

POLÍTICA DE SEGURIDAD Y PRIVACIDAD DE LA
INFORMACIÓN

2025



TABLA DE CONTENIDO

	Pág.
1. INTRODUCCIÓN	5
2. OBJETIVO	5
2.1. OBJETIVO GENERAL	5
2.2. OBJETIVOS ESPECÍFICOS	5
3. ALCANCE	5
4. DEFINICIONES.....	6
5. MARCO LEGAL	9
6. ROLES Y RESPONSABILIDADES	11
6.1. Directivos	11
6.2. Funcionarios/contratistas/terceros:.....	11
6.3. Área de sistemas / Gestión TIC:	11
7. POLÍTICAS	11
7.1. SEGURIDAD DE LOS RECURSOS HUMANOS	12
7.1.1. Talento Humano	12
7.1.2. Gestión TIC	12
7.1.3. Funcionarios	13
7.1.4. Secretaría General.....	13
7.2. GESTIÓN DE ACTIVOS	14
7.2.1. Manejo de medios removibles	15
7.2.2. Uso de internet	15
7.2.3. Unidades de disco de carácter compartido	16
7.2.4. Uso página web, intranet y redes sociales.....	17
7.2.5. Uso del correo electrónico	18
7.3. SEGURIDAD FÍSICA Y DEL ENTORNO	19
7.3.1. Equipo de vigilancia y seguridad.....	19
7.3.2. Perímetro de seguridad física	19
7.3.3. Seguridad de oficinas, recintos e instalaciones	21
7.3.4. Protección contra amenazas externas y ambientales.....	21
7.4. POLÍTICAS DE CONTROL DE ACCESO.....	21
7.4.1. Lineamientos Generales De Control De Acceso	22
7.4.2. Gestión de contraseñas para usuarios.....	23






7.4.3.	Equipo Desatendido, Escritorio y Pantalla Despejada.....	24
7.4.4.	Gestión de acceso a servicios de terceros.....	24
7.5.	ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN.....	25
7.5.1.	Uso de dispositivos móviles.....	25
7.5.2.	Teletrabajo.....	25
7.6.	CONTROLES CRIPTOGRÁFICOS.....	26
7.7.	USO DE LOS RECURSOS TECNOLÓGICOS.....	26
7.8.	SEGURIDAD DE LOS EQUIPOS DE CÓMPUTO.....	26
7.8.1.	Seguridad de los Equipos.....	26
7.8.2.	Mantenimiento de equipos.....	28
7.8.3.	Seguridad de los equipos fuera de las instalaciones y retiro de activos.....	28
7.8.4.	Protección contra códigos maliciosos y móviles.....	29
7.8.5.	Copias de respaldo.....	29
7.9.	MONITOREO DEL USO DE LOS SISTEMAS.....	31
7.10.	ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS DE INFORMACIÓN.....	31
7.10.1.	Requerimientos de seguridad.....	31
7.10.2.	Gestión de vulnerabilidades técnicas.....	32
7.10.3.	Cifrado.....	32
7.10.4.	Seguridad de los archivos del sistema.....	32
7.10.5.	Mantenimiento.....	32
7.11.	GESTIÓN DE VULNERABILIDADES TÉCNICAS.....	32
7.12.	POLÍTICAS DE RELACIONES CON LOS PROVEEDORES.....	33
7.13.	SEGURIDAD DE LA INFORMACIÓN EN LA CONTINUIDAD DE NEGOCIO.....	33
7.14.	POLÍTICAS DE GESTIÓN DE INCIDENTES.....	33
7.15.	SENSIBILIZACIÓN Y COMUNICACIÓN EN SEGURIDAD DE LA INFORMACIÓN.....	34
7.15.1.	Sensibilización y comunicación.....	34
7.15.2.	Capacitaciones En Seguridad.....	34
8.	APROBACIÓN Y REVISIÓN DE LAS POLÍTICAS.....	34
9.	SANCIONES.....	34
10.	POLÍTICA DE CUMPLIMIENTO.....	35
11.	VIGENCIA.....	35



CONTRALORÍA DEPARTAMENTAL DEL META

POLÍTICA DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

CONTROL DE DOCUMENTO Y CAMBIOS			
Versión	Fecha	Cambio	Nombre del editor
2019.05	2019.05.22	Documento nuevo.	Olger Yonatan Cazaran Buitrago
2021.12	2021.12.14	Se actualiza contenido en general, se adicionan capítulos nuevos según requerimiento del Ministerio de las comunicaciones y se reorganiza el contenido de los numerales.	Andrés Leonardo Jiménez Carrillo
2025.03	2025.03.31	Se realiza actualización general del documento, alineando requerimientos de Mintic.	Andrés Leonardo Jiménez Carrillo

Elaboró	Revisó	Aprobó
 Andrés Leonardo Jiménez Carrillo	 Patricia Fierro Cruz	 Jaime Londoño Florez
Profesional Universitario de Gestión TIC	Secretaría General	Contralor Departamental del Meta
Fecha: 2025.03.31		



1. INTRODUCCIÓN

Para la Contraloría Departamental del Meta, en adelante CDM, la información es un activo que es de vital importancia para el desarrollo de las actividades diarias que realizan cada uno de los servidores públicos, siendo las tecnologías de la información, herramientas que han facilitado el desarrollo de los procesos y cumplimiento de los objetivos.

La CDM reconociendo la importancia de proteger la información de una amplia variedad de amenazas, establece una política de seguridad y privacidad de la información acorde a la Misión y Visión de la entidad, proporcionando un marco de referencia para la implementación del Modelo de Seguridad y Privacidad de la Información.

Conscientes de los riesgos que podrían enfrentar los activos de información de la entidad (personal, información, recursos de TI, entre otros.) aplica la gestión de riesgos con el objetivo de prevenirlos o disminuir su impacto y a través de la presente política, garantiza la gestión y administración de la información de forma segura, en busca de la satisfacción de las necesidades y requerimientos de seguridad de la Entidad.

2. OBJETIVO

2.1. OBJETIVO GENERAL

Establecer lineamientos relacionados con la seguridad de la información abordando temáticas específicas, como complemento a lo definido en la "Política General de Seguridad de la Información de la Entidad" con el fin de preservar la confidencialidad, integridad y disponibilidad de los activos de la CDM.

2.2. OBJETIVOS ESPECÍFICOS

- Cumplir con los principios de seguridad y privacidad de la información CID.
- Garantizar la gestión de riesgos e incidentes de seguridad y privacidad de la información.
- Documentar y aplicar los controles y procedimientos necesarios para salvaguardar la integridad, confidencialidad y disponibilidad de los activos de información.
- Fijar las responsabilidades y autoridades de seguridad y privacidad de la información.
- Establecer, implementar, mantener y mejorar continuamente el Modelo de Seguridad y Privacidad de la Información alineado con el Sistema de Gestión de Seguridad de la Información.
- Fortalecer la cultura de seguridad y privacidad de la información en la CDM

3. ALCANCE

El presente manual de políticas, aplica a todos los funcionarios, contratistas, terceros y partes interesadas de la entidad que en el ejercicio de sus funciones utilicen información y servicios TI de la CDM.



4. DEFINICIONES

Activo de información¹: Se refiere a cualquier información o elemento relacionado con el tratamiento de la misma (sistemas, soportes, edificios, personas) que tienen un valor para la entidad.

Activo crítico: Se refiere a instalaciones, sistemas y equipos los cuales, si son destruidos, o es degradado su funcionamiento o por cualquier otro motivo no se encuentran disponibles, afectarán el cumplimiento de los objetivos estratégicos de la CDM.

Administración de Riesgos: Proceso de identificación, control, minimización o eliminación, a un costo aceptable, de los riesgos de seguridad que podrían afectar la información o impactar de manera considerable la operación. Dicho proceso es cíclico y debe llevarse a cabo en forma periódica.

Amenaza: Causa potencial de un incidente no deseado, que puede provocar daños a un sistema o a la entidad.

Autenticidad: Criterio que busca asegurar la validez de la información en tiempo, forma y distribución. Garantizado el origen de la información, en donde se valida el emisor para evitar suplantación de identidades.

Alta Dirección: Persona o grupo de personas que dirigen y controlan al más alto nivel una entidad (Contralor, secretaria general y sub-contralorías).

Centro de cableado: El centro de cableado es el lugar donde se ubican los recursos de comunicación de tecnologías de información, como (Switch, patch, panel, UPS, Router, Cableado de voz y de datos).

Cifrado: Método que permite aumentar la seguridad de un mensaje o de un archivo mediante la codificación del contenido, de manera que sólo pueda leerlo la persona que cuente con la clave de descifrado adecuada.

Control: Son todas aquellas medidas, políticas, procedimientos, prácticas y estructuras organizativas concebidas para mantener los riesgos de seguridad de la información por debajo del nivel de riesgo asumido.

Confidencialidad: Propiedad de la información que la hace no disponible o que no sea divulgada a individuos, entidades o procesos no autorizados.

Código malicioso: Es un código informático que crea brechas de seguridad para dañar un sistema informático.

1

https://minciencias.gov.co/sites/default/files/ckeditor_files/D103M01%20Manual%20Pol%C3%ADticas%20Seguridad%20y%20Privacidad%20Informaci%C3%B3n%20V00.pdf



Custodio: Encargado de administrar y hacer efectivos los controles de seguridad que el propietario de la información haya definido, tales como copias de seguridad, asignación de privilegios de acceso, modificación y borrado.

Dato personal: Cualquier información vinculada o que pueda asociarse a una o a varias personas naturales.

Dato semiprivado: Es semiprivado el dato que no tiene naturaleza íntima, reservada, ni pública y cuyo conocimiento o divulgación puede interesar no solo a su Titular sino a cierto sector o grupo de personas o a la sociedad en general.

Datos sensibles: Se entiende por datos sensibles aquellos que afectan la intimidad del Titular o cuyo uso indebido puede generar su discriminación o que promueva intereses de cualquier tipo, así como los datos relativos a la salud, a la vida sexual, y los datos biométricos.

Datacenter: Se denomina también Centro de Procesamiento de Datos (CPD) a aquella ubicación o espacio donde se concentran los recursos necesarios (TI) para el procesamiento de la información de la CDM.

Disponibilidad: Propiedad de la información donde se garantiza que los usuarios autorizados tengan acceso a la información y a los recursos relacionados con la misma, toda vez que lo requieran.

Dispositivos móviles: Equipo celular Smartphone, equipos portátiles, tablets, o cualquiera cuyo concepto principal sea la movilidad, el cual permite almacenamiento limitado, acceso a internet y cuenta con capacidad de procesamiento.

Evento: Es el suceso identificado en un sistema, servicio o estado de la red que indica una posible brecha en la política de seguridad de la información o fallo de las salvaguardas, o una situación anterior desconocida que podría ser relevante para la seguridad.

Evento de seguridad de la información: Presencia identificada de una condición de un sistema, servicio o red, que indica una posible violación de la política de seguridad de la información o falla de salvaguardas, o una situación desconocida previamente que puede ser pertinente a la seguridad.

Hactivismo: Término que combina dos conceptos, hacker y activismo, ambos se unen en la búsqueda de un cambio social a través del hackeo de sistemas informáticos

Incidente de Seguridad: Evento o serie de eventos de seguridad de la información no deseada o inesperada, que tienen probabilidad significativa comprometer las operaciones del negocio y amenazar la seguridad de la información.

Información: Se refiere a toda comunicación o representación de conocimiento como datos, en cualquier forma, con inclusión de formas textuales, numéricas, gráficas, cartográficas, narrativas o audiovisuales, y en cualquier medio, ya sea magnético, en papel, en pantallas de computadoras, audiovisual u otro.



Integridad: Propiedad de la información que busca salvaguardar la exactitud y totalidad de la información y los métodos de procesamiento.

Impacto: Resultado de un incidente de seguridad de la información.

Mesa de Servicios: Constituye el único punto de contacto con los usuarios finales para registrar, comunicar, atender y analizar todas las llamadas, incidentes reportados, requerimientos de servicio y solicitudes de información. Es a través de la gestión proactiva de la Mesa de Servicios que la Oficina de sistemas, recolecta las necesidades que tienen las dependencias en cuanto a los recursos tecnológicos.

No repudio: El emisor no puede negar que envió porque el destinatario tiene pruebas del envío. El receptor recibe una prueba infalsificable del origen del envío, lo cual evita que el emisor pueda negar tal envío.

Partes interesadas: Persona u organización que puede afectar o ser afectada o percibirse a sí misma como afectada por una decisión o actividad.

Privacidad de la información: Derecho que tienen todos los titulares de la información en relación con la información que involucre datos personales y la información clasificada que estos hayan entregado o esté en poder de la entidad en el marco de las funciones que a ella le compete realizar.

Riesgo: Posibilidad de que una amenaza concreta pueda explotar una vulnerabilidad para causar una pérdida o daño en un activo de información.

Sistema de Gestión de Seguridad de la Información: Es el conjunto de manuales, procedimientos, controles y técnicas utilizadas para controlar y salvaguardar todos los activos que se manejan dentro de una entidad.

Sistema de Información: Se refiere a un conjunto de aplicaciones o conjunto independiente de recursos de información organizados para la recopilación, procesamiento, mantenimiento, transmisión y difusión de información según determinados procedimientos, tanto automatizados como manuales.



5. MARCO LEGAL²

La presente política se fundamenta sobre los lineamientos legales definidos por las leyes colombianas y demás organismos internacionales, facultados para dicha regulación:

Constitución Política de Colombia. Artículo 15.

Ley 44 de 1993: Por la cual se modifica y adiciona la Ley 23 de 1982 y se modifica la Ley 29 de 1944 y Decisión Andina 351 de 2015 (Derechos de autor).

Ley 527 de 1999: Por la cual se define y reglamenta el acceso y uso de los mensajes de datos, del comercio electrónico y de las firmas digitales y se establecen las entidades de certificación y se dictan otras disposiciones.

Ley 594 de 2000: Por medio de la cual se expide la Ley General de Archivos.

Ley 850 de 2003: Por medio de la cual se reglamentan las veedurías ciudadanas

Ley 1221 del 2008: Por la cual se establecen normas para promover y regular el Teletrabajo y se dictan otras disposiciones.

Ley 1266 de 2008: Por la cual se dictan las disposiciones generales del Habeas 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 y se dictan otras disposiciones.

Ley 1273 de 2009: Por medio de la cual se modifica el Código Penal, 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, entre otras disposiciones.

Ley 1341 de 2009: Por la cual se definen principios y conceptos sobre la sociedad de la información y la organización de las tecnologías de la información y las comunicaciones – TIC, se crea la agencia Nacional de espectro y se dictan otras disposiciones.

Ley 1437 de 2011: Por la cual se expide el código de procedimiento administrativo y de lo contencioso administrativo.

Ley 1474 de 2011: Por la cual se dictan normas orientadas a fortalecer los mecanismos de prevención, investigación y sanción de actos de corrupción y la efectividad del control de la gestión pública.

Ley 1581 de 2012: Por la cual se dictan disposiciones generales para la protección de datos personales.

2

https://minciencias.gov.co/sites/default/files/ckeditor_files/D103M01%20Manual%20Pol%C3%ADticas%20Seguridad%20y%20Privacidad%20Informaci%C3%B3n%20V00.pdf



Ley 1712 de 2014: Por medio de la cual se crea la Ley de Transparencia y del Derecho de Acceso a la Información Pública Nacional y se dictan otras disposiciones.

Ley 1915 de 2018: Por la cual se modifica la Ley 23 de 1982 y se establecen otras disposiciones en materia de derecho de autor y derechos conexos.

Ley 1952 de 2019: Por medio de la cual se expide el código general disciplinario

Ley 1581 de 2012: Por la cual se dictan disposiciones generales para la protección de datos personales.

Decreto 2609 de 2012: Por el cual se reglamenta el Título V de la Ley 594 de 2000, parcialmente los artículos 58 y 59 de la Ley 1437 de 2011 y se dictan otras disposiciones en materia de Gestión Documental para todas las Entidades del Estado.

Decreto 0884 del 2012: Por el cual se reglamenta parcialmente la Ley 1221 del 2008.

Decreto 1377 de 2013: Por el cual se reglamenta parcialmente la Ley 1581 de 2012.

Decreto 886 de 2014: Por el cual se reglamenta el Registro Nacional de Bases de Datos.

Decreto 103 de 2015: Por medio del cual se reglamenta parcialmente la Ley 1712 de 2014 y se dictan otras disposiciones.

Decreto 1074 de 2015: Por medio del cual se expide el Decreto Reglamentario del Sector Comercio, Industria y Turismo. Reglamenta parcialmente la Ley 1581 de 2012 e imparten instrucciones sobre el Registro Nacional de Bases de Datos. Artículos 25 y 26.

Decreto 1078 de 2015: Por medio del cual se expide el Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones.

CONPES 3701 de 2011. Lineamientos de Política para Ciberseguridad y Ciberdefensa.

CONPES 3854 de 2016. Política Nacional de Seguridad digital.



6. ROLES Y RESPONSABILIDADES

6.1. Directivos

La Alta Dirección es responsable de garantizar que la seguridad y privacidad de la información se comunique y apropie adecuadamente en la entidad, así como, integrarla en la cultura organizacional. Deben propender a que los servidores públicos y contratistas bajo su responsabilidad conozcan, entiendan y atiendan las políticas contenidas en el presente documento. Así mismo, deben aplicar controles o medidas que garanticen el cumplimiento de las políticas de seguridad informática dentro de los procesos del Sistema Integrado de Gestión que lideren.

6.2. Funcionarios/contratistas/terceros:

Los funcionarios, contratistas, terceros y partes interesadas de la entidad tienen la responsabilidad de implementar y mantener la seguridad y privacidad de la información de la Entidad. Para ello, deben conocer y cumplir las políticas de seguridad y privacidad de la información, reportar las infracciones o incumplimientos que identifique, apoyar a otros servidores en el cumplimiento de las políticas indicadas en este documento.

6.3. Área de sistemas / Gestión TIC:

El área de Sistemas, se encarga de formular y mantener actualizadas las políticas de seguridad informática para toda la entidad, debe revisar, aprobar y mantener el cumplimiento de las políticas, normas y procedimientos de seguridad informática. Adicionalmente, debe promover la seguridad y privacidad de la información en la CDM.

7. POLÍTICAS

La CDM en aras de proteger, preservar y administrar la confidencialidad, integridad, disponibilidad y no repudio de la información de la Entidad, ha definido un manual de política de seguridad y privacidad de la información que permita gestionar de manera integral los riesgos de seguridad informática, a través de la implementación de controles físicos y digitales. Los cuales deberán ser cumplidos por todos los funcionarios, contratistas, terceros, usuarios y visitantes. Los lineamientos de seguridad están clasificados en diferentes temáticas, teniendo en cuenta el contexto interno y externo de la entidad:

La CDM ha definido para tal fin, los siguientes objetivos:

- Establecer las políticas, procedimientos e instructivos en materia de seguridad de la información.
- Implementar, gestionar y mejorar de forma continua, el Sistema de Gestión de Seguridad de la Información.
- Minimizar el riesgo de vulnerabilidad en la seguridad de la información en la ejecución de los procesos misionales de la entidad.
- Cumplir con los principios (Disponibilidad, Integridad y Confidencialidad) de seguridad de la información.



- Proteger los activos de información.
- Fortalecer la cultura de seguridad de la información en los servidores públicos, colaboradores y terceros, que hacen parte de la CDM.
- Verificar de manera periódica el cumplimiento de las políticas de seguridad de la información.
- Propender para que todos los servidores públicos, contratistas y terceros cumplan con las políticas, lineamientos, y buenas prácticas de seguridad de la información establecidas en la presente política.
- Apoyar la innovación tecnológica.
- Mantener la confianza de los servidores públicos, colaboradores y terceros.

7.1. SEGURIDAD DE LOS RECURSOS HUMANOS

El área de Gestión TIC, debe documentar los lineamientos de seguridad que contribuya a reducir los posibles riesgos que el ser humano pueda cometer involuntariamente o voluntariamente; que incluye el uso adecuado de instalaciones y recursos tecnológicos para la seguridad de la información.

7.1.1. Talento Humano

Talento Humano debe:

- Definir procesos de vinculación de personal, dependiendo de la normatividad definida por la entidad.
- Definir procedimientos para la verificación de antecedentes para la contratación
- Establecer y firmar acuerdos de confidencialidad y reserva de la información, que deberán adjuntarse a la hoja de vida del funcionario.
- Informar al personal nuevo que se vincule o contrate en la Entidad la existencia de la normatividad en cuanto a Seguridad y Salud en el Trabajo e implementar el compromiso de confidencialidad de la información y la responsabilidad en materia de seguridad al momento del ingreso a la Entidad; mientras que la oficina asesora de planeación informará acerca del presente manual.
- Notificar de manera oficial a la oficina de Gestión TIC y demás áreas de la entidad, sobre novedades en la contratación para adelantar procesos de asignación/bloqueo de usuario, inventario y activación/desactivación de aplicaciones y servicios a usar.
- Solicitar la devolución de carnet que lo acredita como funcionario de la CDM.

7.1.2. Gestión TIC

Gestión TIC debe:

- Definir las directrices y los lineamientos para la conexión a los activos de Información, de forma segura y confiable.
- Verificar la asignación de privilegios a usuarios.
- Analizar y sugerir medidas a ser implementadas para que el control de acceso a los activos de información y servicios de la Entidad, así como verificar su cumplimiento y su efectividad.



- Verificar el cumplimiento de las pautas establecidas, relacionadas con control de accesos, registro de usuarios, administración de privilegios, administración de claves, utilización de servicios de red, uso controlado de utilitarios del sistema, registro de eventos, verificación de que se ejecuten los procesos de auditoría.
- Apoyar a los usuarios sobre el uso apropiado de claves y de equipos de trabajo.
- Verificar el cumplimiento de los procedimientos de revisión de registros de auditoría.
- Realizar permanentemente campañas de seguridad de la información, dirigidas a todos los usuarios o clientes de los recursos TIC.
- Fomentar el cambio cultural para evitar que las personas realicen descargas de archivos de Internet como de software espía, los troyanos y los atacantes externos etc., y que accedan a sitios desconocidos o de baja confianza, entre otros
- Generar copia de seguridad de buzón de correo electrónico, si le fue asignado.
- La información de la cuenta de correo electrónico, que deba ser asignada a otro funcionario, se realizará en modo de consulta, únicamente.
- Generar copia de seguridad de la información del equipo.

7.1.3. Funcionarios

Cada funcionario de la entidad debe:

- Identificar toda la información que corresponda a su área de responsabilidad cualquiera que sea su forma y medio de conservación.
- Clasificar todos los datos de su propiedad de acuerdo con el grado de criticidad de éstos y mantener un registro actualizado de la información más sensible.
- Autorizar el acceso sobre sus activos de información a colaboradores, contratistas o terceros de la Entidad, de acuerdo con sus respectivas funciones.
- Aprobar y solicitar la asignación de privilegios sobre la información a los diferentes usuarios, ya sea en situaciones rutinarias como excepcionales.
- Informar al jefe inmediato y a la oficina de Gestión TIC, mediante los canales dispuesto para tal fin, sobre novedades e incidentes de seguridad de la información que se materialicen, tomando de ser posible, evidencia de lo acontecido.
- Generar mensualmente, copia de seguridad de la información procesada, dentro de los recursos informáticos dispuestos para tal fin "Unidad Z".
- Al finalizar la vinculación contractual, se debe realizar entrega de toda la información generada y procesada tras el desarrollo de las actividades, e informar la ubicación de dichos documentos.
- Realizar devolución de los activos asignados a su nombre
- De presentarse incumplimiento de la política de seguridad y privacidad de la información, se deberá aplicar los procedimientos establecidos por la entidad para el caso, dispuestos en la normatividad de la CDM.

7.1.4. Secretaría General

La Secretaría General debe:

- Gestionar capacitaciones permanentes a los usuarios o clientes internos en materia de seguridad de la información y difundir las posibles amenazas y riesgos que afectan los recursos TIC de la Entidad.
- Apoyar actividades de divulgación de las políticas definidas



- Apoyar en el aprovisionamiento de recursos necesarios para el desarrollo e implementación de políticas definidas por el área de Gestión TIC.

7.2. GESTIÓN DE ACTIVOS DE INFORMACIÓN

Toda información sea física o digital generada, almacenada o transformada por los funcionarios, contratistas o proveedores de la entidad, utilizando los recursos dispuestos por la entidad para tal fin o en desempeño de sus labores o servicio contratado, son activos de información propiedad de la CDM.

Todas las áreas y dependencias de la entidad deben contar con un inventario de activos y deben estar asignados a cada funcionario que haga uso continuo de él.

La oficina de sistemas, es la encargada de configurar y asegurar los activos informáticos, permitiendo garantizar los principios de confidencialidad, integridad y disponibilidad de la información.

Los funcionarios, no deben realizar instalación de software sin autorización de la oficina de sistemas, los equipos informáticos deben asegurar que las funciones administrativas del equipo estén restringidas.

Los funcionarios públicos, contratistas o terceros, con activos asignados a su nombre deben realizar la entrega formal de estos, al finalizar su relación contractual con la entidad.

No se autoriza a funcionarios, contratistas o terceros, abrir, acceder o modificar los activos informáticos de la entidad. Cualquier novedad, incidente o solicitud deberá notificarse a la oficina de sistemas mediante los canales habilitados para ello.

Cada área deberá definir y clasificar, los activos de información dentro del formato de tabla de retención documental, determinando los controles requeridos para su protección. Así mismo, deberán informar a la oficina de sistemas de dicha clasificación para tener en cuenta a la hora de realizar el tratamiento información.

Los funcionarios, contratistas o terceros deben desarrollar sus procesos bajo los criterios definidos para la clasificación de la información, incluyendo TRD, e inventario de activos.

Cada propietario del activo de Información, debe velar por el cumplimiento de su clasificación de acuerdo con lo establecido en lineamientos para la administración de los archivos y activos de Información

Para el intercambio de información, se debe tener en cuenta su clasificación para su debida protección en términos de confidencialidad.

La oficina de sistemas, debe definir un procedimiento para el uso, protección y prevención de medios removibles.

La oficina de sistemas, debe proveer a los usuarios de la CDM los métodos de cifrado de la información, así como administrar el software o herramienta utilizada para tal fin, y generar la guía de uso para el usuario.



Todo medio removible debe ser escaneado mediante las soluciones de seguridad, que se han establecido en la entidad.

Es responsabilidad de cada Servidor Público, contratista o tercero, tomar las medidas necesarias para la protección de la información contenida en medios removibles, para evitar acceso físico y lógico no autorizado, daños, pérdida de información o extravío del mismo.

La oficina de sistemas, debe generar y aplicar lineamientos para la disposición segura de los dispositivos que almacenen información de la entidad, ya sea cuando son dados de baja o asignados a un nuevo usuario, que incluya borrado o destrucción de datos segura con el fin de la información contenida en estos medios no se pueda recuperar.

7.2.1. Manejo de medios removibles

El uso de medios de almacenamiento removibles tales como CD, DVD, memorias USB, discos duros externos, entre otros, en la infraestructura tecnológica de la Entidad, se autoriza para aquellos funcionarios que lo requieran de acuerdo con el cumplimiento de sus funciones.

Los funcionarios de las otras dependencias, deben asegurar física y lógicamente los dispositivos con el fin de no poner en riesgo la disponibilidad, integridad, y confidencialidad de la información, salvaguardando los medios de daño físico.

Toda memoria o dispositivo extraíble sin excepción, que se conecte a uno de los equipos de la entidad, se debe analizar con el antivirus en busca de software malicioso para evitar una posible infección y posterior pérdida de información.

El área de Gestión TIC, es la encargada de administrar y documentar los procedimientos de medios informáticos removibles, como cintas, discos, casetes, entre otros.

Se debe definir e implementar, mecanismos de cifrado y protección de los medios removibles que almacén información de la entidad, así como capacitar a los funcionarios en su uso adecuado.

7.2.2. Uso de internet

El internet es un recurso valioso para el desempeño de las labores de todos los funcionarios de la entidad, por lo tanto, desde el área de Gestión TIC, se proporciona y controla el servicio de internet, con el fin de mejorar el rendimiento y eficiencia en las actividades que se realizan, encaminadas al cumplimiento de la misión y la visión institucional.

A continuación, se definen lineamientos para su uso adecuado.

El uso de esta herramienta debe hacerse de manera responsable, ética, no abusiva, sin afectar la productividad de la Entidad, sin atentar contra las leyes vigentes y sin poner en riesgo la confidencialidad, integridad y disponibilidad de la plataforma tecnológica.

No está permitido desde la red interna, el acceso a páginas con contenido que atente contra la moral, la ética, los lineamientos de seguridad y la normatividad vigente.



El servicio de internet está destinado a fines laborales, haciendo buen uso de este, por lo cual no se permite el ingreso a páginas que no sean pertinentes para el cumplimiento del cargo, poco fiables, descargas de juegos, música, vídeos, aplicaciones, programas y demás que afecte la gestión de la red.

Si de alguna manera se ve afectado el ancho de banda, la velocidad y perjudicada la red por virus, será necesario el registro de sitios visitados por los funcionarios, donde ellos serán avisados de tal situación, para su posterior tratamiento e investigación a que diere lugar.

El área de Gestión TIC, no es responsable por el contenido de datos ni por el tráfico que en ella circule, la responsabilidad recae directamente sobre el usuario que los genere o solicite.

El área de Gestión TIC podrá restringir el acceso a sitios nocivos y servicios que no sean de utilidad para la Entidad y que demeriten la calidad y agilidad de la red.

Si el acceso a un sitio web, aplicación en la nube, programa informático o software, es restringido o nulo, el funcionario afectado informa a Gestión TIC, quien se encargara de realizar las respectivas correcciones y habilitar el sitio web.

Por razones de seguridad, así como para evitar el daño por virus informáticos queda absolutamente prohibida la instalación de cualquier programa obtenido en la Internet, incluyendo los gratuitos y de evaluación (freeware) y los de comunicación de mensajería instantánea (skype, google talk, facebook, etc.).

Para reducir el riesgo de infección por virus, todos los usuarios deben abstenerse de abrir o enviar archivos extraños posiblemente dañinos o adjuntos en correos, evitar abrir correos de remitentes desconocidos. En caso de recibir alguna información sospechosa notificarla inmediatamente al área de Gestión TIC para su atención, prevención y/o corrección.

Se prohíbe rotundamente realizar actividades hacktivismo desde los equipos de la entidad o dispositivos electrónicos que hagan uso de la red de telecomunicaciones de la entidad.

Estará limitado el acceso a portales de: Juegos, pornografía, drogas, terrorismo, segregación racial, hacking, malware, software gratuito o ilegal y/o cualquier otra página que vaya en contra de las leyes vigentes.

Estará limitado el acceso a redes sociales en general.

Se restringirá el acceso a portales de nube e intercambio de información masiva (exceptuando a la nube corporativa o institucional).

El grupo/oficina de TIC podrá verificar los logs o registros de navegación cuando así se solicite o se requiera para las investigaciones o requerimientos que puedan generarse.

7.2.3. Unidades de disco de carácter compartido

Queda prohibido compartir carpetas desde el equipo asignado al funcionario, en caso de verse la necesidad, la solicitud la realiza el jefe de la dependencia al área de Gestión TIC.



La entidad cuenta con carpetas compartidas desde el servidor, las cuales deben conservar archivos únicamente laborales, es decir, los funcionarios de la CDM, se deben abstener de colgar en ellas música, videos, presentaciones que no sean estrictamente necesarios para las actividades laborales.

Se creará una carpeta pública para compartir información con cualquier funcionario de la entidad, es decir que tendrá libre navegación, edición, modificación y eliminación de la información allí contenida, la información que se suba a esta carpeta es responsabilidad del funcionario, buscando con este lineamiento que se disminuya el uso de memorias usb o dispositivos removibles.

Para cada dependencia, se creará una carpeta, en la cual sólo podrán ingresar los funcionarios adscritos a esta área, tendrán permisos de lectura y edición, la eliminación no será posible.

Cada tres meses, se hará una revisión y/o posible vaciado del contenido en las carpetas de red, con el fin de no saturar el disco duro del servidor y generar lentitud en la red.

Es deber del funcionario, clasificar la información en las carpetas compartidas, con el fin de indicar al profesional de Gestión TIC, qué archivos y carpetas no se deben eliminar a razón de que aún es utilizable la información contenida en ella.

El administrador del sistema, tendrá derecho de acceder y examinar los archivos de los usuarios en los casos de que exista cualquier sospecha de violación a cualquiera de las presentes políticas, infección de virus o de la existencia de materiales nocivos para la CDM, con la previa autorización del jefe inmediato y /o del Contralor.

En el momento en que el área de Gestión TIC expide paz y salvo al funcionario que se retira de manera definitiva de la entidad, dará inicio a la respectiva desactivación de todas las aplicaciones (spark, sysman, directorio activo, etc.), y eliminación de las carpetas del funcionario en la red previo backup de la información.

7.2.4. Uso página web, intranet y redes sociales

La información que se publique o divulgue por cualquier medio de Internet, de cualquier funcionario, contratista o colaborador de la CDM, que sea creado a nombre personal en redes sociales como: instagram, x, facebook, youtube, etc, se considera fuera del alcance del SGSI y por lo tanto su confiabilidad, integridad y disponibilidad y los daños y perjuicios que pueda llegar a causar serán de completa responsabilidad de la persona que las haya generado.

Toda información distribuida en las redes sociales que sea originada por la entidad, debe ser autorizada por el Asesor (a) de Planeación, para ser socializadas y con un vocabulario institucional.

No se debe utilizar el nombre de la entidad en las redes sociales para difamar o afectar la imagen y reputación de los seguidores cuando responden comentarios en contra de la filosofía de la institución.



La publicación de documentos en la página Web e Intranet, deben ser manejados por el área de Gestión TIC, conforme al procedimiento 600.01.69 de divulgación y publicación.

Cada dependencia, podrá elegir libremente los contenidos de la información que se desee incorporar en la página Web, pero deberá contar con el visto bueno del Contralor o el Asesor de Comunicaciones, a fin de verificar la veracidad e integridad de la información a publicar y de esta manera evitar que se exponga la buena imagen de la entidad.

Para la publicación de los documentos en Intranet, Página Web o SECOP se debe crear la incidencia en GLPI y el área de Gestión TIC, tendrá dos días hábiles para hacer la respectiva publicación, excepto los actos contractuales, las cuales deben publicarse el mismo día de recibido.

El funcionario que incumpla lo establecido en estas políticas, será objeto de las correspondientes sanciones disciplinarias.

7.2.5. Uso del correo electrónico

El correo electrónico es una herramienta que agiliza los trámites, cuida el medio ambiente al eliminar la papelería utilizada para fines de distribución, conocimiento y asegura su confidencialidad, integridad y disponibilidad, permitiendo almacenar los testigos de recibido y lectura, asegurando que las personas de interés estén informadas a un mínimo costo.

Desde el área de Gestión TIC, se proporciona a los líderes de proceso, cuentas de correo electrónico institucionales, con el fin de consolidar la imagen institucional y el sentido de pertenencia. Para lo cual, debe dársele un uso racional, responsable, ético y acorde con las funciones desempeñadas.

Los buzones de correo asignados a los funcionarios, contratistas o terceros pertenecen a la CDM, por lo tanto, su contenido también es propiedad de la Entidad.

El usuario con cuenta de correo asignada, debe cambiar periódicamente la contraseña, la cual debe tener como mínimo seis caracteres alfanuméricos.

Es responsabilidad del funcionario, el uso y manejo de la cuenta de correo y así como la privacidad de la contraseña.

Las solicitudes de información de la dependencia, deben realizarse única y exclusivamente desde la cuenta del correo institucional, no está permitido realizar envío de información institucional desde cuentas de correo personales.

La cuenta de correo institucional solo podrá ser utilizar para fines laborales, por tanto, el envío de correo masivo (entiéndase por correo masivo todo aquel que sea ajeno a la Entidad, tales como cadenas, publicidad y propaganda comercial, política, social, etcétera) o que afecte la sensibilidad o reputación de las personas y quede entredicho el buen nombre de la entidad, queda prohibido y se hará la respectiva investigación a que diera lugar.



En caso de requerir el envío de correos masivos, archivos de música y videos es necesaria la autorización del profesional del área de Gestión TIC.

La oficina/grupo de tecnología podrá verificar el contenido de los buzones de los correos telefónicos en los casos que se requiera acudir a información para continuar con la prestación del servicio o para investigaciones específicas.

7.3. SEGURIDAD FÍSICA Y DEL ENTORNO

7.3.1. Equipo de vigilancia y seguridad

La CDM adoptará medidas para el control de acceso físico a las instalaciones y áreas seguras con el fin de mitigar los riesgos asociados a la afectación de la confidencialidad, disponibilidad e integridad de la información.

Para ello, la CDM ha establecido convenio con empresas de vigilancia y seguridad para la prevención de intrusiones no autorizadas a las instalaciones mediante tele-vigilancia 7*24.

Dentro de la oficina de Gestión TIC, se cuenta con dos (2) profesionales Ingenieros de sistemas encargados de mantener, gestionar y monitorizar las operaciones e infraestructura TI de la entidad.

Ambos elementos, están dispuestos para prevenir y atender posibles incidentes de seguridad que atenten contra los sistemas informáticos y los activos de la entidad.

La CDM, definirá áreas seguras y los controles de acceso físico correspondientes para la protección de la información que allí se resguarda.

Todas las personas, que ingresen a las instalaciones de la entidad, deben cumplir con los lineamientos establecidos para el control de acceso físico sin excepción.

7.3.2. Perímetro de seguridad física

La CDM ha definido en su espacio físico, áreas que contiene información y servicios que procesan información como seguras utilizando perímetros modulares para controlar el acceso de personal no autorizado, señalizándolos visiblemente.

Todas las áreas destinadas al procesamiento o almacenamiento de información sensible, así como aquellas en las que se encuentren los equipos y demás infraestructura de soporte a los sistemas de información y comunicaciones, se consideran área de accesos restringidos y seguros. En consecuencia, deben contar con medidas de control de acceso físico en el perímetro tales que puedan ser auditadas, así como con procedimientos de seguridad operacionales que permitan proteger la información, el software y el hardware de daños intencionales o accidentales.

Se debe tener acceso controlado y restringido al cuarto de comunicaciones principales y servidores, garantizando un ambiente seguro y protegido por lo menos con: controles de acceso y seguridad física, detección de incendio y sistemas de extinción de



conflagraciones, controles de humedad y temperatura., bajo riesgo de inundación, sistemas eléctricos regulados y respaldados por fuentes de potencia ininterrumpida (UPS).

En las instalaciones del cuarto de comunicaciones, no está permitido:

- Fumar
- Introducir alimentos o bebidas
- El porte de armas de fuego, corto punzantes o similares.
- Mover, desconectar y/o conectar equipo de cómputo sin autorización.
- Modificar la configuración del equipo o intentarlo sin autorización.
- Alterar software instalado en los equipos sin autorización.
- Alterar o dañar las etiquetas de identificación de los sistemas de información o sus conexiones físicas
- Extraer información de los equipos en dispositivos externos.
- Abuso y/o mal uso de los sistemas de información.
- Toda persona debe hacer uso únicamente de los equipos y accesorios que les sean asignados y para los fines que se les autorice.

Toda información institucional en formato digital, debe ser mantenida en servidores aprobados por el área de Gestión en TIC. No se permite el alojamiento de información institucional en servidores externos sin respectiva aprobación escrita del Comité Institucional de Gestión y Desempeño y/o el Contralor Departamental del Meta.

Los equipos importantes de comunicaciones deben ser alimentados por sistemas de potencia eléctrica regulados y estar protegidos por UPS. El área de Gestión de TIC, debe asegurar que la infraestructura a red de datos de área local, esté cubierta por planes de mantenimiento y soporte adecuados, tanto para hardware como para software.

Las estaciones de trabajo deben estar correctamente aseguradas y operadas por personal de la entidad, el cual debe estar capacitado acerca del contenido de esta política y de las responsabilidades personales en el uso y administración de la información institucional.

Los medios que alojan copias de seguridad deben ser conservados de forma correcta de acuerdo a las políticas y estándares que para tal efecto, establezca el Comité Institucional de Gestión y Desempeño.

Las dependencias tienen la responsabilidad de adoptar y cumplir las normas definidas para la creación y el manejo de copias de seguridad, el área de Gestión TIC elaborará y mantendrá las normas, controles y registros de acceso a dicha área.

Los funcionarios, contratistas y terceros de la entidad, así como los visitantes, deben portar su identificación y/o escarapela de manera visible durante el tiempo que permanezcan dentro de las instalaciones de la organización.

En caso de retiro o desvinculación laboral del funcionario, contratistas y/o tercero, éste debe hacer devolución de la respectiva escarapela asignada en desarrollo de sus funciones, previa liquidación de sus prestaciones sociales y demás obligaciones.



7.3.3. Seguridad de oficinas, recintos e instalaciones

Durante las horas en las que no se labora, la entidad ha contratado el servicio de vigilancia, proceso que se lleva a cabo mediante detectores de movimiento y monitoreo del sistema de cámaras instaladas en los diferentes lugares específicos de la contraloría, el sistema cuenta con línea de comunicación directa con el servicio de vigilancia en caso de que se presente alguna anomalía.

Todos los recursos físicos inherentes a los sistemas de información como las instalaciones, equipos, cableado, expedientes, medios de almacenamiento, etc. deben estar protegidos.

Los recursos TIC utilizados para el procesamiento de la información, deben ser ubicados en sitios estratégicos con mecanismos de seguridad que permita controlar el acceso solo a las personas autorizadas e incluir en la protección de los mismos, los traslados por motivos de mantenimiento u otros escenarios.

7.3.4. Protección contra amenazas externas y ambientales

La entidad a través del Sistema de Gestión de Seguridad y Salud en el Trabajo SGSST, anualmente y según su plan de trabajo, hace inspecciones locativas para identificar amenazas físicas y naturales a las que podría estar expuesta la entidad, así mismo, cuenta con el Plan de Preparación, Prevención y Atención y Respuesta ante Emergencias.

De igual forma, la entidad contrata anualmente pólizas de aseguramiento contra todo riesgo para funcionarios, instalaciones, riesgos a terceros, bienes y personal en caso de accidentes laborales y afectaciones ambientales producidas por agua, fuego y/o explosivos.

7.4. POLÍTICAS DE CONTROL DE ACCESO

La oficina de sistemas, debe establecer las medidas de control de acceso a toda la información propiedad de la Entidad, sin importar el medio en el que se almacene, procese, utilice, transmita, lo cual incluye, pero no limita a recursos de físicos y digitales; ambientes públicos, privados, propios, de terceros o en nube; redes, sistemas operativos, aplicaciones, sistemas de información; servicios de TI, entre otros.

Los controles de acceso deben ser idóneos y robustos, con el fin de impedir el acceso no autorizado a los activos de información de la Entidad. Éstos deben ser conocidos por todos los funcionarios, colaboradores y terceras partes que cuentan con privilegios de acceso a la información de la Entidad y deben controlar los privilegios sobre los activos de información de acuerdo con lo permitido y según lo estrictamente necesario para el desempeño de su función.

Se deben implementar procedimientos para la asignación de privilegios de acceso a los sistemas de información, bases de datos y servicios, estos deben estar claramente documentados, comunicados y controlados en cuanto a su cumplimiento.



Para la protección de los activos de información, se establecerán procedimientos y políticas para el control de acceso a la red, sistemas de información e infraestructura física (Instalaciones), con el fin de mitigar los riesgos asociados al acceso no autorizado a la información.

Todos los usuarios deberán asumir la responsabilidad sobre la información física o digital que accedan y procesan dando un uso adecuado con el fin de salvaguardar la confidencialidad, integridad y disponibilidad de la información.

El área de Gestión TIC define que, para el acceso a la plataforma tecnológica o algunos de sus componentes o aplicaciones, todos los usuarios deben estar identificados y autorizados, previa solicitud del profesional del talento humano, quien es el encargado de llevar los controles pertinentes. La identificación única de los usuarios, permite que queden vinculados y sean responsables de sus acciones.

Para el control de los usuarios, el área de Gestión TIC establece un procedimiento para la alta, modificación y baja de usuarios en los sistemas, con el objeto de permitir el acceso a usuarios nuevos o que han cambiado de funciones y denegar el acceso a usuarios que han dejado la entidad o han cambiado de dependencias.

Los funcionarios deben aplicar las políticas para el control de acceso, utilizando medidas de autenticación para los equipos de cómputo, los sistemas de información y en general, los recursos informáticos utilizados en la CDM.

7.4.1. Lineamientos Generales De Control De Acceso

La Oficina de Planeación y Sistemas, estará a cargo de definir normas y procedimientos para la gestión de accesos a todos los sistemas, bases de datos y servicios de información, el monitoreo del uso de las instalaciones de procesamiento de la información, el uso de dispositivos móviles, y reportes de incidentes relacionados; la revisión de registros de actividades; y el ajuste de relojes de acuerdo con un estándar preestablecido. Además, es responsable de:

- Establecer los mecanismos de control de acceso necesarios con base a los requisitos de seguridad de la información y de los requisitos propios de la Entidad.
- Definir, implementar y monitorear los controles de acceso adecuados para proteger la información y las instalaciones en donde se procesa, almacena, trata y se transmite.
- Analizar y realizar seguimiento permanente de las medidas de control de acceso utilizadas, verificando su eficiencia y efectividad.
- Permitir el acceso a los activos de información y a los servicios y recursos tecnológicos provistos por la CDM, únicamente a los usuarios que hayan sido permitidos específicamente y de acuerdo con el propósito de sus funciones y responsabilidades, verificando los privilegios otorgados sobre los activos de información.
- Se debe realizar la asignación del menor privilegio frente a los activos de información de la Entidad. Los mismos deben ser otorgados únicamente por el tiempo que sea necesario para la ejecución de las funciones y actividades propias del rol.



- Realizar el registro de las actividades relacionadas con el acceso a los activos de información de la Entidad, realizando auditorías continuas sobre los mismos y verificando el cumplimiento de los lineamientos y ejecución efectiva de los procedimientos asociados.
- Verificar el cumplimiento de los lineamientos establecidos, relacionados con control de accesos, registro de usuarios, administración de privilegios, administración de claves, utilización de servicios de red, uso controlado de utilitarios del sistema, registro de eventos, protección de puertos.

El área de Gestión TIC, debe garantizar seguridad en la red a través de medidas de seguridad y protocolos seguros de transferencia:

- Implementación de firewall para el tráfico de red
- Control de acceso a los recursos de la red, mediante uso de credenciales de acceso
- Habilitación de usuarios mediante directorio activo
- Implementación de protocolo TCP/IP para comunicación entre máquinas
- Implementación de protocolo seguro de conexión inalámbrica WPA2 + AES
- Los equipos informáticos usados para comunicación debe estar incluidos dentro de los planes de mantenimiento preventivo/correctivo de la entidad.
- Se debe realizar constante monitoreo de los canales con que la entidad cuenta para prestar servicio de Internet, en aras de prevenir y/o detectar fallos a la seguridad informática de la CDM.
- Se debe realizar registro de navegación y acceso de los funcionarios a Internet
- Dentro de las opciones del firewall se debe realizar control de acceso a sitios web con código malicioso o catalogado como peligrosos.
- Se debe contar con segmentación de red que permita crear zonas delimitadas entre servidores, equipos de funcionarios, áreas de trabajo y visitantes, que limiten o impidan en acceso sin autorización.
- De manera periódica se debe realizar cambio de contraseñas a los equipos de comunicación, servidores y router, mediante uso de contraseñas fuertes y seguras, realizando registro de dichos cambios en bitácoras.

7.4.2. Gestión de contraseñas para usuarios

Desde el área de Gestión TIC se realiza la gestión para que los funcionarios tengan acceso a la plataforma tecnológica, donde deben tener asignado un usuario y contraseña para el uso de los recursos y aplicativos, teniendo en cuenta que las contraseñas deben tener un manejo confidencial.

Los funcionarios deben aplicar buenas prácticas de seguridad en la selección y uso de las contraseñas.

Los usuarios del dominio, serán habilitados únicamente por el administrador de la red "Profesional universitario de Gestión TIC" con el visto bueno del jefe inmediato, mediante formato N° 600.02.67 de asignación de usuarios.

Todas las cuentas de acceso a los sistemas y recursos de las tecnologías de información, son personales e intransferibles. Se permite su uso única y exclusivamente durante la vigencia de derechos del usuario y para actividades relacionadas con la labor asignada.



El nombre de usuario para acceder a la red corresponderá al primer nombre, seguido de un punto y el primer apellido, para no generar conflictos de codificación, los nombres o apellidos que contengan la letra "ñ" serán reemplazados con la letra n y no se tendrán en cuenta las fildes. Estas cuentas serán personalizadas y solo se podrá tener una por funcionario.

El password o contraseña de cada cuenta deberá tener como mínimo 6 caracteres, los cuales serán alfanuméricos y con al menos una letra en mayúscula, y esta debe ser cambiada como mínimo cada dos meses, no se podrá repetir contraseña que haya sido usada en los últimos dos cambios.

La contraseña nunca debe ser pública, es decir, no pegarla en los monitores, teclados, escritorio etc. ni compartirla con el compañero, a razón que cada uno tiene su cuenta de usuario.

7.4.3. Equipo Desatendido, Escritorio y Pantalla Despejada.

Para la oficina de Gestión TIC, es muy importante el buen manejo de la información tanto digital como física y teniendo en cuenta que en los procesos misionales se maneja información de los presuntos responsables fiscales, se requiere tener especial cuidado y atención con la información de carácter confidencial y restringido.

Si de manera temporal el funcionario se levanta del lugar de trabajo, es obligación de todos, bloquear la sesión (digitando las teclas ctrl.+alt+supr y la tecla Enter) o en su defecto apagar el equipo. Al terminar la jornada laboral se deben cerrar las aplicaciones y apagar los equipos de cómputo de manera adecuada.

No deberán dejarse documentos críticos en el "Escritorio" tanto físico como el Escritorio virtual (se denomina "Escritorio" al espacio digital en los equipos de cómputo).

La información sensible que se encuentre en papel o en medios magnéticos debe ser protegida y no dejarse a la vista, especialmente cuando no se esté utilizando, para lo cual debe asegurarse bajo llave en gabinetes, de ser posible u otros sitios seguros.

Los documentos confidenciales o restringidos que se envíen a las impresoras deben retirarse inmediatamente, igualmente aquellos que se copian en unidades de disco compartidas (carpetas compartidas).

7.4.4. Gestión de acceso a servicios de terceros.

La CDM ha definido controles de acceso mediante bitácora de visita, donde los terceros deben realizar registro, ingresado datos personales y de contacto.

Todo el personal, debe portar de manera visible carnet de identificación, así mismo los terceros que ingresan a las instalaciones de la entidad deben portar carnet de visitante que acredite su autorización de acceso.



Los proveedores de servicio, que adelanten actividades dentro de la entidad y que tengan contacto con información y equipos informáticos, deben firmar documento de confidencialidad para poder acceder a dichos equipos.

Los equipos de cómputo que ingresan a la entidad deberán estar autorizados y registrados.

7.5. ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN

7.5.1. Uso de dispositivos móviles

La Entidad establece las directrices de uso y manejo de dispositivos móviles (teléfonos móviles, teléfonos inteligentes "smart phones", tabletas), entre otros, suministrados y/o personales, que hagan uso de los servicios de información de la Entidad.

En el caso del uso de WhatsApp a través de los teléfonos móviles habilitados por la CDM, no se permite por esta aplicación, el envío de fotografías, audios, y videos y cualquier otro tipo de archivo clasificados como información pública reservada o información pública clasificada (privada o semiprivada).

Los usuarios no están autorizados a cambiar la configuración, a desinstalar software, formatear o restaurar de fábrica los equipos móviles institucionales, cuando se encuentran a su cargo, únicamente se deben aceptar y aplicar las actualizaciones.

7.5.2. Teletrabajo

El área de Gestión TIC, debe garantizar al personal autorizado por la alta dirección, el acceso a los recursos e información requerida para la continuidad de las actividades laborales desde ubicaciones distintas a la de la entidad (domicilio del funcionario, visitas a entes de control, etc.). Así mismo, se debe garantizar que existan controles de seguridad que garanticen la seguridad de la información y los activos informáticos. Los controles definidos para tal fin³, son:

- Identificación e inventariado de equipos informáticos, que incluye periféricos.
- Asignación de perfil de usuario limitado
- Definición de contraseñas de acceso
- Implementación de software anti-malware
- Cifrado de unidades
- Planificación de copias de seguridad
- Habilitación de aplicaciones y/o servicios en la web
- Formación sobre seguridad informática.

³ https://www.incibe.es/sites/default/files/contenidos/politicas/documentos/teletrabajo_seguro.pdf



7.6. CONTROLES CRIPTOGRÁFICOS

El área de Gestión TIC debe definir, implementar y gestionar los controles criptográficos para protección de claves de acceso a sistemas, datos y servicios, de acuerdo con el tipo de clasificación dada a los activos de información, asegurando que la información clasificada o reservada cuente con mecanismos de cifrado de datos.

El área de Gestión TIC, debe verificar que los proveedores de desarrollo de software implementen controles criptográficos en los sistemas construidos y que se cumplan con los estándares establecidos por la CDM.

El área de Gestión TIC debe disponer de herramientas necesarias que permitan el cifrado de medios de almacenamiento de información.

7.7. USO DE LOS RECURSOS TECNOLÓGICOS

Las herramientas de cómputo como programas o paquetes utilizados en las actividades de la CDM, serán suministrados exclusivamente por el área de Gestión TIC, la cual lleva un control del listado maestro de licencias de software por equipo.

La configuración de software y hardware está también a cargo del profesional universitario de Gestión TIC. Los usuarios no se encuentran facultados para realizar este tipo de actividades. Se prohíbe la instalación y empleo de cualquier software no instalado o autorizado por el área de Gestión TIC.

El profesional de Gestión TIC, debe revisar y mantener de manera periódica las aplicaciones instaladas a fin de verificar el licenciamiento de las mismas.

El funcionario responsable del equipo de cómputo, también será responsable de software instalado, cualquier modificación o instalación de software que no sea autorizado por el área de Gestión TIC, será responsabilidad del funcionario al cual se le asignó el equipo y será reportado al jefe de inmediato y a la secretaría general para los llamados pertinentes.

El funcionario que requiera de un software en particular, deberá informar al área de Gestión TIC para evaluar la necesidad y solicitar la compra de licencia o autorización de uso, así como el control de su instalación y registro.

7.8. SEGURIDAD DE LOS EQUIPOS DE CÓMPUTO

7.8.1. Seguridad de los Equipos

Los equipos que pertenecen a la infraestructura de tecnología de Información de la dependencia y la entidad, tales como computadores, servidores, equipos de comunicaciones, cableado de energía eléctrica y comunicaciones, UPS, planta telefónica, dispositivos de almacenamiento y demás que sirven como soporte de la información de la Entidad, deberán estar ubicados y protegidos, minimizando los riesgos por pérdida, daño, robo, accesos no autorizados o interrupción de las actividades.



La Entidad se asegurará que la infraestructura de servicios de Tecnologías de información, esté protegida contra fallas en el suministro de energía y demás anomalías relacionadas con ésta, implementando un sistema de alimentación ininterrumpida (UPS), de manera individual que garantice el funcionamiento continuo de los sistemas computacionales que así lo requiera.

Los equipos instalados en las diferentes áreas de la CDM, como computadores, impresoras, ratones (mouse), y cualquier otro dispositivo, solo podrán ser utilizado por el personal de la CDM, para lo cual la Oficina de Almacén, deberá contar con el inventario individual de cada funcionario y comunicarlo al área de Gestión TIC para la actualización del responsable en la hoja de vida de cada equipo.

Queda prohibido a los funcionarios, usar el equipo de cómputo y los servicios de información, para fines distintos a aquellos a los que están destinados y de acuerdo con las funciones institucionales encomendadas.

Todos los funcionarios, son responsables de asegurar la operación correcta y segura de las impresoras, fotocopias o scanner de la Entidad.

El responsable del equipo de cómputo e impresora, deberá hacer un uso adecuado de éstos; queda prohibido abrir físicamente el equipo, así como golpearlo y en general, causar daños por negligencia o de manera intencional. Igualmente, no está permitido consumir alimentos, beber o fumar en el puesto de trabajo.

A cada equipo de cómputo conectado a la red, se le asignara una dirección IP fija, por parte del área de Gestión TIC, y un número de placa asignado por la oficina de almacén.

Las impresoras de trabajo pesado, deberán estar conectadas a la red, y estar disponibles para ser compartidas por los funcionarios que pertenezcan a la dependencia a la cual fue asignada.

Queda prohibido cambiar o conectar elementos de computadores ajenos a los entregados por la Oficina de Almacén para determinado equipo, (conectar parlantes, cambiar Mouse o teclados).

Cada funcionario será responsable de revisar el correcto funcionamiento de su equipo, cuando ocurran fallas en el equipo o impresora, el funcionario deberá cerciorarse que no haya problemas eléctricos que impidan que los dispositivos se pongan operativos, tomar nota de los mensajes de error o la falla en general y reportarlas a través de GLPI bajo los procedimientos estipulados.

Cada funcionario será responsable de apagar el equipo en que esté trabajando (monitor, CPU, impresora, UPS y estabilizador) al terminar la jornada laboral (12 p.m. y 6:00 p.m.) o si se va ausentar del puesto de trabajo en un lapso de tiempo superior a dos horas.

El funcionario es directamente responsable de la seguridad de información contenida en los equipos asignados, es su deber tomar medidas para preservar la integridad y confidencialidad. El área de Gestión TIC asesorará este proceso, pero no será responsable



ante una eventual pérdida de información guardada en los equipos y de la cual el funcionario no generó copia de seguridad.

Queda prohibida la salida de las instalaciones de la CDM, de cualquier equipo de cómputo, periférico y similar, sin la autorización y debidos procedimientos establecidos en el Sistema de Gestión de Calidad de la Entidad.

Todo equipo de cómputo que esté en las instalaciones de la Contraloría y que no pertenezca al inventario de la Entidad, debe contar con la autorización de ingreso del almacenista y debe reposar una copia en el área de Gestión TIC.

En ningún caso, se puede conectar equipos ajenos a la Entidad, en la red privada de la CDM.

7.8.2. Mantenimiento de equipos

La Oficina de Gestión TIC, es quien en primera instancia realiza mantenimiento correctivo, preventivo y adaptativo de la infraestructura tecnológica instalada. En segunda instancia y cuando así lo amerite, la entidad tercerizará el servicio de mantenimiento continuo y adecuado de equipos, mediante contrato de prestación de este servicio con una empresa idónea, que asegure la continua disponibilidad e integridad de estos, de igual manera por cada vigencia, se realizará la contratación del mantenimiento preventivo y correctivo de equipos de cómputo.

7.8.3. Seguridad de los equipos fuera de las instalaciones y retiro de activos

Los equipos o software, no se retiran de las instalaciones de la CDM, sin previa autorización del profesional del área de Gestión TIC, secretaria general y almacenista, informando sus fines y razones de salida, con registro escrito teniendo en cuenta que estos no pueden quedar desatendidos en lugares públicos, deben tener las medidas de seguridad necesarias para ser transportados.

La persona responsable del retiro de equipos, asegura que en todo momento éstos están continuamente vigilados, controlados y manipulados por personal autorizado, manteniendo las medidas de seguridad necesarias para ser transportados evitando robo y daño.

En caso de robo o pérdida, se deberá reportar al profesional de Gestión TIC, secretaria general y almacenista e instaurar la respectiva denuncia ante la autoridad competente.

Los equipos portátiles se deben llevar como equipaje de mano y camuflado, cuando sea posible, durante los viajes y todas las precauciones necesarias a fin de garantizar la confidencialidad, integridad y disponibilidad de los activos de información.

En caso de dar de baja un equipo, se asegura que se haya realizado borrado seguro de información y software licenciado en los medios de almacenamiento.



7.8.4. Protección contra códigos maliciosos y móviles

Se debe proteger todos los sistemas de información, teniendo en cuenta un enfoque multinivel que involucre controles humanos, físicos técnicos y administrativos. El modelo de Seguridad de la Información, garantizará la mitigación de riesgos asociados a amenazas de software malicioso y técnicas de hacking.

La oficina de Gestión TIC para la protección de la infraestructura tecnológica, ha implementado software de seguridad, como antivirus con arquitectura cliente-servidor y capacidad de actualización automática en cuanto a firmas de virus; antispam, antispymware, debidamente licenciado para proteger su plataforma tecnológica de códigos maliciosos y móviles no autorizados. También realiza actividades para concientización de los funcionarios sobre estas amenazas.

Desde la dependencia, se autoriza el uso de estas herramientas y garantiza que éstas no sean deshabilitadas, al igual que su actualización permanente.

No está permitido, sin la autorización de la dependencia de Gestión TIC, desinstalar o deshabilitar las herramientas de seguridad que provee la Entidad, ni el uso de código móvil, ni el ingreso de tecnología móvil a la red de datos, para generar, compilar, propagar, ejecutar o introducir código de programación que este diseñado para producir daño a la infraestructura tecnológica o su rendimiento.

Es deber de la Oficina de Gestión en TICs, hacer seguimiento al tráfico de la red de área local, cuando se tenga evidencias de actividad inusual o detrimentos en el desempeño.

La Oficina de Gestión en TICs, debe mantener actualizada una base de datos con alertas de seguridad, reportadas por organismos competentes y actuar en conformidad, cuando una alerta pueda tener un impacto considerable en el desempeño de los sistemas de información, aplicaciones y software en general.

Es responsabilidad de cada funcionario de la entidad, realizar periódicamente análisis de detección de virus en sus equipos de cómputo asignados, ejecutando el antivirus instalado; para ello, deberá asegurarse de los resultados obtenidos e informar a la oficina de sistemas si se encuentran anomalías, así como realizar el apagado del equipo cuando finalice sus actividades diarias.

Todo funcionario es responsable de la protección de la información a su cargo y no debe compartir, suministrar, publicar o dejar a la vista, datos sensibles como usuarios, passwords, direcciones IP, entre otros.

7.8.5. Copias de respaldo

Toda información que se encuentre contenida en el inventario de activos de información institucional o que sea de interés para un proceso operativo o de misión crítica, debe ser respaldada con copias de seguridad tomadas de acuerdo a los procedimientos documentados por el área de Gestión TIC.



Desde el área de Gestión TIC, se ha definido en el procedimiento de generación de copias de seguridad de la información, que para el desarrollo de las actividades misionales de la entidad, del contenido generado en medios tecnológicos, ésta será almacenada periódicamente de forma que se asegure su identificación, protección, integridad y disponibilidad.

La Oficina de Control Interno, debe efectuar auditorías aleatorias que permitan determinar el correcto funcionamiento de los procesos de copia de seguridad. Las actividades de copias de seguridad de información crítica, deben ser ejecutadas y mantenidas de acuerdo a cronogramas definidos y publicados por el área encargada.

La creación de copias de seguridad de archivos usados, custodiados o producidos por usuarios individuales es responsabilidad exclusiva de dichos usuarios, es decir, la responsabilidad de realizar las copias y mantener actualizadas las mismas, recae directamente sobre cada dueño del activo de la información en la Entidad.

Cada funcionario al momento de la terminación de la relación laboral con la entidad independiente del tipo de contratación deberá entregar copia de seguridad de la información generada en la realización de sus funciones, como requisito para la expedición de paz y salvo del área de Gestión TIC y posterior desvinculación de la Entidad.

Cada usuario debe realizar los respaldos de la información que considere relevante para ejecutar su copia de seguridad, los primeros cinco (05) días hábiles de cada mes o antes que salga en periodo de vacaciones, este respaldo debe contener únicamente la información de gestión del mes inmediatamente anterior.

El funcionario puede solicitar la copia de seguridad de la información de gestión de un determinado tiempo y momento, bajo la solicitud en el formato 600.02.65 y que debe ir firmado por el jefe inmediato.

El procedimiento definido para la generación de copias de seguridad se establece a continuación:

- Se identifica las bases de datos, aplicativos del sistema información de gestión de los funcionarios de lo cual se requiere copias de seguridad.
- El respaldo de información se efectuará en el medio disponible, como son: DVD, Discos duros externos USB, CD o Blu-Ray.
- Se realizan copias de seguridad incremental diaria de aquella información que se actualiza frecuentemente y de alto valor para la Entidad, a las 10:00 p.m. en formato comprimido.
- Se realizan copias de seguridad mensual de la configuración de servidor, de los respaldos incrementales diarios y de la información de gestión de los funcionarios
- Los respaldos mensuales se conservan por los menos dos años.
- Se conserva una copia del último mes de cada año como históricos.

Anualmente, se realizará simulación de recuperación de las copias de seguridad.



Todas las copias de seguridad serán etiquetadas con las siguientes especificaciones: tipo de copia (mensual, diaria), rango de la copia, se debe especificar el contenido (Logs, scripts de configuración, bitácoras, datos).

Se hace registro de la generación de la copia de seguridad, en el formato de registro de generación de copias de seguridad que contiene; código de la copia, nombre de la copia, responsable, lugar de archivo, medio de archivo, tiempo de archivo y disposición. Permitiendo así la trazabilidad de los registros de copias de seguridad.

7.9. MONITOREO DEL USO DE LOS SISTEMAS

El profesional de Gestión TIC, debe asegurar que se generan los registros de eventos de las aplicaciones que hacen parte de la plataforma tecnológica, con el fin de identificar usos no autorizados e incidentes de seguridad de la información. El monitoreo y revisión de estos registros (Logs) se realizan de acuerdo con el nivel de riesgo planteado en el Plan de Tratamiento de Riesgos de la Entidad.

El área de gestión TIC, debe efectuar el monitoreo al crecimiento del volumen de la información de los sistemas que se encuentran en operación y evaluar la capacidad de almacenamiento y procesamiento de los recursos utilizados, con el fin de proyectar el alcance de estos para evitar saturación en los mismos.

Cada usuario de un equipo de cómputo debe conocer los servicios e interacciones del mismo mucho antes de que se presente el evento que atente contra la confidencialidad, integridad y disponibilidad de la información y realizar sugerencias para que Gestión TIC genere los controles que contribuya a minimizar el impacto de que se materialice el incidente.

7.10. ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS DE INFORMACIÓN

Toda aplicación y desarrollo que la CDM implementa, debe contar con protección que asegure los pilares de la seguridad de la información, a través de sus diferentes etapas del ciclo de vida de los sistemas de información, así mismo se debe establecer ambientes separados de desarrollo, pruebas y producción.

7.10.1. Requerimientos de seguridad

Se debe especificar de manera clara y detallada los requisitos relacionados con la seguridad de las aplicaciones, ya sea a desarrollar, adquirir o modificar. Y estas especificaciones deben quedar documentado como evidencia.

La implementación de cualquier sistema de información (propio o de un tercero) debe incluir la documentación, entrenamiento en el uso y gestión de los diferentes módulos, así como la capacitación en la administración de sus funciones de seguridad, y posibles riesgos de seguridad que se puedan materializar.



Se debe definir los requisitos previos a la contratación de proveedores de desarrollo o soporte de software y sistemas de información que incluyan⁴:

- Aseguramiento de la disponibilidad y continuidad del servicio.
- Condiciones para la entrega de código fuente a la CDM, incluyendo cuando el código fuente no sea propiedad de la entidad.
- Acuerdos de niveles de servicio (ANS) adecuados a la criticidad de la aplicación desarrollada o soportada por el proveedor.
- Requisitos de seguridad para el caso desarrollo de aplicativos web.

7.10.2. Gestión de vulnerabilidades técnicas

Es necesario verificar que el funcionamiento de las aplicaciones sea el correcto, tanto en ambiente de producción como de pruebas, validando que se cumplan los requisitos definidos en la etapa de planificación; cualquier vulnerabilidad a la seguridad e integridad es necesaria subsanarla.

7.10.3. Cifrado

Toda aplicación o desarrollo implementado dentro de la entidad, deben seguir los lineamientos y requerimientos de seguridad en cuanto a métodos de encriptación definidos por la CDM. El área de Gestión TIC, se encargará de salvaguardar las llaves criptográficas de las aplicaciones de la entidad.

7.10.4. Seguridad de los archivos del sistema

Si se desarrolla aplicaciones a la medida o en propiedad, solamente el personal autorizado deberá tener acceso al código fuente de la aplicación, no está permitido habilitar en modo producción una aplicación que no haya pasado por la fase de testeo, las pruebas deberán realizarse sobre copias de base de datos en producción.

7.10.5. Mantenimiento

Es necesario que toda aplicación implementada por la CDM, cuente con mantenimiento sobre su base de datos, de tal forma que se asegure un correcto funcionamiento, para ello es importante que se realice copia de seguridad de los archivos y bases de datos antes de ejecutarse, debe quedar documentado el procedimiento realizado y versionada las revisiones hechas. El área de Gestión TIC, debe verificar que la aplicación o sistema de información, garantice los principios de seguridad, disponibilidad e integridad.

7.11. GESTIÓN DE VULNERABILIDADES TÉCNICAS

El área de Gestión TIC debe garantizar, que al menos una vez al año se realice revisión de vulnerabilidades técnicas a los sistemas de información críticos y misionales por medio de

4

https://www.culturantioquia.gov.co/images/2019/MIPG/11_Plan_de_Tratamiento_de_Riesgos_de_Seguridad_y_Privacidad_de_la_Informacion.pdf



ethical hacking y/o pruebas de penetración, donde se documente, informe, gestione y corrijan las vulnerabilidades encontradas, adoptando acciones correctivas para mitigar los hallazgos, minimizar el nivel de riesgo y reducir el impacto.

El área de Gestión TIC, debe restringir a los usuarios finales la instalación de software en los equipos de la entidad a través de directorio activo u otro mecanismo que garantice tal fin.

El área de Gestión TIC, debe monitorear de manera continua la infraestructura tecnológica, para que esta sea usada por los funcionarios, exclusivamente para el desarrollo de las funciones, actividades y obligaciones acordadas o contratadas.

El área de Gestión TIC dentro del desarrollo de los mantenimientos preventivos programados, debe realizar inspección del software instalado en los equipos de la entidad desinstalando el software no autorizado.

7.12. POLÍTICAS DE RELACIONES CON LOS PROVEEDORES

La CDM establecerá políticas y requisitos de seguridad de la información para mitigar los riesgos asociados a cada proceso de contratación.

Antes de iniciar la ejecución de contratos con terceras partes, deberán suscribirse los respectivos acuerdos de confidencialidad que incluyan las cláusulas de confidencialidad y los aspectos de seguridad de la información necesaria durante y después del contrato.

7.13. SEGURIDAD DE LA INFORMACIÓN EN LA CONTINUIDAD DE NEGOCIO

La CDM establecerá un plan de continuidad tecnológica donde se debe incluir la continuidad de la seguridad de la información y restauración oportuna de los servicios en un escenario de contingencia.

La Oficina de TIC generará dicho plan de continuidad tecnológica con base a Planes de Recuperación de Desastres (DRP) y Análisis de Impacto al Negocio (BIA).

7.14. POLÍTICAS DE GESTIÓN DE INCIDENTES

Cada vez que se detecta un evento, incidente o debilidad relacionados con seguridad de la información por parte de un funcionario, contratista o terceras partes, se deberá reportar al área de gestión TIC por cualquiera de los medios dispuestos para tal fin.

Será responsabilidad del área de gestión TIC, seguir los procedimientos establecidos para la gestión de los incidentes que puedan presentarse.



7.15. SENSIBILIZACIÓN Y COMUNICACIÓN EN SEGURIDAD DE LA INFORMACIÓN

7.15.1. Sensibilización y comunicación

La CDM definirá un "Plan de Comunicación en Seguridad de la Información" a través de su oficina de Planeación y comunicación y la Oficina TIC, donde se planificará anualmente la manera en que se comunicarán recomendaciones o tips de seguridad de la información por diferentes medios a todos sus funcionarios y contratistas, con el fin de socializar las políticas institucionales en seguridad de la información o las buenas prácticas en seguridad que se desean socializar para aumentar las capacidades de todas las áreas y procesos de la entidad. La creación de los contenidos se hará con apoyo de la oficina TIC y/o el Oficial de Seguridad de la información.

7.15.2. Capacitaciones En Seguridad

La CDM, a través de sus áreas/procesos de Talento Humano y Contratos, incluirá dentro de sus capacitaciones e inducciones las temáticas de seguridad de la información, con el objetivo de que cualquier funcionario y/o contratista que se vincule a la entidad tenga pleno conocimiento de las políticas de seguridad de la información, el área de gestión TIC y/o el Oficial de Seguridad de la Información apoyará en dichas inducciones.

8. APROBACIÓN Y REVISIÓN DE LAS POLÍTICAS

Las políticas aquí definidas se harán efectivas a partir de su aprobación por la Alta Dirección y serán revisadas por lo menos anualmente, cuando existan incidentes de seguridad de la información o cuando se produzcan cambios estructurales considerables, esto con el fin de asegurar su vigencia y aplicabilidad dentro de CDM

9. SANCIONES

La falta de conocimiento de los presentes lineamientos no libera al personal CDM de las responsabilidades establecidas en ellos por el mal uso que hagan de los recursos de TIC o por el incumplimiento de los lineamientos aquí descritos.

Se aplicarán sanciones de acuerdo con el Código Único Disciplinario.

Pueden aplicarse sanciones de tipo penal según sea el caso y la gravedad de este, si así lo consideran los entes investigativos y judiciales correspondientes.

El área de gestión TIC será el encargado de recopilar y entregar a la Oficina de Control Disciplinario, las evidencias de incumplimiento de los lineamientos, informes de impactos y consecuencias y cualquier otro insumo requerido para formalmente manejar la investigación inicialmente a nivel interno, así mismo, el área de gestión TIC será el encargado de registrar y gestionar el Incidente de seguridad derivado con el incumplimiento de las políticas.



El incumplimiento de la Política de Gestión de Activos de Información de la Entidad podrá constituir falta disciplinaria y será sancionada en el marco del Código Disciplinario Único – Ley 734 de 2002.

10. POLÍTICA DE CUMPLIMIENTO

El área de Gestión TIC dentro del desarrollo de su política de seguridad y privacidad de la información, asegura el correcto uso y disposición de la información que la entidad maneja, asegurando la confiabilidad, integridad y disponibilidad de esta en todo momento. Adicionalmente, la CDM velará por el cumplimiento de la legislación vigente respecto a los requisitos establecidos en la seguridad y privacidad de la información, derechos de propiedad intelectual, protección de datos personales, transparencia y del derecho de acceso a la información pública.

11. VIGENCIA

Esta política en su totalidad entrará en vigencia a partir de su aprobación.

Villavicencio, 31 de marzo de 2025

