POLÍTICAS
Para la Administración y Uso de las TICS

María Liliana Giraldo González
Auxiliar Administrativa Grado 09
Coordinación de Sistemas CMP

Contraloría Municipal de Pereira

1. INTRODUCCIÓN

El presente documento contiene información relevante, concerniente a los alcances y reglamentaciones para la administración de las TIC [Tecnologías de la Información y las Comunicaciones] en la Contraloría Municipal de Pereira.

Cobra relevancia el uso debido de la tecnología de la información y las comunicaciones expedición de diferente normatividad que apoya el uso del documento digital por parte del estado colombiano**(DECRETO 2106 DE 2019 "Por el cual se dictan normas para simplificar, suprimir y reformar trámites, procesos y procedimientos innecesarios existentes en la administración pública"),** por eso este es el documento oficial que reglamenta el debido uso de todos los elementos que conforman la red institucional de la Contraloría Municipal de Pereira y que da cumplimiento a la normatividad Colombiana en términos de Seguridad de la Información e Informática , Cultura de Cero Papel y todas las regulaciones establecidas por el Ministerio de la Tecnología de la Información y las Comunicaciones de Colombia, Ley 23 de 1982, Ley 44 de 1993, Ley 527 de 1999, Ley 1581 de 2012, Ley 1672 de 2013, Ley 1712 de 2014, Decreto 1078 de 2015, entre otras.

Es el Instrumento que define los controles para el buen uso de la tecnología propiedad de la CMP, estableciendo una serie de instrucciones y restricciones sobre los recursos informáticos, con el fin de prevenir la ocurrencia de riesgos ; también la de entrar en sintonía con la constante evolución del gobierno electrónico en Colombia, donde ha dejado clara la importancia de las TIC para mejorar la gestión en las entidades públicas, así como los servicios que el Estado presta al ciudadano, no obstante, ahora surge una nueva realidad en donde la política de Gobierno Digital no solamente mejora los procesos y los servicios existentes, sino que permite llevar a cabo procesos de transformación digital que modifican la forma en que tradicionalmente el Estado se ha venido relacionando con el ciudadano.

2. ANTECEDENTES

El área de Tecnologías de la Información de la Contraloría Municipal de Pereira consciente de la necesidad de reglamentar y regular el uso adecuado de los recursos informáticos en nuestra Organización, con base en los lineamientos del Ministerio de las TIC, plantea la implementación de procesos de seguimiento y control en los procesos de:

1. **Seguridad de la infraestructura tecnológica**
2. **Buenas prácticas para el uso de los recursos informáticos**

3. Ley de protección de datos personales
4. Uso adecuado de los medios de comunicación digital
5. Documento digital

Estos lineamientos están sujetos a cambios y transformaciones por parte del área de tecnologías de la Información de acuerdo con los requerimientos y necesidades que se presenten en la evolución tecnológica de nuestra Organización.

Como equipo de trabajo estamos comprometidos con el cumplimiento de estas políticas, con el apoyo de la alta dirección en cabeza del **Contralor Municipal**, estas en su debido momento se socializarán, para un mejor entendimiento, en los diferentes medios disponibles cómo correo electrónico, intranet, cartelera, mesas de conversación, entre otros), buscando generar un compromiso colectivo.

3. PLANTEAMIENTO DEL PROBLEMA

Este manual se ha elaborado con el propósito de regular el uso de los recursos informáticos de la Organización; planteando la revisión permanente para actualizar sus contenidos con base en la norma y mantener los lineamientos en las nuevas tendencias, y alcanzar un uso eficiente y racional de los servicios que brinda la organización para sus usuarios y clientes.

La **Contraloría Municipal de Pereira** depende en alto grado de los recursos tecnológicos y de la información procesada en ellos, razón por la cual requiere de adecuadas medidas de seguridad, prevención y regularización, necesarias para proteger la integridad, confidencialidad y disponibilidad de la información y recursos tecnológicos.

4. JUSTIFICACIÓN

Todos los procesos institucionales involucran niveles de aseguramiento de la información consistente en proteger los recursos de la Organización, buscando su adecuada administración, manejo, seguimiento y control en aras de prevenir riesgos que afecten la oportunidad, disponibilidad, confiabilidad de la información e integridad de sus registros.
Es responsabilidad de las entidades gubernamentales, en cabeza del alta de dirección y de todos aquellos funcionarios involucrados en el manejo y administración de los recursos tecnológicos, incluirse en estos principios de uso.

5. OBJETIVO GENERAL

Generar políticas que permitan establecer procedimientos de optimización, aseguramiento, seguimiento y control sobre los recursos informáticos de la Organización, manteniendo altos estándares de calidad en los servicios que se prestan.

5.1 OBJETIVOS ESPECÍFICOS

- Establecer e implementar políticas para mantener el uso adecuado de los recursos informáticos de la Organización dentro y fuera de ella.
- Optimizar los recursos tecnológicos e informáticos
- Garantizar la integridad, confidencialidad y disponibilidad de la información.
- Asegurar la calidad de la información, minimizando los indicadores de riesgos de los recursos informáticos inclusive en la realización de tele-trabajo.
- Socializar y sensibilizar a los funcionarios de la Organización sobre los alcances y responsabilidades que se deben acoger como buenas prácticas en la creación, uso de la información y de los recursos informáticos dentro y fuera de la entidad.
- Reglamentar el uso adecuado del software mediante parámetros establecidos para su licenciamiento, evitando las sanciones que puede acarrear el no cumplimiento a las leyes sobre derechos de autor.
- Establecer mecanismos de control y compromisos en el uso de las TI, donde quiera que se ubique el puesto de trabajo, reconociendo siempre la responsabilidad de proteger la información que es propiedad de la Contraloría Municipal de Pereira, guardando siempre la debida confidencialidad.

6. MARCO LEGAL VIGENTE

La Contraloría Municipal de Pereira acorde con los lineamientos que sobre la materia ha expedido el gobierno nacional se somete a la reglamentación expedida en las siguientes normas:

a. Constitución Política de Colombia artículos 23 - "*Por el cual se solicitan derechos de petición a organizaciones gubernamentales*".
b. Constitución Política de Colombia artículos 61 - "*El Estado protegerá la propiedad intelectual por el tiempo y mediante las formalidades que establezca la ley*".
c. Constitución Política de Colombia artículos 74 - "*Todas las personas tienen derecho a acceder a los documentos públicos salvo los casos que establezca la ley*".
d. Ley 44 de 1993 por la cual se modifica la Ley 23 de 1982 - "*Disposiciones legales para la protección de datos y derechos de autor*".

e. Ley 1437 del 18 de enero de 2011 -" Por *medio del cual se expide el Código de Procedimiento Administrativo y de lo Contencioso Administrativo*".
f. Decreto 1377 de 27 junio de 2013 Revisar.
g. Directiva presidencial Nº 004 - "*Por medio del cual se establecen lineamientos de la política de cero papeles en la Administración Pública*".
h. Decreto 2578 de diciembre 13 de 2012 - *"Por medio del cual se establece el Sistema Nacional de Archivos y se dictan otras disposiciones relativas a la administración de los Archivos del Estado"*.
i. Ley 1712 del 6 de marzo 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*".
j. Decreto 943 de 2014 - "*por el cual se establece el modelo estándar de control interno*". Revisar decreto
k. Ley 1952 del 28 enero 2019 - "Por medio del cual se establece el c*ódigo único disciplinario*"
l. Decreto Ley Anti-trámites 2106 de 2019 - "*Por el cual se dictan normas para suprimir o reformar regulaciones, procedimientos y trámites innecesarios existentes en la Administración Pública*".
m. Código de Penal Colombiano artículos 270 - "*Violación de los derechos morales de autor*".
n. Código de Penal Colombiano artículos 271 - "*Violación de los derechos patrimoniales de autor y derechos conexos*".
o. Código de Penal Colombiano artículos 272 - "*Violación a los mecanismos de protección de los derechos de autor y derechos conexos, y otras defraudaciones.*
p. Decreto 1078 de 2015 - "*Por medio del cual se establecen los lineamientos generales de la Estrategia de Gobierno en Línea" Políticas de Seguridad Informática – Gobierno en Línea; Políticas y Estándares para Publicar Información del Estado en Internet"*. Cambio 1082 del 2018. Política de gobierno digital.
q. Resolución 2256/2020 → Que adopta la Política de Seguridad y Privacidad de la Información. Derogan Resoluciones 2999/2008 y 1124/2020.
r. Resolución 924/2020 → Por la cual se actualiza la Política de Tratamiento de Datos Personales del Ministerio TIC.
s. Resolución 1519 de 2020 "Por la cual se definen los estándares y directrices para publicar la información señalada en la Ley 1712 del 2014 y se definen los requisitos materia de acceso a la información pública, accesibilidad web, seguridad digital, y datos abiertos"
t. Decreto 1008de 2018 "Por el cual se establecen los lineamientos generales de la política de Gobierno Digital y se subroga el capítulo 1 del título 9 de la parte 2 del libro 2 del Decreto 1078 de 2015, Decreto Único Reglamentario del sector de Tecnologías de la Información y las Comunicaciones"

u. Decreto 2109 de 2019, "Por el cual se dictan normas para simplificar, suprimir y reformar trámites, procesos y procedimientos innecesarios existentes en la administración pública"
v. Directiva Presidencia No. 04 de 2012 "Eficiencia Administrativa y Lineamientos de la Política Cero Papel en la Administración Pública"
w. Ley 1437 de 2011 "Por la cual se expide el Código de Procedimiento Administrativo y de lo Contenciosos Administrativo" artículo 55°
x. 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"
y. Decreto Ley 2006 de 2019 "Llegó la hora del Cero Papel porque toda comunicación con el Estado será Digital"
z. Ley 1952 de 2019 "Por medio de la cual se establece el Código Único Disciplinario"
aa. Resolución 1519 del 24 de agosto del 2020 "Por la cual se definen los estándares y directrices para publicar la información señalada en la Ley 1712 del 2014 y se definen los requisitos materia de acceso a la información pública, accesibilidad web, seguridad digital, y datos abiertos".

7. USO DE LOS RECURSOS TECNOLÓGICOS

7.1 LA SEGURIDAD DE LA INFRAESTRUCTURA TECNOLÓGICA

Para efectos del presente documento, la Coordinación de Sistemas, en lo sucesivo se denominará Área de Tecnologías de la Información CMP. TIC se refiere a Tecnología de la información y las Comunicaciones que corresponde a todos los dispositivos y recursos que conforman el ecosistema informático sean hardware o software y el presente documento se denominará "Guía para Administración de las TIC".

En términos de recursos informáticos sé definen dos tipos de seguridad:
a) Seguridad Física [hardware], que se constituye en la protección de los elementos tangibles que conforman la tecnología de la información (TI).
b) Seguridad Lógica [software], que corresponde a los datos y aplicaciones.

Se entiende por equipo de cómputo el recurso electrónico - lógico que facilita las labores de procesamiento, almacenamiento de datos y es utilizado como herramienta de productividad; por su dimensión, capacidad y tamaño, estos pueden ser: computadoras de gran escala, minicomputadoras, servidores de red, estaciones de trabajo, portátiles y terminales, incluyendo sus periféricos o dispositivos anexos.

Todas las instrucciones impartidas en el presente documento deben ser de estricto cumplimiento por los funcionarios y contratistas de la organización. Con el propósito de proteger los recursos informáticos de la entidad y buscando su adecuada administración y prevención ante posibles riesgos que los afecten, esta guía propenderá por la optimización del control y administración de los equipos computacionales en la organización. A su vez, ayudará al área de Tecnologías de la Información CMP, a definir los procedimientos relacionados.

7.2 DEL INVENTARIO DE HARDWARE

El inventario tecnológico de los equipos y dispositivos que hacen parte de los recursos informáticos [Software - Hardware] de la organización, es un procedimiento de seguimiento y control que debe ser liderado y auditado por él área de Tecnologías de la Información CMP.

El auxiliar administrativo de inventarios es el funcionario con rol de auditor del proceso de inventario tecnológico que involucra procedimientos tendientes a salvaguardar la infraestructura tecnológica de la organización, además deberá coordinar con el área de Tecnologías de la Información CMP el alcance de las actividades de los recursos informáticos adquiridos, asignación de código de inventario de activos fijos cedidos, en comodato o arrendados, deberá mantener un registro actualizado de reportes, prestamos, incidencias y novedades sobre estos elementos que deberá reportar al superior inmediato.

El funcionario responsable de inventarios deberá crear una carpeta detallada individual, digital con los registros de las mejoras realizadas a los equipos que hacen parte de los recursos informáticos CMP y que deberá ser auditada cada seis [6] meses junto con funcionarios del área de tecnologías de la información.

El propósito es verificar la existencia, estado, y responsable del bien de acuerdo a los registros que contengan los documentos que reposan digitalmente en el área de Inventarios como los registrados en el área de TIC que corresponde a los siguientes formatos de control:

ITEM	NOMBRE DEL FORMATO	DESCRIPCIÓN
1	FORM INV-TI	Formato Control de Inventario Tecnológico
2	FORM INV-EQACT-RED	Formato Control de Inventario de Equipos Activos de Red Puntos y Puertos
3	FORM CRON-MANT-PREV	Formato Programación de Mantenimientos Preventivos Equipos Tecnológicos

4	**FORM PREST-BIENES-TI**	**Formato para préstamo de bienes tecnológicos (Para el área de inventarios)**

[Tabla 1. Documentos de control de equipos TIC]

La información contenida deberá estar actualizada permanentemente para efectos de auditorías externas en infraestructura tecnológica.

7.3 DE LA PROTECCIÓN DE LOS BIENES TECNOLÓGICOS

Referente a la protección de los recursos y bienes tecnológicos CMP, es deber del área de Tecnologías de la Información establecer cronogramas de auditoría para el seguimiento y control de software, además del hardware con el fin de mantener la trazabilidad de la información organizada y debidamente documentada. Para ello tanto el responsable de activos fijos como el responsable de TI deberán realizar seguimiento a los elementos que se encuentran registrados en el software ERP y verificar de forma física cada uno de ellos.

El diligenciamiento oportuno de los formatos será relevante para la Compañía aseguradora, la cual deberá establecer un protocolo de responsabilidad y respuesta a la Contraloría Municipal de Pereira, para los casos de:

a. Préstamo o traslado de recursos informáticos fuera de las instalaciones CMP.
b. Reposición de equipos por daños u otros según sea el alcance de la póliza.

7.4 DEL INVENTARIO DE SOFTWARE CMP

Por “SOFTWARE” se entiende al soporte lógico de un sistema informático que facilita las labores de procesamiento de datos, es utilizado como herramienta de productividad que hace posibles tareas específicas.

Los paquetes se definen cómo el grupo de componentes lógicos rotulados orientados al manejo integral de soluciones de usuario, sistemas aplicativos o de requerimiento específico.

El Área de Tecnologías de la Información CMP, es la encargada de mantener actualizada la relación del software, las bases de datos, aplicaciones e información de la entidad, procurando la debida custodia de las licencias, además de mantener un registro actualizado del mismo.

El funcionario responsable del inventario de los recursos informáticos CMP y el técnico operativo de sistemas tiene dentro de sus alcances el compromiso y responsabilidad de mantener un registro detallado y actualizado del software de la entidad.

Entiéndase también que existen licencias contenidas en los equipos adquiridos, para tal efecto se tendrá el registro de estas con la debida observación.

El software contratado con terceros para soporte de procesos misionales o los desarrollados por funcionarios CMP, se incorporará al inventario de la entidad como un elemento devolutivo en los términos establecidos por el tipo de licencia y adicionalmente será registrado patrimonialmente a nombre de la Contraloría Municipal de Pereira, de acuerdo con las leyes sobre derechos de autor que rigen en la República de Colombia. Si el software corresponde a licencia de uso, se mantendrá copia del contrato y se registrará la observación.

Una vez se adquiera por parte de la Contraloría Municipal de Pereira un bien que corresponda a la descripción de software, será recibido por el funcionario responsable de la Oficina de Tecnologías de la Información CMP, quien se encargará hacer una verificación y validación de las especificaciones técnicas del software adquiridlo con las especificaciones solicitadas en la orden de compra del mismo y posteriormente realizar su registro en el formato de inventario tecnológico, desarrollado para este fin y trasladará la información de la adquisición al funcionario encargado de los inventarios de la entidad para su registro.

La Oficina de Tecnologías de la Información CMP, mantendrá un registro actualizado de control y uso del software adquirido por la entidad, el cual deberá contener información de trazabilidad de:

a) Tipo de medios magnéticos.
b) Versiones.
c) Modificaciones.
d) Copias de respaldo.
e) Manuales de técnicos y de usuario.
f) Parches de actualizaciones.
g) Tipo de licencia del software [suscripción, perpetua, GNU, etc.] o aplicaciones producto de este.

Nota:
Todo software que sea adquirido Contraloría Municipal de Pereira estará debidamente registrado y controlado para su uso exclusivo; no se aprueba su uso a funcionarios o terceros sin la debida autorización. Esto último se hará extensivo a productos,

aplicaciones o servicios derivados del mismo. El no cumplimiento a este alcance será causal de procesos disciplinarios por parte de la entidad.

7.5 DE LA ASIGNACIÓN DE RECURSOS TECNOLÓGICOS A FUNCIONARIOS CMP

Los recursos informáticos [Software - Hardware], serán asignados a los funcionarios por un representante del área de Tecnologías de la Información CMP mediante correo institucional y será reportado al responsable de inventarios para lo de su competencia, además del acuerdo de confidencialidad y responsabilidad que incluye los alcances que deberá mantener el funcionario con el bien CMP asignado, especificando claramente las características técnicas, estado del elemento, valor y alcances. Dichos recursos tecnológicos serán devueltos en iguales condiciones por el funcionamiento al momento de terminación del contrato. La asignación de elementos tecnológicos, usuarios y contraseñas de acceso a servicios y software, se realiza previa instrucción del superior inmediato.

7.6 DE LOS SERVIDORES

Los recursos informáticos con configuración de servidores de red, se encargan de administrar y controlar los accesos a los equipos que conforman la red de área local (LAN), al igual que restringir y proteger el acceso al servicio de Internet y resguardar las copias de seguridad, manejar los servicios que se habiliten con algún fin.

La configuración de red LAN, exige la validación del usuario con nombre de la máquina y contraseña dirección IP fija que configuran los funcionarios de la Oficina de Tecnologías de la Información CMP. Se validan en el servidor para ingresar a los servicios de Internet, intranet, correo, impresión, unidad de almacenamiento en red (NAS), servidor de archivos y acceso a información de las bases de datos.

La CMP cuenta con tres servidores físicos y a su vez estos se han configurado con máquinas virtuales para multiplicar las capacidades de procesamiento y prestar mejores servicios de red; el primer servidor **IBM** contiene por el momento el servidor de Pfsense que controla el Cortafuegos, seguridad perimetral y de navegación en internet además de tener configurada la **VPN** o red privada virtual, que permite conectar de forma segura a las máquinas de la red corporativa CMP con un equipo externo, a través de otro servidor, obteniendo también otra IP diferente a la asignada en la CMP de forma que se genera un canal seguro con el servicio de internet.

El segundo servidor **HP** contiene las máquinas virtuales de MAXCONTROL (CMP-40), base de datos PosGres antigua ERP NES, y Apolo Contabilidad; también contiene el Servidor de

Mensajería Instantánea Openfire Spark y el Servidor virtual de YEMINUS WEB que maneja el módulo de tesorería (CMP-29).
El tercer servidor HP, contiene el servidor de archivos contingencia (anterior a la NAS), Servidor FTP, el servidor del sistema de información ERP YEMINUS y servidor de la base de datos Oracle.

El dispositivo de Almacenamiento en Red NAS es el servidor de archivos en donde se almacena la copia de seguridad de todos los equipos que componen la red corporativa de la entidad, además, es el repositorio de la Data de Yeminus software y copia de los correos institucionales de la entidad. Esta copia se realiza en tiempo real, siempre y cuando el usuario de la estación de trabajo, almacene la información en las carpetas que se comparten con este dispositivo.

Cada máquina se reconocerá en la red con las siglas del dominio que es **CMP** y número de la máquina.

Cada usuario de los servicios de red CMP, se reconocerá con la letra inicial del primer nombre y apellido completo. Ejemplo: **aruiz**, corresponde al usuario Adolfo Ruiz).

Los servicios que requieran identificación de usuario utilizarán este mismo estándar ejemplo correo electrónico: **aruiz@contraloriapereira.gov.co**

El administrador de la red entregará a cada funcionario las credenciales de acceso a la red LAN CMP que comprende “el nombre de usuario y contraseña” para acceder a cada estación de trabajo y diferentes servicios que presta el área de TI.
El usuario es responsable de sus contraseñas; estas son personales e intransferibles. Toda responsabilidad derivada del uso de una contraseña de usuario distinta a la propia recaerá sobre aquel usuario propietario del código utilizado indebidamente.
Los permisos o accesos a los servidores y usuarios de red son concedidos por el administrador de la red, de acuerdo con criterios establecidos en el numeral 6, SEGURIDAD DE LA INFORMACIÓN Y CONFIDENCIALIDAD DE LA INFORMACIÓN

La red eléctrica está respaldada por un sistema ininterrumpido de poder (UPS), que soporte suficientemente los equipos, con la necesaria autonomía para evitar que el sistema sea apagado de manera abrupta y se pierda información. Todos los equipos de cómputo deberán estar conectados a este sistema regulado que es plenamente identificado con toma de color naranja. Este servicio de respaldo es suministrado y administrado por la Secretaría de las TIC del Municipio de Pereira.

La Contraloría Municipal de Pereira podrá acceder a servicios en la nube (o de servidores remotos) donde quede plenamente establecido que el proveedor garantice:

- Alta disponibilidad del servicio y demostración de los medios que lo garantizan.
- Sistemas probados de contingencia efectiva debidamente documentados con puntos de recuperación (RPO) y tiempo de recuperación (RTO).
- Niveles de seguridad explícitamente enunciados.
- Confidencialidad, integridad, integralidad de información que va a entregar la empresa prestadora del servicio.
- Los medios de rescate de la información en caso del que el proveedor sufra una catástrofe.
- Tiempo de respuesta en el soporte.
- Periodicidad de las copias de respaldo.
- Especificación de costos incluidos y costos adicionales.

7.7 DE LAS RESPONSABILIDADES DE LA OFICINA TI CMP

La Oficina de Tecnologías de información CMP, tiene dentro de sus responsabilidades y alcances lo siguiente:

a) Será responsable de la administración, seguridad, calidad, seguimiento y control de toda la información, además de todos los recursos informáticos de la entidad [Software - Hardware] y de los productos y servicios derivados de los mismos.
b) Brindará la información e inducción adecuada a los funcionarios sobre las responsabilidades y manejo del recurso informático entregado, buscando garantizar el buen uso y desempeño de actividades concernientes a su objeto de contrato y cargo. Lo anterior contenido en el manual de funciones y responsabilidades del funcionario.
c) Será responsable de la mesa de ayuda a usuarios, encargada del servicio de soporte técnico [Software - Hardware] al recurso tecnológico y al recurso humano de la entidad, buscando preservar el óptimo funcionamiento y mejoramiento continuo de los productos y servicios CMP.
d) Deberá garantizar que los recursos tecnológicos cómo [Estaciones de trabajo, equipos portátiles, periféricos y consumibles] sean de uso exclusivo de los funcionarios y con propósitos relacionados con la misión de la entidad.
e) Procurará el aseguramiento que los recursos informáticos, los aplicativos Institucionales, los sistemas de Información, las redes de datos y conexiones a Internet no sean utilizados para propósitos distintos de los previstos en la misión de la Contraloría Municipal de Pereira; por lo tanto, se prohíbe cualquier uso con fines comerciales, políticos o personales de estos componentes.

f) Reportará al superior inmediato el uso indebido de los recursos informáticos tales como: Información personal [Documentos, fotos, videos o música] contenida en los equipos de cómputo sin previa autorización, licencia que atente contra los derechos de autor.

g) Garantizará que en ninguna circunstancia los funcionarios o personas ajenas a la entidad, abrirán los diferentes componentes de los recursos tecnológicos de la entidad como [CPU, monitor, unidades de disco, teclados mouse y periféricos], salvo previa autorización y supervisión de un funcionario de la Oficina de Tecnologías de la Información CMP.

h) Verificará y Validará que las estaciones de trabajo y periféricos se mantengan limpias y protegidas de partículas de polvo, además no se deberá alterar su configuración para evitar detrimento de estas e incoherencia en el número de partes e inventario que las componen.

i) Estará atento a recibir y atender de forma adecuada y oportuna los reportes escritos por parte de los funcionarios que evidencien fallas, incidencias, cambio de partes, pérdidas que estén relacionadas con el óptimo funcionamiento de los equipos de cómputo y reportará oportunamente al superior inmediato cualquier anomalía o excepción evidenciada.

j) Monitoreará los niveles de operación de los servidores de información, redes de datos, conectividad con los equipos de cómputo, estado de las actualizaciones, servicio de antivirus, estado de las copias de seguridad y recursos informáticos.

k) Regulará y controlará todo proceso y procedimiento concerniente a recursos informáticos y sistemas de información

l) Garantizará la calidad de la información en los procedimientos referentes a creación, almacenamiento y restauración de copias de seguridad

m) Socializará permanentemente con los funcionarios CMP las actividades de mejora en cuestiones de uso de tecnología, seguridad informática, seguridad de la información y políticas para la administración de la TI al interior de la entidad.

7.8 EL ASEGURAMIENTO DE LOS BIENES

Todos los componentes de la red deben estar asegurados con pólizas de seguros para lo
cual se deben tener en cuenta los siguientes parámetros:

- La vigencia de la póliza.
- El tipo de riesgo de la póliza.
- Cobertura de hardware, software y datos productos de estos. Pérdida de datos o daños de programas por fallas mecánicas, fallas eléctricas o ataques cibernéticos.
- Cobertura por actos deshonestos o fraudes por parte de empleados o intrusos Cobertura para daños por virus a los programas, datos o al hardware Deducciones

sobre el costo de adquisición de los elementos y límites de pérdidas sobre equipos, software, programas de aplicación y datos con alcance de cubrimiento para los valores de actualización de los recursos informáticos.

- Cubrimiento de costos por tiempo muerto.
- Cubrimiento de gastos en que se incurre para reducir pérdidas posteriores o reducir daños luego de un desastre.
- Descuentos por la implementación de sistemas preventivos, protección especial para equipos portátiles.
- Se deben incluir en las pólizas todos los equipos entregados en comodato a la Contraloría Municipal de Pereira.
- Se debe informar a la aseguradora toda novedad que se presente en la adquisición de hardware y software.
- En todo caso el Asesor de Control interno será la persona encargada de programar las auditorías de verificación apoyado por los funcionarios de la Oficina de Tecnologías de la Información CMP.

8. DE LAS CONDICIONES GENERALES PARA EL USO DE LOS RECURSOS TECNOLÓGICOS

Como funcionarios de la Contraloría Municipal de Pereira se tiene el compromiso de vigilar y regular uso de los recursos informáticos para el cumplimiento de la misión Institucional, razón por la cual se informa a los funcionarios el desarrollo de los siguientes procedimientos como buenas prácticas institucionales:

a) Está prohibido la ingesta de alimentos o bebidas en las mesas donde haya equipos de cómputo o periféricos que sean propensos a un accidente que genere daño o detrimento.
b) Está prohibido el consumo de cigarrillo u otros productos que generen humo en las mesas o lugares donde se encuentren equipos de cómputo, dado que el humo genera corrosión en los componentes electrónicos internos altamente sensibles a deterioro y a ser inflamables.
c) Está prohibido conectar en las tomas de energía regulados por UPS [color naranja] radios, ventiladores, móviles, extensiones eléctricas, periféricos, entre otros, dado que estos elementos pueden generar corrientes de retorno y campos magnéticos que afectan los sistemas de energía ininterrumpida UPS.
d) Está prohibido conectar a un multi-toma eléctrico aparatos diferentes a los equipos de cómputo para evitar sobre cargas en el circuito eléctrico.
e) Está prohibido reiniciar los equipos en caliente, sin el apagado debido desde el sistema operativo, cómo también apagar y encender inmediatamente, debido a que se puede presentar daños por energía remanente o estática.

f) Está prohibido colocar objetos que obstaculicen los orificios de salida de aire de las máquinas; se debe mantener libres los espacios de ventilación que tienen las CPU y monitores, debido a que se puede elevar el nivel de temperatura del equipo y producir un bloqueo por sobre calentamiento o corto circuito.

g) Está prohibido pegar adhesivos o elementos extraños a los componentes del equipo de cómputo.

h) Está prohibido exponer los equipos de cómputo a radiación directa del sol o la lluvia, debido a que se puede producir sobre calentamiento, daño en los pixeles del monitor o corto circuito. Se recomienda que los equipos de cómputo permanezcan sobre las mesas de trabajo, nunca deben estar en el suelo sin una base.

i) Está prohibido intercambiar periféricos o elementos entre equipos de cómputo, tales como: teclado, mouse, path mouse, impresoras, monitores, etc. Esto puede generar alteraciones en el inventario inicial del equipo e inventario individual del responsable además de ocasionar daños en los dispositivos por variación de voltaje en los puertos USB, PS2 o fuentes de poder.

j) Está prohibido trasladar equipos dentro de la oficina, ni a otras oficinas salvo previa autorización directa del Contralor y/o Sub-contralor y con la debida supervisión de un funcionario de la Oficina de Tecnologías de la Información. Esto ocasiona alteraciones en el inventario, además de incumplimiento a la norma GTC-45 “Seguridad y Salud en el Trabajo”, la cual exige que los funcionarios no deben desarrollar actividades de fuerza o de altura sin la indumentaria o capacitación debida. Cuando sea necesario el traslado de equipos de cómputo a otra oficina o entidad, se realizará un acta de entrega del equipo y tanto el equipo como la información contenida en las unidades de almacenamiento, quedan bajo la responsabilidad del funcionario que recibe.

k) En ningúnún momento se deberán instalar equipos o periféricos que de alguna manera interactúen con la infraestructura o recursos informáticos de la entidad, sin la supervisión y autorización de la Oficina de Tecnologías de la Información.

l) Está prohibido instalar, reinstalar o realizar las actualizaciones a nuevas versiones de software en las estaciones de trabajo de la entidad, esta es función exclusiva de la Oficina de Tecnologías de la Información de la CMP. Todo software que haya sido instalado sin autorización expresa, podrá ser eliminado sin previo aviso y sin responsabilidad por los datos o información que el usuario reclame como perdidos.

m) Cualquier software que requiera un usuario, deberá ser solicitado a la Oficina de Tecnologías de la Información CMP, mediante solicitud escrita justificando los motivos.

n) El funcionario que instale software ilegal en su equipo asignado, es responsable penal y disciplinariamente del acto que sanciona las leyes sobre derechos de autor. La Contraloría Municipal de Pereira es una Entidad del estado comprometida con el respeto a la propiedad intelectual por lo que no se podrá copiar o redistribuir

software, imágenes, libros, sin la autorización escrita del propietario, o documento que respalde los derechos de uso.

o) Está prohibido utilizar copias de programas gratuitos o juegos para ser instaladas en las estaciones de trabajo, salvo haya sido aprobado por la Oficina de Tecnologías de la Información CMP.

p) Está prohibido el uso de dispositivos de almacenamiento masivos, sin previa vacunación con el antivirus que suministra la entidad

q) Todos los equipos de cómputo deben tener instalado el software antivirus, este permanece actualizado a través de la red e internet y cada funcionario es responsable de realizar revisión a la maquina al menos una vez al mes.

r) Cuando se sospeche o evidencie la presencia de virus en la estación de trabajo asignada, el usuario responsable de esta, debe informar inmediatamente a la Oficina de Tecnologías de la Información CMP para lo de su competencia

s) Está prohibido mantener información institucional, archivos en el escritorio del perfil de usuario, debido a que es información vulnerable a daño o pérdidas en caso de presentan daños en el sistema operativo o en el disco duro generando posible pérdida de información y la correspondiente sanción disciplinaria.

t) Está prohibido la utilización de las redes sociales en jornada laboral, salvo los funcionarios encargados de la administración del espacio institucional.

u) Está prohibido el acceso o manipulación de equipos de cómputo por parte de personas ajenas a la Institución sin el debido acompañamiento de los funcionarios de la Oficina de Tecnologías de la Información

v) Se debe verificar y validar los recursos informáticos recibidos por parte del responsable de inventarios, antes de firmar el acta y el acuerdo de confidencialidad y responsabilidad.

w) Se debe reportar por escrito a la Oficina de Tecnologías de la Información cualquier falla, daño, incidencia o pérdida de información o elemento relacionado con el recurso tecnológico que le sea asignado o que sea común a las actividades cómo equipo de trabajo.

x) Es importante hacer buen uso de las credenciales de ingreso al equipo de cómputo, servicios, aplicaciones de bases de datos y correo institucional CMP, manteniendo un registro reservado de estas y no activar el recordatorio automático de estas que faciliten el uso de estas por parte de personas no autorizadas; recuerde que el uso indebido de contraseñas será responsabilidad del usuario al que se le asignó.

y) Se debe bloquear de la sesión de usuario en la estación asignada, cuando se retira de su puesto de trabajo, con el fin de mitigar riesgos de suplantación de credenciales.

z) Se debe depurar semanalmente la información que no sea útil contenida en los discos duros, verificado que sólo se mantenga la información institucional.

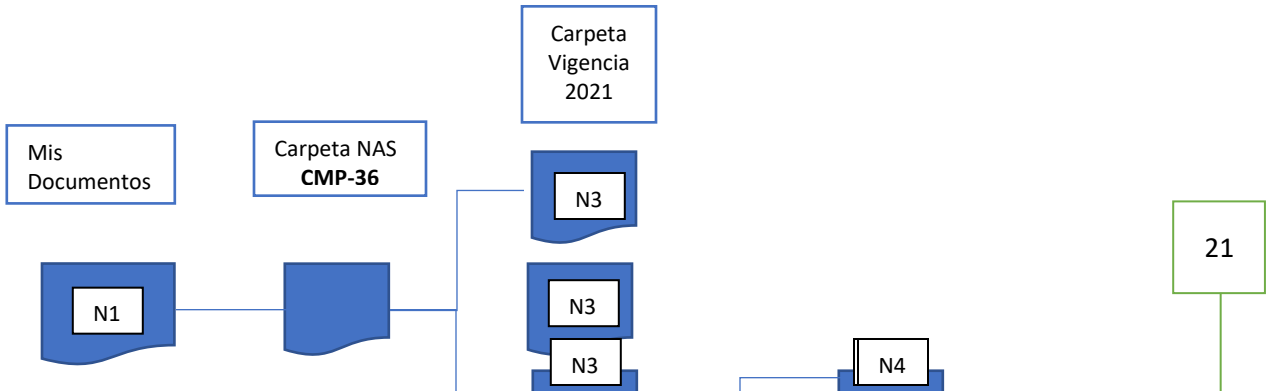
aa) Se debe procurar siempre el uso de los medios digitales ofrecidos por la CMP con el fin de implementar buenas prácticas de optimización de recursos y a cultura de cero papel.
bb) Verificar y validar el apagado del equipo de cómputo, impresoras y luminarias del espacio de trabajo, con el objetivo de minimizar el consumo de energía y posibles fallas por fluido eléctrico, siempre antes de culminar las labores diarias.
cc) Se debe mantener limpio el equipo asignado y responsabilizarse de protegerlo en caso de que se requiera algún trabajo de mantenimiento locativo.

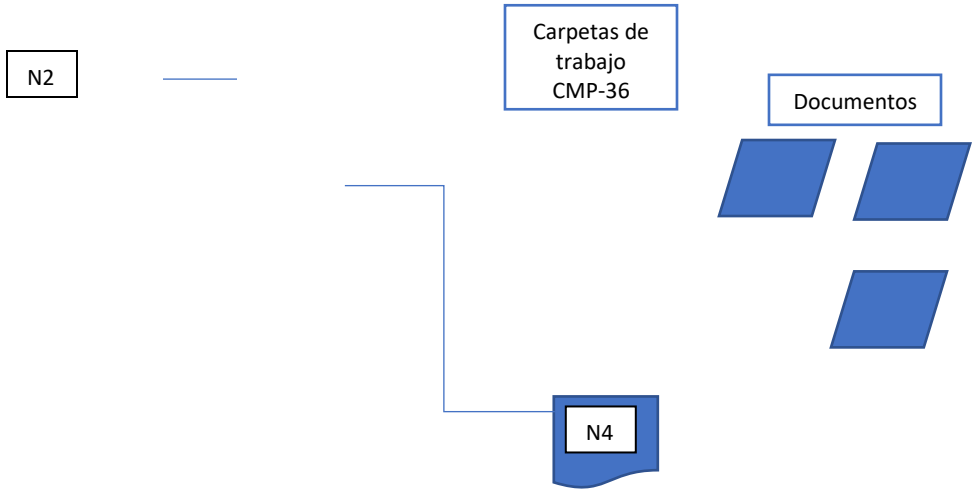
8.1 DEL MANEJO Y ALMACENAMIENTO DE LA INFORMACIÓN

Es relevante hacer uso de buenas prácticas para el almacenamiento y copias de seguridad de la información Institucional CMP.

Al anidar carpetas de información se deberá tener en cuenta la siguiente estructura y jerarquía:

a. Nivel 1: Carpeta principal **"Mis documentos"**
b. Nivel 2: Sub-Carpeta de la copia de seguridad, que en el nuevo sistema de almacenamiento en la red NAS, se denominará con el nombre de la máquina, ejemplo **CMP-01**.
c. Nivel 3: Sub-carpeta donde se almacenan las tres (3) últimas vigencias incluida la actual.
d. Nivel 4: contendrá la clasificación de las carpetas según el tipo de documento que se almacene allí o en su defecto podrían clasificarse por los nombres de las actividades programadas para la vigencia, o procesos de la vigencia.
e. Nivel 5: se mantendrá el estándar definido para la documentación digital que estructura que se establece en el Manual de Gestión Documental.
f. Todos los archivos y carpetas deberán usar lenguaje nemónico, es decir, que el nombre de la carpeta indica su contenido; igual para los archivos, el documento se nombrará de acuerdo a su contenido, con nombres abreviados, sin utilización de tildes, puntos y caracteres especiales que utiliza el sistema operativo como son: la barra extendida (*/*), (****), punto(**.**), paréntesis (**()**), virgulilla (**~**), coma (**,**), punto y coma(**;**), corchetes (**[{ }]**), tildes (¨) porque impiden realizar una copia de seguridad que utiliza estos símbolos o en otros casos no es posible recuperar la información.





Gráfica [Estructura y jerarquía de creación de carpetas y archivos]

- Se recomienda a todos los funcionarios CMP, mantener la estructura y jerarquía para el anudamiento de carpetas y archivos de información, cómo trazabilidad documental para auditorías de Sistema de Información.
- Se recomienda a todos los funcionarios CMP, Usar nombres cortos para las carpetas y archivos máximo de [15] caracteres en los archivos, él no hacerlo causará inconvenientes al momento de efectuar copias de seguridad con los sistemas operativos y posible pérdida de información.
- Recordemos que las subcarpetas y los archivos no deben tener nombres propios. Los nombres de los archivos se asignan según el tema referido en el documento.
- Para nombrar los documentos se tendrá en cuenta utilizar abreviaturas. Ver tabla [Abreviaturas en estructura y jerarquías de información]

AGR = Auditoría General República	CGR = Contraloría General República	CMP = Contraloría Municipal Pereira
ART = Artículo	ACT = Acta	CAP = Capítulo
CC = Cédula de ciudadanía	COD = Código	COM = Comisión
CONCEP = Concepto	INTV = Interventoría	SUPV = Supervisión

COORD= Coordinador	CTA = Cuenta	DIR = Dirección
DPTO = Departamento	DUP = Duplicado	FIG = Figura
VIG = Vigencia	EST = Estado	SIS = Sistema
VOL = Volumen	VER = Versión	VS = Versus
BCO = Banco	MEM = Memorando	DDMMAA = Día Mes Año
FOL = Folio	FACT = Factura	GRAL = General
FORM = Formato	**DOC** = Documento	**MAN** = Manual
GEST = Gestión	**PT** = Papel de trabajo	**CAT** = Catálogo
PREL = Preliminar	**ACEPT** = aceptación	**ADMON** = Administración
GOB = Gobierno	**CAPAC** = Capacitación	**DEV** = Definitivo
IBIDEM = En el mismo lugar	**IDEM** = El mismo, lo mismo	**IMPTO** = Impuesto
INF = Informe	**PER** = Período	**FINAN** = Financiero
ING = Ingeniero	**MAX** = Máximo	**MIN** = Mínimo
PAG = Página	**PPAL** = Principal	**RTE** = Remitente

Nota:
Está lista es susceptible a cambios y los funcionarios pueden solicitar la ampliación de esta según sus necesidades.

- Cada funcionario de la Contraloría Municipal de Pereira es responsable de mantener actualizada la información de las carpetas Institucionales antes mencionadas carpeta CMP- #de la maquina ubicada en “Mis Documentos”, con el objetivo de que se mantenga la copia conectada al dispositivo de red **NAS** (Network Attached Storage) para la realización automática y en tiempo real de copias de seguridad.

- Se recomienda a todos los funcionarios CMP no almacenar datos en el escritorio de las estaciones de traba; este no es un sitio seguro; si se presentaran daños en el sistema operativo o en el disco duro no existiría la posibilidad de recuperación de información.
- Para el proceso de elaboración de copias de seguridad no deberá existir información personal contenida en los equipos de cómputo de la Institución tales como archivos personales, fotos, videos o música.
- Al final de cada documento elaborado, se debe registrar la identificación del creador [iniciales de los nombres], la ruta de ubicación del archivo en el disco duro de la máquina, el nombre del archivo y el nombre de la máquina donde se almacenó; esto con el fin de identificar dónde queda almacenada la información para futura recuperación en la copia de seguridad. Ejemplo: [*jrodas/2020/Actas/entregainv06/CMP-35]*
- Se sugiere a todos los funcionarios CMP que después de la finalización de la vigencia, depurar o limpiar la carpeta que contenga los oficios o cartas de las cuales se conserva copia física o digital en el correo institucional, para efecto de optimizar el uso del espacio en los medios de almacenamiento.
- Las imágenes fotográficas, audios o videos que se toman como material probatorio en un proceso auditor, deben ser almacenadas y conservadas como evidencia en la carpeta de cada auditoría y en medio magnético CD o DVD debidamente etiquetado.
- No se deben guardar varios documentos en un mismo archivo, esta práctica causa confusión de versiones, desorden e imposibilita su ubicación al tratar de recuperar la información a futuro.
- Para el manejo de formatos de calidad, se deben descargar las plantillas ubicadas en la intranet de la entidad, con el fin de evitar errores en uso de versiones del formato o documento.
- No se debe almacenar por ningún motivo, archivos con contenido de música, videos (mp3, mp4, entre otros) en los discos duros de la entidad, que no estén debidamente autorizados, este tipo de archivos se encuentran amparados por las leyes de derechos de autor y no corresponden a la misión institucional CMP (salvo los que se crean para material probatorio de un proceso institucional).
- Para la emisión de la correspondencia interna utilice siempre el correo institucional, para mayor oportunidad en la entrega de comunicaciones oficiales, utilice el correo institucional correo@contraloriapereira.gov.co acorde a lo establecido en la Circular No.002 de 2020.
- Tenga en cuenta que la información que usted procesa dentro de un ejercicio institucional de control fiscal, es propiedad de la Contraloría Municipal de Pereira, por tanto, todos los funcionarios deben mantener en custodia, protegido de pérdida involuntaria y guardar la reserva y confidencialidad de estos, hasta tanto no se

oficialice su publicación por parte del representante legal de la entidad. La pérdida voluntaria o involuntaria de información por acción u omisión de las reglas establecidas en el presente documento, darán lugar a investigación disciplinaria y sanción.

8.2 DE LOS DISPOSITIVOS DE ALMACENAMIENTO EXTERNO

Con el uso de dispositivos de almacenamiento masivo se deben tener las siguientes precauciones:

a. No forzar la entrada del disco, USB o cintas a la unidad.
b. No introducir discos, USB o cintas en mal estado, sucias o mojadas.
c. No colocar los discos flexibles, USB o cintas cerca a campos magnéticos ni exponer al calor.
d. Tener la precaución de revisar con antivirus antes de ejecutar o abrir archivos contenidos en las unidades de almacenamiento.
e. No introducir por la ranura de la unidad, ningún elemento diferente a los discos o elementos de almacenamiento masivo.
f. En caso de que se dude sobre la procedencia de un disco o elementos de almacenamiento masivo, consulte inmediatamente el área de sistemas.
g. Cada usuario deberá responder por custodiar y proteger la información que se procese en el equipo de cómputo asignado.

8.3 DE LAS IMPRESORAS

La Contraloría Municipal acogiéndose a la Directiva Presidencial No 04 del 3 de abril de 2012 “Eficiencia Administrativa y Lineamientos de la Política Cero Papel en la Administración Pública” y la Ley 1437 de 2011 “Por la cual se expide el código de Procedimiento Administrativo y de lo Contencioso Administrativo, artículo 55° establece las siguientes reglas para para racionalizar el uso de la papelería.

Artículo 55. *Documento público en medio electrónico.* Los documentos públicos autorizados o suscritos por medios electrónicos tienen la validez y fuerza probatoria que le confieren a los mismos las disposiciones del Código de Procedimiento Civil.

Las reproducciones efectuadas a partir de los respectivos archivos electrónicos se reputarán auténticas para todos los efectos legales.

Actualmente la Contraloría Municipal cuenta con dos multifuncionales de red ubicadas en el área administrativa y financiera de la entidad; cada máquina soporta los trabajos de impresión de las áreas asignadas y se encuentran configuradas para que únicamente los

líderes de procesos y sus asistentes, impriman los trabajos o documentos oficiales y para de esta manera controlar el servicio.

La CMP actualmente contrata el servicio de copiado e impresión dados los costos que implica el mantenimiento de estas máquinas cuando son propiedad de la entidad.

La impresora de tinta es utilizada para realizar impresión de alta calidad habilitada para el equipo de edición de documentos correspondientes a informes de ley con destino a imprentas, para la emisión de revistas de la entidad o correspondencia despachada externa; las tarjetas de invitación o de actos protocolarios del despacho del contralor que solo serán autorizados por contralor o subcontralor.

Los documentos o informes voluminosos se graban en formato CD o DVD, con la respectiva etiqueta a fin de reducir costos de papelería.

La fuente o tipo de letra que se recomienda para realizar la documentación de la CMP es ARIAL a 11 puntos y se trabajará con espacio interlineal sencillo, salvo la separación de párrafos y títulos, esto con el fin de reducir el consumo de papel.

Toda confirmación de recibo de la información que sea presentada por medios digitales o programas de rendición podrá guardarse como constancia en la carpeta de [Mis Imágenes/constancias] y deberá dejarse en forma digital o de imagen y guardar copia de seguridad de esta información.

Todos los documentos internos se tramitarán a través del servicio de correo institucional y la mensajería interna.

Se prohíbe la impresión de documentos personales, normas, manuales o documentos que pueden ser consultados en la pantalla de la computadora o a través de internet o intranet.

Para optimizar el uso de papel las impresiones de documentos se realizarán a dos caras y se admite el uso de hojas de reciclaje con excepción de las comunicaciones oficiales o cartas.

Se prohíbe la fotocopia de documentos personales o con fines que no corresponden a la misión de la entidad.

La información que se recopila dentro del proceso auditor debe ser solicitada a los sujetos de control en forma digital con el fin de contribuir a la eficiencia en el consumo de papel, salvo las que exija la ley en forma física.

La información que sea solicitada por los entes de control en su proceso de auditoría a la CMP se suministrará en forma digital salvo las que exija la ley en forma física.

La información que se procesa en sistemas de información que almacenan y dejan disponibilidad de acceder a estos en cuanto se requieran, por ningún motivo deben imprimirse; si se requiere la firma se permite la digitalización de esta por parte del responsable (ver numeral **10.4** Acerca de la validez de la firma escaneada)

Los mensajes de correo no deben ser impresos si se requiere la evidencia existen medios de recuperación como son la copia de seguridad de cada correo institucional y la opción de guardar el mensaje desde la mensajería de Microsoft Outlook

Es obligación de los funcionarios de la CMP:

- Reutilizar las hojas de las impresiones a una parte dañadas, por lo que se recopilarán en la Coordinación de Sistemas para ser reusadas.
- Reducir los espacios interlineales de los documentos que se emiten. (evitar doble espacio).
- Revisar y corregir en pantalla antes de enviar el documento original a impresión.
- Utilizar los medios oficiales digitales de comunicación que son suministrados por la CMP como son el correo electrónico, la intranet y el servicio de mensajería interna SPARK.
- Solicitar a la ventanilla única la digitalización de la información que se emite dentro de algún proceso misional y entregar a quien le compete la mencionada información en CD o DVD.
- Solicitar en forma digital la información requerida dentro de un ejercicio auditor o proceso misional.
- Controlar la emisión de copias de los documentos que deben ser impresos de tal manera que se imprima el original, se firme y luego se envíen las copias en forma digital.

8.4 DE LOS EQUIPOS PORTÁTILES CMP

La oficina de Tecnologías de la Información CMP será responsable de las copias de seguridad y la actualización del antivirus, siempre y cuando la computadora se conecte periódicamente a la red wifi de la entidad de lo contrario la información es responsabilidad del funcionario a quien se le asigne el equipo.

Por ninguna razón se justifica la pérdida de información de los grupos de trabajo, si no se han cumplido con los requisitos previos de mantener copia de respaldo de los documentos elaborados y si no se ha realizado la actualización del antivirus. Para efectos de manejo de la información digital se tiene en cuenta las mismas reglas establecidas en el numeral 3.2 del presente documento.

Es responsabilidad de cada usuario a quien se le asignó el equipo, el uso de software ilegal que instale desconociendo la reglamentación establecida en las Leyes que rigen sobre derechos de autor y en el presente documento.

Ningún equipo portátil que no pertenezca a la Contraloría Municipal de Pereira podrá ingresar al dominio de la entidad, sin embargo, podrá utilizar la red wifi bajo las condiciones y restricciones establecidas por las presentes políticas.

La computadora portátil se entregará configurada para trabajo en la red wifi institucional, con el fin de que cada funcionario responsable realice las actualizaciones del antivirus y copia de seguridad de archivos importantes en el directorio *[home]* del servidor de red, además de tener acceso a consultas de Internet e intranet y mensajería instantánea por lo tanto no se puede modificar esta configuración.

Una red inalámbrica es efectiva para los usuarios, pero al mismo tiempo fácilmente accesible y por lo tanto vulnerable para intrusos y usuarios ilegítimos; si va a ingresar con un portátil de la entidad a una red inalámbrica libre, tenga cuidado de que las carpetas de su equipo no estén compartidas y verifique antes que el antivirus esté actualizado.

En caso de pérdida por robo, el funcionario responsable del portátil deberá formular la respectiva denuncia y presentar informe a la Subcontraloría para proceder a la reclamación del elemento a la aseguradora.

Los equipos portátiles son entregados para apoyar las labores de control fiscal cuando los funcionarios lo requieran o para ayudas audiovisuales en procesos de capacitación.

El funcionario al que se le hace entrega de equipo, se le asigna la responsabilidad del buen manejo y conservación del elemento y será registrado al inventario individual por parte del funcionario encargado.

Cada portátil será entregado con su respectivo maletín y el responsable deberá devolver el elemento en igual estado en que lo recibió diligenciando el formato FO 1.2.2.2-2 “Devolución de Bienes”.

La solicitud del elemento se realiza a través del funcionario encargado de los inventarios y una vez el área de sistemas asigne el elemento, el auxiliar de inventarios deberá entregar el portátil y una carta de autorización de salida del equipo del edificio cuando se requiera el desplazamiento.

La computadora portátil tendrá un usuario y contraseña para el ingreso al sistema operativo que garantice la seguridad de los archivos contenidos en esta.

9. DE LOS SERVICIOS DE RED DE DATOS

La Entidad, provee a sus colaboradores los servicios necesarios para el cumplimiento de la misión institucional, controlados y administrados a través de la Oficina de Tecnologías de la información; para ello cuenta con la infraestructura necesaria que le permite entregar:

- Credenciales y políticas de acceso a la red institucional restringida, además de uso exclusivo para funcionarios y contratistas de la entidad.
- Credenciales y políticas de acceso a Internet, con el objeto de dar apoyo en las labores de investigación y comunicación. Este acceso a Internet está controlado a través de un servidor proxy que permite establecer restricciones, seguridades y es constantemente monitoreado por la Oficina de Tecnologías de la Información CMP.
- El servicio de la página web institucional CMP, permite la comunicación con el ciudadano y sujetos de control además de presentar ante el mundo la identidad estatal del sujeto de control del municipio de Pereira y por ser un medio de comunicación masivo y no excluyente, es necesario homogenizar el lenguaje que se utiliza y la forma de presentar los contenidos para mantener una imagen consolidada de la Contraloría Municipal de Pereira para que sea coherente con los cambios y transformaciones de la entidad. Adicionalmente se cuenta con una intranet donde se publica información institucional para los funcionarios y contratistas.
- El servicio de correo institucional es un medio oficial de comunicaciones internas y externas; se accede por medio del programa Microsoft Outlook residente en cada máquina. Otro medio de acceso al correo se realiza a través de la página web institucional, link ***CORREO INSTITUCIONAL*** el cual se utiliza en caso en que el funcionario no tenga disponibilidad de la estación de trabajo asignada en las instalaciones de la entidad o requiera ingresar desde otro lugar. Es importante entender que al acceder desde la página web, no es posible revisar el correo que ya se visualizó desde Microsoft Outlook, éste descarga la información del servidor de correos al disco duro de la estación asignada.
- Teniendo en cuenta que en aspectos técnicos no se puede trabajar sobre supuestos debe darse un respaldo y un seguimiento continuo a los recursos que agilizan las labores, para esto en cada uno de los equipos de cómputo de la entidad (estaciones

de trabajo y computadoras portables), se debe efectuar la producción de copias de seguridad de los archivos procesados en los discos duros siguiendo reglas y programación estricta y regular. La CMP cuenta con un dispositivo NAS (network Attached Storage) almacenamiento conectado a la red corporativa que opera como servidor de archivos y mantiene copia de seguridad de toda la información almacenada en cada estación de trabajo carpeta CMP- #de máquina.

- Se cuenta con servicio de impresión copiado y escaneo en red contando actualmente con dos multifuncionales una de ellas se encuentra en alquiler puesto que este servicio provee a la entidad ahorro en costes de insumos y mantenimiento.
- Servicio de mensajería instantánea, manera informal de transmitir comunicación interna y archivos pequeños que no requiere seguimiento o trazabilidad.
- Servicio de soporte de nivel 1 y 2 dependiendo de la complejidad del caso por lo que en lo posible se atiende rápidamente.
- Servicio de tele conferencia a través de las cuentas de Microsoft Teams adquiridas para facilitar las reuniones virtuales, capacitaciones con funcionarios y clientes externos.
- El servicio de VPN red privada virtual, que básicamente es una red segura de navegación privada que permite que los programas y dispositivos se conecten por medio de una extensión de internet, sin estar vinculados físicamente a la red, lo que puede asegurar una transmisión fiable de los datos. Este servicio se habilitó para que la CMP mantuviera sus servicios aún en trabajo asistido por tecnología.

9.1 DEL USO DEL SERVICIO DE INTERNET

El servicio de internet es un recurso informático que debe ser orientado y aprovechado para el uso de investigación, además para la búsqueda de información relacionadas con su trabajo; y como tal este deberá primar sobre cualquier otro objetivo o interés personal; cualquier uso inadecuado de estos servicios que interfiera con la imagen de la Contraloría Municipal de Pereira es considerado una violación a esta política y está sujeto a las sanciones correspondientes.

La Contraloría Municipal de Pereira se reserva el derecho a filtrar el contenido al que el usuario puede acceder a través de Internet desde los recursos y servicios propiedad de la Entidad, así como a monitorear y registrar los accesos realizados desde los mismos, buscando mantener la seguridad perimetral.

Los funcionarios tendrán disponibilidad de los servicios de Internet e intranet de la Contraloría Municipal de Pereira, para ello el funcionario responsable de la Oficina de recursos humanos deberá reportar el ingreso del nuevo funcionario o contratista directamente a la Oficina de Tecnologías de la Información CMP, donde se crearán las

credenciales [usuarios y contraseñas] para acceder a los servicios y recursos informáticos.

El servicio de internet por Wi-Fi solo se prestará con restricción de contraseña. La máquina que ingrese a la red CMP no podrá ingresar al servicio de internet vía Wi-Fi; salvo cuando sea estrictamente necesario y en caso de contingencia por razones de seguridad y preservación de la información.

El servicio de Wi-Fi está restringido a través del servidor proxy, su uso se encuentra habilitado para las computadoras portátiles de la entidad, contratistas y visitantes en cumplimiento de las políticas del gobierno nacional, Estrategia de Gobierno en Línea. La Entidad da cumplimiento a las normas legales que regulan el sector de las TICs y adopta las guías que aplican a la entidad.

En caso de que un usuario requiera descargar información desde Internet deberá tener en cuenta la propiedad intelectual. Los usuarios deben respetar y dar cumplimiento a las disposiciones legales de derechos de autor, marcas registradas y derechos de propiedad intelectual.

Está prohibido la descarga de material gráfico que contenga actividad sexual, nudismo, violencia o cualquier otra actividad que vaya en contra de los principios y valores de la Entidad; el incumplimiento de esta política será causa justificada para una sanción disciplinaria, como tampoco se puede utilizar el servicio de internet para ninguna actividad ilegal o que atente contra la ética, buen nombre y dignidad de la Contraloría Municipal de Pereira.

A través de Internet se puede acceder a otras redes de diferentes países, cada uno de estos países cuenta con normatividad diferente a Colombia en cuanto al uso de la información dispuesta para sus visitantes, en todo caso el usuario debe conservar el respeto y el cumplimiento a las leyes dispuestas en cada uno, para no comprometer en nada el nombre de la Entidad.

Se recomienda cerrar las páginas que requieran actualización periódica, así como el uso de conexiones simultáneas de portales web.

Está prohibido la instalación y el uso de aplicaciones multimedia y podcast como: [Emisoras web, iTunes, Spotify, Winamp, Real audio, Music Match, Oozic player entre otras].

Está prohibido la instalación y el uso de aplicaciones de mensajería instantánea, video conferencia y VoIP como: [MSN Messenger, Yahoo! Messenger, Tango, WhatsApp, Skype, Zoom, entre otros].

Lo anterior para evitar el consumo elevado de recursos de máquina y congestión del tráfico en la red de datos local, que distan de las actividades y de la misión institucional CMP.

9.2 DEL USO DEL SERVICIO DE INTRANET

El servicio de intranet CMP, se considera una red privada similar al servicio de Internet, la cual permite compartir información competente a la organización; el principal beneficio es que se tiene toda la información institucional en cualquier lugar, siempre y cuando exista acceso a Internet; se accede a través de un usuario y una contraseña que suministra el administrador del servicio.

Dentro de la intranet institucional CMP, se conservan los documentos de conocimiento general de la Contraloría Municipal de Pereira, además de las noticias, circulares, folletos, eventos y plantillas de uso institucional por lo que este se restringe explícitamente a los funcionarios y contratistas de la entidad.

9.3 DEL ALCANCE EN EL USO DE LOS SERVICIOS DE INTERNET E INTRANET

Todas las comunicaciones de carácter institucional y que sean de interés general deberán ser publicadas en la intranet.

Los usuarios de Internet e intranet se comprometen a dar el uso racional, responsable y adecuado a estos servicios.

Cada funcionario de la Institución es el único responsable de las actividades realizadas en la navegación en Internet e Intranet con su usuario de acceso.

Todos los usuarios conocen y aceptan las cláusulas de privacidad que se presentan a continuación, por lo que no constituirá violación de su privacidad cualquier tema contemplado.
El servidor de acceso a Internet cuenta con las bitácoras de trazabilidad que permiten conocer los lugares visitados, tiempos consumidos, las horas de entrada - salida de dichos lugares, así como los nombres y tamaños de la información enviada y recibida en los equipos d cómputos o dispositivos asociados a la red de datos incluyendo Wi-Fi.

La Oficina de Tecnologías de la Información CMP, está facultada para generar los informes relacionados al manejo por usuario de estos servicios, a solicitud de los jefes de Área o líderes de procesos, que permita monitorear la utilización de este servicio.

Los lugares o sitios que se visiten en Internet serán de completa responsabilidad del usuario desde la estación de trabajo asignada y en todo caso deberán basarse en la racionalidad y la responsabilidad individual. Se asume que en ningún momento dichos lugares atenten contra la moral, ni en contra de los intereses de personas individuales, los de nuestra Institución, así como de ninguna otra.

Está prohibido utilizar el servicio de Internet institucional para subscribirse a listas de distribución que envían material no útil para desempeñar el trabajo de la Institución.

Está prohibido utilizar el Internet para perder deliberadamente el tiempo, visitando portales que no provean información útil para el desarrollo de sus actividades diarias.

Los líderes de procesos son los encargados de suministrar la información que se debe publicar en el portal institucional o intranet; ellos se encargarán de mantener los contenidos actualizados para que la ciudadanía pueda consultarlos; el Comité de dirección establece los parámetros de publicación acorde con las “Políticas y Estándares para publicar información del Estado en Internet” y en cumplimiento de la Estrategia de Gobierno en línea. En todo caso el funcionario encargado del manejar el administrador de contenidos es responsable de conservar los estándares de la estructura que establece el Manual de Comunicaciones de la entidad y es responsable de la oportunidad en la publicación; la actualización y veracidad de la información es responsabilidad de cada líder de proceso.

Los usuarios de la intranet CMP, deben revisar permanentemente la información contenida en el sitio para mantenerse informados. Se entiende por informada y recibida, la comunicación que se cargue en la intranet.

La contraseña de acceso al servicio de intranet se deshabilita con la inactividad en el uso del servicio, por lo que el funcionario que deje de consultar este sitio deberá remitirse a la Oficina de Tecnologías de la información CMP para solicitar una nueva contraseña.

El uso de los documentos del Sistema de Gestión de Calidad debe hacerse a través la intranet y cada vez que se requiera el documento controlado, se deberá realizar la operación para no incurrir en errores por el uso de formatos desactualizados.

Se prohíbe realizar conversaciones en el servicio de cibercharla y el uso de los sitios de redes sociales dentro de la institución salvo para administración y consulta del sitio institucional.

Se prohíbe transferir música o programas a través del servicio de internet, e instalar todo tipo de programas en los equipos de cómputo de la entidad. Esta función es estrictamente competencia del área de sistemas.

Se prohíbe el ingreso a páginas obscenas, sitios de comunidad virtual para hacer contactos con personas, sitios de descargas, sitios shock, sitios de subasta y sitios de juegos interactivos.

Por ningún motivo los funcionarios introducirán información no relacionada con la misión de la entidad en los discos duros de la entidad.

Se prohíbe utilizar el recurso para el envío o reenvío de mensajes en cadena a múltiples contactos.

La Oficina de Tecnologías de la Información mantendrá el log o registro de seguimiento de auditoría para realizar control del acceso a cada usuario y se presentará informe de las inconsistencias detectadas al subcontralor con copia a la Oficina de control interno.

9.4 DEL USO DEL CORREO ELECTRÓNICO

El correo electrónico es un servicio de red de datos CMP, que permite enviar y recibir información entre los usuarios que comparten los servicios de internet e intranet, el cual se encuentra debidamente regulado en primera medida por la ley 527 de 1999, la cual lo establece como mensaje de datos en los siguientes términos:

Artículo 2º. DEFINICIONES. Para los efectos de la presente ley se entenderá por:

a) Mensaje de datos. La información generada, enviada, recibida, almacenada o comunicada por medios electrónicos, ópticos o similares, como pudieran ser, entre otros, el Intercambio Electrónico de Datos (EDI), Internet, el correo electrónico, el telegrama, el télex o el telefax; (...)" (Subrayado fuera del texto).

Así mismo determina en cuanto a los requisitos jurídicos de los mensajes de datos:

"APLICACIÓN DE LOS REQUISITOS JURÍDICOS DE LOS MENSAJES DE DATOS"

Artículo 6º. ESCRITO. Cuando cualquier norma requiera que la información conste por escrito, ese requisito quedará satisfecho con un mensaje de datos, si la información que éste contiene es accesible para su posterior consulta.
Lo dispuesto en este artículo se aplicará tanto si el requisito establecido en cualquier norma constituye una obligación, como si las normas prevén consecuencias en el caso de que la información no conste por escrito.

Artículo 15º. RECONOCIMIENTO DE LOS MENSAJES DE DATOS POR LAS PARTES. En las relaciones entre el iniciador y el destinatario de un mensaje de datos, no se negarán efectos jurídicos, validez o fuerza obligatoria a una manifestación de voluntad u otra declaración por la sola razón de haberse hecho en forma de mensaje de datos. (...)

Artículo 23º. TIEMPO DEL ENVÍO DE UN MENSAJE DE DATOS. De no convenir otra cosa el iniciador y el destinatario, el mensaje de datos se tendrá por expedido cuando ingrese en un sistema de información que no esté bajo control del iniciador o de la persona que envió el mensaje de datos en nombre de éste".
En esta medida se debe tener presente que la Ley 527 de 1999 tiene como ámbito de aplicación todo tipo de información en forma de mensaje de datos, excepto:

- En las obligaciones contraídas por el Estado colombiano en virtud de convenios o tratados internacionales, y
- En las advertencias escritas que por disposición legal deban ir necesariamente impresas en cierto tipo de productos en razón al riesgo que implica su comercialización, uso o consumo.

En este orden de ideas encontramos la Ley 962 de 2005, por medio de la cual se dictan disposiciones sobre la racionalización de trámites y procedimientos administrativos de los organismos y entidades del Estado, la cual señala en su artículo 10.

Artículo 10º. UTILIZACIÓN DEL CORREO PARA EL ENVÍO DE INFORMACIÓN. Modifíquese el artículo 25 del Decreto 2150 de 1995, el cual quedará así:

"Artículo 25º. Utilización del correo para el envío de información. Las entidades de la Administración Pública deberán facilitar la recepción y envío de documentos, propuestas o solicitudes y sus respectivas respuestas por medio de correo certificado y por correo electrónico. (...)" (Subrayado y negrilla fuera del texto).

Así mismo el Decreto 2150 de 1995, por el cual se suprimen y reforman regulaciones, procedimientos o trámites innecesarios existentes en la Administración Publica, señala en su artículo 26:

Artículo 26º. UTILIZACIÓN DE SISTEMAS ELECTRÓNICOS DE ARCHIVO Y TRANSMISIÓN DE DATOS. Las entidades de la Administración Pública deberán habilitar sistemas de transmisión electrónica de datos para, que los usuarios envíen o reciban información requerida en sus actuaciones frente a la administración. (...) (Subrayado y negrilla fuera del texto).

Acorde con lo establecido en la Directiva Presidencial 04 de 2012, a partir de la fecha, la Contraloría Municipal de Pereira intercambia la correspondencia interna a través de medios electrónicos para lo cual se ha creado el correo napellido@contraloriapereira.gov.co , que es medio oficial de comunicación de interés institucional para los funcionarios de la entidad; este servicio guarda todos los mensajes enviados y recibidos con fecha y hora en la carpeta Archivos de Outlook, ubicada dentro de Mis documentos en el disco duro de cada equipo y el área de sistemas es responsable de conservar copia de respaldo actualizada de esta carpeta.

El correo institucional es también un medio autorizado para comunicaciones oficiales entre el ente de control y los sujetos de control acorde con lo establecido en la Ley 2080 de 2021 " *Por medio de la cual se reforma el Código de Procedimiento Administrativo y de lo Contencioso Administrativo -Ley 1437 de 2011- y se dictan otras disposiciones en materia de descongestión en los procesos que se tramitan ante la jurisdicción" expresa en sus artículos 8°,9°, 10°,11°, 12° y 14°.*

Artículo 8. Adiciónese a la Ley 1437 de 2011 el artículo 53A, el cual será del siguiente tenor:
Artículo 53A. *Uso de medios electrónicos. Cuando las autoridades habiliten canales digitales para comunicarse entre ellas, tienen el deber de utilizar este medio en el ejercicio de sus competencias.*

Las personas naturales y jurídicas podrán hacer uso de los canales digitales cuando así lo disponga el proceso, trámite o procedimiento.

El Gobierno nacional, a través del Ministerio de Tecnologías de la Información y las Comunicaciones, podrá a través de reglamento establecer para cuáles procedimientos, trámites o servicios será obligatorio el uso de los medios electrónicos por parte de las personas y entidades públicas. El ministerio garantizará las condiciones de acceso a las autoridades para las personas que no puedan acceder a ellos.

Artículo 9. Modifíquense los incisos primero y segundo del artículo 54 de la Ley 1437 de 2011, el cual quedará así:

Artículo 54. *Registro para el uso de medios electrónicos. Toda persona tiene el derecho de actuar ante las autoridades utilizando medios electrónicos, caso en el cual deberá realizar sin ningún costo un registro previo como usuario ante la autoridad competente. Sí así lo hace, las autoridades continuarán la actuación por este medio.*

Las peticiones de información y consulta hechas a través de medios electrónicos no requerirán del referido registro y podrán ser atendidas por la misma vía. El registro del que trata el presente artículo deberá contemplar el Régimen General de Protección de Datos Personales.

Artículo 10. Modifíquese el artículo 56 de la Ley 1437 de 2011, el cual quedará así:

Artículo 56. *Notificación electrónica. Las autoridades podrán notificar sus actos a través de medios electrónicos, siempre que el administrado haya aceptado este medio de notificación.*

Sin embargo, durante el desarrollo de la actuación el interesado podrá solicitar a la autoridad que las notificaciones sucesivas no se realicen por medios electrónicos, sino de conformidad con los otros medios previstos en el Capítulo Quinto del presente Título, a menos que el uso de medios electrónicos sea obligatorio en los términos del inciso tercero del artículo 53A del presente título.

Las notificaciones por medios electrónicos se practicarán a través del servicio de notificaciones que ofrezca la sede electrónica de la autoridad.

Los interesados podrán acceder a las notificaciones en el portal único del Estado, que funcionará como un portal de acceso.

La notificación quedará surtida a partir de la fecha y hora en que el administrado acceda a la misma, hecho que deberá ser certificado por la administración.

Artículo 11. Modifíquese el artículo 59 de la Ley 1437 de 2011, el cual quedará así:

Artículo 59. *Expediente electrónico. El expediente electrónico es el conjunto de documentos electrónicos correspondientes a un procedimiento administrativo, cualquiera que sea el tipo de información que contengan. El expediente electrónico deberá garantizar condiciones de autenticidad, integridad y disponibilidad.*

La autoridad respectiva garantizará la seguridad digital del expediente y el cumplimiento de los requisitos de archivo y conservación en medios electrónicos, de conformidad con la ley.

Las entidades que tramiten procesos a través de expediente electrónico trabajarán coordinadamente para la optimización de estos, su interoperabilidad y el cumplimiento de estándares homogéneos de gestión documental.

Artículo 12. Modifíquese el artículo 60 de la Ley 1437 de 2011, el cual quedará así:

Artículo 60. *Sede electrónica. Se entiende por sede electrónica, la dirección electrónica oficial de titularidad, administración y gestión de cada autoridad competente, dotada de las medidas jurídicas, organizativas y técnicas que garanticen calidad, seguridad, disponibilidad, accesibilidad, neutralidad e interoperabilidad de la información y de los servicios, de acuerdo con los estándares que defina el Gobierno nacional.*
Toda autoridad deberá tener al menos una dirección electrónica.

Artículo 14. Modifíquese el artículo 61 de la Ley 1437 de 2011, el cual quedará así:

Artículo 61. Recepción de documentos electrónicos por parte de las autoridades. Para la recepción de documentos electrónicos dentro de una actuación administrativa, las autoridades deberán contar con un registro electrónico de documentos, además de:

1. Llevar un estricto control y relación de los documentos electrónicos enviados y recibidos en los sistemas de información, a través de los diversos canales, incluyendo la fecha y hora de recepción.

2. Mantener los sistemas de información con capacidad suficiente y contar con las medidas adecuadas de protección de la información, de los datos y en general de seguridad digital.

3. Emitir y enviar un mensaje acusando el recibo o. salida de las comunicaciones indicando la fecha de esta y el número de radicado asignado.

La entidad cuenta con los siguientes correos institucionales, según sea el asunto del mensaje, para enviar y recibir comunicaciones, notificaciones oficiales y en general atención al cliente externo: correo@contraloriapereira.gov.co, soporte@contraloriapereira.gov.co,

Nota: Se entiende que todos los correos de los funcionarios y líderes de proceso, son medios oficiales de comunicación y cuando el asunto corresponde directamente al ejercicio de sus funciones, es decir, si se asigna un proceso auditor a un grupo de funcionarios y a cada uno se le entrega responsabilidad sobre un tema o área específica de estudio; este funcionario podrá solicitar directamente información a través del correo institucional a su cargo para tratar temas específicos de comisión.

El servidor de correos de la entidad se encuentra incluido dentro del servicios de hospedaje de la página; este servicio se presta a través del software Microsoft Outlook habilitado en cada máquina de la entidad, lo que implica que cada responsable de equipo (portátil o estación de trabajo) tendrá acceso a la bandeja de correos en la computadora asignada. Los funcionarios del área de sistemas son responsables de configurar el servicio para que esté disponible en cada equipo de la entidad.

También es posible acceder a este servicio desde otros lugares siempre y cuando exista disponibilidad de internet y no se restrinja el uso de los puertos de entrada y salida de correos que se encuentran configurados por defecto en el servidor de correos. Para acceder a las bandejas del correo de este modo, se debe ingresar a la página web o la intranet institucional, haciendo clic en el enlace **CORREO INSTITUCIONAL,** para ello se utiliza el software libre WEBMAIL suministrado por la empresa prestadora del servicio de alojamiento de la página web institucional.

Para acceder al servidor de correo institucional, el usuario deberá ingresar desde un navegador de internet, página principal, botón **Correo**, este lo llevará al gestor de correo electrónico ***horde*** teniendo en cuenta que una vez culmine su sesión se debe cerrar el servicio con el fin de mantener la seguridad del contenido en su correo.

Los correos institucionales serán revisados diariamente por funcionarios de la CMP a quienes les compete esta labor y se realizarán los procedimientos establecidos en el Manual de Procesos y Procedimientos,

Toda la comunicación interna se realizará por el correo institucional sin que se tenga que imprimir el mensaje tanto enviado como recibido. Se entiende que este es el medio oficial de comunicación interna y por lo tanto queda registrado en las bandejas de Microsoft Outlook y custodiado en copia de seguridad que reposa en la oficina de Tecnología de la información.

Los funcionarios de la Contraloría Municipal de Pereira deberán acatar las políticas que se presentan a continuación:

La Oficina de Tecnologías de la Información CMP administra la creación, modificación eliminación y cambio de credenciales de acceso al correo institucional, y se manejará un estándar para denominar la cuenta: letra inicial del primer nombre, seguido el primer apellido, @contraloriapereira.gov.co.

La creación de las cuentas de correo electrónico deberán ser solicitadas formalmente por escrito a la Oficina de Tecnologías de la Información CMP por medio del Técnico de la

Oficina de Recurso Humano o el director del área donde esté adscrito el funcionario, para efectos de trazabilidad, adjuntando la siguiente información:

- Nombre y apellidos completos del usuario.
- Identificación y cargo que va a desempeñar.
- Oficina en la que va a prestar sus servicios.
- Estación de trabajo que se le va a asignar.

9.5 DEL ALCANCE EN EL USO DEL CORREO ELECTRÓNICO

El funcionario responsable de la oficina de Recursos humanos notificará a la Oficina de Tecnologías de la Información CMP el retiro de usuarios de forma escrita, para proceder a suspender el servicio una vez se realice la última copia de seguridad.

Es responsabilidad del usuario "emisor" la información contenida en el mensaje y en todo caso deberán basarse en la racionalidad y la responsabilidad individual que ejerce como funcionario de la Contraloría Municipal.
Se asume que en ningún momento dichos mensajes podrán emplearse en contra de los intereses individuales, los de la Institución, así como de ninguna otra Institución y que puedan generar daños y perjuicios en la buena imagen de la CMP.

Los funcionarios deberán revisar el correo institucional al menos una vez en la mañana y una en la tarde, durante todos los días hábiles y dentro de los horarios oficialmente establecidos como "Horario Laboral". La no revisión de los correos institucionales, no exime del cumplimiento de instrucciones remitidas y cumplimiento de términos preestablecidos a través de este medio.

No se deberá hacer uso del correo electrónico CMP para fines políticos, religiosos, comerciales, ofensivos o de otra índole que no sean los contenidos en la misión de la entidad. Este servicio no deberá usarse para enviar mensajes no solicitados, ni tampoco para enviar material obsceno e ilegal, invitaciones o información personal; recuerde que es de uso exclusivo institucional.

Cadenas y Múltiples Usuarios: Está prohibido el fomentar el envío o reenvío de cadenas de mensajes a múltiples usuarios. Solo se acepta el envío de circulares informativas a grupos de usuarios por parte de funcionarios del nivel directivo.

Por ningún motivo se guardarán mensajes personales en los discos duros de las estaciones de trabajo.

El usuario debe identificarse mediante sus credenciales de acceso al correo electrónico siempre que ingrese al servicio.

Se advierte que las claves pueden configurarse para que el sistema las recuerde siempre que se ingrese, pero en igual medida el usuario debe ser cuidadoso en el préstamo del equipo asignado, puesto que no se le exime de responsabilidad por el mal uso del servicio.

La solicitud de cambio de clave se hace personalmente y por escrito al administrador del servicio de correo electrónico.

El administrador del servicio se compromete a proteger los datos personales de los usuarios CMP: Nombre Apellidos y dirección de correo electrónico de acuerdo con la legislación sobre protección de datos de carácter personal; siendo de uso exclusivo de la entidad y trasladados a terceros con autorización previa del usuario.

Está completamente prohibido realizar cualquiera de las actividades definidas en el apartado bajo el título “Tipos de Abuso en el uso del Correo Electrónico”. Así como las prohibiciones que se listan a continuación:

- Iniciar o dar seguimiento a “cadenas de correo” que contengan mensajes que no sean relacionados al trabajo.
- Distribuir, ya sea de forma masiva o no, mensajes con contenidos inapropiados para la institución.
- Falsificar el origen o el encabezado de los correos electrónicos.
- Utilizar las cuentas de la institución para recibir correos reenviados automáticamente (forwarded) desde una cuenta externa de correo electrónico.
- El envío de correos electrónicos masivos sin autorización previa
- La suscripción a listas de distribución de correo electrónico que no tengan relación con la misión de la entidad.
- Utilizar la cuenta de correo para perder deliberadamente el tiempo en horarios de trabajo, por medio del envío y/o lectura de mensajes ajenos a la actividad diaria que se desarrolla; es decir, mensajes de entretenimiento y con archivos adjuntos, tales como, presentaciones o imágenes, en especial aquellas que atenten contra la moral (entiéndase entre otros: contenido pornográfico, violencia y sexo).

9.6 DE LOS ABUSOS EN EL USO DEL CORREO ELECTRÓNICO

Las actividades catalogadas como Abuso de Correo Electrónico se pueden clasificar en cuatro grupos así:

Difusión de contenido inadecuado
Contenido ilegal por naturaleza (todo el que constituya complicidad con hechos delictivos). Ejemplos: apología del terrorismo, programas piratas, pornografía, amenazas, estafas, xenofobia, esquemas de enriquecimiento piramidal, virus o código hostil en general.

Difusión a través de canales no autorizados
Uso no autorizado de los servidores de correo electrónico de la Institución para reenviar correo de beneficio propio, por ejemplo, con el envío de publicidad u ofrecimiento de venta. Aunque el mensaje en sí sea legítimo, se están utilizando recursos de la institución sin autorización para usos particulares.

Difusión masiva no autorizada
Es el uso de servidores de correo electrónico propios o ajenos para enviar de forma masiva publicidad o cualquier otro tipo de correo no solicitado. Su principal agravante es que el anunciante descarga en transmisores y destinatarios el costo de sus operaciones publicitarias, aunque el usuario no esté de acuerdo.

Ataques con objeto de imposibilitar o dificultar el servicio
Puede ser dirigido a un usuario o al propio sistema de correo. En ambos casos el ataque consiste en el envío de un número alto de mensajes por segundo, o cualquier variante, que tenga el objetivo neto de paralizar el servicio por saturación de la capacidad de CPU del servidor, o del espacio en disco de servidor o usuario.

Detección y eliminación de virus
El correo electrónico es uno de los medios de difusión de virus informáticos más importantes. Para prevenir la propagación masiva de virus y gusanos informáticos, se aplican las siguientes medidas sobre todos los mensajes que entran o salen en su servicio de correo CMP:

- Está prohibido el contenido de mensajes de correo con anexos ejecutables o susceptibles, incluso con dudosa procedencia. Ejemplo [*.exe, *.dmg, *.cdbr, *.bat, *.dat, entre otros].
- Verificar y validar la procedencia y emisor de mensajes que puedan contener código malicioso.
- Al enviar mensajes verifique el correo electrónico del destinatario y tenga en cuenta que, si desea enviar un archivo ejecutable o de base de datos, deberá quitar la extensión del archivo y comprimirlo. Ejemplo: Word.exe reemplazar por archivo comprimido en formato [zip, rar, tar, gpzip, entre otros] Word.zip, cuando se descomprima el archivo se deberá agregar la extensión [.exe] nuevamente.

- Tenga como buena práctica antes de enviar o abrir archivos por correo electrónico, examinar con el software antivirus cada uno de estos para prevenir propagación de códigos maliciosos al interior de la red de datos CMP.
- Tenga en cuenta siempre llenar el campo del asunto del encabezado del correo electrónico, ser consciente del contenido y compresión de los archivos adjuntos, además de verificar y validar el correo del destinatario.

9.7 DE LAS NORMAS BÁSICAS DE ETIQUETA PARA EL USO DEL CORREO ELECTRÓNICO

- Asegúrese que el campo asunto (subject) del correo no vaya en blanco, debe de contener una breve descripción del contenido del mensaje clara, directa y sencilla.
- El contenido del correo electrónico debe ser conciso, coherente, correcto y respetuoso al destinatario.
- Se debe de utilizar un lenguaje apropiado que represente el profesionalismo de nuestra Institución. Entiéndase que no debe ofender o incitar actitudes en contra de los intereses de la Contraloría Municipal de Pereira o de sus funcionarios o cualquier ente externo.
- Sea puntual en sus solicitudes y preguntas, una buena práctica es numerarlas, para que el destinatario pueda ser objetivo en sus respuestas.
- Al momento de redactar el mensaje hágalo sin involucrar emociones, debido a que en el lenguaje escrito se pueden presentar malas interpretaciones; de igual forma se debe evitar **escribir en mayúscula sostenida,** debido que es interpretado entre los internautas cómo lenguaje ofensivo (grito o regaño). Sí lo que se desea es hacer énfasis en un tema específico, se deberá utilizar la mayúscula sostenida con comillas o resaltado con negrita o subrayado. Debe ser discreto en el uso de los signos de puntuación e ideas si se está comunicando en otro idioma diferente.
- Lea detenidamente los correos electrónicos antes de ser enviados, para asegurarse que transmiten la idea correcta al destinatario, evite utilizar abreviaturas o modismos.
- Utilice en el contenido del mensaje formalismos de profesión, nombre y apellidos completos, cargo que representa y empresa del destinatario.
- Sea prudente al utilizar el campo “para”, CC, CCO, (Copia, copia oculta) puesto que, en muchas ocasiones, este tipo de prácticas colapsa el servidor de correo y pone en aprietos la toma de decisiones (Saturación del servicio). Absténgase de reenviar correos a varios destinatarios o a grupos de correo, si el asunto o contenido de este no es importante para el conocimiento de varias personas o funcionarios de la entidad
- Todos los correos deben de incluir una firma que incluya los siguientes datos: nombre completo, cargo, área o dirección donde labora. Se sugiere incluir el número telefónico y algún otro medio alterno de comunicación para contactarlo.

- Antes de enviar un correo verifique y valide con la Oficina de Tecnologías de la Información la capacidad máxima para el envío de archivos en megas, con el fin de no exceder está capacidad y generar congestión en el servidor de correos. De ser un archivo grande consulte si puede enviar fraccionado el archivo o utilizar una herramienta para compartir archivos en nube.
- Se recomienda hacer carpetas y establecer reglas para guardar los mensajes por destinatarios.
- Se recomienda depurar cada sesenta [60] días el cliente de correo electrónico, con el fin de no ocasionar saturación de los buzones de correo en el servidor de correo, buscando optimizar el espacio de este.

9.8 DE LAS RECOMENDACIONES A LA HORA DE RECIBIR MENSAJES

Sea crítico con el servicio de correo, aplique algunas reglas de sentido común si:

- El remitente es desconocido
- El campo Asunto no tiene sentido
- El correo contiene un enlace, y usted no está seguro a dónde le direccionará en Internet
- El correo electrónico como tal es sospechoso.
- El correo electrónico contiene un adjunto sospechoso.
- El correo electrónico parece ser de un vendedor de software con un programa adjunto que dice ser una actualización de seguridad. Los fabricantes de software nunca envían actualizaciones de seguridad como correo electrónico distribuidos masivamente.
- Usted nunca debe responder a los mensajes spam.

Podrá denegarse el acceso a los servicios de correo electrónico e inspeccionar, monitorear y cancelar una cuenta de correo:

- Cuando haya requerimientos legales que lo exijan.
- Cuando por orden de Contralor se dé la instrucción previa sospecha fundada de violación de la política interna de la institución, como comercio electrónico, solicitudes inapropiadas, falsificación de direcciones, amenazas etc.
- Cuando por razones de investigación disciplinaria la autoridad principal de la entidad así lo disponga.

9.9 DE LA DECLINACIÓN DE RESPONSABILIDADES – CORREO ELECTRÓNICO

Las opiniones que contenga este mensaje son exclusivas de su autor y no necesariamente representan la opinión oficial de la CONTRALORÍA MUNICIPAL DE PEREIRA o de sus autoridades. El receptor deberá verificar posibles virus informáticos que tenga el correo electrónico o cualquier anexo a él, razón por la cual la CONTRALORÍA MUNICIPAL DE PEREIRA, no es responsable de los daños causados por cualquier virus transmitido en este correo electrónico. La información contenida en este mensaje y en los archivos electrónicos adjuntos es confidencial y reservada, conforme a lo previsto en la Constitución y en las políticas de la CONTRALORÍA MUNICIPAL DE PEREIRA, y está dirigida exclusivamente a su destinatario, sin la intención de que sea revelada o divulgada a otras personas. El acceso al contenido de esta comunicación por cualquier otra persona diferente al destinatario no está autorizado por la CONTRALORÍA MUNICIPAL DE PEREIRA y está sancionado de acuerdo con las normas legales aplicables. El que ilícitamente sustraiga, oculte, extravíe, destruya, intercepte, controle o impida esta comunicación, antes de que llegue a su destinatario, estará sujeto a las sanciones penales correspondientes.

Igualmente, incurrirá en sanciones penales el que, en provecho propio o ajeno o con perjuicio de otro, divulgue o emplee la información contenida en esta comunicación. En particular, las personas que reciban este mensaje están obligadas a asegurar y mantener la confidencialidad de la información contenida en el mismo y en general a cumplir con los deberes de custodia, cuidado, manejo y demás previstos en la Ley. Si por error recibe este mensaje, le solicitamos enviarlo de vuelta al, correo electrónico institucional de la CONTRALORÍA MUNICIPLA DE PEREIRA a la dirección de correo electrónico que se lo envió y borrarlo de sus archivos electrónicos o destruirlo.

9.10 DE LAS RESPONSABLIDADES ASOACIADAS A LA PROPAGACIÓN DE VIRUS

La entidad declina cualquier responsabilidad derivada de la propagación de virus y gusanos informáticos a través del correo electrónico, siendo responsabilidad del usuario, el tomar las medidas necesarias para evitar la infección y sus consecuencias; entre las medidas se incluyen:

- Está prohibido abrir ficheros adjuntos en mensajes de correo no solicitados, aunque procedan de remitentes conocidos.
- Mantener actualizado el software antivirus en el equipo de cómputo y activar los módulos de escaneo automático para protección de identidad en línea, antispam, antispyware, correo electrónico y redes sociales.

- Efectuar copias de seguridad periódicas de los programas, datos y configuraciones del equipo de cómputo asignado.

Las principales causas de virus en la red son ocasionadas por los servicios de correo electrónico y el uso indebido de éste

9.11 SERVICIO DE PUBLICACIÓN EN LA PÁGINA WEB INSTITUCIONAL

La publicación de la información en la página web institucional, se regirá por la directiva presidencial número 002 de 2000 “Políticas y Estándares para Publicar Información del Estado en Internet" y en concordancia a esta norma, se publica en la página web, la información que remitan los líderes de proceso quienes son los encargados de mantener la actualidad de los contenidos

En cumplimiento de la Ley de Transparencia y Acceso a la Información Pública, la Contraloría Municipal de Pereira publicara toda la información oficial que se emite dentro la misión institucional.

El técnico operativo de la Oficina de Tecnologías de la Información CMP es quien carga y actualiza la información remitida por los líderes de procesos responsables de la administración de contenidos, de la veracidad e idoneidad de las fuentes.

La información debe ser entendible, de fácil lectura, vigente, veraz, relevante, verificable y completa.

No se deben usar abreviaturas, ni tecnicismos (sólo los estrictamente necesarios)

El asesor de Control Interno y el responsable de la Oficina de Tecnologías de la Información CMP solicitarán informe al técnico del área responsable de las publicaciones, sobre los contenidos de la página web y se presentará informe ante el comité de dirección. Cada líder de proceso es responsable de mantener al día la información publicada en su sección y en la sección de Transparencia y Acceso a la Información.

La información publicada (texto, imágenes o videos), deberá mantener la fuente u origen de esta a fin de preservar los derechos de autor.

Dentro de la página web sólo se publicará lo pertinente a la entidad y sus actores (preservando la intimidad de estos), la misión, visión, organigrama, funciones por área, la normatividad que la rige, informes, contactos, guías para el usuario.

La página web contiene un espacio donde se puede realizar peticiones quejas y reclamos sobre el actuar de la administración, pública, su manejo es responsabilidad de la dirección de participación en cabeza del líder del proceso.

Las peticiones, quejas y reclamos deberán ser atendidas por el funcionario del área de participación ciudadana en cumplimiento del artículo 23º y 74º de la Constitución Política Colombiana y seguirá el trámite contemplado en el manual de procesos y procedimientos de la Contraloría Municipal de Pereira y en los términos que establece la Ley

9.12 SERVICIO DE COPIAS DE SEGURIDAD O DE RESPALDO

La Oficina de Tecnologías de la Información CMP es responsable de mantener copia de respaldo de la información contenida en las estaciones de trabajo y portátiles de la entidad teniendo una cuenta que existen un enlace permanente entre la carpeta creada por el por la oficina de tecnología de la Información y el dispositivo NAS que guarda toda la información en tiempo real; el técnico operativo accede cada fin de mes a la NAS para extraer una copia de cada carpeta de las estaciones de trabajo en red con el fin de almacenarla en disco duro extraíble y enviarla a el archivo histórico de la entidad que actualmente se encuentra ubicado en bodega del Estadio Hernán Ramírez Villegas. El disco extraíble se entrega al responsable de la ventanilla única para su inmediato envío a la bodega cumpliendo con las reglas establecidas en el Plan de contingencia del área de Tecnología de la Contraloría Municipal de Pereira.

Cada usuario es responsable de mantener copia de respaldo de la información que procesa en el ejercicio de sus funciones y cuando se encuentre en comisión fuera de la Contraloría o trabajo en casa. Sin embargo, entendiendo que estos documentos son propiedad de la CMP, cada funcionario deberá almacenar la información en la carpeta establecida para que se guarde en el dispositivo de red NAS luego deberá reportar a la Oficina de TI y al líder de procesos. Esta labor debe ejecutarla cada dos meses, o cuando culmine su proceso auditor.

De igual manera los contratistas que ejerzan labor específica en la entidad, deberán entregar toda la información procesada digital o analógicamente al supervisor o interventor del contrato.

Nota: Sólo se realiza copia de seguridad a la información contenida dentro de la carpeta de la vigencia actual que debe estar almacenada en la carpeta “Mis documentos” del perfil del responsable de la máquina.
La Oficina de Tecnologías de la Información CMP no se hará responsable de la información que el usuario almacene fuera de la carpeta principal “Mis Documentos”.

Las copias de seguridad de los equipos portátiles se realizarán cada vez que el equipo ingrese a la red wi-fi de la CMP.

Para la recuperación de información contenida en las copias de seguridad el funcionario que así lo requiera, deberá diligenciar el formato FO 1.2.3.1-3 “SOLICITUD DE INFORMACION EN COPIA DE SEGURIDAD”.

La Oficina de Tecnologías de la Información CMP deberá mantener un duplicado de cada uno de los programas pertenecientes a la entidad.
Los medios como fuentes al igual que las copias de respaldo y las licencias de software, deberán estar custodiados por la Oficina de Tecnologías de la Información CMP.

Las copias de seguridad para las bases de datos y de los servidores virtuales quedaran almacenadas dentro de la NAS para uso de contingencia en caso de falla.

10. LA GESTIÓN DE DOCUMENTOS ELECTRÓNICOS

Definición: se define como la información generada, enviada, recibida, almacenada y comunicada por medios electrónicos, ópticos o similares.

El Comité de Archivo junto con el área de Gestión Documental o quien haga sus veces, debe establecer un programa para la gestión de documentos y expedientes electrónicos y contemplar dichos componentes dentro de la arquitectura de Información de la institución.

Al existir diversas referencias y definiciones relacionadas, es importante tener claridad en los siguientes conceptos:

Mensaje de datos: Información generada, enviada, recibida, almacenada, comunicada por medios electrónicos, ópticos o similares, entre otros. Por lo general, se extiende a comunicaciones efectuadas mediante el Intercambio Electrónico de Datos (EDI), Internet y el correo electrónico.

Equivalencia entre documento electrónico y mensaje de datos*:* Como puede inferirse de las definiciones anteriores, existe una equivalencia entre la definición de documento electrónico y mensaje de datos, teniendo en cuenta que su estructura conceptual indica que es toda “información generada, enviada, recibida, almacenada y comunicada por medios electrónicos, ópticos o similares”.

Aclaración: Todos los documentos electrónicos son mensajes de datos, pero NO todos los mensajes de datos son documentos electrónicos de archivo.

Documento Electrónico de Archivo: Es el registro de información generada, recibida, almacenada y comunicada por medios electrónicos, que permanece en estos medios durante su ciclo vital; es producida por una persona o entidad en razón de sus actividades y debe ser tratada conforme a los principios y procesos archivísticos.

10.1 CLASES DE DOCUMENTOS ELECTRÓNICOS

Los documentos electrónicos pueden clasificarse de acuerdo con ciertos criterios, por ejemplo:

*Por su forma de creación****,*** que se divide en documentos nativos electrónicos, cuando han sido elaborados desde un principio en medios electrónicos y permanecen en estos durante toda su vida o documentos electrónicos digitalizados, cuando se toman documentos en soportes tradicionales (como el papel) y se convierten o escanean para su utilización en medios electrónicos.

Por su origen, ya que pueden ser hechos por la administración pública o presentados por los ciudadanos, empresas y organizaciones.

*Por su formato****,*** pues encontramos documentos ofimáticos, cartográficos, correos electrónicos, imágenes, videos, audio, mensajes de datos de redes sociales, formularios electrónicos, bases de datos, entre otros. Respecto a estos formatos se presentan a continuación una serie de recomendaciones para su buen manejo.

Documento Ofimático: Documentos de procesadores de texto, hojas de cálculo, gráficos, etcétera, que son producidos con distintos programas o paquetes de software y en diferentes versiones de un mismo software.

Cartográficos: Mapas y planos, algunos de ellos con valores históricos y en muchos casos artísticos. Estos documentos, debido a su naturaleza y origen, deben ser tratados de manera específica (utilizar un escáner especial, metadatos particulares, entre otros).

Correo Electrónico Institucional: El correo electrónico (e-mail) es uno de los servicios más usados en Internet que permite el intercambio de mensajes entre las personas conectadas a la red, de manera similar a como funcionaba el correo tradicional. Básicamente es un servicio que nos permite enviar mensajes a otras personas de una forma rápida y económica, facilitando el intercambio de todo tipo de archivos, dando clic en el link “adjuntar” que aparece en pantalla.

Los documentos que se adjuntan comienzan a ser nombrados como documentos electrónicos de archivo, debido a que incorporan información de alto valor, que sirve de soporte y evidencia para las entidades. Constituye un tipo de documento en el que con mayor frecuencia se incluyen datos de gran valor documental.

Imágenes, Audios y Videos: Los archivos creados en estos tipos de formatos se admiten como pruebas en el sistema judicial colombiano, cumpliendo con las normas que establezca el Gobierno Nacional.

Mensajes generados en redes sociales: En algunos casos este tipo de mensajes pueden ser utilizados dentro de algún proceso llevado a cabo por la administración (Twitter, Facebook, Instagram, entre otros). En el caso de la Contraloría Municipal de Pereira, las redes sociales son medios efectivos de comunicación con la ciudadanía y son utilizados para que la comunidad pereirana pueda formular solicitudes, peticiones, quejas reclamos y felicitaciones, adoptadas por el Sistema de Gestión de Calidad una vez se declaró la emergencia sanitaria Covid-19.

Formularios Electrónicos: Formatos que pueden ser diligenciados por los ciudadanos para realizar trámites en línea. Por ejemplo: “Formularios de contacto” o “Formularios para peticiones, quejas y reclamos”.

Bases de datos: Colección datos afines, relacionados entre sí y estructurados de forma tal que permiten el rápido acceso, manipulación y extracción de ciertos subconjuntos de esos datos por parte de programas creados para tal efecto o lenguajes de búsqueda rápida.

Página web: Una página web está compuesta principalmente por información (texto y/o módulos multimedia), así como por hipervínculos. Además, puede contener o asociar datos sobre el estilo que debe tener y cómo debe visualizarse y también aplicaciones “embebidas” con las que se puede interactuar para hacerlas dinámicas.

10.2 CARACTERÍSTICAS DEL DOCUMENTO ELECTRÓNICO

De acuerdo con la Norma NTC/ISO 15489-1 para que sirvan de apoyo a la gestión de las entidades y puedan servir de prueba, los documentos electrónicos deben poseer ciertas características a saber:

Autenticidad. Que pueda demostrarse que el documento es lo que afirma ser, que ha sido creado o enviado por la persona que afirma haberlo creado o enviado, y que ha sido creado o enviado en el momento que se afirma.

Para garantizar la autenticidad de los documentos, las entidades deben implantar y documentar políticas y procedimientos para el control de la creación, recepción, transmisión, mantenimiento y disposición de los documentos, de manera que se asegure que los creadores de los mismos estén autorizados e identificados y que los documentos estén protegidos frente a cualquier adición, supresión, modificación, utilización u ocultación no autorizadas.

Integridad. Hace referencia al carácter completo e inalterado del documento electrónico. Es necesario que un documento esté protegido contra modificaciones no autorizadas. Las políticas y los procedimientos de gestión de documentos deben decir qué posibles anotaciones o adiciones se pueden realizar sobre el mismo después de su creación y en qué circunstancias se pueden realizar. No obstante, cualquier modificación que se realice, debe dejar constancia para hacerle su seguimiento.

Fiabilidad. Su contenido representa exactamente lo que se quiso decir en él. Es una representación completa y precisa de lo que da testimonio y se puede recurrir a él para demostrarlo. Los documentos de archivo deben ser creados en el momento o poco después en que tiene lugar la operación o actividad que reflejan, por individuos que dispongan de un conocimiento directo de los hechos o automáticamente por los instrumentos que se usen habitualmente para realizar las operaciones.

Disponibilidad. Se puede localizar, recuperar, presentar, interpretar y leer. Su presentación debe mostrar la actividad que lo produjo. Los contextos de los documentos deben ser suficientemente claros y contener la información necesaria para la comprensión de las operaciones que los crearon y usaron. Debe ser posible identificar un documento en el contexto amplio de las actividades y las funciones de la organización. Se deben mantener los vínculos existentes entre los documentos que reflejan una secuencia de actividades.

En toda actuación administrativa o judicial, no se negará eficacia, validez o fuerza obligatoria y probatoria a todo tipo de información en forma de un mensaje de datos, por el sólo hecho que se trate de un mensaje de datos.

El mensaje de datos debe recibir el mismo tratamiento de los documentos consignados en papel, es decir, debe dársele la misma eficacia jurídica, por cuanto el mensaje de datos comporta los mismos criterios de un documento.

El Artículo 11 de la Ley 527 de 1999, define las características esenciales para valorar la fuerza probatoria de los mensajes de datos o documento electrónico, así:
La confiabilidad en la forma en que se haya generado.

La confiabilidad en la forma en que se haya archivado.
La confiabilidad en la forma en que se haya comunicado el mensaje.
La confiabilidad en la forma en que se haya conservado.
La integridad de la información.
La forma en la que se identifique a su iniciador.

Documento Digitalizado: Consiste en una representación digital, obtenida a partir de un documento registrado en un medio o soporte físico, mediante un proceso de digitalización. Se puede considerar como una forma de producción de documentos electrónicos, realizada con los siguientes objetivos principales:

Consulta: cuando sirve para permitir el acceso a la información.
Trámite: cuando sirve de apoyo a la gestión administrativa. Incorpora técnicas estándares y procedimientos que permiten garantizar las características de autenticidad, integridad y disponibilidad que se definen en el documento "Protocolo de digitalización de la información".

Como medida de seguridad, ya sea con fines de copia de seguridad o contingencia, para lo cual se deberán analizar y determinar los aspectos jurídicos y técnicos para cuando se refiera a una copia exacta de los documentos originales, como por ejemplo el establecimiento de un procedimiento de digitalización certificada que se utiliza para el caso de digitalización del archivo histórico de la entidad.

Es importante mencionar que la digitalización de documentos de ninguna manera implica la eliminación o "destrucción" física de los originales. El Archivo General de la Nación establece en el parágrafo del artículo 18 del Acuerdo 003 de 2015 que: "Los procesos de digitalización en ningún caso podrán aumentar o disminuir los tiempos de retención documental establecido en las Tablas de Retención Documental, así como tampoco podrán destruirse documentos originales con el argumento de que han sido digitalizados".

Los documentos originales que posean valores históricos NO podrán ser destruidos, aun cuando hayan sido reproducidos y/o almacenados mediante cualquier medio. (Parágrafo 2º del artículo 19, de la ley 594 de 2000. "Soporte documental".

Nota: Si el documento desde su origen es digital no implica que deba ser trasladado a físico, siempre y cuando se conserven las características de Documento Electrónico

10.3 ESTRUCTURA DEL DOCUMENTO ELECTRÓNICO

Los documentos electrónicos cuentan con una estructura física que hace referencia al hardware, software y formato usados para su creación, y una estructura lógica que hace referencia al contenido, a los datos de identificación y a los metadatos con los que es creado el documento.

Contenido: Es la materia del documento electrónico, es decir, el conjunto de datos e información del documento. Dependiendo del formato en el que se cree será la forma definitiva del documento.

Firma del documento electrónico: El artículo 7° de la Ley 527 de 1999 establece que "cuando cualquier norma exija la presencia de una firma o establezca ciertas consecuencias en ausencia de la misma, en relación con un mensaje de datos, se entenderá satisfecho dicho requerimiento si:

a) Se ha utilizado un método que permita identificar al iniciador de un mensaje de datos y para indicar que el contenido cuenta con su aprobación;
b) Que el método sea tanto confiable como apropiado para el propósito por el cual el mensaje fue generado o comunicado".

En Colombia se han reglamentado dos mecanismos de firma: la firma electrónica y la firma digital.

La firma electrónica corresponde a métodos tales como códigos, contraseñas, datos biométricos o claves criptográficas privadas, que permitan identificar a una persona en relación con un mensaje, siempre y cuando el mismo sea confiable y apropiado respecto de los fines para los que se utiliza la firma, teniendo en cuenta todas las circunstancias del caso, así como cualquier acuerdo pertinente.

La firma digital es un valor numérico que se adhiere a un mensaje de datos y que, utilizando un procedimiento matemático conocido, vinculado a la clave de quien origina el mensaje y al texto que contiene, permite determinar que este valor se ha obtenido exclusivamente con clave iniciador y que el mensaje inicial no ha sido modificado después de efectuada la transformación.

Esta firma digital está basada en un certificado reconocido y generada mediante un dispositivo seguro de creación.

La firma digital tiene, respecto de los datos consignados en forma electrónica, el mismo valor que la firma manuscrita en relación con los consignados en papel.

La legislación colombiana actualmente lo establece en la Ley 527 de 1999 - Por medio de 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. Modificada después por el Decreto 19 de 2012 Por el cual se dictan normas para suprimir o reformar regulaciones, procedimientos y trámites innecesarios existentes en la Administración Pública.

Más adelante se expide el Decreto 2364/2012 - Establece la reglamentación del artículo 7º de la Ley 527 de 1999, complementando el marco jurídico de los mecanismos de autenticación previstos en Colombia. Y luego se expide el Decreto Legislativo 491 del 28 de marzo de 2020 - Por el cual se adoptan medidas de urgencia para garantizar la atención y la prestación de los servicios por parte de las autoridades públicas y los particulares que cumplan funciones públicas y se toman medidas para la protección laboral y de los contratistas de prestación de servicios de las entidades públicas, en el marco del Estado de emergencia económica. Y el Decreto 1287 del 24 de septiembre de 2020 - Por el cual se reglamenta el Decreto Legislativo 491 del 28 de marzo de 2020, en lo relacionado con la seguridad de los documentos firmados durante el trabajo en casa, en el marco de la emergencia sanitaria.

10.4 ACERCA DE LA VALIDEZ DE LAS FIRMAS ESCANEADAS EN COLOMBIA

En el contexto de la situación ocasionada por el Covid-19, donde el distanciamiento social se hace necesario y el uso de la tecnología se vuelve aún más imprescindible que antes, la forma de hacer negocios también sufre cambios. Esto es especialmente cierto en nuestro país, donde estamos acostumbrados a las formas y a las formalidades.

Con la nueva dinámica social que supone el Covid-19, las compañías están adaptando sus prácticas comerciales y para muchos surge la pregunta sobre si una firma escaneada es válida en Colombia.

La legislación nacional contempla dos tipos de firmas electrónicas: la firma electrónica propiamente dicha y la firma digital.

Es cierto que ninguna de estas definiciones contiene el término “firma escaneada”, por lo se opina que un contrato compartido en formato PDF con firmas escaneadas, no contiene firmas válidas. Sin embargo, según se indicó, en norma, la firma electrónica puede consistir en datos biométricos que permitan identificar a una persona. Los datos biométricos más conocidos son el rostro, la huella digital y el iris. Pero también existen datos biométricos de comportamiento como el tono de voz y la escritura.

Así pues, la firma manuscrita, independientemente de que sea original o escaneada es un dato biométrico, pues es un rasgo que permite identificar a una persona.

Quiere decir que al firmar un contrato y escanearlo, o al incluir la firma escaneada en el contrato, para luego compartirlo vía correo electrónico, dicha firma escaneada puede ser considerada como un tipo de firma electrónica bajo la legislación colombiana.

La Corte Suprema de Justicia ha indicado que la firma electrónica puede comprender las firmas escaneadas, sosteniendo que “todo dato que en forma electrónica cumpla una función identificadora, con independencia del grado de seguridad que ofrezca, puede catalogarse como firma electrónica.” Según el Decreto 2364/2012, la firma electrónica contenida en un mensaje de datos tendrá la misma validez y efectos jurídicos que la firma manuscrita, si aquella es igualmente confiable y apropiada para los fines con los cuales se generó o comunicó ese mensaje, a la luz de todas las circunstancias del caso, incluido cualquier acuerdo entre las partes contratantes.

Así, salvo que la ley exija una formalidad particular (por ejemplo, en el caso de procesos ejecutivos, donde el título ejecutivo debe ser presentado en original con firma manuscrita), las partes pueden válidamente acordar que su contrato, será firmado con firmas escaneadas y tales firmas tendrán la misma validez y efectos jurídicos que la firma manuscrita.

En resumen, el Art. 11 del Decreto Legislativo 2364 de 2012 se expresa en relación a las firmas de los actos, providencias, decisiones y la misma Sentencia C-242 del 9 de julio de 2020, señaló que la autorización para el uso de firmas mecánicas, digitalizadas y escaneadas es una medida temporal que permite la consecución de un fin superior de la sociedad, como el adecuado funcionamiento de la administración, que la misma tiene

concordancia con la habilitación del trabajo en casa, por cuanto permite que los servidores no tengan que desplazarse en forma presencial a las entidades.

10.5 METADATOS DEL DOCUMENTO ELECTRÓNICO

Los metadatos son los datos que describen el contexto, el contenido y la estructura de los documentos del archivo y su gestión a lo largo del tiempo

Definición de Metadatos.

Se definen los metadatos como los datos que describen otros datos, tal como su prefijo lo indica, y, de acuerdo a La Norma UNE-ISO 15489-1 se los define “como datos que describen el contexto, contenido y estructura de los documentos, así como su gestión a lo largo del tiempo”. Por ende, los metadatos resumen información básica sobre los datos, lo que puede facilitar la búsqueda y el trabajo con instancias particulares de datos.

Los metadatos se utilizan para:

- Correspondencia de entrada y salida.
- Correos electrónicos.
- Informes.
- Transcripciones.
- Contenidos digitales
- Manuales técnicos o administrativos.
- Registros de audio.
- Fotografías
- video
- imágenes gráficas digitales.
- Operaciones sobre de bases datos
- páginas web

Los metadatos se pueden crear manualmente o ser añadidos a los archivos electrónicos mediante el procesamiento de información automatizada. La creación manual tiende a ser más precisa, lo que permite al usuario ingresar cualquier información que considere relevante o necesaria para ayudar a describir el archivo. La creación automatizada, sin embargo, tiende a tener información más simplificada, pudiendo ser esta, el tamaño del archivo, la extensión del archivo, fecha de creación y quién lo creó. Es por tanto menester indicar, que para preservar o distribuir el material documental y, que los elementos archivísticos se desplacen, se divulguen, se consulten ampliamente, es necesario el uso de metadatos para la actividad de normalización descriptiva en archivos, dado que, estos proveen la cadena de custodia para los documentos, con lo cual se garantiza su autenticidad, integridad y fiabilidad.

10.6 LOS METADATOS PARA LA GESTIÓN DE DOCUMENTOS

De acuerdo con la norma UNE-ISO 23081-1: 2008 los metadatos son “información estructurada o semiestructurada que posibilita la creación, registro, clasificación, acceso, conservación y disposición de los documentos a lo largo del tiempo”. Los metadatos incluyen una amplia información que se puede utilizar para identificar, autenticar y

contextualizar los documentos, las personas, los procesos de negocio, la regulación y sus relaciones.

Existen dos momentos claves para la asignación de los metadatos; el primero de ellos en la creación del documento, en donde, se asignan para identificar el contexto y el control en la gestión del documento; el segundo es posterior a la creación en donde se generan nuevos metadatos de acuerdo al uso y contexto en el desarrollo del ciclo de vida del documento.

Importancia de los Metadatos: En las instituciones y organizaciones se gestionan una infinidad de documentos físicos, análogos, electrónicos y digitales, los cuales necesitan de información contextual que ayude a su entendimiento, uso, acceso y gestión durante su ciclo de vida. Esta información contextual son los metadatos, los cuales permiten asegurar la autenticidad, integridad, fiabilidad, usabilidad y valor probatorio de los documentos.

El implementar un esquema de metadatos en una organización trae como beneficios:

- La buena gestión de sus documentos en los sistemas de información, permitiendo a los documentos apoyar los procesos de trabajo y cumplir con los procesos de gestión documental.
- Proporcionar vínculos entre los documentos y su contexto de creación, con el fin de que estos sean auténticos, íntegros, confiables, usables y con valor probatorio.
- Intercambiar información entre sistemas (Interoperabilidad), permitiendo reconocer, procesar y usar documentos creados en otros entornos.
- Cumplir con los requisitos legales y evitar o mitigar riesgos a partir de la autenticidad, confiabilidad e integridad de los documentos.
- Aumentar la calidad de la información y reducir los costos de recuperación de los documentos.
- Reducir el riesgo del acceso no autorizado a los documentos, permitiendo asegurar la trazabilidad y protección de estos.
- Fortalecer la continuidad de negocio, asegurando que, sin importar los cambios administrativos, de procesos, de responsabilidades, entre otros; los documentos son identificados y transferidos a nuevos sistemas, áreas o responsables.
- Facilitar los procesos de conversión, migración y conservación a largo plazo de los documentos electrónicos.

10.7 MODELO DE METADATOS PARA LA GESTIÓN DE DOCUMENTOS

La organización debe definir los requisitos para diseñar e implementar los metadatos para la gestión de documentos y como estos interactúan con los sistemas de

información; estos requisitos deberían establecerse a partir de la identificación del entorno legal y reglamentario, los riegos asociados a los procesos y las necesidades.

El diseño e implementación de metadatos, conlleva a que las instituciones definan los roles y responsabilidades de las personas y establezcan un esquema de metadatos.

Modelo Conceptual de Metadatos

Para la creación de un esquema de metadatos se hace necesario definir previamente el modelo conceptual, el cual permite desarrollar descripciones de cada uno de los elementos que lo integran. Para la gestión de documentos, el modelo conceptual de metadatos se encuentra integrado por entidades y relaciones.

Entidades: Las entidades representan los principales componentes que permiten comprender el entorno de las actividades de gestión de la entidad u organización, entre estos se encuentran incluidos los documentos. Las entidades son el elemento principal para la definición del esquema de metadatos para la gestión de documentos.

Relaciones: Son importantes para el modelo conceptual de metadatos porque permiten contextualizar la entidad o sujeto documento; se hace necesario que se evidencien las relaciones entre entidades, de tal manera que estas se encuentren vinculadas al documento a través de los metadatos, otorgándole valor probatorio, demostrando la ejecución de actividades y quienes participaron en la producción y uso del mismo.

Modelo Entidad Relación

El concepto entidad relación está muy arraigado en el desarrollo de bases de datos; de hecho, algunos lo conceptualizan como “una herramienta para el modelado de datos que permite representar las entidades relevantes de un sistema de información, así como sus interrelaciones y propiedades y, otros, como la “herramienta que permite representar de manera simplificada los componentes que participan en un proceso de negocio y el modo en el que estos se relacionan entre sí”.

¿Qué significa lo anterior? Simplemente, que el modelo entidad relación asocia a las entidades (personas, instituciones, sistemas, etc.) a partir de unas acciones o características específicas; por ejemplo, un vendedor con las ventas que ha efectuado. En consecuencia, a la hora de construir un esquema de metadatos para la gestión de documentos es importante identificar las entidades que participan en el desarrollo de los procesos administrativos y cómo estas se relacionan entre sí, determinar los metadatos que describen la relación y los eventos generados a partir de ella.

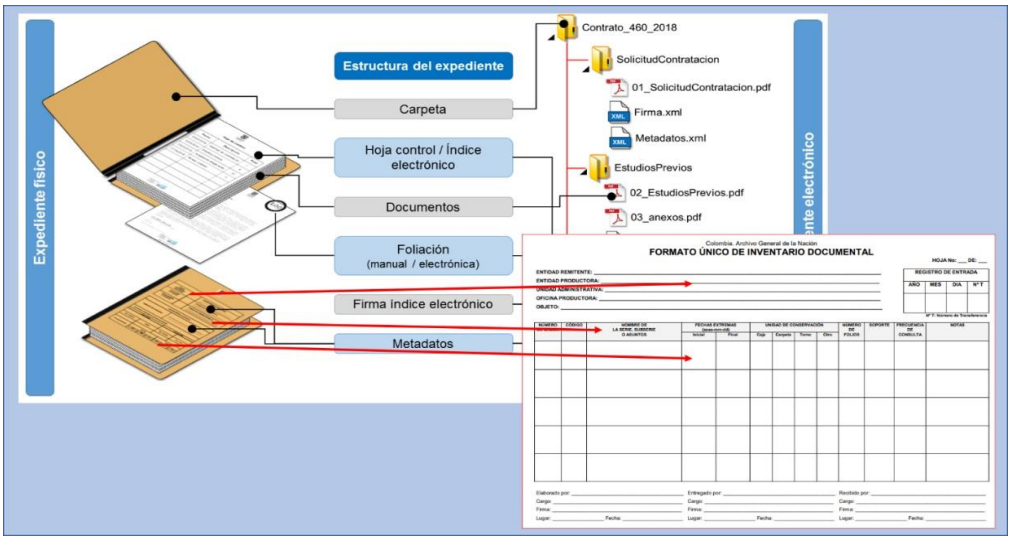
Evento: Es una actividad que se genera para cumplir una función y se gestiona mediante un flujo de un sistema de información generalmente activado por un usuario. Es importante tener presente que en un evento se deben conservar los metadatos sobre

la función que se realizó, cuándo se realizó, quién la realizó, las entidades participantes, y qué metadatos fueron modificados, entre otros. Ello significa que es una acción realizada por un Agente sobre una Entidad, en un instante de tiempo determinado y que produce un resultado. Por ejemplo, un documento es firmado, un usuario es creado en el sistema, un expediente es cerrado.

El Archivo General de la Nación de Colombia, indica que los metadatos sirven para describir el contexto de producción, el contenido y estructura de los documentos e incluso su gestión a lo largo del tiempo.

Un ejemplo, enfocado en los temas propios de la archivística, se encuentra en la elaboración de los inventarios documentales: en estos, es posible ingresar los datos sobre un expediente de manera estructurada de acuerdo a un esquema prestablecido, con el fin de probar la existencia del expediente, los documentos que lo conforman, el productor, entre otros, mediante el registro de sus metadatos que comprueban su autenticidad, integridad, fiabilidad y permiten su disponibilidad.

Metadatos de un expediente físico capturados manualmente en el esquema FUID



Fuente: Guía Esquema de Metadatos para Bogotá

De lo anterior se reafirma que los metadatos son datos (elementos de información) que identifican, caracterizan y contextualizan objetos del mundo físico o del mundo digital a los que denominamos Entidades.

10.8 FINES Y USOS DE LOS METADATOS EN LA GESTIÓN DE DOCUMENTOS

Con frecuencia se suele asociar los metadatos al momento de efectuar transferencias documentales, bien sea primarias o secundarias, y a la ejecución de procesos de descripción documental; sin embargo, es necesario señalar que, contrario a esta idea, los metadatos se producen desde el mismo momento en el cual se crean los documentos y se van incrementando durante su ciclo de vida, si bien en función de diversos propósitos y momentos tienen diferente utilidad.

Se identifican varios usos para los metadatos en la gestión de documentos: registrar aspectos propios del sistema(s) en el cual fueron producidos y gestionados los documentos (fechas de creación o modificación de un documento, el registro del software en el cual fue elaborado, el tiempo de edición, el tamaño, el autor o usuario que lo ha modificado; asociarlos con un contexto administrativo (productores, funciones, normas, agrupaciones documentales, eventos, reglas de negocio); localizarlos (ruta de almacenamiento); controlar su acceso (permisos, opciones de visualización y edición, descarga) y describir los aspectos necesarios para su preservación (formatos, políticas de migración, objetos relacionados, propiedad y derechos de uso).

Adicionalmente, los metadatos permiten la interoperabilidad a través de la definición de estructuras de metadatos, metadatos y elementos de metadatos compatibles entre aplicaciones en sistemas de información.

Los metadatos proveen la cadena de custodia para los documentos, misma que permite garantizar su autenticidad, integridad y fiabilidad. Esto se observa en el hecho de que los metadatos permiten establecer que el usuario que creó un documento tenía la competencia y permisos para hacerlo, y usó el formato definido por la entidad; o que un documento fue radicado en la fecha y hora que indica el rótulo, o que fue integrado a un expediente determinado en un instante de tiempo x, o que un expediente fue transferido al archivo central en un momento determinado bajo unas condiciones específicas.

Ahora bien, son tantos y tan diversos los metadatos, que se puede pensar en alguna forma de tipificarlos o agruparlos, con el fin de poder estudiarlos o estructurar un esquema de metadatos; sin embargo, esta tarea resulta compleja.
A continuación, se presentan varias propuestas de clasificación de metadatos en función de criterio, tales como:

Tabla 1 Grupos de metadatos para la gestión de documentos según NTC-ISO-23081-2

Grupo	Definición	Ejemplos

Grupo	Definición	Ejemplos
Identidad	Identifican la entidad	Tipo entidad, agrupación
Descripción	Representan la entidad para su uso	Título, resumen, clasificación
Uso	Facilitan el uso	Entorno técnico, derechos, lenguaje
Plan de eventos	Permiten la gestión de la entidad	Relaciones, desencadenantes de eventos, fecha y hora del evento
Historial de eventos	Documentan los eventos sobre la entidad y sobre sus metadatos	Fecha y hora del evento, descripción del evento
Relación	Asocian dos o más entidades	Identificador de la relación, fecha de la relación

En general, los metadatos generados por sistemas de información y aplicativos informáticos permiten identificar las características técnicas de producción de los documentos electrónicos, muchos de estos generalmente son embebidos automáticamente en los documentos por las aplicaciones o sistemas en los cuales son producidos.

11. DE LA SEGURIDAD DE LA INFORMACIÓN Y SEGURIDAD INFORMÁTICA

Los principales objetivos de control para cualquier sistema de información son entre otros, el de poseer una adecuada seguridad y confidencialidad de la información de acuerdo con su valor y sensibilidad; también es, el de mantener la integridad de la información procesada por las aplicaciones, con el fin de hacer uso apropiado de la misma y mantener la disponibilidad de la información procesada para la utilización de los usuarios autorizados de acuerdo con sus necesidades.

Para proteger la información y cualquier aplicación es necesario adoptar medidas de seguridad en varios niveles:

Físico: La localidad que contiene al área de sistemas de computadoras debe protegerse físicamente contra la penetración clandestina de intrusos. Se deben tener en cuenta las regulaciones establecidas en el numeral 3, Instructivo de seguridad física del presente documento.

El traslado de equipos de cómputo de la entidad siempre debe estar monitoreado por funcionarios de la Oficina de Tecnologías de la Información CMP.

Los equipos de cómputo sólo serán manipulados por funcionarios de la entidad, tampoco están autorizados para cambiar o alterar la configuración de estos, como perfil de usuario del sistema operativo, direccionamiento IP, nombre del equipo o grupo de trabajo en la red de datos, incluyendo controladores del sistema como [audio, video, tarjeta de red entre otros].

Ningún usuario está autorizado a abrir los equipos de cómputo y demás recursos informáticos, esta labor es exclusiva de los funcionarios Oficina de Tecnologías de la Información CMP.

Por seguridad los equipos de cómputo deben permanecer con las sesiones de inicio bloqueados (Ctrl + Alt + Sup), mientras el usuario no se encuentre al frente de la máquina.

El acceso a la Oficina de Tecnologías de la Información CMP está restringido para personas ajenas a la entidad y debe permanecer cerrada la puerta, mientras no se encuentren funcionarios del área.

11.1 UBICACIÓN DE LA OFICINA DE TECNOLOGÍAS DE LA INFORMACIÓN.

Los parámetros para tener en cuenta para la ubicación y operatividad de la Oficina de Tecnologías de la Información CMP son las siguientes:

- El área o espacio deberá tener una buena distribución entre los puestos de trabajo, que permita el fácil acceso, además de un perímetro principal para la evacuación en caso de una emergencia.
- La Oficina deberá estar equidistante al resto de oficinas de la entidad con el objetivo de prestar un mejor servicio para la atención de usuarios y en términos de logística para contingencias o suporte a equipos de cómputo, servidores y Centro de Datos.
- Deberá contar con la señalética adecuada informativa, de emergencias, evacuación, incluyendo un mapa del área y contar con acceso fácil a botiquín, camilla y extintor de incendios.
- Deberá contar con un sistema de suministro de energía no regulado de [110-120 V] en sus tomas, además de suministro de energía regulado UPS [110-120 V], con suministro hasta para 20 minutos, y protección para servidores, lo anterior debidamente identificados, de acuerdo con los puestos de trabajo.
- Deberá contar con cableado estructurado UTP Cat 6, faceplay Cat 6, debidamente identificado de acuerdo con los puestos de trabajo.

- El área o espacio deberá estar lo suficientemente iluminada, con buen flujo y tránsito de aire, además de un sistema de aire acondicionado de precisión, que permita mantener una temperatura constante para funcionarios y equipos de cómputo.
- Por motivos de protección y privacidad deberá contar con una puerta de acceso para limitar el acceso de personal no autorizado al área o personas ajenas a la misma.
- El área deberá estar segura de deslizamientos de tierra, fugas de agua, inundaciones o vulnerabilidad de incendios.
- El área deberá contar con protocolos para el ingreso y salida de personal de sus instalaciones, así como del Centro de Datos o espacios del rack de comunicaciones.

11.2 CONSIDERACIONES PARA TENER EN CUENTA OFICINA TI-CMP

Humano: Se debe tener cuidado al conceder autorización a los usuarios para reducir la probabilidad de que un intruso ingrese a la red de datos, sea de manera arbitraria o de modo autorizado.

El dueño de la información es responsable por la clasificación, aprobación de usuarios autorizados, privilegios de acceso, uso y disposición definitiva de la información. Sin embargo, toda la información que se procesa dentro del ejercicio del control fiscal es propiedad de la Contraloría Municipal de Pereira.

Si se requiere de niveles elevados de seguridad y no se posee el suficiente adiestramiento para limitar accesos, se debe recurrir a los funcionarios de la Oficina de Tecnologías de la Información, quienes se encargarán de aprovisionar y habilitar las políticas de restricción de acuerdo con la solicitud del usuario. En todo caso el usuario solicitante será el encargado de custodiar la clave.

Para limitar el uso de las estaciones y resguardar la información, el responsable del equipo podrá solicitar a la Oficina de Tecnologías de la Información, la habilitación de la clave de entrada al equipo y claves de acceso a la red, las cuales son personales e intransferibles; se recomienda cambiar periódicamente las claves de acceso.

Sistema Operativo: Aunque un sistema de base de datos esté bien protegido, si no se protege de forma adecuada el sistema operativo de los equipos de cómputo, éste puede servir para obtener acceso sin autorización a la base de datos. Dado que casi todos los sistemas de base de datos permiten acceso remoto a través de terminales o redes, la seguridad a nivel software dentro del sistema operativo es tan importante como la seguridad física.

El administrador de la red de datos es el responsable de crear los usuarios del dominio y de acuerdo con solicitud del jefe inmediato establecerá roles y perfiles de usuario con las restricciones a que haya lugar.

Una vez definido el usuario en el dominio se entregarán las claves de acceso a la red y se establecerá permiso para acceder a las aplicaciones teniendo en cuenta niveles jerárquicos.

En cada estación de trabajo con sistema operativo Windows XP o Windows 7 se configuran los perfiles de usuarios que corresponden al administrador de la red con acceso ilimitado al equipo y el usuario que es a quien se asigna la responsabilidad de uso de la máquina y tendrá perfil de administrador de la máquina. Los demás usuarios que se configuren tendrán acceso restringido al usuario principal y a algunos recursos del sistema.

Ningún equipo se conecta de manera remota salvo el autorizado por el funcionario responsable de la Oficina de Tecnologías de la información.

Sistemas de base de datos: Cada sistema de base de datos deberá contener una bitácora que permita determinar las responsabilidades de quienes maneja determinada cuenta con determinados roles; puede darse el caso de que algunos usuarios estén autorizados sólo para tener acceso a una porción limitada de la base de datos. Es posible también que a algunos usuarios se les permita hacer consultas, pero se les prohíbe modificar la base de datos. El sistema de base de datos tiene la responsabilidad de garantizar que no se violen estas restricciones y de que se mantenga activa la auditoria a estas actividades.

Dentro de las restricciones a establecer para la seguridad en los sistemas se incluyen:

- Protección de menús.
- Protección de funciones o transacciones.
- Protección de la consulta de datos o bases de datos.

La aplicación debe suministrar control para el acceso por medio de la utilización de códigos de identificación de los usuarios (ID) y métodos de autenticación como claves.

El software interactúa con las solicitudes para acceder a funciones de procesamiento computarizadas y que garantizan el acceso una vez se digite correctamente el nombre del usuario y la clave.

Un usuario puede tener varias formas de autorización, entre ellas se encuentran las siguientes:

- **Autorización de lectura:** capacidad para mirar la información permite consultar, pero no modificar.
- **Autorización de inserción:** que permite introducir datos nuevos, pero no modificar los ya existentes.
- **Autorización de actualización:** capacidad para cambiar información o programas, permite modificar la información, pero no permite la eliminación de datos.
- **Autorización de borrado:** que permite la eliminación de datos. El acceso de borrado puede ser permitido en el ámbito de archivo, registro o campo.
- **Autorización de Fusión:** capacidad de combinar información a partir de dos fuentes separadas.
- **Autorización de Ejecución:** capacidad para ejecutar una versión compilada de un programa.

Un usuario puede tener asignados todos, ninguno o una combinación de diferentes tipos de autorización anteriores dependiendo del perfil que tenga, para lo cual se deben revisar las descripciones del trabajo y las funciones que desempeña, con el fin de determinar si poseen la competencia, además de la experiencia necesaria para llevar a cabo responsabilidades asignadas.

Una vez determinado el perfil de usuario por parte del superior inmediato del mismo, se procede a solicitar la creación del usuario en el sistema y la asignación de los permisos, este debe realizase por escrito, además de ser dirigido al administrador del software.

El funcionario responsable de la Oficina de Tecnologías de la Información entrega personalmente al funcionario o contratista, las credenciales [nombre usuario y contraseña] que le permitirá acceder a la aplicación; dentro del mismo documento, se le especificaran las responsabilidades adquiridas con la información y con las contraseñas asignadas.

11.3 DE LA ADMINISTRACIÓN Y CONTROL DE CONTRASEÑAS DE ACCESO

La forma fundamental de autoridad y jerarquía de un sistema de información es aquella se confiere al administrador quien puede entre otras cosas autorizar y crear nuevos usuarios, reestructurar, modificar, borrar y proporcionar accesos. Esta forma de autoridad es análoga a la que se provee a un “súper-usuario” o al operador para el sistema operativo.
Al usuario al que se le ha concedido alguna forma de autoridad no se le permite pasar autoridad a otros usuarios.

El sistema de seguridad lógica debe ser administrado por un supervisor, esta administración debe mantener un registro para cada función asignada que tenga como mínimo:

Nombre del usuario
Fecha del último cambio de contraseña
Funciones asignadas
Nivel de acceso por categoría

Los sistemas de información deben poseer bitácoras de auditoría que permitan obtener trazabilidad con reporte de las actividades efectuadas en la estación de trabajo, éstas deben contener:

- Intentos denegados y permitidos del sistema.
- Intentos no autorizados de utilizar programas restringidos Salidas del sistema y tiempo de permanencia en el sistema.

Registro actualizado de todas las operaciones realizadas en el equipo Tiempos ociosos o libres.

Las aplicaciones que se operan en la CMP son propiedad intelectual de terceros, sin embargo, estas deben garantizar que contienen control de acceso y deben establecerse claramente estas condiciones en los contratos o convenios suscrito con la entidad.

LAS CONTRASEÑAS: Todo usuario registrado en la red será responsable de proteger su código de usuario y datos de cualquier acceso no autorizado y el uso indebido de las claves de acceso al equipo y red corporativa generará causal de mala conducta y su respectiva penalización.

Las contraseñas de seguridad de cada usuario deben tener como mínimo ocho [8] caracteres, incluyendo mayúsculas, números y un carácter especial, además no deben contener información acerca de la identidad del usuario. Las credenciales de acceso [usuario-contraseña] del sistema de información CMP, se recomiendan no hacer referencia a cuentas o datos personales usados en otros sistemas de información, como Facebook, correos electrónicos personales o bancarios.

La contraseña es secreta, personal e intransferible y no debe ser confiada a ninguna otra persona, el hacerlo, expone al usuario a las consecuencias por las acciones que terceros efectúen con esa contraseña, cada usuario es responsable por las transacciones realizadas con la misma.

El usuario no debe guardar su contraseña en una forma legible en archivos en disco, y tampoco debe escribirla en papel y dejarla en sitios donde pueda ser encontrada. Si, hay razón para creer que una contraseña ha sido comprometida, debe cambiarla inmediatamente. No deben usarse contraseñas que son idénticas o substancialmente similares a contraseñas previamente empleadas. Además, se recomienda como buena práctica dejar una copia de la contraseña con el administrador del sistema de información de la Oficina de Tecnologías de la Información CMP.

Los usuarios no deben intentar violar los sistemas de seguridad y/o control de acceso CMP. Acciones de esta naturaleza se consideran violatorias de las políticas de la confidencialidad de la información y causal de sanciones.

No se permite compartir ningún directorio sin especificar contraseña.

Ningún usuario podrá establecer contraseñas en el archivo Boot del setup en la BIOS de la máquina esta labor es estrictamente competencia de la oficina de tecnología de la información CMP.

11.4 DE LOS PROTOCOLOS PARA LA CREACIÓN, MODIFICACIÓN O SUSPENSIÓN DE PRIVILEGIOS DE ACCESO A LOS USUARIOS DEL SISTEMA DE INFORMACIÓN CMP

El jefe de cada dependencia debe solicitar por escrito al encargado de la Oficina de Tecnologías de la Información, la asignación de una contraseña, la modificación de privilegios de acceso o el retiro como usuario del sistema, para cada uno de funcionarios a su cargo que así lo requieran. Estas solicitudes se pueden generar en cada una de las siguientes situaciones:

Cuando se libera total o parcialmente una aplicación por parte de la Oficina de Tecnologías de la Información CMP. En este caso el funcionario encargado de dicha oficina debe hacer las recomendaciones pertinentes a los jefes de dependencia, respecto a la creación de nuevos usuarios de la aplicación y sus privilegios.
Cuando hay relevo del cargo de un funcionario que es usuario del sistema. El jefe de la dependencia deberá informar por escrito al responsable Oficina de Tecnologías de la Información CMP, el nombre del usuario saliente, el nombre, cargo del usuario que lo reemplazará, teniendo en cuenta no modificar la identificación, además de los privilegios del usuario, pero la contraseña y el alias si deben ser cambiados.

Cuando se requiere un nuevo usuario para una aplicación determinada, el funcionario debe suministrar al administrador del sistema los datos personales tales como el

nombre, número de cédula, fecha de nacimiento, cargo que desempeña teléfono y las funciones que va a desempeñar para establecer los privilegios de acceso.

Cuando sea necesario cambiar los privilegios de acceso para un usuario del sistema, el jefe de la dependencia debe especificar el nombre del usuario, su identificación, los privilegios de acceso que se deben eliminar y los que se deben crear.

Cuando se requiere eliminar un usuario del sistema. El funcionario encargado de la Oficina de Recursos Humanos debe notificar el retiro del funcionario de todos los servicios ofrecidos y de los accesos a los sistemas de información.

Los usuarios autorizados que van a ingresar por primera vez al sistema deben recibir inducción de un funcionario de la Oficina de Tecnologías de la Información CMP, quien indicará las políticas y condiciones de uso de la Tecnología de información disponible por la Contraloría Municipal de Pereira.

El encargado de la Oficina de Tecnologías de la Información CMP debe dar una breve inducción sobre aspectos tales como:

- Forma de ingresar y salir del sistema de información.
- Forma de ingresar y salir de los aplicativos CMP.
- Desplazamiento entre menús, funciones y opciones permitidos.
- Información sobre procedimientos efectuados, registro de operaciones, además se le indicarán los pasos a seguir en caso de requerir ayuda de tipo técnico.

Todo usuario respetará la naturaleza confidencial de datos o cualquier otra información que pueda estar en su poder, bien sea como parte de su trabajo o por accidente.

Queda estrictamente prohibido el uso, autorizado o no, de credenciales de acceso de usuario distinto al propio con el fin de evadir normas de control de recursos.

Toda responsabilidad derivada del uso indebido de credenciales de usuario distinto al propio recaerá sobre aquel usuario infractor.

El usuario debe solicitar cambio de contraseña por escrito a la Oficina de Tecnologías de la Información CMP.

El jefe de dependencia debe reportar a la Oficina de Tecnologías de la Información CMP, cualquier novedad o cambio en las funciones de usuario, ya sea por causa de vacaciones, licencia, comisión, traslado, ascenso o retiro, que implica la asignación de otros privilegios de acceso o suspensión temporal o definitiva de la contraseña.

Igualmente, la reactivación de la contraseña debe hacerse por escrito con la aprobación del jefe de la dependencia.

Es responsabilidad de cada usuario al momento de retirarse de la pantalla, verificar que las aplicaciones no queden disponibles para otro tipo de usuarios, porque de lo contrario incurrirá en responsabilidad so pena de ser sancionado.

12. DEL USO DEL SOFTWARE CMP

Para el entendimiento y aplicación de las normas inherentes a la formalización del software, es necesario identificar las definiciones que hacen parte del concepto y que se indican a continuación:

***Propiedad intelectual*:** Es la ley colombiana que establece que un programa [software] original de computadora es propiedad intelectual de la persona o empresa que lo creó. Es la protección a las producciones del talento de sus creadores por el tiempo y mediante las formalidades que establezca la ley. La expresión propiedad intelectual se utiliza en términos amplios para hacer referencia a todas las creaciones del ingenio humano y se define como la disciplina jurídica que tiene por objeto la protección de bienes inmateriales de naturaleza intelectual y de contenido creativo, así como de sus actividades conexas.

***Derecho de autor*:** Es el conjunto de facultades que la ley colombiana reconoce a favor del creador de obras literarias o artísticas originales, otorgándole protección para que goce de dos prerrogativas, una de carácter moral o personal, llamada derechos morales, y la otra de contenido económico, llamada también derechos patrimoniales.

La Contraloría Municipal de Pereira cumple con las leyes colombianas que protegen los derechos de autor y propiedad intelectual. Todo el software adquirido por la entidad e instalado en los PC están debidamente licenciados y registrados.

- Formas de piratería de Software.
- Piratería del usuario Final.
- Cargar discos duros.
- Venta de software pirata.
- Falsificación de programas.
- Copia de manuales.
- Renta de programas piratas.

***Derechos conexos al derecho de autor*:** Son el conjunto de facultades reconocidas a artistas intérpretes o ejecutantes, productores de fonograma y organismos de

radiodifusión en relación con sus interpretaciones o ejecuciones, fonogramas y emisiones de radiodifusión respectivamente.

Propiedad industrial: Es el conjunto de disposiciones cuyo objeto es la protección de las creaciones que tienen aplicación en el campo de la industria y el comercio.
***Titularidad originaria*:** El título originario sobre la obra pertenece a quien la ha creado, ésta condición le permite conservar al autor los derechos morales que son intransferibles y transferir, de manera total o parcial, los patrimoniales sobre la obra.
***Titularidad derivada*:** Es la que surge de circunstancias distintas del hecho de la creación, en virtud de la cual los derechos patrimoniales pueden transmitirse a un tercero, sea por mandato o presunción legal, o bien por cesión mediante acto entre vivos o por transmisión mortis causa.

***Obra*:** Es toda creación intelectual original de naturaleza artística o literaria, susceptible de ser divulgada o reproducida en cualquier forma.

***Obra en colaboración*:** Es la creada conjuntamente por dos o más personas naturales que hacen aportes propios. Para que haya colaboración es preciso, además, que la titularidad del derecho de autor no pueda dividirse sin alterar la naturaleza de la obra. En la obra en colaboración se da la coautoría entre partícipes.

***Obra colectiva*:** Es la creada por varios autores, que realizan su trabajo según un plan diseñado por un director que puede ser persona natural o jurídica y es quien la produce, dirige, edita, divulga y publica con su propio nombre y sólo tiene, respecto de los autores las obligaciones que haya contraído para con éstos en el respectivo contrato.

***Obras creadas por encargo*:** Es la realizada por uno o varios autores por mandato expreso de un comitente, según un plan señalado por éste y por su cuenta y riesgo. Los autores sólo percibirán por la ejecución del plan los honorarios pactados en el respectivo contrato, y por este solo acto se entiende que el autor o autores transfieren los derechos patrimoniales sobre la obra al comitente, pero conservan las prerrogativas morales consagradas en la ley.

***Obras audiovisuales*:** Es la expresada por medio de una serie de imágenes asociadas, para ser mostradas a través de aparatos de proyección o cualquier otro medio de comunicación de la imagen y de sonido.

Reproducción: Es la fijación material de la obra por cualquier forma o procedimiento que permite hacerla conocer al público y obtener copias de toda o parte de ella.

***Reproducción reprográfica*:** Es la realización de copias en facsímil de ejemplares originales o de copias de una obra por medios distintos a la impresión, como la fotocopia.

***Medidas tecnológicas*:** Toda técnica, dispositivo o componente que, en su funcionamiento normal, esté destinado a impedir o restringir actos referidos a obras o prestaciones protegidas que no cuenten con la autorización del titular de los derechos de autor o de los derechos afines a los derechos de autor establecidos en el presente reglamento y en la ley.

***Base de datos*:** Es la compilación de obras, hechos o datos en forma impresa, en unidades de almacenamiento de computador o de cualquier otra forma.

***Programas de computador o software*:** Es la expresión de un conjunto de instrucciones mediante palabras, planes, códigos o cualquier otra forma que, al ser incorporados en un dispositivo de lectura autorizado, hace que un aparato electrónico realice el proceso de datos para obtener información, ejecute determinadas tareas u obtenga determinados resultados.

Licencia de Software*:* *La licencia explica los alcances de operación de un software adquirido, según el autor, los términos bajo los cuales puede utilizarse el producto específico. El precio del programa o software adquirido puede incluir la adquisición legal de la licencia y obliga al comprador a utilizar el programa solo de acuerdo con los términos estipulados en la misma.*

Copias no autorizadas: *A no ser que esté estipulado de manera distinta, la compra de la licencia de un Programa permite a quien la adquiere, realizar una copia de seguridad ("backup"), para ser utilizada en caso de que el medio magnético original se averíe o destruya, la cual se identifica como copia autorizada.*

Cualquier otra copia del programa original es considerada como una copia no autorizada, no regulada y es una violación al acuerdo de licencia del software, además a la ley sobre los derechos de autor que protegen al programa y gobiernan su uso.

Software no autorizado*:* *Hace referencia al uso indebido de un programa o software de computadora en cualquier forma distinta a la permitida por la ley de derechos de autor o a la licencia de este. Se considera software no autorizado todo programa ejecutable de función específica que resida en una computadora sin su correspondiente licencia individual de uso oficial. Cualquier funcionario involucrado en la reproducción no autorizada de software, está cometiendo un acto ilegal que viola las leyes de derechos de autor vigentes en Colombia.*

Autor: Es la persona natural que realiza la creación intelectual en un área del conocimiento.

Artista intérprete o ejecutante: Es la persona que representa, canta, lee, recita, interpreta o ejecuta en cualquier forma una obra.

De los derechos morales: Son todos los derechos que nacen desde el momento de la creación de la obra, son personales e irrenunciables, por su carácter extra-patrimonial no pueden enajenarse ni embargarse, no prescriben y son de duración ilimitada. Son derechos morales:

- Reivindicar la paternidad sobre la obra y exigir que el nombre del autor y el título de la obra sean mencionados cada vez que ésta se utilice, publique o divulgue.
- Velar por la integridad de la obra, a efecto de que no sea mutilada o deformada.
- Optar por publicar la obra o por dejarla inédita. El autor puede publicar la obra con su nombre propio, o bajo un seudónimo o en forma anónima.
- Modificar la obra en cualquier tiempo y retirarla de la circulación, previo el pago de las indemnizaciones a que haya lugar.
- Retractarse o retirar la obra del acceso al público, aún después de haberlo autorizado, previa compensación económica por los daños que puedan ocasionarse.

De los derechos patrimoniales: Son las prerrogativas que se otorgan al autor para beneficiarse y explotar económicamente la obra, por cualquier medio conocido o por conocer. Los derechos patrimoniales son renunciables, prescriptibles, embargables y ejercidos por persona natural o jurídica, transferibles entre vivos, en todo o en parte, o por causa de muerte. Son Derechos patrimoniales: El autor y sus derechos habientes detentan el derecho para autorizar, permitir y prohibir los distintos actos de explotación de la obra y recibir un beneficio Económico por ellos, entre los cuales se enuncian los siguientes:

- La reproducción de la obra bajo distintas formas, tales como la publicación impresa, la grabación sonora, etc.
- La comunicación de la obra al público, por cualquier procedimiento, como la interpretación, ejecución, recitación; la radiodifusión sonora o audiovisual; la difusión por parlantes, equipos de sonido o por cualquier otro medio de comunicación conocido o por conocer.
- La distribución de los ejemplares de la obra mediante la venta, arrendamiento o alquiler.
- La transformación tales como adaptación, traducción a otros idiomas, arreglos musicales, compilaciones, etc.

Limitaciones de los derechos patrimoniales: Las limitaciones a los derechos patrimoniales de autor permiten la utilización de la obra sin autorización, ni contraprestación alguna. Y entre las cuales se encuentran:

Derecho de cita: Citar en una obra otras publicadas, siempre que se indique la fuente y el nombre del autor, transcribiendo los pasajes pertinentes, con la condición de que éstos no sean tantos y seguidos, que puedan considerarse como una reproducción simulada y sustancial.

Reproducción para fines de enseñanza: Reproducir por diversos medios como fotocopia, fotografía, etc. para fines de enseñanza, artículos publicados en periódicos o colecciones periódicas, o breves extractos de obras lícitamente publicadas, a condición de que tal utilización se haga conforme a los usos honrados, en la medida justificada por el fin que se persiga, y que no sea objeto de transacción a título oneroso, ni tenga directa o indirectamente fines de lucro.

Reproducción en biblioteca o centro de documentación: Reproducir una obra en forma individual por la biblioteca o un centro de documentación, sin fines de lucro, con el fin de:

- Preservar el ejemplar o sustituirlo en caso de extravío, destrucción o inutilización.
- Sustituir en la colección permanente de otra biblioteca o centro de documentación un ejemplar que se haya extraviado, destruido o inutilizado.

Copia de seguridad: Es permitido realizar una copia de los programas de ordenador, sobre el ejemplar del cual la Contraloría Municipal de Pereira, tiene propiedad siempre y cuando:

- Sea indispensable para la utilización del programa.
- Sea con fines de archivo en el caso de que la copia legítimamente adquirida se haya perdido, destruido o sea inutilizable.

Reproducción y comunicación para fines de información: Reproducir o comunicar una obra cuando el acto tenga como exclusivo fin de informar al público y con carácter de noticia o acontecimiento de actualidad en los casos siguientes:

- Reproducir y distribuir en periódicos, boletines, emitir por radiodifusión o transmisión pública, artículos, fotografías, ilustraciones que hayan sido difundidos por otros medios de comunicación social, salvo que esos derechos se hayan reservado expresamente.

- Reproducir, distribuir y comunicar al público conferencias, discursos, alocuciones, debates judiciales o de autoridades administrativas y otras obras similares que hayan sido pronunciadas en público y que no hayan sido previa y expresamente reservadas.
- Reproducir y comunicar y poner al alcance del público, informaciones sobre hechos o sucesos que hayan sido públicamente difundidos por los medios de comunicación.

Reproducción de obras expuestas en lugares públicos: Reproducción de obras expuestas de manera permanente en lugares públicos, por un medio distinto al empleado para la elaboración del original (por ejemplo, por medio de la pintura, el dibujo y la fotografía).

Comunicación para fines didácticos: No se requiere la autorización del autor para la utilización de una obra, cuando la comunicación se realice con fines exclusivamente didácticos, en instituciones de enseñanza, en el curso de las actividades académicas, por ejemplo, la representación de una obra de teatro o la ejecución de una obra musical; siempre que no persiga fines de lucro.

Copia privada: Reproducir por cualquier medio una obra literaria o científica, ordenada u obtenida por el interesado, en un solo ejemplar para uso privado y sin fines de lucro.

12.1 DE LOS ACUERDOS DE LICENCIA DE SOFTWARE

Licencias de uso individual:

- Uso individual y por máquina/Licencia PC.
- Licencias por individuo.
- Licencias por máquina.
- Medios duales.
- Paquetes, Suites

Licencia de uso concurrente*:* *Permite a un número limitado de usuarios conectarse simultáneamente a un programa de computadora de aplicación. Se están popularizando debido al incremento de los ambientes de redes.*

Licencias para uso en red:

- Generalmente está limitada a una red LAN o un servidor individual.
- Son diferentes a las licencias de uso concurrente en una red todos sus miembros tienen acceso al programa de cómputo.
- Es instalada en una sola computadora.
- El número de usuarios está limitado al número de conexiones del sistema operativo de la red.

Licencias Corporativas: *Se utilizan para una organización en varias áreas geográficas, una división corporativa o en pisos separados.*

Licencia de Usuario Final: *Es una licencia por la cual el uso de un producto sólo está permitido para un único usuario (el comprador). En este tipo de contrato, el dueño de los derechos de un producto insta al usuario final de éste a que reconozca tener conocimiento de las restricciones de uso, de los derechos del autor (copyright), de las patentes, etc. y que acepte de conformidad.*

Licencia Pública General GNU (GNU General Public License GPL): Es la licencia que acompaña los paquetes distribuidos por el Proyecto GNU, más una gran variedad de software que incluye el núcleo o kernel del sistema operativo Linux o Unix.

Licencias Software de Dominio Público *(sin licencia): Se permite uso, copia, modificación o redistribución con o sin fines de lucro.*

12.2 DE LOS PROCEDIMIENTOS QUE SON ILEGALES

- Copiar o distribuir software, códigos fuentes o documentación de este sin licencia.
- Instalar o ejecutar software o código fuente en dos o más computadoras simultáneamente, a no ser que esté dentro de los alcances permitidos en la licencia.
- Estimular, permitir, obligar o presionar a los funcionarios en las empresas a hacer o utilizar copias no autorizadas.
- Infringir las leyes sobre copias no autorizadas porque alguien lo pida o lo exija.
- Prestar el software, códigos fuente o documentación para que sean copiados o copiar los programas que han sido pedidos en préstamo.
- Fabricar, importar, poseer o negociar con artículos que faciliten la copia de software, código fuente o documentación propia de una licencia o desarrollo de software.
- A menos que se indique lo contrario, los usuarios asumen la responsabilidad que todo software, código fuente y documentación de la Contraloría Municipal de Pereira, está protegido por derechos de autor y requiere licencia de uso, por lo tanto, es ilegal y está terminantemente prohibido hacer copias, reproducciones o usar estos medios para fines personales.

- No se debe utilizar software o código fuente obtenido a través de Internet y en general software que provenga de una fuente no confiable, a menos que haya sido comprobado en forma rigurosa y que esté debidamente aprobado su uso por la Oficina de Tecnologías de la información CMP.
- Se prohíbe estrictamente la instalación de software y código fuente no autorizado, incluyendo el que haya sido adquirido por el propio usuario o mediante la instalación de dispositivos periféricos.
- No se permite el uso de software o código fuente de distribución gratuita o shareware, a menos que haya sido previamente aprobado por la Oficina de Tecnologías de la información CMP.
- LA Oficina de Tecnologías de la información CMP, debe realizar chequeos al software y código fuente instalado en cada equipo de cómputo y presentar el informe correspondiente al superior inmediato.
- La entidad tiene licencias de todos los programas de software y código fuente utilizado para las operaciones misionales CMP.
- La entidad no es la propietaria de ese software, código fuente o de sus manuales, y a menos que sea autorizada por el productor de software, no tiene derecho a reproducirlo.
- En cuanto al uso de software o sus derivados en redes o amparado bajo licencia corporativa, los funcionarios CMP, solo utilizarán el software o código fuente de acuerdo con lo convenido en las licencias de uso.

De acuerdo con las leyes de propiedad intelectual vigentes, la reproducción no autorizada de software o código fuente está sujeta a indemnizaciones por perjuicios civiles y a demandas penales. En lo posible, estas condiciones deben ser firmadas por todos usuarios de recursos computacionales para probar su aceptación.

Por ningún motivo la Contraloría Municipal de Pereira permite la instalación de software o código fuente para compartir archivos entre cibernautas, situación que puede poner en riesgo la seguridad de la información y de la red.

12.3 CAMPAÑA DE EDUCACIÓN A LOS FUNCIONARIOS QUE LABORAN EN LA ENTIDAD

La Oficina de Tecnologías de la Información y Control Interno CMP deben promulgar las políticas y restricciones mediante la emisión de circulares informativas. También pueden utilizarse los recursos de la computadora para visualizar en pantalla este tipo de información, la mensajería o en su defecto en las carteleras de la entidad.

Nota: De acuerdo al procedimiento PR 1.2.3.4 GS-1 del Manual de Procesos y Procedimientos de la CMP, los cambios o ajustes que se requieran al presente

documento se presentarán mediante acciones de mejora del SGC para la aprobación del Comité respectivo.

13. POLÍTICAS DE TRATAMIENTO DE DATOS

El presente documento se ha creado con el fin de dar cumplimiento a lo establecido en la Ley Estatutaria 1581 de 2012 "**Por la cual se dictan disposiciones generales para la protección de datos personales" y reglamentada por e**l Decreto 1377 de 2013, con el propósito de adopta la política para el tratamiento de datos personales, la cual será informada a todos los titulares de los datos recolectados o que en el futuro se obtengan en el ejercicio de las actividades misionales y administrativas de la Contraloría Municipal de Pereira.

La Contraloría Municipal de Pereira manifiesta que garantiza los derechos a la privacidad, la intimidad, el buen nombre y la autonomía, en el tratamiento de los datos personales y en consecuencia todas sus actuaciones se regirán por los principios de legalidad, finalidad, libertad, veracidad, calidad, transparencia, acceso y circulación restringida, seguridad y confidencialidad.
Todas las personas que en desarrollo de diferentes actividades misionales o administrativas llegaran a suministrar a la Contraloría Municipal de Pereira cualquier tipo de información o dato personal, podrá conocerla, actualizarla y rectificarla.

13.1 IDENTIFICACIÓN DEL RESPONSABLE DEL TRATAMIENTO

NOMBRE DE LA INSTITUCIÓN: Contraloría Municipal de Pereira**,** que en adelante se denominará LA CMP, entidad del estado del orden municipal, identificada con NIT Número 800182573-0 con domicilio en Pereira en la carrera 7ª No. 18- 55 piso 7, con teléfonos de contacto 3248282 3248278
CORREO ELECTRÓNICO: correo@contraloriapereira.gov.co
TELÉFONO: 3248278 3248282

13.2 MARCO LEGAL VIGENTE

Constitución Política, artículo 15°, Ley 1266 de 2008, Ley 1581 de 2012
Decretos Reglamentarios 1727 de 2009 y 2952 de 2010, Decreto Reglamentario parcial 1377 de 2013, Sentencias C – 1011 de 2008, y C - 748 del 2011, de la Corte Constitucional,
Artículo 2.2.9.1.1.3 de Decreto 1078 de 2015, subrogado por el artículo 1° del decreto 1008 de 2018, Decreto 2106 de 2019 artículo 16°

ÁMBITO DE APLICACIÓN

La presente política será aplicable a los datos personales registrados en cualquier base de datos de la Contraloría Municipal de Pereira, cuyo titular sea una persona natural.

13.3 DEFINICIONES

Para los efectos de la presente política y en concordancia con la normatividad vigente en materia de protección de datos personales, se tendrán en cuenta las siguientes definiciones:

Autorización: Consentimiento previo, expreso e informado del titular para llevar a cabo el tratamiento de datos personales.

***Aviso de privacidad*:** Comunicación verbal o escrita generada por el responsable, dirigida al titular para el tratamiento de sus datos personales, mediante la cual se le informa acerca de la existencia de las políticas de tratamiento de información que le serán aplicables, la forma de acceder a las mismas y las finalidades del tratamiento que se pretende dar a los datos personales.

***Base de Datos*:** Conjunto organizado de datos personales que sea objeto de tratamiento.

Causahabiente: Persona que ha sucedido a otra por causa del fallecimiento de ésta (heredero).

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

Dato público: Es el dato que no sea semiprivado, privado o sensible. Son considerados datos públicos, entre otros, los datos relativos al estado civil de las personas, a su profesión u oficio y a su calidad de comerciante o de servidor público. Por su naturaleza, los datos públicos pueden estar contenidos, entre otros, en registros públicos, documentos públicos, gacetas y boletines oficiales y sentencias judiciales debidamente ejecutoriadas que no estén sometidas a reserva.

***Datos sensibles*:** Se entiende por datos sensibles aquellos que afectan la intimidad del Titular o cuyo uso indebido puede generar su discriminación, tales como que revelen el origen racial o étnico, la orientación política, las convicciones religiosas o filosóficas, la pertenencia a sindicatos, organizaciones sociales, de derechos humanos o que promueva intereses de cualquier partido político o que garanticen los derechos y

garantías de partidos políticos de oposición, así como los datos relativos a la salud, a la vida sexual, y los datos biométricos.

***Encargado del Tratamiento*:** Persona natural o jurídica, pública o privada, que por sí misma o en asocio con otros, realice el Tratamiento de datos personales por cuenta del responsable del Tratamiento.

***Responsable del Tratamiento*:** Persona natural o jurídica, pública o privada, que por sí misma o en asocio con otros, decida sobre la base de datos y/o el Tratamiento de los datos.

***Titular**:* Persona natural cuyos datos personales sean objeto de Tratamiento.

***Tratamiento*:** Cualquier operación o conjunto de operaciones sobre datos personales, tales como la recolección, almacenamiento, uso, circulación o supresión.

***Transferencia*:** la transferencia de datos tiene lugar cuando el responsable y/o encargado del tratamiento de datos personales, ubicado en Colombia, envía la información o los datos personales a un receptor, que a su vez es responsable del tratamiento y se encuentra dentro o fuera del país.

***Transmisión*:** tratamiento de datos personales que implica la comunicación de estos dentro o fuera del territorio de la República de Colombia cuando tenga por objeto la realización de un tratamiento por el encargado por cuenta del responsable.

13.4 PRINCIPIOS

Los principios incluidos en este documento son tomados de la normatividad vigente en Colombia que regula la protección de datos personales.

Para efectos de garantizar la protección de datos personales, La Contraloría Municipal de Pereira aplicará de manera armónica e integral los siguientes principios, a la luz de los cuales se deberá realizar el tratamiento, transferencia y transmisión de datos personales:

***Principio de legalidad en materia de Tratamiento de datos*:** El tratamiento de datos es una actividad reglada, la cual deberá estar sujeta a las disposiciones legales vigentes y aplicables que rigen el tema.

Principio de finalidad: La actividad del tratamiento de datos personales que realice LA CMP o a la cual tuviere acceso, obedecerán a una finalidad legítima en consonancia con

la Constitución Política de Colombia, la cual deberá ser informada al respectivo titular de los datos personales.

***Principio de libertad*:** El tratamiento de los datos personales sólo puede realizarse con el consentimiento, previo, expreso e informado del titular. Los datos personales no podrán ser obtenidos o divulgados sin previa autorización, o en ausencia de mandato legal, estatutario, o judicial que releve el consentimiento.

***Principio de veracidad o calidad**:* La información sujeta a tratamiento de datos personales debe ser veraz, completa, exacta, actualizada, comprobable y comprensible**.** Se prohíbe el tratamiento de datos parciales, incompletos, fraccionados o que induzcan a error.

Principio de transparencia: En el tratamiento de datos personales, La Contraloría Municipal de Pereira garantizará al titular su derecho de obtener en cualquier momento y sin restricciones, información acerca de la existencia de cualquier tipo de información o dato personal que sea de su interés o titularidad.

***Principio de acceso y circulación restringida*:** El tratamiento de datos personales se sujeta a los límites que se derivan de la naturaleza de éstos, de las disposiciones de la ley y la Constitución. En consecuencia, el tratamiento sólo podrá hacerse por personas autorizadas por el titular y/o por las personas previstas en la ley. Los datos personales, salvo la información pública, no podrán estar disponibles en internet u otros medios de divulgación o comunicación masiva, salvo que el acceso sea técnicamente controlable para brindar un conocimiento restringido sólo a los titulares o terceros autorizados conforme a la ley. Para estos propósitos la obligación de La Contraloría Municipal de Pereira será de medio.

Principio de seguridad: La información sujeta a tratamiento por La Contraloría Municipal de Pereira, se deberá manejar con las medidas técnicas, humanas y administrativas que sean necesarias para otorgar seguridad a los registros evitando su adulteración, pérdida, consulta, uso o acceso no autorizado o fraudulento.

Principio de confidencialidad: Todas las personas que, en La Contraloría Municipal de Pereira administren, manejen, actualicen o tengan acceso a información de cualquier tipo que se encuentre contenida en “Bases de Datos”, están obligadas a garantizar la reserva de la información, por lo que se comprometen a conservar y mantener de manera estrictamente confidencial y no revelar a terceros, toda la información que llegaren a conocer en la ejecución y ejercicio de sus funciones; salvo cuando se trate de actividades autorizadas expresamente por la ley de protección de datos. Esta obligación

persiste y se mantendrá inclusive después de finalizada su relación con alguna de las labores que comprende el Tratamiento.

13.5 DERECHOS DEL TITULAR DE LA INFORMACIÓN

De acuerdo con lo contemplado por la normatividad vigente aplicable en materia de protección de datos, los siguientes son los derechos de los titulares de los datos personales:

- Acceder, conocer, actualizar y rectificar sus datos personales frente a la Contraloría Municipal de Pereira en su condición de responsable del tratamiento. Este derecho se podrá ejercer, entre otros, frente a datos parciales, inexactos, incompletos, fraccionados, que induzcan a error, o aquellos cuyo tratamiento esté expresamente prohibido o no haya sido autorizado.
- Ser informado por la Contraloría Municipal de Pereira, previa solicitud, respecto del uso y manejo que se les ha dado a sus datos personales.
- Presentar ante la Superintendencia de Industria y Comercio, o la entidad que hiciere sus veces, quejas por infracciones a lo dispuesto en la ley 1581 de 2012 y las demás normas que la modifiquen, adicionen o complementen, previo trámite de consulta o requerimiento ante la Contraloría Municipal de Pereira
- Revocar la autorización y/o solicitar la supresión del dato cuando en el Tratamiento no se respeten los principios, derechos y garantías constitucionales y legales.
- Acceder en forma gratuita a sus datos personales que hayan sido objeto de tratamiento, al menos una vez cada mes calendario, y cada vez que existan modificaciones sustanciales de la presente política que motiven nuevas consultas.

13.6 DE LOS DERECHOS EJERCIDOS POR EL TITULAR Y APODERADOS

- El titular, quien deberá acreditar su identidad en forma suficiente por los distintos medios que le ponga a disposición la Contraloría Municipal de Pereira.
- Los causahabientes del titular, quienes deberán acreditar tal calidad.
- El representante y/o apoderado del titular, previa acreditación de la representación o apoderamiento.
- Otro a favor o para el cual el titular hubiere estipulado.

13.7 DE LOS DERECHOS DE LOS NIÑOS Y ADOLESCENTES

Ley 1581 de 2012. Artículo 10**. *Casos en que no es necesaria la autorización.*** La autorización del Titular no será necesaria cuando se trate de:

Información requerida por una entidad pública o administrativa en ejercicio de sus funciones legales o por orden judicial; Datos de naturaleza pública; Casos de urgencia médica o sanitaria; Tratamiento de información autorizado por la ley para fines históricos, estadísticos o científicos; Datos relacionados con el Registro Civil de las Personas. Quien acceda a los datos personales sin que medie autorización previa deberá en todo caso cumplir con las disposiciones contenidas en la presente ley establecida para estos casos.

En el tratamiento de datos personales se asegurará el respeto a los derechos prevalentes de los menores.

Queda proscrito el tratamiento de datos personales de menores, salvo aquellos datos que sean de naturaleza pública, y en este caso el tratamiento deberá cumplir con los siguientes parámetros:

- Responder y respetar el interés superior de los menores.
- Asegurar el respeto de los derechos fundamentales de los menores.
- Es tarea del Estado, además de las entidades educativas de todo tipo proveer información y capacitar a los representantes legales y tutores sobre los eventuales riesgos a los que se enfrentan los niños, niñas y adolescentes respecto del Tratamiento indebido de sus datos personales, incluso proveer de conocimiento acerca del uso responsable y seguro por parte de niños, niñas y adolescentes de sus datos personales, su derecho a la privacidad y protección de su información personal y la de los demás.

13.8 DEBERES DE LA CONTRALORÍA MUNICIPAL DE PEREIRA COMO RESPONSABLE Y ENCARGADA DEL TRATAMIENTO DE LOS DATOS PERSONALES

La Contraloría Municipal de Pereira reconoce la titularidad que de los datos personales ostentan las personas y en consecuencia ellas de manera exclusiva pueden decidir sobre los mismos. Por lo tanto, utilizará los datos personales para el cumplimiento de las finalidades autorizadas expresamente por el titular o por las normas vigentes.

En el tratamiento y protección de datos personales, la Contraloría Municipal de Pereira tendrá los siguientes deberes, sin perjuicio de otros previstos en las disposiciones que regulen o lleguen a regular esta materia:

- Garantizar al titular, en todo tiempo, el pleno y efectivo ejercicio del derecho de hábeas data.

- Solicitar y conservar, copia de la respectiva autorización otorgada por el titular para el tratamiento de datos personales.
- Informar debidamente al titular sobre la finalidad de la recolección y los derechos que le asisten en virtud de la autorización otorgada.
- Conservar la información bajo las condiciones de seguridad necesarias para impedir su adulteración, pérdida, consulta, uso o acceso no autorizado o fraudulento.
- Garantizar que la información sea veraz, completa, exacta, actualizada, comprobable y comprensible.
- Actualizar oportunamente la información, atendiendo de esta forma todas las novedades respecto de los datos del titular. Adicionalmente, se deberán implementar todas las medidas necesarias para que la información se mantenga actualizada.
- Rectificar la información cuando sea incorrecta y comunicar lo pertinente.
- Respetar las condiciones de seguridad y privacidad de la información del titular.
- Tramitar las consultas y reclamos formulados en los términos señalados por la ley.
- Identificar cuando determinada información se encuentra en discusión por parte del titular.
- Informar a solicitud del titular sobre el uso dado a sus datos.
- Informar a la autoridad de protección de datos cuando se presenten violaciones a los códigos de seguridad y existan riesgos en la administración de la información de los titulares.
- Cumplir los requerimientos e instrucciones que imparta la Superintendencia de Industria y Comercio sobre el tema en particular.
- Usar únicamente datos cuyo tratamiento esté previamente autorizado de conformidad con lo previsto en la ley 1581 de 2012.
- Velar por el uso adecuado de los datos personales de los niños, niñas y adolescentes, en aquellos casos en que se entra autorizado el tratamiento de sus datos.
- Registrar en la base de datos las leyendas "reclamo en trámite" en la forma en que se regula en la ley.
- Insertar en la base de datos la leyenda "información en discusión judicial" una vez notificado por parte de la autoridad competente sobre procesos judiciales relacionados con la calidad del dato personal.
- Abstenerse de circular información que esté siendo controvertida por el titular y cuyo bloqueo haya sido ordenado por la Superintendencia de Industria y Comercio.
- Permitir el acceso a la información únicamente a las personas que pueden tener acceso a ella.
- Usar los datos personales del titular sólo para aquellas finalidades para las que se encuentre facultada debidamente y respetando en todo caso la normatividad vigente sobre protección de datos personales.

13.9 AUTORIZACIÓN Y CONSENTIMIENTO DEL TITULAR

La Contraloría Municipal de Pereira requiere del consentimiento libre, previo, expreso e informado del titular de los datos personales para el tratamiento de estos, exceptos en los casos expresamente autorizados en la ley, a saber:

- Información requerida por una entidad pública o administrativa en ejercicio de sus funciones legales o por orden judicial.
- Datos de naturaleza pública.
- Casos de urgencia médica o sanitaria.
- Tratamiento de información autorizado por la ley para fines históricos, estadísticos o científicos.
- Datos relacionados con el Registro Civil de las Personas.

13.10 MANIFESTACIÓN DE LA AUTORIZACIÓN

La autorización a la Contraloría Municipal de Pereira para el tratamiento de los datos personales será otorgada por:

- El titular, quien deberá acreditar su identidad en forma suficiente por los distintos medios que le ponga a disposición LA CMP, diligenciando la “Carta de Consentimiento Informado PARA TRATAMIENTO DE DATOS PERSONALES” formato FO 1.2.3.4-1.
- Los causahabientes del titular, quienes deberán acreditar tal calidad.
- El representante y/o apoderado del titular, previa acreditación de la representación o apoderamiento.
- Otro a favor o para el cual el titular hubiere estipulado.

13.11 MEDIOS PARA OTORGAR LA AUTORIZACIÓN

La Contraloría Municipal de Pereira obtendrá la autorización mediante diferentes medios, entre ellos el documento físico, electrónico, mensaje de datos, Internet, Sitios Web, o en formato “Carta de Consentimiento Informado PARA TRATAMIENTO DE DATOS PERSONALES” formato FO 1.2.3.4-1que en todo caso permita la obtención del consentimiento mediante conductas inequívocas a través de las cuales se concluya que de no haberse surtido la misma por parte del titular o la persona legitimada para ello, los datos no se hubieran almacenado o capturado en la base de datos CMP.

La autorización será solicitada por la Contraloría Municipal de Pereira de manera previa al tratamiento de los datos personales.

13.12 PRUEBA DE LA AURORIZACIÓN

La Contraloría Municipal de Pereira conservará la prueba de la autorización otorgada por los titulares de los datos personales para su tratamiento, para lo cual utilizará los mecanismos disponibles a su alcance en la actualidad al igual que adoptará las acciones necesarias para mantener el registro de la forma, fecha y en la que obtuvo ésta. En consecuencia, La Contraloría Municipal de Pereira podrá establecer archivos físicos o repositorios electrónicos realizados de manera directa o a través de terceros contratados para tal fin.

13.13 REVOCATORIA DE LA AUTORIZACIÓN

Los titulares de los datos personales pueden en cualquier momento revocar la autorización otorgada a la Contraloría Municipal de Pereira para el tratamiento de sus datos personales o solicitar la supresión de estos, siempre y cuando no lo impida una disposición legal o contractual. La Contraloría Municipal de Pereira establecerá mecanismos sencillos y gratuitos que permitan al titular revocar su autorización o solicitar la supresión sus datos personales, al menos por el mismo medio por el que lo otorgó.

Para lo anterior, deberá tenerse en cuenta que la revocatoria del consentimiento puede expresarse, por una parte, de manera total en relación con las finalidades autorizadas, y por lo tanto la Contraloría Municipal de Pereira deberá cesar cualquier actividad de tratamiento de los datos; y por la otra de manera parcial en relación con ciertos tipos de tratamiento, en cuyo caso serán estos sobre los que cesarán las actividades de tratamiento, como para fines publicitarios, entre otros. En este último caso, LA CMP como entidad oficial del Estado podrá continuar tratando los datos personales para aquellos fines en relación con los cuales el titular no hubiera revocado su consentimiento.

13.14 TRATAMIENTO AL CUAL SERÁN SOMETIDOS LOS DATOS Y FINALIDAD DE ESTE

El tratamiento de los datos personales de empelados, exempleados, jubilados, proveedores, contratistas, ciudadanos o de cualquier persona con la cual la Contraloría Municipal de Pereira tuviere establecida o estableciera una relación, permanente u ocasional, lo realizará en el marco legal que regula la materia y en virtud de su condición de entidad de control fiscal del estado y serán todos los necesarios para el cumplimiento de la misión institucional.

En todo caso, los datos personales podrán ser recolectados y tratados para:

- Realizar el envío de información relacionada con programas, actividades, noticias, contenidos por área de interés, productos y demás servicios ofrecidos por la Contraloría Municipal de Pereira.
- Desarrollar la misión de La Contraloría Municipal de Pereira conforme a La Constitución y la Ley.
- Cumplir con la normatividad vigente en Colombia para las entidades del estado del orden territorial.
- Cumplir las normas aplicables a proveedores y contratistas, incluyendo, pero sin limitarse a las tributarias y comerciales.
- Cumplir lo dispuesto por el ordenamiento jurídico colombiano en materia laboral y de seguridad social, entre otras, aplicables a exempleados, empleados actuales y candidatos a futuro empleo.
- Realizar encuestas relacionadas con los servicios que presta la Contraloría Municipal de Pereira.
- Desarrollar programas o actividades conforme a la misión de la entidad.
- Informar sobre oportunidades de empleos, capacitaciones, actividades de promoción a la participación ciudadana.
- Cumplir todos sus compromisos contractuales.
- Para el tratamiento de datos personales de niños, niñas y adolescentes se procederá de acuerdo con lo contemplado en la presente política en el aparte relacionado con los derechos de éstos.

13.15 TRATAMIENTO A DATOS SENSIBLES

Para el caso de datos personales sensibles, la Contraloría Municipal de Pereira podrá hacer uso y tratamiento de ellos cuando:

- El titular haya dado su autorización explícita, salvo en los casos que por ley no sea requerido el otorgamiento de dicha autorización.
- El tratamiento sea necesario para salvaguardar el interés vital del Titular y este se encuentre física o jurídicamente incapacitado. En estos eventos, los representantes legales deberán otorgar su autorización.
- El tratamiento sea efectuado en el curso de las actividades legítimas y con las debidas garantías por parte de una fundación, ONG, asociación o cualquier otro organismo sin ánimo de lucro, cuya finalidad sea política, filosófica, religiosa o sindical, siempre que se refieran exclusivamente a sus miembros o a las personas que mantengan contactos regulares por razón de su finalidad. En estos eventos, los datos no se podrán suministrar a terceros sin la autorización del titular.
- El Tratamiento se refiera a datos que sean necesarios para el reconocimiento, ejercicio o defensa de un derecho en un proceso judicial.

- El Tratamiento tenga una finalidad histórica, estadística o científica. En este evento deberán adoptarse las medidas conducentes a la supresión de identidad de los titulares.

Sin perjuicio de las excepciones previstas en la ley, en el tratamiento de datos sensibles, se requiere la autorización previa, expresa e informada del titular, la cual deberá ser obtenida por cualquier medio que pueda ser objeto de consulta y verificación posterior.

13.16 AVISO DE PRIVACIDAD

El Aviso de Privacidad es el documento físico, electrónico o en cualquier otro formato, puesto a disposición del titular para informarle acerca del tratamiento de sus datos personales. A través de este documento se comunica al titular la información relacionada con la existencia de las políticas de tratamiento de información de a Contraloría Municipal de Pereira y que le serán aplicables, la forma de acceder a las mismas y las características del tratamiento que se pretende dar a los datos personales.

El aviso de privacidad deberá contener, como mínimo, la siguiente información:

- La identidad, domicilio y datos de contacto del responsable del tratamiento.
- El tipo de tratamiento al cual serán sometidos los datos y la finalidad de este.
- Los derechos del titular.
- Los mecanismos generales dispuestos por el responsable para que el titular conozca la política de tratamiento de la información y los cambios sustanciales que se produzcan en ella. En todos los casos, debe informar al titular cómo acceder o consultar la política de tratamiento de información.
- El carácter facultativo de la respuesta relativa a preguntas sobre datos sensibles.

13.17 GARANTÍAS DEL DERECHO DE ACCESO

Para garantizar el derecho de acceso del titular de los datos, la Contraloría Municipal de Pereira pondrá a disposición de éste, previa acreditación de su identidad, legitimidad, o personalidad de su representante, sin costo o erogación alguna, de manera pormenorizada y detallada, los respectivos datos personales a través de todo tipo de medio, incluyendo los medios electrónicos que permitan el acceso directo del titular a ellos. Dicho acceso deberá ofrecerse sin límite alguno y le deben permitir al titular la posibilidad de conocerlos y actualizarlos en línea.

13.18 PROCEDIMIENTO PARA LA ATENCIÓN DE CONSULTAS, RECLAMOS, PETICIONES DE RECTIFICACIÓN, ACTUALIZACIÓN Y SUPRESIÓN DE DATOS

CONSULTAS: Los titulares o sus causahabientes podrán consultar la información personal del titular que repose en la Contraloría Municipal de Pereira, quien suministrará toda la información contenida en el registro individual o que esté vinculada con la identificación del Titular.

Con respecto a la atención de solicitudes de consulta de datos personales la Contraloría Municipal de Pereira garantiza:

- Habilitar medios de comunicación electrónica u otros que considere pertinentes.
- Establecer formularios, sistemas y otros métodos simplificados, los cuales deberán ser informados en el aviso de privacidad.
- Utilizar los servicios de atención al cliente o de reclamaciones que tiene en operación.
- En cualquier caso, independientemente del mecanismo implementado para la atención de solicitudes de consulta, las mismas serán atendidas en un término máximo de diez (10) días hábiles contados a partir de la fecha de su recibo. Cuando no fuere posible atender la consulta dentro de dicho término, se informará al interesado antes del vencimiento de los diez (10) días, expresando los motivos de la demora y señalando la fecha en que se atenderá su consulta, la cual en ningún caso podrá superar los cinco (5) días hábiles siguientes al vencimiento del primer plazo.
- Las consultas podrán formularse al correo institucional correo@contraloriapereira.gov.co

RECLAMOS: El Titular o sus causahabientes que consideren que la información contenida en una base de datos debe ser objeto de corrección, actualización o supresión, o cuando adviertan el presunto incumplimiento de cualquiera de los deberes contenidos en la ley, podrán presentar un reclamo ante la Contraloría Municipal de Pereira, el cual será tramitado bajo el siguiente procedimiento:

- El reclamo del titular se formulará mediante solicitud dirigida a la Contraloría Municipal de Pereira al correo electrónico correo@contraloriapereira.gov.co o mediante comunicación escrita dirigida a la SUBCONTRALORIA, con la identificación del titular, la descripción de los hechos que dan lugar al reclamo, la dirección, y acompañando los documentos que se quiera hacer valer. Si el reclamo resulta incompleto, se requerirá al interesado dentro de los cinco (5) días siguientes a la recepción del reclamo para que subsane las fallas. Transcurridos dos (2) meses desde la fecha del requerimiento, sin que el solicitante presente la información requerida, se entenderá que ha desistido del reclamo.

- En caso de que quien reciba el reclamo no sea competente para resolverlo, dará traslado a quien corresponda en un término máximo de dos (2) días hábiles e informará de la situación al interesado.
- Una vez recibido el reclamo completo, éste se catalogará con la etiqueta "reclamo en trámite" y el motivo de este, en un término no mayor a dos (2) días hábiles. Dicha etiqueta se mantendrá hasta que el reclamo sea decidido.
- El término máximo para atender el reclamo será de quince (15) días hábiles contados a partir del día siguiente a la fecha de su recibo. Cuando no fuere posible atender el reclamo dentro de dicho término, se informará al interesado los motivos de la demora y la fecha en que se atenderá su reclamo, la cual en ningún caso podrá superar los ocho (8) días hábiles siguientes al vencimiento del primer término.

PETICIÓN DE ACTUALIZACIÓN Y/O RECTIFICACIÓN: La Contraloría Municipal de Pereira rectificará y actualizará, a solicitud del titular, la información de éste que resulte ser incompleta o inexacta, de conformidad con el procedimiento y los términos antes señalados, para lo cual se tendrá en cuenta:

- El titular deberá allegar la solicitud al correo electrónico correo@contraloriapereira.gov.co o en medio físico dirigido a la SUBCONTRALORIA, indicando la actualización y/o rectificación a realizar y aportará la documentación que sustente su petición.
- La Contraloría Municipal de Pereira podrá habilitar mecanismos que le faciliten el ejercicio de este derecho al titular, siempre y cuando éstos lo beneficien. En consecuencia, se podrán habilitar medios electrónicos u otros que considere pertinentes, los cuales serán informados en el aviso de privacidad y se pondrán a disposición de los interesados en la página web CMP.

PETICIÓN DE SUPRESIÓN DE DATOS: El titular de los datos personales tiene el derecho de solicitar a la Contraloría Municipal de Pereira, su supresión (eliminación) en cualquiera de los siguientes eventos siempre y cuando:

- Considere que los mismos no están siendo tratados conforme a los principios, deberes y obligaciones previstas en la normatividad vigente.
- Hayan dejado de ser necesarios o pertinentes para la finalidad para la cual fueron recabados.
- Se haya superado el periodo necesario para el cumplimiento de los fines para los que fueron recabados.

Esta supresión implica la eliminación total o parcial de la información personal de acuerdo con lo solicitado por el titular en los registros, archivos, bases de datos o tratamientos realizados por la Contraloría Municipal de Pereira. Sin embargo, este

derecho del titular no es absoluto y en consecuencia LA CMP podrá negar el ejercicio de este siempre y cuando:

- El titular tenga un deber legal o contractual de permanecer en la base de datos.
- La eliminación de datos obstaculice actuaciones judiciales o administrativas vinculadas a obligaciones fiscales, la investigación y persecución de delitos o la actualización de sanciones administrativas.
- Los datos sean necesarios para proteger los intereses jurídicamente tutelados del titular; para realizar una acción en función del interés público, o para cumplir con una obligación legalmente adquirida por el titular.

13.19 REGISTRO NACIONAL DE BASE DE DATOS

La Contraloría Municipal de Pereira, se reserva, en los eventos contemplados en la ley y en sus estatutos y reglamentos internos, la facultad de mantener y catalogar determinada información que repose en sus bases o bancos de datos, como confidencial de acuerdo con las normas vigentes, sus estatutos y reglamentos.

La Contraloría Municipal de Pereira, procederá de acuerdo con la normatividad vigente y la reglamentación que para tal fin expida el Gobierno Nacional, a realizar el registro de sus bases de datos, ante El Registro Nacional de Bases de Datos (RNBD) que será administrado por la Superintendencia de Industria y Comercio. El RNBD, es el directorio público de las bases de datos sujetas a tratamiento que operan en el país; y que será de libre consulta para los ciudadanos, de acuerdo con la normatividad que para tal efecto expida el Gobierno Nacional.

13.20 SEGURIDAD DE LA INFORMACIÓN Y MEDIDAS DE SEGURIDAD

Dando cumplimiento al principio de seguridad establecido en la normatividad vigente, la Contraloría Municipal de Pereira adoptará las medidas técnicas, humanas y administrativas que sean necesarias para otorgar seguridad a los registros evitando su adulteración, pérdida, consulta, uso o acceso no autorizado o fraudulento.

13.21 UTILIZACIÓN Y TRANSFERENCIA INTERNACIONAL DE DATOS E INFORMACIÓN PERSONALES POR PARTE DE LA CMP

En cumplimiento de la misión institucional y atendiendo a la naturaleza de las relaciones permanentes u ocasionales que cualquier persona titular de datos personales pueda tener para con la Contraloría Municipal de Pereira, ésta podrá realizar la transferencia y transmisión, incluso internacional, de la totalidad de los datos personales, siempre y cuando se cumplan los requerimientos legales aplicables; y en consecuencia los titulares

con la aceptación de la presente política, autorizan expresamente para transferir y transmitir, incluso a nivel internacional, los datos personales. Los datos serán transferidos, para todas las relaciones que puedan establecerse con LA CMP.

Para la transferencia internacional de datos personales de los titulares, la **Contraloría Municipal de Pereira** tomará las medidas necesarias para que los terceros conozcan y se comprometan a observar la presente política, bajo el entendido que la información personal que reciban únicamente podrá ser utilizada para asuntos directamente relacionados con la Contraloría Municipal de Pereira y solamente mientras ésta dure, incluso no podrá ser usada o destinada para propósito o fin diferente. Para la transferencia internacional de datos personales se observará lo previsto en el artículo 26 de la Ley 1581 de 2012.

Las transmisiones internacionales de datos personales que efectúe la Contraloría Municipal de Pereira no requerirán ser informadas al titular ni contar con su consentimiento cuando medie un contrato de transmisión de datos personales de conformidad al artículo 25 del Decreto 1377 de 2013.

La Contraloría Municipal de Pereira, también podrá intercambiar información personal con autoridades gubernamentales o públicas de otro tipo (incluidas, entre otras autoridades judiciales o administrativas, autoridades fiscales y organismos de investigación penal, civil, administrativa, disciplinaria y fiscal), y terceros participantes en procedimientos legales civiles y sus contadores, auditores, abogados y otros asesores y representantes, porque es necesario o apropiado:

a. Para cumplir con las leyes vigentes, incluidas las leyes distintas a las de su país de residencia.
b. Para cumplir con procesos jurídicos.
c. Para responder las solicitudes de las autoridades y del gobierno, y para responder las solicitudes de las autoridades y del gobierno distintas a las de su país de residencia.
d. Para hacer cumplir nuestros términos y condiciones.
e. Para proteger nuestras operaciones.
f. Para proteger nuestros derechos, privacidad, seguridad o propiedad, los suyos o los de terceros.
g. Obtener las indemnizaciones aplicables o limitar los daños y perjuicios que nos puedan afectar.

13.22 RESPONSABLE Y ENCARGADO DEL TRATAMIENTO DE DATOS PERSONALES

La Contraloría Municipal de Pereira será la responsable del tratamiento de los datos personales. La Asesoría Jurídica, será la encargada del tratamiento de los datos personales, por cuenta de LA CMP.

14. DOCUMENTOS COMPLEMENTARIOS PARA TENER EN CUENTA EN EL USO DE OTROS DISPOSITIVOS TECNOLÓGICOS

Se han tenido en cuenta documentos adicionales del estado colombiano, donde se normalizan temas inherentes al control y manejo de tecnología que no necesariamente tiene que ver de forma directa con la Coordinación de TI y que reglamentan el uso de dispositivos o servicios tecnológicos.

PROTECCIÓN DE DATOS PERSONALES EN SISTEMAS DE VIDEO VIGILANCIA – Superintendencia de Industria y Comercio

LINEAMIENTOS DETALLADOS PARA LA IMPLEMENTACION DE PROCESOS ELECTRÓNICOS – Ministerio de Tecnologías de la Información y las Telecomunicaciones MinTIC

GUIA DE METADATOS -Archivo General de la Nación

LINEAMIENTOS Y RECOMENDACIONES PARA EL USO DE MEDIOS SOCIALES EN EL ESTADO COLOMBIANO - Ministerio de Tecnologías de la Información y las Telecomunicaciones MinTIC

15. FORMATOS ANEXOS

NOMBRE DEL FORMATO	DESCRIPCION
FORM INV-TI	**Formato Control de Inventario Tecnológico**
FORM INV-EQACT-RED	**Formato Control de Inventario de Equipos Activos de Red Puntos y Puertos**
FORM AUDIT-SOFT	**Formato Auditoria al Software de la CMP**
FORM CRON-MANT-PREV	**Formato Programación de Mantenimientos Preventivos Equipos Tecnológicos**
FORM PREST-BIENES-TI	**Formato para préstamo de bienes tecnológicos (Para el área de inventarios)**

16. BIBLIOGRAFÍA

- GUIA PARA LA GESTIÓN DE DOCUMENTOS Y EXPEDIENTES ELECTRÓNICOS - MINTIC
- LINEAMIENTOS DE ADMINISTRACIÓN DE SEGURIDAD TIC – PRESIDENCIA DE LA REPÚBLICA DE COLOMBIA
- GUIA DE METADATOS – ARCHIVO GENERAL DE LA NACIÓN
- GUIA ESQUEMA DE METADATOS DE BOGOTA PARA DOCUMENTOS ELECTRÓNICOS DE ARCHIVO
- LINEAMIENTOS Y RECOMENDACIONES PARA USO DE MEDIOS SOCIALES EN EL ESTADO COLOMBIANO- MINTIC
- GUIA DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN - MINTIC
- GUIA PARA LA DIGITALIZACION DE DOCUMENTOS – PRESIDENCIA DE LA REPUBLICA

VIGENCIA

La presente política rige a partir de la publicación del documento aprobado por el comité de SGC y publicada la actualización de Las Políticas para la Administración de las TIC en la Contraloría de Municipal de Pereira.