



**CONTRALORÍA DEPARTAMENTAL DEL META**

Control fiscal con calidad, independencia y de cara a la comunidad.

# MANUAL DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

VERSIÓN 4.0

ELABORÓ	REVISÓ	APROBÓ
OLGER YONATAN CAZARAN BUIRAGO	OLGER YONATAN CAZARAN BUIRAGO	CARLOS ALBERTO LÓPEZ LÓPEZ
PROFESIONAL UNIVERSITARIO	PROFESIONAL UNIVERSITARIO	CONTRALOR DEPARTAMENTAL DEL META
FECHA	FECHA	FECHA
23-04-2020	23-04-2020	23-04-2020

DE USO EXCLUSIVO PARA LA CONTRALORÍA DEPARTAMENTAL DEL META

	<b>CONTRALORÍA DEPARTAMENTAL DEL META</b> Control fiscal con calidad, independencia y de cara a la comunidad.	
	MANUAL DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN	CÓDIGO: 600.01.101 VERSIÓN 4.0

## CONTENIDO

1.	INTRODUCCIÓN .....	5
2.	OBJETIVO.....	5
3.	ALCANCE .....	5
4.	PRINCIPIOS .....	5
5.	DEFINICIONES .....	7
6.	COMPROMISO DE LA DIRECCIÓN .....	7
7.	ROLES Y RESPONSABILIDADES EN EL SGSI.....	8
7.1.	ROLES.....	8
7.2.	RESPONSABLES .....	9
8.	POLÍTICA GENERAL DEL SISTEMA DE GESTIÓN DE SEGURIDAD SGSI .....	10
9.	ACUERDOS DE CONFIDENCIALIDAD .....	11
10.	CONTACTOS CON LAS AUTORIDADES .....	11
11.	REVISIÓN INDEPENDIENTE DE LA SEGURIDAD DE LA INFORMACIÓN.....	12
12.	PARTES EXTERNAS Y COORDINACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN. ....	12
13.	GESTIÓN DE ACTIVOS .....	12
13.1.	CLASIFICACIÓN DE LA INFORMACIÓN .....	13
14.	GESTIÓN DE OPERACIONES Y COMUNICACIONES .....	15
14.1.	DOCUMENTACIÓN DE LOS PROCEDIMIENTOS DE OPERACIÓN.....	15
14.2.	GESTIÓN DEL CAMBIO .....	15
14.3.	GESTIÓN DE LA CAPACIDAD DEL SISTEMA .....	16
14.4.	ACEPTACIÓN DEL SISTEMA .....	16
15.	POLÍTICA DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN .....	16
15.1.	INTRODUCCIÓN A LA POLÍTICA DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN.....	16
15.2.	OBJETIVO DE LA POLÍTICA DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN 17	17
15.2.1.	Objetivo general de la Política de Seguridad y Privacidad de la Información 17	17
15.2.2.	Objetivos específicos de la Política de Seguridad y Privacidad de la Información.....	17
15.3.	ALCANCE DE LA POLÍTICA DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN 17	17
15.4.	RESPONSABILIDADES.....	17

	<b>CONTRALORÍA DEPARTAMENTAL DEL META</b> Control fiscal con calidad, independencia y de cara a la comunidad.	
	MANUAL DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN	CÓDIGO: 600.01.101 VERSIÓN 4.0

15.5.	LINEAMIENTOS DE LA POLITICA DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN.....	18
15.5.1.	Seguridad de los recursos humanos.....	18
15.5.2.	Seguridad física y del entorno .....	19
15.5.2.1.	<i>Perímetro de seguridad física .....</i>	19
15.5.2.2.	<i>Seguridad de oficinas, recintos e instalaciones.....</i>	21
15.5.2.3.	<i>Protección contra amenazas externas y ambientales .....</i>	21
15.6.	SEGURIDAD DE LOS EQUIPOS DE CÓMPUTO .....	21
15.6.1.	Seguridad de los Equipos .....	21
15.6.2.	Mantenimiento de equipos .....	23
15.6.3.	Seguridad de los equipos fuera de las instalaciones y retiro de activos 24	
15.6.4.	Protección contra códigos maliciosos y móviles.....	24
15.6.5.	Copias de respaldo .....	25
15.7.	MANEJO DE MEDIOS REMOVIBLES .....	27
15.8.	USO DE INTERNET .....	28
15.9.	USO DEL CORREO ELECTRÓNICO .....	29
15.10.	USO DE LOS RECURSOS TECNOLÓGICOS .....	30
15.12.	USO PÁGINA WEB, INTRANET Y REDES SOCIALES.....	31
15.13.	MONITOREO DEL USO DE LOS SISTEMAS .....	32
15.14.	CONTROL DE ACCESO .....	33
15.14.1.	Gestión de contraseñas para usuarios.....	33
15.14.2.	Equipo Desatendido, Escritorio y Pantalla Despejada.....	34
15.16.	SEPARACIÓN DE LAS REDES E IDENTIFICACIÓN DE LOS EQUIPOS .....	36
15.17.	ADQUISICIÓN DE SISTEMAS DE INFORMACIÓN.....	36
15.18.	GESTIÓN DE LOS INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN.....	37
15.18.1.	Reporte de Eventos o Incidentes .....	37
15.18.2.	Manejo de Incidentes de Seguridad.....	38
15.19.	GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO .....	38
16.	CUMPLIMIENTO DE NORMAS POLÍTICAS DE SEGURIDAD DE INFORMACIÓN .....	39
17.	GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO.....	39
18.	SANCIONES .....	39
19.	CUMPLIMIENTO.....	40
20.	CRONOGRAMA .....	41

	<b>CONTRALORÍA DEPARTAMENTAL DEL META</b> Control fiscal con calidad, independencia y de cara a la comunidad.	
	MANUAL DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN	CÓDIGO: 600.01.101 VERSIÓN 4.0

21.	SEGUIMIENTO Y EVALUACIÓN .....	41
22.	MARCO LEGAL .....	41
23.	DOCUMENTOS RELACIONADOS .....	42

	<b>CONTRALORÍA DEPARTAMENTAL DEL META</b> <small>Control fiscal con calidad, independencia y de cara a la comunidad.</small>	
	<b>MANUAL DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN</b>	<b>CÓDIGO: 600.01.101</b> <b>VERSIÓN 4.0</b>

## 1. INTRODUCCIÓN

Para la Contraloría Departamental del Meta, la seguridad de la información es un reto que se ha construido a través de un cuidadoso proceso que se articula con el Plan Estratégico Institucional. En el desarrollo de esta estrategia se ha revisado el enfoque basado en procesos de la organización y se han definido procedimientos documentados del sistema de gestión de la seguridad de la información.

Este manual permite visualizar la entidad como un sistema que interactúa en forma alineada y articulada con los objetivos de la organización, buscando agregar valor a funcionarios proveedores, comunidad, su entorno y especialmente a la ciudadanía en general.

## 2. OBJETIVO

Gestionar el Sistema de Gestión Seguridad y Privacidad de la Información (SGSI) de la Contraloría Departamental del Meta, con base en el Modelo de Seguridad y Privacidad de la Información del MINTIC, manteniendo niveles óptimos de seguridad y privacidad de la información, con la implementación de políticas, controles y procedimientos que permitan de manera oportuna la atención de riesgos en los activos de la entidad.

## 3. ALCANCE

El contenido del SGSI contempla la estructura de gobierno y los lineamientos principales para la seguridad de la información en la Contraloría Departamental del Meta, todos estos deben ser cumplidos por funcionarios, contratistas, terceros y ciudadanía en general que tengan acceso, procesen o transmitan información dentro, fuera o con ocasión de la gestión institucional de la entidad.

## 4. PRINCIPIOS

A continuación, se establecen los principios de seguridad que soportan el Modelo de Seguridad y Privacidad de la Información alineado con el Sistema de Gestión de Seguridad de la Información.

- Las responsabilidades frente a la seguridad y privacidad de la información serán definidas, compartidas y publicadas a los funcionarios, contratistas, terceros y partes interesadas.

	<b>CONTRALORÍA DEPARTAMENTAL DEL META</b> Control fiscal con calidad, independencia y de cara a la comunidad.	
	MANUAL DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN	CÓDIGO: 600.01.101 VERSIÓN 4.0

- La CDM protegerá la información generada, transmitida, procesada y resguardada por el personal vinculado bajo alguna de las modalidades contractuales vigentes, los procesos de negocio y su infraestructura tecnológica, de los riesgos que se puedan generar por los accesos otorgados o el uso indebido de la información. Para ello es fundamental la aplicación de controles de acuerdo con la clasificación de la información de su propiedad o en custodia.
- Los usuarios responsables de la información de la CDM, deberán identificar los riesgos a los que está expuesta la información de sus áreas, teniendo en cuenta que la información pueda ser copiada, divulgada, modificada o destruida física o digitalmente por personal interno o externo.
- La CDM protegerá las instalaciones de procesamiento y la infraestructura tecnológica que soporta sus procesos críticos, mediante la implementación de controles de acceso a la información, sistemas y recursos de red.
- La CDM controlará la operación de sus procesos de negocio garantizando la seguridad de los recursos tecnológicos y las redes de datos.
- La CDM garantizará que la seguridad sea parte integral de los procesos de la entidad, mediante la aplicación de políticas, análisis de riesgos y buenas prácticas en temas de seguridad.
- La CDM promoverá la gestión adecuada de incidentes, eventos y debilidades de seguridad para lograr el mejoramiento continuo de su modelo de seguridad.
- La CDM garantizará la disponibilidad de sus procesos de negocio y la continuidad de su operación basada en el impacto que pueden generar los eventos e incidentes de seguridad.
- La CDM se compromete a realizar todas las actividades tendientes para el cumplimiento de las obligaciones legales, regulatorias y contractuales establecidas.

	<b>CONTRALORÍA DEPARTAMENTAL DEL META</b> Control fiscal con calidad, independencia y de cara a la comunidad.	
	MANUAL DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN	CÓDIGO: 600.01.101 VERSIÓN 4.0

## 5. DEFINICIONES

**Activo de Información:** Conocimientos o datos que tienen valor para la Institución.

**Información:** Todo aquel conjunto de datos organizados en poder de una entidad que sean valor para la misma, independientemente de la forma en que se guarde o transmita (escrita, en imágenes, oral, impresa en papel, almacenada electrónicamente, proyectada, enviada por correo, fax o e-mail, transmitida en conversaciones, etc.), de su origen (de la propia organización o de fuentes externas) o de la fecha de elaboración.

**Seguridad de la Información:** Es la preservación de la Confidencialidad, Integridad y Disponibilidad de la información Institucional y. Preservación de la confidencialidad, integridad y disponibilidad de la información para propender por la autenticidad, trazabilidad, no repudio y fiabilidad de la misma.

**Riesgo de Seguridad de la Información:** Posibilidad que una amenaza dada explote vulnerabilidades de un activo o de un grupo de activos y por lo tanto cause daño a la Institución.

**Integridad:** Propiedad de salvaguardar la exactitud y completitud de los activos

**Sistema de Gestión:** Marco de políticas, procedimientos, guías y recursos asociados para lograr los objetivos de la Institución.

**Políticas:** Intenciones globales y orientación tal como se expresan formalmente por la dirección.

**Procedimiento:** Forma especificada para llevar a cabo una actividad o un proceso

**Registro:** Documento que presenta resultados obtenidos o proporciona evidencias de actividades desempeñadas.

## 6. COMPROMISO DE LA DIRECCIÓN

El comité directivo muestra su compromiso y apoyo en el diseño, implementación y mantenimiento del Sistema de Gestión de Seguridad de

	<b>CONTRALORÍA DEPARTAMENTAL DEL META</b> Control fiscal con calidad, independencia y de cara a la comunidad.	
	MANUAL DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN	CÓDIGO: 600.01.101 VERSIÓN 4.0

la Información a través de la asignación de recursos, la definición de la política de información, los lineamientos de seguridad y el establecimiento del Gobierno de seguridad, cuya conformación y responsabilidades se describen a continuación.

Desde la oficina del despacho de la Contraloría Departamental del Meta, se define el propósito de crear los espacios necesarios para la capacitación y la asignación de recursos pertinentes y suficientes para velar por el dominio y conocimiento de las políticas de seguridad de la información contenidas en la norma ISO 27001 para el área de Gestión TIC.

## 7. ROLES Y RESPONSABILIDADES EN EL SGSI

Los actuales roles se articulan conforme lo planteado en el Esquema de Gobierno TI de la Entidad.

### 7.1. ROLES

Rol	Objetivo
Comité Institucional de Gestión y Desempeño.	<ul style="list-style-type: none"> <li>• Aprobar los lineamientos estratégicos en cuanto a seguridad de la información, garantiza los recursos y la toma de decisiones orientadas al cumplimiento de la estrategia por ellos definida.</li> <li>• Coordinar y dirigir acciones específicas que ayuden a proveer un ambiente seguro y establecer los recursos de información que sean consistentes con las metas y objetivos de Nombre de la entidad.</li> <li>• Supervisa la aplicación de los requisitos definidos por Gobierno Digital en lo relacionado con la seguridad de la información</li> </ul>
Oficial de seguridad de la información (CISO)	<ul style="list-style-type: none"> <li>• Tiene la responsabilidad de guiar y realizar el seguimiento de la implementación de los planes de seguridad definidos.</li> </ul>
Líderes de procesos	<ul style="list-style-type: none"> <li>• Tienen la responsabilidad de dar la cobertura de los lineamientos de</li> </ul>



	<b>CONTRALORÍA DEPARTAMENTAL DEL META</b> Control fiscal con calidad, independencia y de cara a la comunidad.	
	MANUAL DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN	CÓDIGO: 600.01.101 VERSIÓN 4.0

Rol	Objetivo
	seguridad a cada uno de sus procesos operacionales.

## 7.2. RESPONSABLES

Representante legal, Contralor(a) Departamental del Meta, se encarga de la revisión y puesta en marcha del SGSI, así como de su aprobación, así mismo se encarga de la aprobación del presupuesto o recursos necesarios para la ejecución del Sistema de Gestión de Seguridad y Privacidad de la Información dentro del Modelo de Seguridad y Privacidad de La Información.

Líderes de proceso identificados en el manual de procesos y procedimientos vigente, son los responsables de:

- Identificar los activos de su proceso.
- Custodia, resguardo y aplicación de controles para los riesgos identificados para los activos de información a cargo.
- Remitir a Gestión TIC los entregables de los mismos.

Comité Institucional de Gestión y Desempeño y responsable del área de sistemas como transversal se integrarán al análisis y valoración de los riesgos con la metodología dispuesta para tal fin frente a la seguridad y privacidad de la información, es decir que en los periodos de reunión se abrirán los espacios necesarios para el seguimiento correspondiente a los controles donde se involucrará al responsable del área de sistemas.

Seguidamente en el Comité Institucional de Gestión y Desempeño se presentará informe del avance en la implementación de la SGSI que conste por medio de acta, mecanismo a través del cual se oficializará las decisiones necesarias para ser reglamentadas por la Línea estratégica a través de actos administrativos.

Control Interno le corresponde el rol de evaluación independiente quién de manera subjetiva realizará los procesos de auditoría interna y seguimiento al mapa de riesgos teniendo presente el presente manual de Seguridad y Privacidad de la Información.

	<b>CONTRALORÍA DEPARTAMENTAL DEL META</b> <small>Control fiscal con calidad, independencia y de cara a la comunidad.</small>	
	MANUAL DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN	CÓDIGO: 600.01.101 VERSIÓN 4.0

Se considera al responsable de la oficina de Gestión TIC como transversal en todo el proceso de Seguridad de la Información por lo que se debe involucrar en las decisiones que correspondan al SGSI. Esta dependencia será la responsable de:

- Implantar y administrar sistemas informáticos en el entorno mono y multiusuario de manera segura
- Proponer y coordinar cambios para mejorar la explotación del sistema informático y las aplicaciones con los controles previstos en el SGSI
- Administrar los usuarios y contraseñas de los empleados en la plataforma tecnológica de la empresa
- Velar por la seguridad del sistema operativo bloqueando sitios web que puedan afectar la integridad del sistema
- Generar copias de seguridad incrementales diarias de las bases de datos de la entidad.
- Verificar el licenciamiento de software instalado en la plataforma tecnológica de la empresa
- Coordina y efectuar el mantenimiento preventivo y correctivo de los equipos de cómputo.

## 8. POLÍTICA GENERAL DEL SISTEMA DE GESTIÓN DE SEGURIDAD SGSI

La información es un recurso valioso para la Contraloría Departamental del Meta, apoyada en la misión, visión y objetivos del plan estratégico, expresa su compromiso en la minimización de los riesgos a los cuales está expuesta la información que maneja, impulsando una cultura de seguridad y calidad en todos sus procesos, gestionando los incidentes de seguridad que se puedan presentar con el fin de garantizar la seguridad y continuidad de los procesos principales de la entidad.

El área de Gestión TIC propende por la evaluación, vigencia y conformación de esta política, al igual que los demás elementos del SGSI.

Los activos de información estarán clasificados e identificados a fin de establecer los niveles adecuados de protección.

Los funcionarios y líderes de proceso deben garantizar la protección de la información, a la cual tengan acceso para evitar pérdida, daño o uso no autorizado.

	<b>CONTRALORÍA DEPARTAMENTAL DEL META</b> Control fiscal con calidad, independencia y de cara a la comunidad.	
	MANUAL DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN	CÓDIGO: 600.01.101 VERSIÓN 4.0

La entidad implementará controles que permitan salvaguardar los activos de información, para evitar accesos no autorizados, alteraciones o uso indebido de los recursos, garantizando la continuidad de la prestación de los servicios internos y usuarios.

Para lograr lo anteriormente enunciado la Alta Dirección asignará los recursos tanto humanos, presupuestales y tecnológicos necesarios que permitan realizar el seguimiento y evaluación a la implementación y efectividad de esta política y sub-políticas que se deriven del SGSI.

## 9. ACUERDOS DE CONFIDENCIALIDAD

La Secretaría General incorpora en los contratos, cláusulas de confidencialidad y no divulgación de la información, determinando el alcance del incumplimiento a esta política, su responsabilidad civil y penal al que hubiere lugar de acuerdo con lo establecido en la Ley 1273 de 2009 y 1581 de 2012.

Estos acuerdos deben aceptarse por cada uno de ellos como parte del proceso de contratación, razón por la cual dicha cláusula y/o acuerdo de confidencialidad hace parte integral de cada uno de los contratos.

Los funcionarios, contratistas y terceros que tengan vínculos con la entidad aceptan los acuerdos de confidencialidad y no divulgación, que establecen los compromisos de cumplir con los lineamientos de seguridad de la información, dando un manejo adecuado a la información y salvaguardando su confidencialidad.

## 10. CONTACTOS CON LAS AUTORIDADES

La entidad en cabeza de la oficina de Gestión TIC reconoce, identifica y establece contacto con las autoridades como Policía Judicial, CTI, fiscalía, en temas de informática forense y grupos especializados en seguridad de la información, para investigar los incidentes de seguridad de la información y determinar las responsabilidades civiles y penales.

Para mejorar el sistema de seguridad de la dependencia, la entidad a través del funcionario de la oficina de sistemas mantiene contacto con grupos de profesionales especializados, el programa presidencial Gobierno Digital del Ministerio de las Tecnologías, las asociaciones de ingenieros especialistas en seguridad de la información, y foros especializados.

	<b>CONTRALORÍA DEPARTAMENTAL DEL META</b> Control fiscal con calidad, independencia y de cara a la comunidad.	
	MANUAL DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN	CÓDIGO: 600.01.101 VERSIÓN 4.0

## 11. REVISIÓN INDEPENDIENTE DE LA SEGURIDAD DE LA INFORMACIÓN

La Auditoría es una actividad independiente y objetiva de asesoría que le permite medir a la entidad el grado de cumplimiento con el sistema de Gestión de Seguridad de la Información, para mantenerlo, controlarlo y operarlo conforme a las necesidades establecidas en las políticas del SGSI. Para verificar el cumplimiento del SGSI, se realiza una actividad de auditoría en el año y cuando se requiera, se puede realizar revisiones totales o parciales al proceso, determinando los hallazgos no conformes y las observaciones con miras a la planificación de acciones correctivas.

Las auditorías internas son realizadas por funcionario o terceros que cumplan los requisitos establecidos, siguiendo los lineamientos de independencia, objetividad, libre de cualquier perjuicio o conflicto de intereses, y que no audite su propio trabajo.

## 12. PARTES EXTERNAS Y COORDINACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN

La auditoría a los servicios que requieren tercerización de servicios permite establecer medidas de revisión y control en cada uno de los procesos relacionados al SGSI, con miras a determinar el grado de cumplimiento en seguridad, confianza, confidencialidad, integridad y disponibilidad de la información objeto de tratamiento en la gestión de la entidad. La oficina de Gestión TIC socializa las Políticas de Seguridad de la Información a través de sensibilizaciones y capacitaciones con las partes externas, en los procesos relacionados al SGSI.

## 13. GESTIÓN DE ACTIVOS

Todos los activos de la entidad están claramente identificados, plaquetados, rotulados y asignados al responsable o funcionario de la oficina.

La información, archivos físicos, los sistemas, los servicios y los equipos (estaciones de trabajo, portátiles, impresoras, redes, Internet, correo electrónico, herramientas de acceso remoto, aplicaciones, teléfonos, entre otros) propiedad de la Contraloría Departamental del Meta, son activos de

	<b>CONTRALORÍA DEPARTAMENTAL DEL META</b> <small>Control fiscal con calidad, independencia y de cara a la comunidad.</small>	
	MANUAL DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN	CÓDIGO: 600.01.101 VERSIÓN 4.0

la entidad y se proporcionan a los funcionarios, contratistas y terceros autorizados, para cumplir con los propósitos de la misión.

Gestión TIC debe documentar y controlar la conexión remota y el acceso a los sistemas de información de la Entidad con el fin de minimizar el riesgo de accesos no autorizados, así como, administrar, controlar y documentar los perímetros de seguridad que implemente mediante la instalación y configuración de “gateways” con funcionalidades de “firewall” o redes privadas virtuales, para filtrar el tráfico entre los dominios y bloquear el acceso no autorizado.

El acceso a los documentos físicos y digitales estará determinado por las normas relacionadas con el acceso y las restricciones a los documentos públicos, a la competencia del área o dependencia específica y a los permisos y niveles de acceso de los funcionarios, contratistas y terceros determinadas por los Líderes de proceso.

La consulta de expedientes o documentos que reposan en las diferentes oficinas y/o áreas de la entidad se permitirá en días y horas laborales, con la presencia del funcionario o servidor responsable de aquellos.

El funcionario de almacén es el responsable de clasificar, elaborar y mantener actualizado un inventario de activos de información, con el fin de garantizar la disponibilidad, integridad y confidencialidad de estos. Que permita fácilmente ser identificado en serie, nombre, fecha de inventario.

El archivo central, archivos satélites y archivos de gestión de la entidad están organizados conforme con el sistema general de archivo (ley 594 de 2000), y se encuentra actualizado, plenamente etiquetado y almacenado. El funcionario del almacén verifica el cumplimiento de lo descrito.

### 13.1. CLASIFICACIÓN DE LA INFORMACIÓN

La información es uno de los activos más importantes que tiene la Contraloría Departamental del Meta. El proceso de clasificación le permite consolidar su buen nombre con terceros, proveedores y clientes, por el manejo seguro que le hace a su información pues tal acción permite demostrar el cumplimiento de regulaciones internas y gubernamentales. La información se clasifica de acuerdo con su importancia, a su valor, al dueño, al custodio y a los usuarios de la misma.

	<b>CONTRALORÍA DEPARTAMENTAL DEL META</b> Control fiscal con calidad, independencia y de cara a la comunidad.	
	MANUAL DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN	CÓDIGO: 600.01.101 VERSIÓN 4.0

La Contraloría Departamental del Meta, con el fin de resguardar la información que pueda ser divulgada de forma no autorizada o manipulada erróneamente por parte de sus funcionarios, contratistas, proveedores o ciudadanía, ha establecido niveles para la clasificación de la información, incluyendo la información que puede encontrarse en medio electrónico, impreso, verbal o que sea transmitida por cualquier medio.

El Líder de proceso o jefe de área, serán quienes determinen el carácter de información clasificada o reservada. Todos los funcionarios y terceros que manipulen información en el desarrollo de sus funciones deberán firmar un “Acuerdo de Confidencialidad de la Información”, donde individualmente se comprometan a no divulgar, usar o explotar la información confidencial a la que tengan acceso, respetando los lineamientos definidos en los lineamientos del presente documento. En caso de violación de la información será considerado como un incidente de seguridad y se procederá de acuerdo con lo definido al tratamiento de este tipo de incidentes.

**Información pública:** Es toda información que un sujeto obligado genere, obtenga, adquiera, o controle en su calidad de tal.<sup>1</sup>

**Información pública clasificada:** Es aquella información que estando en poder o custodia de un sujeto obligado en su calidad de tal, pertenece al ámbito propio, particular y privado o semiprivado de una persona natural o jurídica por lo que su acceso podrá ser negado o exceptuado, siempre que se trate de las circunstancias legítimas y necesarias y los derechos particulares o privados consagrados en el artículo 18 de la ley 1712 de 2014.<sup>2</sup>

**Información pública reservada:** Es aquella información que estando en poder o custodia de un sujeto obligado en su calidad de tal, es exceptuada de acceso a la ciudadanía por daño a intereses públicos y bajo cumplimiento de la totalidad de los requisitos consagrados en el artículo 19 de la ley 1712 de 2014.<sup>3</sup>

<sup>1</sup> Ley 1712 de 2014, recuperado de: <http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=56882>

<sup>2</sup> Ley 1712 de 2014, recuperado de: <http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=56882>

<sup>3</sup> Ley 1712 de 2014, recuperado de: <http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=56882>

	<b>CONTRALORÍA DEPARTAMENTAL DEL META</b> Control fiscal con calidad, independencia y de cara a la comunidad.	
	MANUAL DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN	CÓDIGO: 600.01.101 VERSIÓN 4.0

## 14. GESTIÓN DE OPERACIONES Y COMUNICACIONES

### 14.1. DOCUMENTACIÓN DE LOS PROCEDIMIENTOS DE OPERACIÓN

Los procedimientos operativos relacionados con los servicios de comunicaciones y procesamiento de la información de la entidad, se mantendrán documentados, actualizados y disponibles con el fin de garantizar el correcto funcionamiento de la plataforma tecnológica.

Gestión TIC debe garantizar el correcto funcionamiento y seguro de todas las operaciones que se realizan con relación al procesamiento de la información y comunicaciones, así mismo, es el área encargada de definir las responsabilidades funcionales y operativas, los requerimientos para resguardar la información macro.

La administración de las instalaciones de procesamiento o las operaciones que se encuentren tercerizadas en instalaciones externas a la de la Entidad deben incluir los controles y estar soportadas en el contrato de tercerización.

Gestión TIC es el área encargada de evaluar los posibles cuellos de botella, que puedan generar amenaza a la seguridad o a la continuidad del procesamiento; también debe planificar la acción correctiva que corresponda.

### 14.2. GESTIÓN DEL CAMBIO

El profesional universitario de la oficina de Gestión TIC controla los cambios en los servicios y los sistemas de procesamiento de la información, evaluando aspectos técnicos y de seguridad, y verifica su correcta implementación.

El Profesional de Gestión TIC debe verificar que los cambios en los componentes operativos y de comunicaciones no afecten la seguridad de los mismos ni de la información que soportan, analizando el posible impacto operativo de los cambios previstos y verificar su correcta implementación.

	<b>CONTRALORÍA DEPARTAMENTAL DEL META</b> <small>Control fiscal con calidad, independencia y de cara a la comunidad.</small>	
	MANUAL DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN	CÓDIGO: 600.01.101 VERSIÓN 4.0

### 14.3. GESTIÓN DE LA CAPACIDAD DEL SISTEMA

A través de la dependencia de Gestión TIC se realiza seguimiento y evaluación a la infraestructura tecnológica a fin de identificar el uso de los recursos, su proyección o escalabilidad. Permitiendo adquirir nuevos recursos de ser necesario una vez identificadas las necesidades, para asegurar el óptimo desempeño del sistema.

### 14.4. ACEPTACIÓN DEL SISTEMA

La oficina de Gestión TIC tiene definido el protocolo de implementación de sistemas de información nuevos, actualizaciones o nuevas versiones ejecutando pruebas suficientes para la aceptación antes de su integración.

## 15. POLÍTICA DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

### 15.1. INTRODUCCIÓN A LA POLÍTICA DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

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 a través de la presente política.



	<b>CONTRALORÍA DEPARTAMENTAL DEL META</b> <small>Control fiscal con calidad, independencia y de cara a la comunidad.</small>	
	<b>MANUAL DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN</b>	<b>CÓDIGO: 600.01.101</b> <b>VERSIÓN 4.0</b>

## 15.2. OBJETIVO DE LA POLÍTICA DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

### 15.2.1. Objetivo general de la Política de Seguridad y Privacidad de la Información

Establecer los lineamientos de seguridad de la información que permitan garantizar la protección de los datos personales y los activos de información con que cuenta la CDM.

### 15.2.2. Objetivos específicos de la Política de Seguridad y Privacidad de la Información

- Cumplir con los principios de seguridad y privacidad de la información.
- 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

## 15.3. ALCANCE DE LA POLÍTICA DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

Esta política 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.

## 15.4. RESPONSABILIDADES

El personal encargado de la seguridad de la información es responsable de promover la seguridad y privacidad de la información en la CDM.

	<b>CONTRALORÍA DEPARTAMENTAL DEL META</b> Control fiscal con calidad, independencia y de cara a la comunidad.	
	MANUAL DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN	CÓDIGO: 600.01.101 VERSIÓN 4.0

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.

Los funcionarios, contratistas, terceros y partes interesadas de la entidad tienen la responsabilidad de mantener la seguridad y privacidad de la información de la Entidad.

## 15.5. LINEAMIENTOS DE LA POLÍTICA DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

### 15.5.1. Seguridad de los recursos humanos

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.

La CDM a través de la dependencia de Talento Humano debe 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.

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.

Gestión TIC debe realizar permanentemente campañas de seguridad de la información, dirigidas a todos los usuarios o clientes de los recursos TIC y 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.

	<b>CONTRALORÍA DEPARTAMENTAL DEL META</b> Control fiscal con calidad, independencia y de cara a la comunidad.	
	MANUAL DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN	CÓDIGO: 600.01.101 VERSIÓN 4.0

## 15.5.2. Seguridad física y del entorno

### 15.5.2.1. *Perímetro de seguridad física*

La Contraloría Departamental del Meta 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 acceso restringido. 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, bajo riesgo de inundación, sistemas eléctricos regulados y respaldados por fuentes de potencia ininterrumpida (UPS).

En las instalaciones del cuarto de telecomunicaciones, 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.

	<b>CONTRALORÍA DEPARTAMENTAL DEL META</b> <small>Control fiscal con calidad, independencia y de cara a la comunidad.</small>	
	MANUAL DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN	CÓDIGO: 600.01.101 VERSIÓN 4.0

- 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 este cubierta por 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, 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.

	<b>CONTRALORÍA DEPARTAMENTAL DEL META</b> Control fiscal con calidad, independencia y de cara a la comunidad.	
	MANUAL DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN	CÓDIGO: 600.01.101 VERSIÓN 4.0

#### 15.5.2.2. 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.

#### 15.5.2.3. 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 contraloría, 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, explosivos.

### 15.6. SEGURIDAD DE LOS EQUIPOS DE CÓMPUTO

#### 15.6.1. 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

	<b>CONTRALORÍA DEPARTAMENTAL DEL META</b> <small>Control fiscal con calidad, independencia y de cara a la comunidad.</small>	
	<b>MANUAL DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN</b>	<b>CÓDIGO: 600.01.101 VERSIÓN 4.0</b>

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 Contraloría Departamental del Meta, 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 mantener un uso adecuado, 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 para identificar la respectiva asignación.

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.

	<b>CONTRALORÍA DEPARTAMENTAL DEL META</b> <small>Control fiscal con calidad, independencia y de cara a la comunidad.</small>	
	MANUAL DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN	CÓDIGO: 600.01.101 VERSIÓN 4.0

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 en apoyo de la oficina de almacén.

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 Contraloría Departamental del Meta.

#### 15.6.2. Mantenimiento de equipos

La Oficina de Gestión TIC, es quien en primeria instancia realiza mantenimiento correctivo, preventivo y adaptativo de la infraestructura tecnológica instalada. En segunda instancia y cuando así lo amerite, la

	<b>CONTRALORÍA DEPARTAMENTAL DEL META</b> <small>Control fiscal con calidad, independencia y de cara a la comunidad.</small>	
	MANUAL DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN	CÓDIGO: 600.01.101 VERSIÓN 4.0

entidad terceriza el servicio de mantenimiento continuo y adecuado de equipos mediante contrato de prestación de este servicio con una empresa idónea que asegura la continua disponibilidad e integridad de estos, de igual manera por cada vigencia se realiza la contratación del mantenimiento preventivo y correctivo de equipos de cómputo.

#### 15.6.3. Seguridad de los equipos fuera de las instalaciones y retiro de activos

Los equipos o software no se retiran de las instalaciones de la Contraloría Departamental del Meta, sin previa autorización del profesional 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.

#### 15.6.4. 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.



	<b>CONTRALORÍA DEPARTAMENTAL DEL META</b> Control fiscal con calidad, independencia y de cara a la comunidad.	
	MANUAL DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN	CÓDIGO: 600.01.101 VERSIÓN 4.0

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.

El área encargada 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.

El día jueves de cada semana se ejecutara tarea de análisis del antivirus después de las 6:00 p.m. para no entorpecer la labor del funcionario, razón por la cual se requiere que dejen los equipos encendidos.

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 sensitivos como usuarios, passwords, direcciones IP entre otros.

#### 15.6.5. 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

	<b>CONTRALORÍA DEPARTAMENTAL DEL META</b> <small>Control fiscal con calidad, independencia y de cara a la comunidad.</small>	
	MANUAL DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN	CÓDIGO: 600.01.101 VERSIÓN 4.0

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 la dependencia de Gestión TIC se ha definido en el procedimiento de generación de copias de seguridad de la información para el desarrollo de las actividades misionales de la Entidad, contenida en medios tecnológicos. Será almacenada periódicamente de forma que se asegure su identificación, protección, integridad y disponibilidad.

Los registros de copias de seguridad deberán almacenarse en una base de datos creada para tal fin. El comité debe definir el procedimiento de copia de seguridad, administración y custodia de los backups.

La Oficina de Gestión en TIC debe proveer las herramientas para que las dependencias puedan consultar la bitácora de la información y registros de copias de seguridad.

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 debe ser ejecutada y mantenida 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.

	<b>CONTRALORÍA DEPARTAMENTAL DEL META</b> Control fiscal con calidad, independencia y de cara a la comunidad.	
	MANUAL DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN	CÓDIGO: 600.01.101 VERSIÓN 4.0

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 en la Entidad DVD, Discos duros externos, 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.
- Se realiza cada seis meses 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 realiza las pruebas de funcionalidad a las copias de seguridad.
- Se hace registro de estas acciones 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.

#### 15.7. 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.

	<b>CONTRALORÍA DEPARTAMENTAL DEL META</b> <small>Control fiscal con calidad, independencia y de cara a la comunidad.</small>	
	MANUAL DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN	CÓDIGO: 600.01.101 VERSIÓN 4.0

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.

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.

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

#### 15.8. USO DE INTERNET

Desde Gestión TIC se proporciona 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.

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.

	<b>CONTRALORÍA DEPARTAMENTAL DEL META</b> <small>Control fiscal con calidad, independencia y de cara a la comunidad.</small>	
	MANUAL DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN	CÓDIGO: 600.01.101 VERSIÓN 4.0

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 encargará 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.

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.

#### 15.9. 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 Gestión TIC, se proporciona a los líderes de proceso aquellos autorizados por el Contralor Departamental, cuentas de correo electrónico institucionales, con el fin de consolidar la imagen institucional y el sentido

	<b>CONTRALORÍA DEPARTAMENTAL DEL META</b> <small>Control fiscal con calidad, independencia y de cara a la comunidad.</small>	
	MANUAL DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN	CÓDIGO: 600.01.101 VERSIÓN 4.0

de pertenencia. Para lo cual, debe dársele un uso racional, responsable, ético y acorde con las funciones desempeñadas.

El usuario 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 institucionales, por tanto, el envío de correo masivo (entiéndase por correo masivo todo aquel que sea ajeno a la Las 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 de Gestión TIC.

#### 15.10. USO DE LOS RECURSOS TECNOLÓGICOS

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

La configuración de software y hardware está también a cargo de la oficina de Gestión TIC. Los funcionarios no se encuentran facultados y autorizados 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.

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

	<b>CONTRALORÍA DEPARTAMENTAL DEL META</b> Control fiscal con calidad, independencia y de cara a la comunidad.	
	MANUAL DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN	CÓDIGO: 600.01.101 VERSIÓN 4.0

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 secretaria general para los llamados pertinentes.

El funcionario que requiera de un software en particular, deberá informar a 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.

#### 15.11. POLÍTICA PARA USO DE DISPOSITIVOS MÓVILES

La Entidad establece las directrices de uso y manejo de dispositivos móviles (teléfonos móviles, teléfonos inteligentes "smart phones"), suministrados y 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 identificados como información pública reservada o información pública clasificada.

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.

Todas las llamadas que se realicen desde las líneas celulares son única y exclusivamente con fines institucionales, quien no se ajuste a esta obligación puede estar inmerso en investigaciones a que haya lugar.

#### 15.12. 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: twitter, facebook, youtube linkedin, blogs, instagram, 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.

	<b>CONTRALORÍA DEPARTAMENTAL DEL META</b> Control fiscal con calidad, independencia y de cara a la comunidad.	
	MANUAL DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN	CÓDIGO: 600.01.101 VERSIÓN 4.0

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.

### 15.13. 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.

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.



	<b>CONTRALORÍA DEPARTAMENTAL DEL META</b> <small>Control fiscal con calidad, independencia y de cara a la comunidad.</small>	
	MANUAL DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN	CÓDIGO: 600.01.101 VERSIÓN 4.0

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.

#### 15.14. CONTROL DE ACCESO

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, 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 Contraloría Departamental del Meta.

##### 15.14.1. Gestión de contraseñas para usuarios

Desde 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", mediante formato N° 600.02.67 de asignación de usuarios.

	<b>CONTRALORÍA DEPARTAMENTAL DEL META</b> <small>Control fiscal con calidad, independencia y de cara a la comunidad.</small>	
	MANUAL DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN	CÓDIGO: 600.01.101 VERSIÓN 4.0

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 tildes. 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.

#### 15.14.2. 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 obligacion 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.

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.

	<b>CONTRALORÍA DEPARTAMENTAL DEL META</b> <small>Control fiscal con calidad, independencia y de cara a la comunidad.</small>	
	MANUAL DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN	CÓDIGO: 600.01.101 VERSIÓN 4.0

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).

#### 15.15. UNIDADES DE DISCO DE CARÁCTER COMPARTIDO (CARPETAS COMPARTIDAS)

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 Contraloría Departamental del Meta, 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 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 que 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

	<b>CONTRALORÍA DEPARTAMENTAL DEL META</b> <small>Control fiscal con calidad, independencia y de cara a la comunidad.</small>	
	MANUAL DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN	CÓDIGO: 600.01.101 VERSIÓN 4.0

existencia de materiales nocivos para la Contraloría Departamental del Meta, con la previa autorización del jefe inmediato y /o del Contralor.

En el momento en que 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.

#### 15.16. SEPARACIÓN DE LAS REDES E IDENTIFICACIÓN DE LOS EQUIPOS

La plataforma tecnológica bajo supervisión de la oficina de Gestión TIC, se encuentra separada de otras redes de datos que prestan servicios a la comunidad en general.

Los equipos que se conecten a la plataforma tecnológica están identificados y autorizados por el área de Gestión TIC, donde se establecen los controles pertinentes.

Gestión TIC documenta procedimientos e implementa controles relacionados con el ruteo de redes, las conexiones informáticas y los flujos de información. Estos controles deben incluir como mínimo verificar positivamente las direcciones de origen y destino así como los dispositivos de red tales como Hubs, Switches, Bridges, Modems o Routers que tenga la Plataforma Tecnológica en la Entidad.

Gestión TIC define las pautas para garantizar la seguridad de los servicios de redes tanto públicos como privados de la Entidad y documenta el riesgo de acceder al sistema operativo de forma insegura y determinar el procedimiento de conexión segura al sistema informático con el fin de reducir el riesgo de accesos no autorizados, así como, el uso de utilitarios de sistema que pueden tener la capacidad de pasar por alto los controles de sistemas y aplicaciones. Su uso debe ser limitado y minuciosamente controlado.

#### 15.17. ADQUISICIÓN DE SISTEMAS DE INFORMACIÓN

La oficina de Gestión TIC adelanta la contratación para la adquisición de productos tecnológicos necesarios para el desarrollo y mantenimiento de la plataforma tecnológica, evaluando las características técnicas,

	<b>CONTRALORÍA DEPARTAMENTAL DEL META</b> <small>Control fiscal con calidad, independencia y de cara a la comunidad.</small>	
	MANUAL DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN	CÓDIGO: 600.01.101 VERSIÓN 4.0

definiendo acuerdos sobre licencias de uso, propiedad de los códigos y derechos de propiedad intelectual.

Antes de poner en funcionamiento las aplicaciones, se realizan pruebas para detectar fallos que puedan atentar contra la seguridad de la información de la Entidad.

La Política aplica a todos los sistemas informáticos, tanto desarrollos propios o de terceros, y a todos los Sistemas Operativos y/o Software de Base que integren cualquiera de los ambientes donde aplique.

El procedimiento para el desarrollo de nuevos sistemas, actualización o mantenimiento debe incluir controles en las diferentes etapas del proceso tales como en el análisis y diseño que permita evaluar el avance del sistema, así como detectar las posibles fallas potenciales de diseño y estructural que deben ser corregidos a tiempo antes de que sea implementado.

Gestión TIC debe garantizar que los desarrollos y actividades de soporte a los sistemas adquiridos o actualizados se lleven a cabo de manera segura con los controles necesarios para permitir el acceso a los archivos solo al personal autorizado.

Toda aplicación o desarrollo que adquiera la Entidad de un tercero debe tener un único responsable, el cual es sugerido por Gestión TIC y designado formalmente.

Las empresas desarrolladoras del nuevo sistema así como los programadores o analistas de desarrollo y mantenimiento de aplicaciones deben trabajar en un esquema de pruebas y no acceder a los ambientes de producción. Las pruebas de los sistemas se deben ser efectuadas en conjunto con los propietarios de la información y Gestión TIC.

## 15.18. GESTIÓN DE LOS INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN

### 15.18.1. Reporte de Eventos o Incidentes

Es deber de todos los funcionarios, reportar al área de Gestión TIC toda situación que genere un evento o incidente de seguridad que atente

	<b>CONTRALORÍA DEPARTAMENTAL DEL META</b> <small>Control fiscal con calidad, independencia y de cara a la comunidad.</small>	
	<b>MANUAL DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN</b>	<b>CÓDIGO: 600.01.101 VERSIÓN 4.0</b>

contra el normal desarrollo de las actividades de la Entidad, allí se evaluará la situación y dará el tratamiento requerido.

Desde la secretaría general se reportará las situaciones ante las autoridades competentes cuando haya implicaciones legales ya sean penales o civiles.

#### 15.18.2. Manejo de Incidentes de Seguridad

Los incidentes de seguridad deben ser registrados en documento físico o digital indicando el tipo de incidencia, fecha y hora de la incidencia, fecha de reporte, persona que realiza el reporte, persona a quien comunica la incidencia, descripción detallada de la incidencia, efectos y posibles consecuencias, acciones adoptadas para subsanar las consecuencias.

El profesional de Gestión TIC será el responsable de evaluar el incidente o designar el personal idóneo para realizar estas funciones. Para el desarrollo de estas labores puede requerirse el apoyo de otras dependencias o Entidades externas.

Una situación donde se presente un incidente o evento de seguridad permite identificar oportunidades de mejora y aprender de estos fallos.

#### 15.19. GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO

La oficina de Gestión TIC contará con un plan de continuidad de las actividades más críticas, que permita reanudar sus actividades ante la presencia de interrupciones prolongadas en la prestación de los servicios, ya sea por fallos o desastres naturales.

De acuerdo con el análisis de riesgos, se identificarán los eventos con alto impacto en la dependencia, probabilidad de ocurrencia y sus consecuencias. Para implementar planes que permitan reanudar las actividades.

Los planes deberán estar documentados, probados, actualizados de acuerdo con las características de la Entidad y deben ser de conocimiento de los funcionarios, de tal manera que sean conscientes de sus roles y responsabilidades.

	<b>CONTRALORÍA DEPARTAMENTAL DEL META</b> <small>Control fiscal con calidad, independencia y de cara a la comunidad.</small>	
	MANUAL DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN	CÓDIGO: 600.01.101 VERSIÓN 4.0

## 16. CUMPLIMIENTO DE NORMAS POLÍTICAS DE SEGURIDAD DE INFORMACIÓN

La entidad debe cumplir con el marco normativo colombiano y para ello la dependencia identifica los requerimientos normativos aplicables y contractuales pertinentes para los sistemas de información.

La dependencia propenderá por el cumplimiento de los derechos de propiedad intelectual y sobre el uso de productos de software patentados, y realizará revisiones periódicas a fin de que se cumpla esta reglamentación.

Hace parte de los derechos de propiedad Intelectual, la información que se genere como propia del conocimiento de la entidad, códigos fuente.

Gestión TIC es el área encargada de velar por la correcta aplicación y control de las licencias de productos de software y hardware, así como el número de usuarios permitidos. Está prohibido el uso de productos ilegales o sin licencia.

## 17. GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO

La oficina de Gestión TIC contará con un plan de continuidad de las actividades más críticas, que permita reanudar sus actividades ante la presencia de interrupciones prolongadas en la prestación de los servicios, ya sea por fallos o desastres naturales.

De acuerdo con el análisis de riesgos, se identificarán los eventos con alto impacto en la dependencia, probabilidad de ocurrencia y sus consecuencias. Para implementar planes que permitan reanudar las actividades.

Los planes deberán estar documentados, probados, actualizados de acuerdo con las características de la empresa y deben ser de conocimiento de los empleados, de tal manera que sean conscientes de sus roles y responsabilidades.

## 18. SANCIONES

El Comité Institucional de Gestión y desempeño evaluará las violaciones a las políticas de seguridad de la información, lo que puede dar lugar a las

	<b>CONTRALORÍA DEPARTAMENTAL DEL META</b> <small>Control fiscal con calidad, independencia y de cara a la comunidad.</small>	
	<b>MANUAL DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN</b>	<b>CÓDIGO: 600.01.101</b> <b>VERSIÓN 4.0</b>

sanciones establecidas en el Código Disciplinario Único (Ley 734 de 2002) para los funcionarios públicos y la legislación vigente establecida en la Constitución Política de la República de Colombia: Decreto 2364 de noviembre 22 de 2012, Ley 1266 de 2008, Ley estatutaria 1581 de octubre 17 de 2012, Ley 1273 de 2009, Ley 527 de 1999, así como los decretos a que hubiese lugar para las terceras partes. El Comité notificará a la Oficina de Control Disciplinario o a las autoridades competentes, para que estos incidentes sigan el conducto regular y el debido proceso, según sea el caso.

## 19.CUMPLIMIENTO

La entidad debe cumplir con el marco normativo colombiano y para ello la dependencia identifica los requerimientos normativos aplicables y contractuales pertinentes para los sistemas de información.

La dependencia propenderá por el cumplimiento de los derechos de propiedad intelectual y sobre el uso de productos de software patentados, y realizará revisiones periódicas a fin de que se cumpla esta reglamentación.

Hace parte de los derechos de propiedad Intelectual, la información que se genere como propia del conocimiento de la entidad, códigos fuente.

El profesional universitario de sistemas es el encargado de velar por la correcta aplicación y control de las licencias de productos de software y hardware, así como el número de usuarios permitidos. Está prohibido el uso de productos ilegales o sin licencia.

La dependencia tiene definidos acuerdos contractuales con los proveedores que realizan arrendamiento de software, donde se señalan los acuerdos de protección de la propiedad intelectual.

Es deber de todos los funcionarios velar por el buen manejo y protección de los datos e información personal, de la cual puedan tener conocimiento por el ejercicio de sus funciones.



	<b>CONTRALORÍA DEPARTAMENTAL DEL META</b> Control fiscal con calidad, independencia y de cara a la comunidad.	
	MANUAL DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN	CÓDIGO: 600.01.101 VERSIÓN 4.0

## 20. CRONOGRAMA

La Entidad define y mantiene un cronograma de actividades en cumplimiento a los propósitos internos de seguridad y privacidad de la información basada en el ciclo de operación MSPI.

## 21. SEGUIMIENTO Y EVALUACIÓN

Al finalizar cada etapa se realizará una reunión con el Comité Institucional de Gestión y Desempeño para presentar el informe del avance del manual y de esta manera evaluar todos los pasos que se han ido realizando.

## 22. MARCO LEGAL

- Constitución Política de Colombia 1991. Artículo 15. Reconoce como Derecho Fundamental el Habeas Data.
- Artículo 20. Libertad de Información.
- Código Penal Colombiano - Decreto 599 de 2000
- Ley 906 de 2004, Código de Procedimiento Penal.
- Ley 87 de 1993, por la cual se dictan Normas para el ejercicio de control interno en las entidades y organismos del Estado, y demás normas que la modifiquen.
- Ley 734 de 2002, del Congreso de la República de Colombia, Código Disciplinario Único.
- Ley 23 de 1982 de Propiedad Intelectual - Derechos de Autor.
- Ley 594 de 2000 - Ley General de Archivos.
- Ley 80 de 1993, Ley 1150 de 2007 y decretos reglamentarios.
- 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.
- Directiva presidencial 02 del año 2000, Presidencia de la República de Colombia, Gobierno en línea.
- Ley 1032 de 2006, por el cual se dictan disposiciones generales del Habeas Data y se regula el manejo de la información contenida en base de datos personales.
- Ley 1266 de 2007, por la cual se dictan disposiciones generales del Habeas Data y se regula el manejo de la información contenida en base de datos personales.
- Ley 1273 de 2009, "Delitos Informáticos" protección de la información y los datos.

	<b>CONTRALORÍA DEPARTAMENTAL DEL META</b> Control fiscal con calidad, independencia y de cara a la comunidad.	
	MANUAL DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN	CÓDIGO: 600.01.101 VERSIÓN 4.0

- Ley 1437 de 2011, "Código de procedimiento administrativo y de lo contencioso administrativo".
- Ley 1581 de 2012, "Protección de Datos personales".
- Decreto 2609 de 2012, por la cual se reglamenta la ley 594 de 200 y ley 1437 de 2011.
- Decreto 1377 de 2013, por la cual se reglamenta la ley 1581 de 2012.
- Ley 1712 de 2014, "De transparencia y del derecho de acceso a la información pública nacional".
- Ley 962 de 2005. "Simplificación y Racionalización de Trámite. Atributos de seguridad en la Información electrónica de entidades públicas;"
- Ley 1150 de 2007. "Seguridad de la información electrónica en contratación en línea"
- Ley 1341 de 2009. "Tecnologías de la Información y aplicación de seguridad".
- Decreto 2952 de 2010. "Por el cual se reglamentan los artículos 12 y 13 de la Ley 1266 de 2008".
- Decreto 886 de 2014. "Por el cual se reglamenta el artículo 25 de la Ley 1581 de 2012".
- Decreto 1083 de 2015. "Por el cual se reglamenta el artículo 25 de la Ley 1581 de 2012".
- CONPES 3701 de 2011 Lineamientos de Política para Ciberseguridad y Ciberdefensa.
- CONPES 3854 de 2016 Política Nacional de Seguridad digital.

### 23. DOCUMENTOS RELACIONADOS

- Política de uso y tratamiento de datos
- Política de Administración de riesgos de proceso, corrupción y seguridad digital
- Política de seguridad web (digital)

### 24. ANEXOS

Cronograma del Sistema de Gestión de Seguridad de la Información SGSI 2020