1. OBJETIVO

Las políticas de Uso de Servicios, Recursos Informáticos y Telecomunicaciones tienen por objeto establecer las medidas de índole técnica y de organización, necesarias para garantizar la seguridad de los recursos tecnológicos y de las personas que interactúan haciendo uso de los servicios, reduciendo los riesgos asociados a pérdida de información y/o accesos no autorizados a la infraestructura tecnológica además de asegurar el eficiente cumplimiento de las funciones sustantivas del Ente Territorial apoyadas en un correcto sistema de información.

2. ALCANCE

La política de uso de servicios, recursos informáticos y telecomunicaciones se implementa en cumplimiento de las disposiciones legales vigentes, con el objeto de gestionar la seguridad de la información, los sistemas informáticos y el ambiente tecnológico de Las Ceibas Empresas Públicas de Neiva E.S.P.

Es de obligatorio cumplimiento para todas las dependencias que conforman Las Ceibas Empresas Públicas de Neiva E.S.P., sus recursos, los procesos internos o externos vinculados a través de contratos o acuerdos con terceros y a todo el personal, cualquiera sea su situación contractual, la dependencia a la cual se encuentre adscrito y el nivel de las tareas que desempeñe y a la ciudadanía en general.

3. TERMINOLOGÍA Y DEFINICIONES

SISTEMAS DE INFORMACIÓN: Un sistema de información (SI) es un conjunto de elementos orientados al tratamiento y administración de datos e información, organizados y listos para su uso posterior, generados para cubrir una necesidad u objetivo.

INFRAESTRUCTURA TECNOLÓGICA: Se entiende por infraestructura tecnológica al conjunto de todos los elementos tecnológicos, hardware, y software: servidores, computadores, portátiles, impresoras, Switches, Router, firewall, escáner, cableado estructurado, equipos de comunicaciones, internet, redes.

BASE DE DATOS: Es un conjunto de datos pertenecientes a un mismo contexto y almacenados sistemáticamente para su posterior uso.

MULTIMEDIA: Tecnologías que involucren para su creación Voz, Audio y video.

APLICATIVOS: Programa informático que permite a un usuario utilizar un computador con un fin específico. Las aplicaciones son parte del software de una computadora, y suelen ejecutarse sobre el sistema operativo.

HARDWARE: El equipo físico que compone el sistema se conoce con la palabra inglesa "hardware", que en castellano se puede traducir como "soporte físico". Es el conjunto de dispositivos electrónicos y electromecánicos, circuitos y cables que componen el ordenador.

SISTEMAS OPERATIVOS: Es el software básico de una computadora que provee una interfaz entre el resto de los programas del computador, los dispositivos hardware y el usuario. Las funciones básicas del Sistema Operativo son administrar los recursos de la máquina, coordinar el hardware y organizar archivos y directorios en dispositivos de almacenamiento.

SOFTWARE: Para que el sistema trabaje, necesita que le suministren una serie de órdenes que indiquen qué es lo que queremos que haga. Estas órdenes se le suministran por medio de programas. El software o "soporte lógico" está compuesto por todos aquellos programas necesarios para que el ordenador trabaje. El software dirige de forma adecuada a los elementos físicos o hardware.

MESA DE AYUDA: La mesa de ayuda proporciona un único punto de contacto para todos los usuarios de servicios relacionados con las Tecnologías de Información, respondiendo a las preguntas y problemas, brinda un apoyo inmediato en línea acerca de los problemas relacionados con el software y hardware. La mesa de ayuda resuelve los requerimientos e indica los procedimientos para solicitar los servicios proporcionados por la Dirección de Arquitectura Empresarial y de Gobierno Abierto y deriva la llamada al personal apropiado.

GD (GOBIERNO DIGITAL): Política del Gobierno Nacional enfocada a la reducción de los trámites y servicios y el aumento de la transparencia de la gestión pública utilizando las tecnologías de la información y la comunicación, con el objetivo de generar valor público.

BACK UP: Es la copia total o parcial de información importante del disco duro, CD´s, bases de datos u otro medio de almacenamiento. Esta copia de respaldo debe ser guardada en algún otro sistema de almacenamiento masivo.

RECURSOS INFORMÁTICOS: Son las aplicaciones, herramientas, dispositivos (periféricos) y capacidades con los que cuenta una computadora

4. SOPORTE NORMATIVO

- Ley 1581 de 2012 Por la cual se dictan disposiciones generales para la protección de datos personales.
- LEY 1474 DE 2011 Por la cual se dictan normas orientadas a fortalecer los mecanismos de prevención, investigación y sanción de actos de corrupción y la efectividad del control de la gestión pública.
- Ley 1266 de 2008 Por la cual se dictan las disposiciones generales del hábeas data y se regula el manejo de la información contenida en bases de datos personales, en especial la financiera, crediticia, comercial, de servicios y la proveniente de terceros países y se dictan otras disposiciones.
- Decreto 1078 de 2015 Por medio del cual se expide el Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones

- Decreto 3572 de 2014 Por el cual se establecen los lineamientos generales de la Estrategia de Gobierno en línea, se reglamenta parcialmente la Ley 1341 de 2009 y se dictan otras disposiciones.
- Decreto 2573 DE 2014 Por el cual se establecen los lineamientos generales de la Estrategia de Gobierno en línea, se reglamenta parcialmente la Ley 1341 de 2009 y se dictan otras disposiciones.
- Decreto 3816 de 2013 Por el cual se crea la Comisión Intersectorial de Políticas y de Gestión de la Información para la Administración Pública.
- Decreto 1151 del 2008 Por el cual se establecen los lineamientos generales de la Estrategia de Gobierno en Línea de la República de Colombia, se reglamenta parcialmente la Ley 962 de 2005, y se dictan otras disposiciones.

5. CONDICIONES GENERALES

Las Ceibas Empresas Públicas de Neiva E.S.P., determina una política de administración y uso de las tecnologías de la información y las comunicaciones, para asegurar el desempeño adecuado de sus procesos y asegurar la prestación del servicio de acueducto y alcantarillado con continuidad, eficacia, eficiencia y efectividad; para lo cual asegura que:

- Esté alineada con los objetivos de la entidad.
- Identifica los servicios ligados a las tecnologías de la información y las comunicaciones para cada uno de los procesos.
- Determina las acciones a desarrollar, teniendo en cuenta tiempo, recursos, responsables y talento humano requerido.
- Verifica su cumplimiento a través de la gestión realizada por la subgerencia TIC de Las Ceibas Empresas Públicas de Neiva E.S.P.

6. POLÍTICAS ADMINISTRACIÓN Y USO DE LAS TECNOLOGIAS DE LA INFORMACIÓN Y LAS COMUNICACIONES

6.1. POLITICAS DE USO DE SERVICIOS

6.1.1. USO DE CONTRASEÑAS Y CONTROL DE ACCESO A LA RED DE DATOS

Todos los usuarios que acceden a recursos informáticos de la red de Las Ceibas Empresas Públicas de Neiva E.S.P. requieren de una identificación (única e intransferible), la cual consiste en un nombre de usuario con su respectiva contraseña.

La Subgerencia TIC, entrega un usuario y contraseña a cada funcionario, mediante formato "**ASIGNACIÓN DE USUARIO (GTI-FR-02)"**; la cual es de carácter privado e individual.

Es responsabilidad de cada usuario manejar la confidencialidad de esta identificación, por lo tanto, se recomienda no entregar su cuenta de usuario, ni contraseña a nadie.

Cada usuario es responsable de cambiar periódicamente su contraseña de acceso al sistema, mínimo cada mes.

Ningún usuario debe utilizar la identificación (nombre de usuario y contraseña) de otro usuario para acceder a los servicios de la red (por ejemplo: los diferentes sistemas de información, el correo electrónico, la agenda y todos los servicios en general).

En caso de retiro del funcionario y/o contratista, se debe cancelar los derechos otorgados como usuario informático.

6.1.2. USO DEL CORREO ELECTRÓNICO

El uso del correo electrónico es primordial para el apoyo en el desempeño de las labores inherentes a cada cargo y facilita la comunicación y conectividad institucional.

Todo usuario del correo electrónico institucional debe leer y responder oportunamente los mensajes y citaciones que se le envíen por este medio; con el fin de aprovechar el mayor beneficio que ofrece este servicio, rapidez y efectividad de las comunicaciones. Acorde a esto se establece la **"POLÍTICA DE USO CORREO ELECTRÓNICO INSTITUCIONAL (GTI-DA-02)"**, mediante la cual se asegura una comunicación adecuada y trazabilidad de la información enviada a través de correo electrónico tanto por personal de planta como contratistas, Las Ceibas Empresas Públicas de Neiva E.S.P, asigna a su recurso humano de planta o contratista según lo requiera una cuenta de correo electrónico institucional (@lasceibas.gov.co) bajo OFFICE365, para lo cual la aplicación de esta política busca establecer las responsabilidades y lineamientos mínimos que deben cumplir los usuarios del correo institucional para garantizar su correcto uso y asegurar un mejor aprovechamiento del correo como una herramienta de trabajo y de esta manera evitar la exposición de la empresa a pérdidas de información y/o daño a los recursos disponibles.

6.1.3. USO DE INTERNET

Con el ánimo de fomentar la investigación y la búsqueda de nuevos conocimientos relacionados con su trabajo, que contribuyan a su mejoramiento personal y/o profesional, deberá usarse moderadamente y siguiendo los lineamientos establecidos en estas políticas:

Internet es para el uso de investigación y la búsqueda de información relacionados con su trabajo; y como tal este deberá primar sobre cualquier otro objetivo o uso que se le quiera dar; cualquier uso inadecuado de estos servicios que interfiera con la imagen de Las Ceibas Empresas Públicas de Neiva E.S.P. es considerado una violación a esta política y está sujeto a las sanciones correspondientes.

Las Ceibas Empresas Públicas de Neiva E.S.P. 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; en caso de que un usuario considere necesario acceder a alguna dirección incluida en una de las categorías filtradas, debe hacer solicitud mediante la Mesa de servicio de la subgerencia TIC.

Se deberán adoptar las siguientes directrices:

a) Por motivos de seguridad y para evitar virus, está prohibido la descarga de software desde Internet; en caso de necesitar debe ser con la autorización expresa de la Subgerencia TIC.

b) En caso de necesitar descargar información desde Internet debe 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.

c) El usuario debe tener precaución al usar cuentas de FTP ANONYMOUS, debido a que estas cuentas llevan un registro de uso para sus propias estadísticas y análisis de utilización. Esto es, en virtud de que algunas anomalías en su uso pueden resultar perjudiciales para la Entidad por lo que le recomendamos consultar al personal de la subgerencia TIC.

d) 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.

e) El uso de Internet para la revisión de correo electrónico que el usuario tenga en otras páginas está permitido, pero cuando se haga desde un computador de la red de Las Ceibas Empresas Públicas de Neiva E.S.P., deben conservar los mismos lineamientos estipulados para la utilización del servicio de correo interno.

f) No se puede utilizar el servicio de Internet para ninguna actividad ilegal o que atente contra la ética, buen nombre y dignidad de Las Ceibas Empresas Públicas de Neiva E.S.P.

g) A través de Internet se puede acceder a otras redes de diferentes países, cada uno con normatividad diferente 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.

h) No es recomendable dejar abiertas páginas que se actualizan periódicamente ni varias conexiones simultáneas, ya que consumen recursos y congestionan la red innecesariamente.

i) El usuario no debe instalar ningún programa para escuchar MP3, RA, WAV, o emisoras de radio vía Internet.

6.1.4. SEGURIDAD PERIMETRAL

La seguridad perimetral es uno de los métodos posibles de protección de la Red, basado en el establecimiento de recursos de seguridad en el perímetro externo de la red y a diferentes niveles. Esto permite definir niveles de confianza, permitiendo el acceso de determinados usuarios internos o externos a determinados servicios, y denegando cualquier tipo de acceso a otros.

Firewall (UTM)

a) La solución de seguridad perimetral debe ser controlada con un Firewall por Hardware (físico) que se encarga de controlar puertos y conexiones, es decir, de permitir el paso y el flujo de datos entre los puertos, ya sean clientes o servidores.

b) Este equipo deberá estar cubierto con un sistema de alta disponibilidad que permita la continuidad de los servicios en caso de fallo.

c) El firewall debe bloquear las “conexiones extrañas” y no dejarlas pasar para que no causen problemas.

d) El firewall debe controlar los ataques de “Denegación de Servicio” y controlar también el número de conexiones que se están produciendo, y en cuanto detectan que se establecen más de las normales desde un mismo punto bloquearlas y mantener el servicio a salvo.

e) Controlar las aplicaciones que acceden a Internet para impedir que programas a los que se han permitido explícitamente acceso a Internet, puedan enviar información interna al exterior (tipo troyanos).

6.2. POLÍTICAS USO DE HARDWARE

6.2.1. USO DE EQUIPOS DE ESCRITORIO Y PORTÁTILES

Todo usuario de estos recursos debe velar por la preservación de estos, teniendo presente las siguientes directrices:

a) Mantener limpia la zona donde se encuentran los equipos.

b) No ingerir alimentos ni bebidas cerca o sobre los equipos; con ello se evita la caída o derrame que cause posible deterioro a los componentes de los equipos

c) El teclado y mouse deben ser tratados con suavidad, no hay necesidad de golpear o presionar fuertemente las teclas; por ningún motivo agarre estos elementos por el cable, puede ocasionar averías.

d) Realice el apagado del computador con el procedimiento adecuado para ello, que es con el sistema operativo Windows, opción apagar.

e) Los equipos y demás recursos informáticos asignados a cada funcionario son para uso en trabajos de la Entidad y no para realizar trabajos de tipo personal, tales como: colegio, universidad, postgrado, entre otros. Además, no deben ser usados como “laboratorio”, intentando manipular los archivos de configuración del sistema, para lo cual solo está autorizado el personal de la Subgerencia TIC.

f) Está totalmente prohibido el uso de los computadores, y recursos informáticos en general, por parte de personal ajeno a la Entidad.

g) Informar a la Subgerencia TIC cualquier novedad que se presente en la red, las aplicaciones, los equipos o sus instalaciones.

h) Ningún usuario puede desconectar o desconectar el hardware o alterar las conexiones existentes en la red de Las Ceibas Empresas Públicas de Neiva E.S.P. a fin de no alterar los recursos informáticos ofrecidos por la Entidad.

i) No se deben intercambiar elementos entre equipos sin la autorización de la Subgerencia TIC.

j) Solo el personal de la Subgerencia TIC está autorizado para realizar las configuraciones de los equipos e instalar el software en los mismos.

k) No se deben conectar equipos diferentes al computador, en las tomas color naranja (tomas de la UPS).

l) Por ningún motivo conecte equipos o impresoras adicionales sin previa autorización de la Subgerencia TIC.

m) Se debe tener especial cuidado con los cables, ya que de este depende una buena comunicación de los datos a través de la red.

n) Las revisiones técnicas de los equipos sólo pueden ser realizadas por personal autorizado de la Subgerencia TIC, por lo tanto, en ningún momento, quien opere o maneje determinado equipo, debe efectuar arreglos o intentos de reparación.

o) La responsabilidad de manejo, control, protección, administración y utilización del equipo está en cabeza de cada uno de los usuarios y cada uno de éstos tiene registrado en su cartera, los recursos informáticos asignados.

6.2.2. USO DE IMPRESORAS Y ESCANER

a) Ningún recurso de impresión y escáner puede usarse para fines diferentes a los asuntos de la Entidad. Las impresiones que se elaboren con estos recursos en ningún momento pueden ser de carácter personal.

b) En caso de presentar problemas al momento de imprimir y/o escanear, debe evitar manipular los elementos de la impresora, se debe reportar inmediatamente el incidente a la Mesa de servicio de la Subgerencia TIC.

6.2.3. USO DE LECTORES BIOMÉTRICOS

La Subgerencia TIC es la encargada de instalar y configurar los lectores biométricos, cualquier cambio debe ser autorizado por esta dependencia.

a) El lector biométrico debe ser tratado con suavidad, no hay necesidad de golpear o presionar fuertemente la ventana del lector de huellas; Presione de manera firme y pareja, el lector efectivamente capturara su huella.

b) No ingerir alimentos ni bebidas cerca o sobre los lectores biométricos; con ello se evita la caída o derrame que cause posible avería a los componentes de los equipos.

c) Informar a la Subgerencia TIC cualquier novedad que se presente en los lectores biométricos.

6.3. POLÍTICAS USO DE SOFTWARE

6.3.1. USO DE PROGRAMAS Y APLICATIVOS

a) Se prohíbe instalar y utilizar software no autorizado por la Subgerencia TIC.

b) Se prohíbe copiar archivos o programas de propiedad de Las Ceibas Empresas Públicas de Neiva E.S.P. y/o alterar el software instalado.

c) Ningún usuario o dependencia debe adquirir software sin la debida aprobación y autorización de la Subgerencia TIC.

d) Sólo personal autorizado por Subgerencia TIC puede realizar instalación de software en los computadores de la Entidad.

e) Todo programa o aplicación que desarrolle un funcionario de Las Ceibas Empresas Públicas de Neiva E.S.P. por encargo y autorización de los directivos de la Entidad, es propiedad de ésta, tanto en fuentes como en objetos.

f) El software instalado en los diferentes equipos de Las Ceibas Empresas Públicas de Neiva E.S.P., es de uso exclusivo de la Entidad y ningún usuario puede disponer de el para fines personales o de terceros.

g) Se prohíbe el retiro o copia de cualquier aplicativo o licencia propiedad de Las Ceibas Empresas Públicas de Neiva E.S.P., lo que constituye hurto y se convierte en piratería, con efectos penales.

h) No se permite instalar ni temporal, ni permanentemente, software que no haya sido adquirido por Las Ceibas Empresas Públicas de Neiva E.S.P. Si por algún motivo es necesario instalar un software de propiedad del usuario en un computador, debe hacerse bajo autorización de la Subgerencia TIC y la licencia debe permanecer en las instalaciones de la Entidad, durante el tiempo que se tenga instalado dicho software.

i) Todo software o aplicativa propiedad de Las Ceibas Empresas Públicas de Neiva E.S.P., debe tener la respectiva licencia que da derecho a su utilización; en caso de ser software de uso libre se debe tener el soporte de la página web que especifica dicho tipo de licencia.

j) Los siguientes casos se consideran copia ilegal de software (piratería) y está expresamente prohibido:

- **i.** Hacer copia de un programa o legítimo.
- **ii.** Piratería a través de boletines electrónicos (BBS) e Internet, cuando en un boletín electrónico se instala software con derechos de autor, sin la autorización del titular.
- **iii.** Se entiende como copia ilegal de un programa, la copia de este en otro medio, como DVD, disco externo o USB, desde el disco duro de un computador.

k) Las licencias server, otorgan derecho a instalar un software determinado en un servidor de red. Para acceder o utilizar los servicios del software del servidor, desde una estación de trabajo (cliente), es necesario adquirir una licencia de acceso de cliente; es decir, la licencia de servidor permite su instalación en el servidor de red, y la licencia de acceso de cliente permite utilizarla.

l) Teniendo en cuenta estas normas, Las Ceibas Empresas Públicas de Neiva E.S.P. define que, si en algún momento la Entidad se ve afectada por una situación de este tipo, el usuario del equipo responde en forma personal por las demandas legales y situaciones de deshonra que se cursen contra la Entidad.

m) Toda incidencia de funcionabilidad o técnica de los aplicativos se debe registrarse en la mesa de servicio de la subgerencia TIC.

n) Las claves de acceso a los aplicativos, los da la Subgerencia TIC, con la autorización de los jefes inmediatos del área respectiva o por el líder del aplicativo.

o) Se deben cancelar o suspender los permisos de los usuarios a la aplicativa previa notificación, cuando se le solicite mediante un documento explícito por el área usuaria en los siguientes casos:

- **i** Si la cuenta no se está utilizando con fines institucionales.
- **ii** Si pone en peligro el buen funcionamiento de los sistemas.
- **iii** Si se sospecha de algún intruso utilizando una cuenta ajena.

p) Se deberá ingresar de forma remota a computadoras única y exclusivamente para la solución de problemas a los aplicativos, de acuerdo con solicitud explícita y autorización del supervisor del contrato o si el contrato de mantenimiento lo expresa.

q) No se debe realizar pruebas en los aplicativos que estén en ambiente de producción.

r) Cuando el proveedor libere una nueva versión del aplicativo, se debe primero instalar en el servidor de pruebas y una vez sea revisado y comprobado su funcionamiento correcto por parte de los usuarios, se instala en el servidor de producción.

s) Para la adquisición de aplicativos se deberá cumplir con lo establecido en la Ley de contratación y adquisición de bienes.

t) El software aplicativo licenciado por la entidad no podrá ser copiado o reproducido para darle utilización en aspectos diferentes a los definidos en su adquisición o intereses particulares.

6.3.2. ANTIVIRUS

a) Todos los equipos de cómputo de Las Ceibas Empresas Públicas de Neiva E.S.P. deberán tener instalada una solución Antivirus.

b) Periódicamente se debe realizar el rastreo en los equipos de cómputo de Las Ceibas Empresas Públicas de Neiva E.S.P., y se realizará la actualización de las firmas de antivirus proporcionadas por el fabricante de la solución antivirus en los equipos conectados a la Red.

c) La detección y bloqueo automático de ataques de red y a navegadores de internet, debe permanecer activado globalmente.

d) El usuario no deberá desinstalar la solución antivirus de su computadora pues ocasiona un riesgo de seguridad ante el peligro de virus.

e) Si el usuario hace uso de medios de almacenamiento personales, éstos serán rastreados por la solución antivirus en la computadora del usuario o por el equipo designado para tal efecto.

f) El usuario deberá comunicarse con la Subgerencia TIC en caso de problemas de virus para buscar la solución.

6.4. POLÍTICAS DE USO Y MANEJO DE LA INFORMACIÓN

La información es uno de los activos más valiosos de una organización por lo tanto debemos cumplir con las siguientes normas para el manejo de esta:

a) Cada que se borren archivos y se envíen a la papelera de reciclaje, se debe tener la precaución de eliminarla al finalizar la sesión de trabajo con el perfil de usuario respectivo, de lo contrario cualquiera podría recuperar sus archivos y obtener información privada, además de que se estaría llenando inadvertidamente el disco duro.

b) Las carpetas compartidas con determinados usuarios deben ser restringidas mediante permisos para que solo accedan los usuarios autorizados.

c) Está prohibido divulgar información reservada de la Entidad a otras personas de la misma Entidad o terceros, si no se está autorizado para ello.

d) No se permite alterar o manipular información en contra de la Entidad.

e) No se permite borrar la información contenida en los equipos de cómputo de la entidad, salvo comprobación por parte de la subgerencia TIC.

f) Los usuarios deben tener la precaución de bloquear la sesión de trabajo en el sistema, cada vez que se ausenten de su escritorio, para que no se pierda la confidencialidad de la información que está a su cargo.

g) Es responsabilidad de cada usuario la confidencialidad de sus claves como de la información de los aplicativos y del uso que se le dé, por lo tanto, se recomienda que no compartan las claves con otras personas.

h) Los usuarios deberán velar por que los datos que se registran a través de la aplicación que estén operando, que sean exactos de acuerdo con las operaciones o documentos que estén ingresando y puestos al día en la actualización de estos.

i) El acceso de terceras personas, a los aplicativos debe ser autorizado e identificado plenamente, controlado y vigilado durante el acceso, por el supervisor del contrato de mantenimiento

6.5. POLÍTICA DE USO DE LAS COPIAS DE SEGURIDAD

a) La Subgerencia TIC es responsable de efectuar el procedimiento para la copia de seguridad que se realiza a las bases de datos de los servidores que tiene bajo su custodia.

b) Cada usuario es responsable de mantener respaldada su información más relevante, con el fin de poder recuperarla en caso de daños de su equipo, en caso de no tener los medios necesarios deberá reportar a la subgerencia TIC para el apoyo en la actividad.

c) Cualquier dependencia, funcionario o tercero que requiera la copia de una de las bases de datos de la Entidad, debe pedir la respectiva autorización a la gerencia de Las Ceibas Empresas Públicas de Neiva E.S.P. o a través de la subgerencia TIC.

d) Los usuarios son los responsables de realizar periódicamente el respaldo de la información vital de su misión, así mismo el jefe de cada dependencia debe reportar dicha información a la subgerencia TIC para que esta implemente las políticas necesarias para el resguardo de su información, estipulando mecanismos y tiempos para la realización de las copias de seguridad y controlar el cumplimiento de este procedimiento.

7. CONTROL DE CAMBIOS

VERSIÓN	DESCRIPCIÓN DEL CAMBIO	FECHA
01	Versión inicial	23/01/2023
02	Modificación del nombre del proceso GESTIÓN DE TECNOLOGÍAS DE LA INFORMACIÓN Y LA COMUNICACIÓN con código (TI) por GESTIÓN DE TECNOLOGÍA DE LA INFORMACIÓN Y LA COMUNICACIÓN TIC con código (GTI). Por lo tanto,	02/10/2023

	el código pasa de TI-D-05 a GTI-DA-05. En el numeral 6.1.1. USO DE CONTRASEÑAS Y CONTROL DE ACCESO A LA RED DE DATOS se modifica el Código del formato referenciado a "GTI-FR-02" y en el numeral 6.1.2. USO DEL CORREO ELECTRONICO se modifica el código del documento referenciado a "GTI-DA-02". Según lo establecido en el procedimiento GI-PR-01 INFORMACION DOCUMENTADA versión 16.	