aplicaciones, teléfonos y fases, entre otros) propiedad de LA ALCALDÍA DE TULUÁ, son activos de la institución y se proporcionan a los funcionarios y terceros autorizados, para cumplir con los propósitos institucionales de la Administración.

Toda la información sensible de LA ALCALDÍA DE TULUÁ, así como los activos donde ésta se almacena y se procesa deben ser asignados a un responsable, inventariados y posteriormente clasificados, de acuerdo con los requerimientos y los criterios que dicte la Secretaria de DESARROLLO INTITUCIONAL – Oficina de Archivo Municipal. Los propietarios de los activos de información deben llevar a cabo el levantamiento y la actualización permanente del inventario de activos de información al interior de sus procesos o áreas

12.2. PROPIETARIOS DE LOS ACTIVOS DE INFORMACIÓN

Responsabilidades

Los propietarios de la información deben ser los encargados de clasificarla de acuerdo con su grado de sensibilidad y criticidad, de documentar y mantener actualizada la clasificación efectuada y de definir las funciones que deberán tener permisos de acceso a la información.

El Responsable de Seguridad Informática es el encargado de asegurar que los lineamientos para la utilización de los recursos de la tecnología de información contemplen los requerimientos de seguridad establecidos según la criticidad de la información que procesan

- La alta Dirección, los Secretarios de despacho, directivos, coordinadores (Los empleados de libre nombramiento y remoción de carrera, provisionales, profesionales universitarios, auxiliar, administrativo, tecnólogo admtivo) de la **ALCALDÍA DE TULUÁ**, debe contar con un perfil de uso de los recursos de información, incluyendo el hardware y software asociado y actuar como propietarios de la información física y electrónica de la entidad.

- El Comité de Seguridad de la Información determina cuales son los atributos que deben definirse para los diferentes perfiles.

- El Comité de Seguridad de la Información debe elaborar, mantener, actualizar, mejorar y difundir el manual de “Responsabilidades Personales para la Seguridad de la Información en la ALCALDÍA DE TULUÁ”.

- Los propietarios de los activos de información deben clasificar su información de acuerdo con la guía y formato de clasificación de la Información establecida.

- Los propietarios de los activos de información deben generar un inventario de dichos activos para las áreas o procesos que lideran, acogiendo las indicaciones de las guías de clasificación de la información; así mismo, deben mantener actualizado el inventario de sus activos de información.

- Los propietarios de los activos de información deben monitorear periódicamente la validez de los usuarios y sus perfiles de acceso a la información, la clasificación de sus activos de información y de ser necesario realizar su re-clasificación.

- La responsabilidad de custodia de cualquier documento o archivo mantenido, usado o producido por el personal que se retira, o cambia de cargo, recae en el jefe de departamento, secretaría o dependencia o supervisor del contrato; en todo caso el proceso de cambio en la cadena de custodia de la información

debe hacer parte integral del procedimiento de terminación de la relación contractual o de cambio de cargo.

12.3 RESPONSABILIDADES DEPARTAMENTO ADMINISTRATIVO DE LAS TIC.

- El Departamento de las TIC, es el propietario de los activos de información correspondientes a la plataforma tecnológica de la ALCALDIA DE TULUÁ y, en consecuencia, debe asegurar su apropiada operación y administración.

- El Departamento de las Tic, es quien debe autorizar la instalación, cambio o eliminación de componentes de la plataforma tecnológica de la ALCALDÍA DE TULUA.

- El Departamento de las TIC debe establecer una configuración adecuada para los recursos tecnológicos, con el fin de preservar la seguridad de la información y hacer un uso adecuado de ellos.

- El Departamento de las TIC, es responsable de preparar las estaciones de trabajo fijas y/o portátiles de los funcionarios y de hacer entrega de las mismas.

12.4 RESPONSABILIDAD OFICINA DE CONTROL INTERNO

- La Oficina de Control Interno, debe realizar un análisis de riesgos de seguridad de manera periódica, sobre los procesos de la ALCALDÍA DE TULUÁ.

- La Oficina Control Interno, debe definir las condiciones de uso y protección de los activos de información, tanto los tecnológicos como aquellos que no lo son.

- La Oficina Control Interno debe realizar revisiones periódicas de los recursos de la plataforma tecnológica y los sistemas de información de la Entidad.

12.5 RESPONSABILIDAD DE TODOS LOS USUARIOS

- Todas y todos los servidores públicos de la ALCALDÍA DE TULUÁ, independiente del tipo de vinculación laboral o contractual, departamento, secretaría o dependencia, a la cual se encuentre adscrito y las tareas o labores que desempeñe debe suscribir un acuerdo que contenga los términos y condiciones que regulan el uso de recursos de TI y las reglas y perfiles que autorizan el uso de la información institucional.

- Los recursos tecnológicos de la ALCALDÍA DE TULUÁ, deben ser utilizados de forma ética y en cumplimiento de las leyes y reglamentos vigentes, con el fin de evitar daños o pérdidas sobre la operación o la imagen de la Entidad.

- Los recursos tecnológicos de la ALCALDÍA DE TULUÁ provistos a funcionarios y personal suministrado por terceras partes, son proporcionados con el único fin de llevar a cabo las labores del Entidad; por consiguiente, no deben ser utilizados para fines personales o ajenos a este.

- Los funcionarios no deben utilizar sus equipos de cómputo y dispositivos móviles personales para desempeñar las actividades laborales.

- Los funcionarios no deben utilizar software no autorizado o de su propiedad en la plataforma tecnológica de ALCALDÍA DE TULUÁ.

- Todas las estaciones de trabajo, dispositivos móviles y demás recursos tecnológicos son asignados a un responsable, por lo cual es su compromiso hacer uso adecuado y eficiente de dichos recursos.

- En el momento de desvinculación o cambio de labores, los funcionarios deben realizar la entrega de su puesto de trabajo al Director, secretario o Jefe de Oficina o quien este delegue; así mismo, deben encontrarse a paz y salvo con la entrega de los recursos tecnológicos y otros activos de información suministrados en el momento de su vinculación.

12.6 INVENTARIO DE ACTIVOS

Se deben identificar los activos importantes asociados a cada sistema de información, sus respectivos propietarios y su ubicación, para luego elaborar un inventario con dicha información.

El mismo debe ser actualizado ante cualquier modificación de la información registrada y revisado con una periodicidad no mayor a 6 meses.

El encargado de elaborar el inventario y mantenerlo actualizado es el Responsable de cada Área.

13. POLÍTICA DE CLASIFICACIÓN Y MANEJO DE LA INFORMACIÓN

LA ALCALDÍA DE TULUÁ, definirá los niveles más adecuados para clasificar su información de acuerdo con su sensibilidad, y generará una guía de Clasificación de la Información para que los propietarios de la misma la cataloguen y determinen los controles requeridos para su protección. Toda la información de la ALCALDIA DE TULUÁ debe ser identificada, clasificada y documentada de acuerdo con las guías de Clasificación de la Información establecidas por el Comité de Seguridad de la Información. Una vez clasificada la información, LA ALCALDÍA proporcionará los recursos necesarios para la aplicación de controles

en busca de preservar la confidencialidad, integridad y disponibilidad de la misma, con el fin de promover el uso adecuado por parte de los funcionarios de la Administración y personal provisto por terceros (CONTRATISTAS) partes que se encuentre autorizado y requiera de ella para la ejecución de sus actividades clasificación y manejo de la información.

COMITÉ DE SEGURIDAD DE LA INFORMACION

- El Comité de Seguridad de la Información debe recomendar los niveles de clasificación de la información propuestos por la Secretaría de Desarrollo Institucional- Oficina de Archivo Municipal y la guía de clasificación de la Información de la ALCALDÍA DE TULUÁ para que sean aprobados por la Alta Dirección.

  - Desarrollo Institucional

- La Secretaria de Desarrollo Institucional debe definir los niveles de clasificación de la información para LA ALCALDÍA DE TULUÁ y, posteriormente generar la guía de clasificación de la Información.

- La Secretaria de Desarrollo Institucional, debe socializar y divulgar la guía de clasificación de la Información a los funcionarios de la Entidad.

- La Secretaria de Desarrollo Institucional, debe monitorear con una periodicidad establecida la aplicación de la guía de clasificación de la Información.

  - Departamento Administrativo de las TIC.

- El Departamento de las TIC, debe proveer los métodos de cifrado de la información, así como debe administrar el software o herramienta utilizado para tal fin.

- El Departamento de las TIC, debe efectuar la eliminación segura de la información, a través de los mecanismos necesarios en la plataforma tecnológica, ya sea cuando son dados de baja o cambian de usuario.

- El Departamento de las TIC, debe definir los métodos de cifrado de la información de la Entidad de acuerdo al nivel de clasificación de los activos.

Oficina de Archivo

- La Oficina de Archivo debe utilizar los medios de los cuales está dotada para destruir o desechar correctamente la documentación física, con el fin de evitar

la reconstrucción de la misma, acogiéndose a procedimiento establecido para tal fin.

- La Oficina de Archivo debe realizar la destrucción de información cuando se ha cumplido su ciclo de almacenamiento.

- La Oficina de Archivo debe verificar su cumplimiento con base en los medios de almacenamiento y documentos de la Entidad.

Todos los Usuarios

- Los usuarios deben acatar los lineamientos guía de clasificación de la Información para el acceso, divulgación, almacenamiento, copia, transmisión, etiquetado y eliminación de la información contenida en los recursos tecnológicos, así como de la información física de la Entidad.

- La información física y digital de la ALCALDÍA DE TULUÁ debe tener un periodo de almacenamiento que puede ser dictaminado por requerimientos legales o misionales; este período debe ser indicado en las tablas de retención documental y cuando se cumpla el periodo de expiración, toda la información debe ser eliminada adecuadamente.

- Los usuarios deben tener en cuenta estas consideraciones cuando impriman, escaneen, saquen copias y envíes faxes: verificar las áreas adyacentes a impresoras, escáneres, fotocopiadoras y máquinas de fax para asegurarse que no quedaron documentos relacionados o adicionales; asimismo, recoger de las impresoras, escáneres, fotocopiadoras y máquinas de fax, inmediatamente los documentos confidenciales para evitar su divulgación no autorizada.

- Tanto los funcionarios, contratistas y el personal provisto por terceras partes deben asegurarse que en el momento de ausentarse de su puesto de trabajo, sus escritorios se encuentren libres de documentos y medios de almacenamiento, utilizados para el desempeño de sus labores; estos deben contar con las protecciones de seguridad necesarias de acuerdo con su nivel de clasificación.

- La información que se encuentra en documentos físicos debe ser protegida, a través de controles de acceso físico y las condiciones adecuadas de almacenamiento y resguardo

13.1 Etiquetado y manejo de Información

Todos los Funcionarios, Colaboradores y terceros cuando sea el caso, deben mantener organizado el archivo de gestión, siguiendo los lineamientos establecidos por el Proceso de Gestión Documental.

Los Directores, Jefes de Oficina, Coordinadores de Área deben establecer mecanismos de control de documentos, con el fin de garantizar y mantener la disponibilidad, integridad y confidencialidad de la información.

Todos los Funcionarios, Colaboradores y Terceros cuando sea el caso de LA ENTIDAD son responsables de la organización, conservación, uso y manejo de los documentos.

Todas las dependencias de LA ENTIDAD deben enviar al Archivo Central la documentación de forma ordenada y organizada, de acuerdo a los tiempos de retención establecidos en la Tabla de Retención Documental y el Manual de Gestión Documental, acompañado del formato único de inventario documental y en medio magnético.

El Archivo Central de LA ENTIDAD recibe las transferencias documentales de acuerdo al cronograma anual de transferencia Documentales.

Los archivos de Gestión de las oficinas de LA ENTIDAD deben custodiar sus documentos de acuerdo a lo especificado en las tablas de Retención Documental.

La plataforma tecnológica usada para salvaguardar, conservar y facilitar la información de los documentos en medios magnéticos, debe garantizar los principios fundamentales de la seguridad como son la integridad, confidencialidad y disponibilidad de la información y por gestión documental usabilidad y acceso.

Se debe definir procedimientos de etiquetado de la información, de acuerdo con el esquema de clasificación definido por LA ENTIDAD.

El etiquetado de información debe incluir la información física y electrónica.

Las etiquetas de la información, se deben identificar y reconocer fácilmente.

Se debe garantizar la conservación, uso y recuperación de la información contenida en medios digitales, físicos y otros.

13.2 ACCESO A LA INFORMACIÓN

Todos los funcionarios públicos, contratistas y terceros que laboran para la ALCALDÍA, deben tener acceso sólo a la información necesaria para el desarrollo de sus actividades. Para esto, toda novedad en personal debe ser reportada por el área competente (Contratación, Recursos Humanos, etc.) a la Dirección de Planeación y Departamento de las TIC, al encargado de Sistemas de Información

El otorgamiento de acceso a la información debe ser autorizado por el área solicitante y debe estar regulado mediante las normas y procedimientos definidos para tal fin, por el Departamento de las TIC.

Todos los privilegios para el uso de los Sistemas de Información de la Entidad, deben terminar inmediatamente después de que el trabajador cesa de prestar sus servicios a la misma.

Proveedores o terceras personas solamente deben tener privilegios durante el periodo del tiempo requerido para llevar a cabo las funciones aprobadas por el área implicada.

13.3 Usos no aceptables

Hacer caso omiso, retardar o no entregar de manera oportuna las respuestas a las peticiones, quejas, reclamos, solicitudes y denuncias, de igual forma retenerlas o enviarlas a un destinatario que no corresponde o que no esté autorizado, que lleguen por los diferentes medios, presencial, verbal, escrito, telefónico, correo y web.

Dañar o dar como perdido los expedientes, documentos o archivos que se encuentren bajo su administración por la naturaleza de su cargo.

Divulgación no autorizada de los expedientes, documentos, información o archivos.

Realizar actividades tales como borrar, modificar, alterar o eliminar información de LA ENTIDAD de manera malintencionada.

14. POLÍTICAS DE CONTROL DE ACCESO

14.1 Política de acceso a redes y recursos de red

- El Departamento Administrativo de las TIC debe establecer un procedimiento de autorización y controles para proteger el acceso a las redes de datos y los recursos de red de la ALCALDÍA DE TULUÁ.

14.2 Acceso áreas restringidas

- Existe un lugar de recepción que regula el acceso a las distintas áreas del Departamento Administrativo de las TIC, por lo tanto, está prohibido acceder al área restringida sin la autorización correspondiente.

- Todos los funcionarios al ingresar al Departamento Administrativo de las TIC,

deben tener autorización y acompañamiento por el funcionario que atiende la solicitud.

- Los funcionarios de la entidad y visitantes externos, podrán acceder al centro de datos, acompañados por un responsable del Departamento Administrativo de las TIC.

- El centro de datos deberá permanecer cerrado bajo llave, la cual deberá reposar en un lugar seguro del Departamento de las TIC.

- Cuando exista una novedad de personal por traslado o desvinculación de la entidad, todos los códigos de acceso del funcionario implicado deben ser cambiados o desactivados.

- Toda información crítica debe estar provista de la seguridad necesaria por quien la maneja para evitar el uso indebido por parte de personal no autorizado.

- Al terminar la jornada laboral, los escritorios y áreas de trabajo deben quedar desprovistos de documentos sensibles que puedan comprometer los intereses de la entidad. Estos deben quedar bajo llave en archivadores, cajas fuertes o demás medios de almacenamiento físico seguros.

15. POLÍTICA DE ADMINISTRACIÓN DE ACCESO DE USUARIOS

LA ALCALDÍA DE TULUÁ, establecerá privilegios para el control de acceso lógico de cada usuario o grupo de usuarios a las redes de datos, los recursos tecnológicos y los sistemas de información de la Entidad. Así mismo, velará porque los funcionarios y contratistas, tengan acceso únicamente a la información necesaria para el desarrollo de sus labores y porque la asignación de los derechos de acceso esté regulada por normas y procedimientos establecidos para tal fin.

15.1DE RESPONSABILIDADES DE ACCESO DE LOS USUARIOS

- Los usuarios de los recursos tecnológicos y los sistemas de información de la ADMINISTRACIÓN MUNICIPAL DE TULUÁ, realizarán un uso adecuado y responsable de dichos recursos y sistemas, salvaguardando la información a la cual les es permitido el acceso.

- Los usuarios de la plataforma tecnológica, los servicios de red y los sistemas de información de la ADMINISTRACIÓN DE TULUÁ, deben hacerse responsables de las acciones realizadas en los mismos, así como del usuario y contraseña asignados para el acceso a estos.

- Los funcionarios no deben compartir sus cuentas de usuario y contraseñas con otros funcionarios o con personal provisto por contratistas y terceras partes.

- Los funcionarios, contratistas y personal provisto por terceras partes que posean acceso a la plataforma tecnológica, los servicios de red y los sistemas de información de la Administración Municipal, deben acogerse a lineamientos para la configuración de contraseñas implantados por la Entidad.

- En la canaleta eléctrica solo deberán conectarse los equipos de cómputo e impresoras de la entidad, con excepción a ciertos tipos de impresoras, previa evaluación del Departamento Administrativo de Informática, los demás dispositivos eléctricos y/o electrónicos, como ventiladores, radios, cargadores de celulares ó similares no deberán ser conectados, ya que pueden poner en riesgo la estabilidad del sistema.

- Cada usuario debe cerrar su sesión y bloquear el equipo, cuando deba ausentarse de su puesto de trabajo, independientemente del tiempo que lo requiera.

- Los usuarios deben informar inmediatamente al Departamento Administrativo de Informática, toda vulnerabilidad encontrada en los sistemas, aparición de virus o programas sospechosos e intentos de intromisión y no deben distribuir este tipo de información interna o externamente.

- Como mecanismo de prevención todos los funcionarios no deben comer, fumar o beber cerca de los equipos de cómputo y herramientas informáticas, al hacerlo estarían exponiendo los equipos a daños eléctricos y riesgos de contaminación sobre los dispositivos de almacenamiento.

- Los usuarios no deben intentar sobrepasar la seguridad de los sistemas, examinar los equipos de cómputo, servidores y redes de la entidad en busca de archivos de otros usuarios.

- Los usuarios no deben introducir intencionalmente software diseñado para causar daño o impedir el normal funcionamiento de los sistemas.

- Los usuarios no deben recibir archivos que no hayan sido solicitados, a través de redes externas (Internet). Tiene una alta probabilidad de contener software malicioso.

- La fecha y hora de los equipos de cómputo debe estar establecida de acuerdo a la hora legal especificada por la Superintendencia de Industria y Comercio, por tanto los usuarios no están autorizados para modificarla.

- Por razones de compatibilidad entre los diferentes sistemas operativos, no se recomienda publicar, ni nombrar archivos con caracteres no válidos como vocales con tilde, ñ, $, &, etc.

- Los usuarios no deben poner objetos encima del monitor o la CPU, (Ej: cactus, peluches, portarretratos, pisa papeles, etc…) ni colocar adhesivos, diferentes a los usados por la entidad para llevar control del inventario.

16. POLÍTICA DE GESTIÓN DE MEDIOS DE ALMACENAMIENTO

Proteger la información de LA ENTIDAD velando por la protección de la confidencialidad, integridad y disponibilidad de la información que se encuentra en unidades de almacenamiento.

16.1 Gestión y Disposición de medios removibles

Todos los dispositivos y unidades de almacenamiento removibles, tales como cintas, CD's, DVD's, dispositivos personales "USB", discos duros externos, cámaras fotográficas, cámaras de video, celulares, entre otros, deben ser controlados desde su acceso a la red de LA ENTIDAD y uso hasta finalización de su contrato o cese de actividades.

Toda la información clasificada 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 Departamento Administrativo de las Tecnologías de la Información y las Comunicaciones, específicamente aquellas referentes al empleo de técnicas de cifrado.

Se debe llevar el registro de todos los medios removibles de LA ENTIDAD y mantenerlo actualizado.

Todos los medios removibles deben ser almacenados de manera segura.

El Departamento Administrativo de la Información y las Comunicaciones puede restringir que medios de almacenamiento removibles se conecten a los equipos de cómputo que sean propiedad de LA ENTIDAD o que estén bajo su custodia, y puede llevar a cabo cualquier acción de registro o restricción, con el fin de evitar fuga de información a través de medios removibles.

Los medios de almacenamiento removibles que se conecten a la red de datos de LA ENTIDAD o que se encuentren bajo su custodia, están sujetos a monitoreo por parte del Departamento Administrativo de las Tecnologías de la Información y las Comunicaciones.

Todos los retiros de medios de almacenamiento de las instalaciones de LA ENTIDAD, como discos duros externos, se deben realizar con la autorización del propietario del proceso misional, estratégico, mejora continua o de apoyo, definidos de acuerdo al mapa de procesos de LA ENTIDAD, a través del formato orden de salida de elementos.

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.

16.2 Retiro de los derechos de acceso

Cada uno de los procesos de la Entidad es responsable de comunicar a la Secretaria de Desarrollo Institucional y talento Humano, el cambio de cargo, funciones o actividades o la terminación contractual de los Colaboradores pertenecientes al proceso. La Secretaria de Desarrollo Institucional son las encargadas de comunicar a la Oficina de Tecnologías de la Información y las Comunicaciones sobre estas novedades, con el fin de retirar los derechos de acceso a los servicios informáticos y de procesamiento de información.

16.3 Control de contraseña:

- Los usuarios deben mantener sus contraseñas personales en secreto. Las contraseñas que les sean otorgadas a los funcionarios son responsabilidad exclusiva de cada uno de ellos y no deben ser divulgadas, ni transferidas a ninguna persona, a menos que exista un requerimiento legal o un procedimiento que implique hacerlo.

- Los usuarios no deben obtener contraseñas de otros usuarios que pueda permitirles un acceso indebido.

- Los usuarios son responsables de todas las actividades llevadas a cabo con su nombre de usuario y respectiva contraseña.

- Los usuarios deben cambiar su contraseña de dominio cada vez que el sistema lo solicite. Dicha frecuencia es establecida por el Departamento Administrativo de las TIC.

- Las contraseñas deben ser establecidas de acuerdo a las siguientes reglas:

a) Debe ser fácil de recordar.

b) Con una longitud mínima de 7 caracteres.
c) Utilizar letras mayúsculas y minúsculas de la A a la Z.
d) Dígitos en base 10, de 0 a 9.
e) No deben estar basadas en algún dato que otra persona pueda adivinar u obtener fácilmente mediante información relacionada con la persona, por ejemplo: nombres, números de teléfono, fecha de nacimiento, etc;

- Los usuarios no deben llevar un registro en papel de las contraseñas que le han sido asignadas, a menos que dicho papel pueda ser almacenado de manera segura.

17. *POLÍTICA DE PROTECCIÓN CONTRA CÓDIGO MALICIOSO*

Objetivo: Definir las medidas de prevención, detección y corrección frente a las amenazas causadas por códigos maliciosos en LA ENTIDAD.

Toda la infraestructura de procesamiento de información de LA ENTIDAD, cuenta con un sistema de detección y prevención de intrusos, herramienta de Anti-Spam y sistemas de control de navegación, con el fin de asegurar que no se ejecuten virus o códigos maliciosos.

Se debe restringir la ejecución de aplicaciones y mantener instalado y actualizado el antivirus, en todas las estaciones de trabajo y servidores de LA ENTIDAD.

Se debe restringir la ejecución de código móvil, aplicando políticas a nivel de sistemas operativos, navegadores y servicio de control de navegación.

Todos los Funcionarios, Colaboradores y Terceros que hacen uso de los servicios de tecnología de la información y comunicaciones de LA ENTIDAD son responsables del manejo del antivirus para analizar, verificar y (si es posible) eliminar virus o código malicioso de la red, el computador, los dispositivos de almacenamiento fijos, removibles, archivos, correo electrónico que estén utilizando para el desempeño de sus funciones laborales.

LA ENTIDAD cuenta con el software necesario como antivirus para protección a nivel de red y de estaciones de trabajo, contra virus y código malicioso, el servicio es administrado por la Oficina de Tecnologías de la Información y las Comunicaciones.

Los antivirus adquirido por LA ENTIDAD, sólo debe ser instalados por los responsables de la Oficina de Tecnologías de la Información y las Comunicaciones.

Los equipos de terceros que son autorizados para conectarse a la red de datos de LA ENTIDAD deben tener antivirus y contar con las medidas de seguridad apropiadas.

Todos los equipos conectados la red de LA ENTIDAD pueden ser monitoreados y supervisados por la Oficina de Tecnologías de la Información y las Comunicaciones.

Se debe mantener actualizado a sus últimas versiones funcionales las herramientas de seguridad, incluido, motores de detección, bases de datos de firmas, software de gestión del lado cliente y del servidor, etc.

Se debe hacer revisiones y análisis periódicos del uso de software no malicioso en las estaciones de trabajo y servidores. La actividad debe ser programada de forma automática con una periodicidad semanal y su correcta ejecución y revisión estará a cargo de la Oficina de Tecnologías de la Información y las Comunicaciones.

La Entidad debe contar con controles para analizar, detectar y restringir el software malicioso que provenga de descargas de sitios web de baja reputación, archivos almacenados en medios de almacenamiento removibles, contenido de correo electrónico, etc.

Se deben hacer campañas de sensibilización a todos los Funcionarios, Colaboradores y Terceros de ser el caso de LA ENTIDAD, con el fin de generar una cultura de seguridad de la información entre los Funcionarios, Colaboradores y Terceros de LA ENTIDAD.

Los Funcionarios, Colaboradores y Terceros de LA ENTIDAD pueden iniciar en cualquier momento un análisis bajo demanda de cualquier archivo o repositorio que consideren sospechoso de contener software malicioso. En cualquier caso, los Funcionarios, Colaboradores y Terceros cuando sea necesario siempre podrán consultar a la Oficina de Tecnologías de la Información y las Comunicaciones sobre el tratamiento que debe darse en caso de sospecha de malware.

Los usuarios no podrán desactivar o eliminar la suite de productos de seguridad, incluidos los programas antivirus o de detección de código malicioso, en los equipos o sistemas asignados para el desempeño de sus funciones laborales.

Todo usuario es responsable por la destrucción de archivos o mensajes, que le haya sido enviado por cualquier medio provisto por LA ENTIDAD, cuyo origen le sea desconocido o sospechoso y asume la responsabilidad de las consecuencias que puede ocasionar su apertura o ejecución. En estos casos no se deben contestar dichos mensajes, ni abrir los archivos adjuntos, el usuario debe reenviar el correo a la cuenta **soporte@tulua.gov.co.**

El único servicio de antivirus autorizado en la entidad es el asignado directamente por el Departamento Administrativo de las Tecnologías de la Información y las Comunicaciones DATIC, el cual cumple con todos los requerimientos técnicos y de seguridad necesarios para evitar ataques de virus, spyware y otro tipo de software

malicioso. Además este servicio tiene diferentes procesos de actualización que se aplican de manera periódica y segura. Excepcionalmente se podrá realizar la ejecución de otro programa antivirus, únicamente por personal autorizado por la Oficina de Tecnologías de la Información y las Comunicaciones, a efectos de reforzar el control de presencia o programación de virus o código malicioso.

El Departamento de Tecnologías de la Información y las Comunicaciones es el responsable de administrar la plataforma tecnológica que soporta el servicio de Antivirus para los equipos de cómputo conectados a las redes de LA ENTIDAD.

El Departamento de Tecnologías de la Información y las Comunicaciones se reserva el derecho de monitorear las comunicaciones y/o la información que se generen, comuniquen, transmitan o trasporten y almacenen en cualquier medio, en busca de virus o código malicioso.

El Departamento de Tecnologías de la Información y las Comunicaciones se reserva el derecho de filtrar los contenidos que se trasmitan en la red de LA ENTIDAD, con el fin de evitar amenazas de virus.

Todos los correos electrónicos serán revisados para evitar que tengan virus. Si el virus no puede ser eliminado, la información será borrada.

18. POLÍTICA DE COPIAS DE RESPALDO DE LA INFORMACIÓN

La información correspondiente a los procesos críticos de la Administración Municipal y que se encuentra alojada en los servidores a cargo del Departamento Administrativo de las TIC, debe contar con un proceso de respaldo frecuente, según los procedimientos establecidos para tal efecto.

Los respaldos deberán ser almacenados en un lugar externo al Departamento Administrativo de Informática.

Los funcionarios de la administración municipal, deben guardar única y exclusivamente la información indispensable para el correcto desempeño de sus funciones laborales, en la carpeta asignada por el Departamento Administrativo de Informática (Carpeta U). Está información no incluye archivos de uso personal.

El Departamento Administrativo TIC es responsable del respaldo de la información que se encuentre por fuera del espacio de almacenamiento asignado para los usuarios. (Carpeta U).

Si el equipo de cómputo del usuario se encuentra fuera de la red de la entidad, y no es posible realizar una conexión con el servidor donde se aloja la

carpeta laboral correspondiente (Carpeta U), el usuario es responsable de hacer la copia de seguridad de la información laboral respectiva, haciendo uso de dispositivos de almacenamiento como CD's y DVD's.

Si se considera necesario, los usuarios pueden llevar de manera continua los medios de almacenamiento que han sido utilizados para los respaldos de la información al Departamento Administrativo TIC, para que sean trasladados posteriormente a sitios externos.

18.1 Seguridad de la documentación del sistema

Los documentos que especifican el desarrollo de las actividades realizadas en el Departamento Administrativo de las TIC, como procedimientos e instructivos, deben contar con una copia actualizada en un lugar externo al Departamento.

La documentación de todos los Sistemas de información que se manejan en la entidad, deben estar organizados y almacenados en un lugar seguro dentro del Departamento Administrativo de informática, evitando el acceso no autorizado.

18.2 Medios de Respaldo

Las cintas magnéticas y discos se deben ubicar en áreas restringidas dentro del Departamento Administrativo TIC, y en sitios externos con acceso únicamente a personas autorizadas.

El lugar donde se encuentran los medios magnéticos deben contar con condiciones adecuadas para su almacenamiento, según las especificadas por sus fabricantes o proveedores.

18.3 Eliminación Segura

Los medios de almacenamiento que contengan información crítica de la entidad, deben ser físicamente destruidos o sobrescritos de forma segura. Por ejemplo: incinerarlos, hacerlos trizas ó eliminar los datos.

Si existen medios de almacenamiento dañados, se deben revisar en busca de información sensible para la entidad y determinar si deben ser destruidos o reparados.

No se recomienda acumular los medios de almacenamiento para su posterior eliminación, ya que la información contenida en ellos se torna más crítica que la información contenida en un sólo medio

19. POLITICA USO DE CONTROLES CRIPTOGRAFICOS

El objetivo del presente documento es definir reglas para el uso de los controles y claves criptográficas para proteger la confidencialidad, integridad de la información.

Alcance

Este documento se aplica a todo el alcance del Sistema de gestión de seguridad de la información (SGSI); incluidos todos los sistemas de información utilizados en el SGSI.

19.1 USO CONTROLES CRIPTOGRAFICOS

De acuerdo con la Política de clasificación de la información, como también con obligaciones legales y contractuales, la organización debe proteger a los sistemas individuales o a la información a través de los siguientes controles criptográficos:

- Opción de cifrado de Winzip
- Contraseña para los documentos office.
- Utilización de aplicaciones como PGP, Certicamaras, Versing, etc.

La contraseña de cifrado debe ser de más de 8 caracteres (mayúsculas, minúsculas, numero o signos); cumplir con las políticas de claves establecidas.

20. POLÍTICA DE REPORTE Y REVISION DE INCIDENTES DE SEGURIDAD

El personal vinculado a la ALCALDÍA DE TULUÁ, debe reportar con diligencia, eficiencia y responsabilidad presuntas violaciones de seguridad a través de su jefe de dependencia al Departamento Administrativo de las TIC. Cuando la ocasión lo amerite y existan casos especiales dichos reportes podrán realizarse directamente por la persona que encuentre el incidente o novedad.

El Departamento Administrativo de las TIC, debe garantizar las herramientas informáticas para que se realicen tales reportes. El Comité de Seguridad de la Información debe diseñar, mantener y difundir las normas, procesos y guías para el reporte y revisión de incidentes de seguridad.

De conformidad con la ley, la ALCALDÍA DE TULUÁ podrá interceptar o realizar seguimiento a las comunicaciones por diferentes mecanismos previa autorización

del Comité de seguridad de la información, y en todo caso notificando previamente a los afectados por esta decisión. El departamento Administrativo TIC-mantendrá procedimientos escritos para la operación de sistemas de información cuya no disponibilidad suponga un impacto alto en el desarrollo normal de actividades o afecte la continuidad del negocio. Se debe realizar seguimiento a los procedimientos establecidos para asegurar la confiabilidad del servicio que prestan

21. POLÍTICA DE GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO

Se debe garantizar que los planes de continuidad de negocios se ejecuten de forma segura sin exponer la información de LA ENTIDAD.

Establecer los controles para reducir los efectos de las interrupciones de actividad y proteger los procesos esenciales de la empresa contra averías y siniestros mayores. Se debe evaluar el impacto de los diferentes procesos en el organismo y realizar planes de mitigación y continuidad para aquellos que resulten críticos.

Los planes de mitigación y continuidad deben considerar medidas tanto técnicas como administrativas y de vínculo con entidades externas; deben probarse y revisarse periódicamente, y deben permanecer articulados con los diferentes recursos tecnológicos y no tecnológicos existentes en todo el organismo

LA ENTIDAD cuenta con un Plan de Contingencia que asegura la continuidad de las operaciones tecnológicas de sus procesos críticos, teniendo en cuenta las buenas prácticas de seguridad de la información establecidas en este documento.

Los niveles de recuperación mínimos requeridos, así como los requerimientos de seguridad, funciones y responsabilidades relacionados con el plan, deben estar incorporados y definidos en los Planes de contingencias.

Se debe establecer un plan de pruebas periódico del plan de Contingencia de la Plataforma Tecnológica de LA ENTIDAD.

22. POLITICA DE GESTIÓN DOCUMENTAL

Esta política se definió e incorporó en el Programa de Gestión Documental 2016-2019 de la Entidad, para lo cual se tuvieron en cuenta las directrices definidas en el Decreto 2609 de 2012, Artículo 6, en el cual se establecen los componentes mínimos que debe incorporar. Dicha política fue aprobada mediante Acta aprobada en el Comité de Archivo

23. POLÍTICA DE NO REPUDIO

Con el fin de garantizar la disponibilidad, integridad y confidencialidad de la información, la ALCALDÍA DE TULUÁ, empleará y distribuirá equipos con los controles criptográficos en toda la organización, conforme se establece en LAS POLITCAS DE CONTROLES CRIPTOGRAFICOS.

24. POLÍTICA DE PRIVACIDAD

LA ENTIDAD se compromete a otorgar los recursos necesarios para garantizar los tres (3) pilares fundamentales de la privacidad de la información como son la finalidad, consentimiento y responsabilidad de información.

La Dirección General se compromete a velar por la aplicación y cumplimiento adecuado de la presente política de privacidad de la información y todas las que se deriven de ella, por parte de todos los Funcionarios, Colaboradores y Terceros de LA ENTIDAD.

La Entidad 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 decreto 1377 o la que la adicione, modifique o derogue.