PROGRESO PARA NUNCHÍA

MANUAL DE PROCEDIMIENTOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACION (MPSI)

FREDY HIGUERA MÁRQUEZ
Alcalde Municipal

EQUIPO DE GOBIERNO

SANDRA JUDITH GARZON MALDONADO
Secretaría de Desarrollo Social

PEDRO MALDONADO MACIAS
Secretaría de Hacienda

DIEGO ORLANDO GONZALEZ ROA
Secretaría de Planeación y Obras Públicas

ENRIQUETA FORERO PARADA
Secretaría General y de Gobierno

GELBER VARGAS
Director UAESP

WALTER ACHAGUA
Control Interno

FABIO ANRES MARQUEZ
Almacén Municipal

Elaboró
CÉSAR NEYITH OSORIO MOLINA
Web Máster, Sistemas y Enlace TIC

TABLA DE CONTENIDO

Contenido

INTRODUCCION

La seguridad de la información es una prioridad para la administración municipal, es por eso que en este documento se implementa reglas y lineamientos técnicos para el uso controlado de activos de información que minimice el riesgo de pérdida de datos, accesos no autorizados, divulgación no controlada, duplicación e interrupción intencional de la información y demás amenazas que afecten la integridad de la información. Por lo tanto es deber de los funcionarios, contratistas y/o terceros acatar y proteger las políticas que este documento expresa con el fin de asegurar la continuidad de los procesos, actividades y servicios de igual manera maximizando la eficiencia y la mejora continua de los procesos administrativos para con la comunidad.

MARCO LEGAL

Derechos de Autor

Ley 44 de 1993

Por el cual de modifica y adiciona la Ley 23 de 1982 y se modifica la Ley 29 de 1944

Ley 565 de 2000

Por medio de la cual se aprueba el "Tratado de OMPI-Organización Mundial de la Propiedad Intelectual – sobre Derechos de Autor (WTC)", adoptado en Ginebra, el 20 de Diciembre de 1996.

Ley 603 de 2000

Esta ley se refiere la protección de los derechos de autor en Colombia.

Ley 719 de 2001

Por cual se modifican las Leyes 23 de 1982 y 44 de 1993 y se dictan otras disposiciones.

Decreto 1377 de 2013

Decreto por el cual se reglamenta parcialmente la Ley 1581 de 2012.

Decreto 460 de 1995

Por el cual se reglamente el Registro Nacional del Derecho de Autor y se regula el Deposito Legal.

Decreto 162 de 1996

Por el cual se reglamenta la Decisión Andina 351 de 1993 y la Ley 44 de 1993, en relación con las Sociedades de Gestión Colectiva de Autor o de Derechos Conexos.

Decreto 1360 de 1989

Por el cual se reglamente la inscripción de soporte lógico (software) en el Registro Nacional del Derecho de Autor.

Propiedad Industrial

Ley 463 de 1998

Por medio de la cual se aprueba el "Tratado de cooperación en materia de patentes (PCT)", elaborado en Washington el 19 de Junio de 1970, enmendado el 28 de Septiembre de 1979 y modificado el 3 de Febrero de 1984, y el reglamento del tratado de cooperación en materia de Patentes.

Ley 170 de 1994

Por medio de la cual se aprueba el Acuerdo por el que se establece la Organización Mundial de Comercio (OMC), suscrito en Marrakech (Marruecos) el 15 de abril de 1994, sus acuerdos multilaterales anexos y el Acuerdo Plurilateral anexo sobre la Carne de Bovino.

Ley 178 de 1994

Por medio de la cual se aprueba el "Convenio de París para la Protección de la Propiedad Industrial", hecho en París el 20 de Marzo de 1883, revisado en Bruselas el 14 de diciembre de 1900, en Washington el 2 de junio de 1911, en la Haya el 6 de noviembre de 1925, en Londres el 2 de Junio de 1934, en Lisboa el 31 de octubre de 1958, en Estocolmo el 14 de julio de 1967 y enmendado el 2 de octubre de 1979.

Decreto 2591 de 2000

Por el cual se reglamenta parcialmente la Decisión 486 de la Comisión de la Comunidad Andina.

Ley 1341 de 2009

Por la cual se definen los principios y conceptos sobre la sociedad de la información y la organización de las Tecnologías de la información y las comunicaciones-TIC-, se crea la Agencia Nacional del Espectro y se dictan otras disposiciones.

Comercio Electrónico y Firmas Digitales

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.

Decreto 1747 de 2000

Por el cual se reglamenta parcialmente la Ley 527 de 199, en los relacionados con las entidades de certificación, los certificados y las firmas digitales.

Resolución 26930 de 2000

Por la cual se fijan los estándares para la autorización y funcionamiento de las entidades de certificación y sus auditores.

Ley 1266 de 2008

Por la cual se dictan las disposiciones generales del Habeas Data y se regula el manejo de la información contenida en bases de datos personales, en especial la financiera, crediticia, comercial, de servicios y la proveniente de terceros países y se dictan otras disposiciones.

Ley 1273 de 2009

Por medio de la cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado – denominado “de la protección de la información y de los datos”- y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones.

Ley 1712 de 2014

Por medio de la cual se crea la ley de transparencia y del derecho de acceso a la información pública nacional y se dictan otras posiciones.

GLOSARIO

Seguridad de la Información: Conjunto de medidas preventivas y reactivas de las organizaciones y de los sistemas tecnológicos que permiten resguardar y proteger la información buscando mantener la confidencialidad, la disponibilidad e integridad de datos y de la misma.

Acceso a la Información: Conjunto de técnicas para buscar, categorizar, modificar y acceder a la información que se encuentra en un sistema de bases de datos, bibliotecas, archivos e Internet.

Roles y Privilegios: La autenticación para verificar la identidad, para demostrar que una persona es quien dice ser y también para permitir una política de autorización con el fin de definir qué es lo que determinada identidad puede "ver y hacer" con la información.

Seguridad de Comunicaciones: Consiste en prevenir que alguna entidad o persona no autorizada pueda interceptar comunicaciones o acceder de forma inteligible a información.

Software: Se conoce como software al equipo lógico o soporte lógico de un sistema informático, que comprende el conjunto de los componentes lógicos necesarios que hacen posible la realización de tareas específicas, en contraposición a los componentes físicos que son llamados hardware.

Hardware: Partes físicas tangibles de un sistema informático; sus componentes eléctricos, electrónicos, electromecánicos y mecánicos. Cables, gabinetes o cajas, periféricos de todo tipo y cualquier otro elemento físico involucrado.

Seguridad Lógica: Medidas establecidas por la administración de usuarios y administradores de recursos de tecnología de información para minimizar los riesgos de seguridad asociados con sus operaciones cotidianas llevadas a cabo utilizando los recursos tecnológicos y medios de información.

Inventario Tecnológico: Se refiere al inventario de dispositivos electrónicos que hacen parte de los activos de la entidad.

Topología de Red: Se define como el mapa físico o lógico de una red para intercambiar datos. En otras palabras, es la forma en que está diseñada la red, sea en el plano físico o lógico. El concepto de red puede definirse como "conjunto de nodos interconectados".

Router: También conocido como enrutador o encaminador de paquetes es un dispositivo que proporciona conectividad a nivel de red o nivel tres en el modelo OSI. Su función principal consiste en enviar o encaminar paquetes de datos de una red a otra.

Switch: Dispositivo digital lógico de interconexión de equipos que opera en la capa de enlace de datos del modelo OSI. Su función es interconectar dos o más segmentos de red, de manera similar a los puentes de red, pasando datos de un segmento a otro de acuerdo con la dirección MAC de destino de las tramas en la red y eliminando la conexión una vez finalizada esta.

Servidor: El término *servidor* es ampliamente utilizado en el campo de las tecnologías de la información. A pesar de la amplia disponibilidad de productos etiquetados como productos de servidores (tales como versiones de hardware, software y OS diseñadas para servidores), en teoría, cualquier proceso computacional que comparta un recurso con uno o más procesos clientes es un servidor.

Licenciamiento: Una licencia de software es un contrato entre el licenciante (autor/titular de los derechos de explotación/distribuidor) y el licenciatario del programa informático (usuario consumidor /usuario profesional o empresa), para utilizar el software cumpliendo una serie de términos y condiciones establecidas dentro de sus cláusulas.

Seguridad de Aplicaciones: Es una rama de la Seguridad Informática que se encarga específicamente de la seguridad de sitios web, aplicaciones web y servicios web.

Sistema Operativo: Programa o conjunto de programas de un sistema informático que gestiona los recursos de hardware y provee servicios a los programas de aplicación de software, ejecutándose en modo privilegiado respecto de los restantes.

Seguridad Física: Consiste en la aplicación de barreras físicas y procedimientos de control como medidas de prevención y contra medidas ante amenazas a los recursos y la información confidencial, se refiere, a los controles y mecanismos de seguridad dentro y alrededor de la obligación física de los sistemas informáticos así como los medios de acceso remoto al y desde el mismo, implementados para proteger el hardware y medios de almacenamiento de datos.

Equipamiento: Dícese de bienes materiales, físicos, destinados a soportar directa o indirectamente los servicios que presta la organización, siendo pues depositarios temporales o permanentes de los datos, soporte de ejecución de las aplicaciones informáticas o responsables del procesado o la transmisión de datos.

Rack: Soporte metálico destinado a alojar equipamiento electrónico, informático y de comunicaciones. Las medidas para la anchura están normalizadas para que sean compatibles con equipamiento de distintos fabricantes. También son llamados bastidores, cabinas, gabinetes o armarios.

Cuarto de Comunicaciones: Es un área utilizada para el uso exclusivo de equipos asociados con el sistema de cableado de telecomunicaciones de la entidad. El cuarto de telecomunicaciones debe ser capaz de albergar los equipos de telecomunicaciones, terminaciones de cable y cableado de interconexión asociado.

Soporte Técnico: Rango de servicios por medio del cual se proporciona asistencia a los usuarios al tener algún problema al utilizar un producto o servicio, ya sea este el *hardware* o *software* de una computadora de un servidor de Internet, periféricos, artículos electrónicos, maquinaria, o cualquier otro equipo o dispositivo.

Incidencias: Circunstancia o suceso secundario que ocurre en el desarrollo de un asunto o negocio, pero que puede influir en el resultado final.

Red de datos: Una red de datos es un conjunto de ordenadores que están conectados entre si compartiendo recursos, información, y servicios.

Dispositivos de Red: Las redes o infraestructuras de telecomunicaciones proporcionan la capacidad y los elementos necesarios para mantener a distancia un intercambio de información y/o comunicación, ya sea en forma de voz, datos y videos.

OBJETIVO GENERAL

Promover de forma clara y coherente los elementos que conforman la política de seguridad que deben cumplir los funcionarios, contratistas y terceros que presten sus servicios o tengan al algún tipo de relación con la Administración Municipal “Progreso para Nunchía 2016-2019”

OBJETIVO ESPECIFICO

- Crear, implementar y concientizar a los funcionarios, contratistas y proveedores de la administración municipal de Nunchía sobre la seguridad de la información y su importancia.
- Actualizar los procesos informáticos de la administración Municipal con el fin de mejorar el desarrollo de las actividades institucionales y sus servicios.

VISIÓN

Para el año 2025 Nunchía será un territorio de Paz con una economía propia de impacto local y regional destacada por una oferta de servicios agroindustriales, turísticos y ambientales, que generen un desarrollo sostenible y sustentable en lo humano, lo físico, lo económica, lo social y lo ambiental para todos sus habitantes, quienes gozaran de una mejor calidad de vida con oportunidades de trabajo digno, inclusión y participación social.

MISION

Nunchía es una entidad territorial comprometida con la prestación eficiente de los servicios públicos y con el enaltecimiento de los principios y los valores humanos para garantizar bienestar y la calidad de vida de todos sus habitantes a través de una gerencia pública eficaz en el uso racional de los recursos humanos, financieros, físicos y tecnológicos, que ayuden a impulsar el desarrollo físico, humano, económico, social y ambiental del municipio.

1. POLITICAS DE SEGURIDAD

a.) ACCESO A LA INFORMACION:

De acuerdo a las actividades del contratista y el manual de funciones de cada dependencia, únicamente tendrán acceso a la información necesaria para el desarrollo de sus actividades.

Los usuarios de los sistemas de información que la administración municipal posee o adquiera tendrán un único usuario y contraseña para consulta y edición de la información, dependiendo del área o dependencia, los funcionarios tendrán acceso a la información, dicho acceso será controlado por el Secretario o quien haga sus veces, quien a su vez será responsable del hurto, sustracción daño parcial o total de la información que se genere, ingrese y se edite en el área que tiene a cargo.

El área de control interno estará delimitando las políticas de acceso a la información mediante el cumplimiento del presente documento, de igual manera notificara al encargado se sistemas los cambios de funcionarios o usuarios en los sistemas de información para el respectivo cambio de usuario y contraseña o en su defecto la eliminación de la cuenta.

b.) SEGURIDAD DE LA INFORMACION:

Los funcionarios, contratistas y proveedores de la Alcaldía Municipal de Nunchía son responsables de la información que por medio magnético, escrito o verbal le sea entregado y cumplirán de igual manera con los principios de confidencialidad protegiendo la integridad de la información y la buena imagen de la Entidad Municipal.

Llegado el caso un funcionario, contratista o proveedor tenga acceso a información la cual no es de su área o dependencia deberá informar en el menor tiempo posible a la oficina de control Interno o al funcionario encargado de sistemas.

c.) SEGURIDAD PARA SERVICIOS INFORMATICOS:

Se entiende por servicios informáticos todas aquellas plataformas de escritorio o vía web que facilitan el desarrollo de las actividades de los funcionarios, contratistas y proveedores de la administración Municipal.

Correo Electrónico:
Las cuentas de correo son creadas por el Ministerio de las TIC con el fin de mejorar la comunicación entre entidades públicas a nivel nacional, departamental e interno, por lo tanto serán las únicas cuentas de correo utilizadas para el desarrollo de las actividades y no se deberá reproducir, copiar y enviar información por distintas cuentas de correo, se hará excepciones en las cuales el Secretario o quien haga sus veces autorice y será responsable por la información.
El correo institucional cuenta con un servicio de chat el cual deberá ser usado de manera responsable para la comunicación interna administrativa con el fin de reducir costos en llamadas telefónicas e impresiones.

d.) Seguridad en estaciones de trabajo:
Una vez el funcionario se le asigne un equipo de cómputo o dispositivos será responsable por la información e integridad de los equipos y mantendrá las configuraciones que se le asignen.

- ***Administración de usuarios:***
  Cada funcionario deberá crear una contraseña de mínimo 8 caracteres incluyendo números, letras mayúsculas, letras minúsculas y símbolos, esta contraseña deberá cambiarse con una periodicidad mensual y no podrá ser repetida.

- ***Roles y privilegios de acceso a la información:***
  El funcionario y/o contratista solo podrá acceder a la información para el buen desarrollo de sus actividades el cual lo especificara el manual de funciones o contrato.

e.) Seguridad de Comunicaciones:
Las bases de datos, información contable, claves de acceso, aplicaciones web o de escritorio, información personal y sistemas de información que no sea autorizada para la publicación por el Alcalde Municipal, Secretario de la dependencia o Supervisor, deberá ser tratada como información reservada y será prohibida su reproducción, edición, impresión o divulgación.

f.) Software de la Entidad:
Todo software que ingrese a la entidad municipal deberá ser adquirido bajo el marco legal vigente, de igual manera deberá tener un manual de usuario, manual de seguridad, proveedor, tipo de licenciamiento y fecha de

caducidad de la licencia, además, el proveedor deberá dejar copia a la entidad de las capacitaciones y soporte técnico ofrecido.

g.) Actualización de hardware:

La adquisición de nuevos equipos se deberá realizar bajo la norma técnica de estandarización, registros de soporte técnico y control de insumos para la toma de decisiones de adquisición de equipos y dispositivos.

h.) Equipos de cómputo personales:

No se permitirán equipos personales en las instalaciones de la alcaldía municipal, en caso de ser necesario, se deberá estudiar la adquisición de nuevos equipos de cómputo, se notificara mediante oficio al alcalde municipal quien a su vez autorizará y notificará a control interno y al funcionario encargado de sistemas, para permitir el ingreso de un equipo personal por parte de un funcionario.

i.) Disposición de la Información:

En los escritorios de los funcionarios de la administración municipal no deberán reposar, USB, Discos Duros Externos, Documentos Impresos o cualquier dispositivo de almacenamiento, todo esto con el fin de reducir los riesgos de acceso no autorizado a la información, deberán estar en un gabinete bajo llave según lo considere el Secretario o quien haga sus veces.

j.) Prácticas de uso de Internet:

Los funcionarios de la administración municipal deberán tener en cuenta las siguientes normas para el acceso a Internet.

- No tendrán acceso a las redes sociales, chats, blogs u otras plataformas que no sean para el buen desarrollo de sus actividades se realizaran excepciones previa autorización y supervisión del Secretario o quien haga sus veces.
- No se permitirán descargas Multimedia, aplicaciones, etc., que no sean autorizadas por el Secretario y funcionario encargado del área sistemas de la administración municipal.
- No abrir correos, archivos adjuntos o aplicaciones desconocidas, ya que pueden estar infectados con software malicioso (virus), en caso de ser abiertos o iniciados, informar al funcionario encargado de Sistemas en el menor tiempo posible.
- Se establecerán políticas internas de las dependencias o secretarias para salvaguardar la integridad y confidencialidad de la información y los

dispositivos, ya sea mediante el software antivirus u otro aplicativo previamente autorizado por el funcionario encargado del área de sistemas.

- Los funcionarios de la administración municipal no podrán utilizar la cuenta de correo institucional con fines personales.
- Todos los funcionarios, contratistas y proveedores tienen prohibido descargar, consultar o reproducir contenido sexual o material pornográfico tanto de internet como en los equipos de cómputo.

2. SEGURIDAD LOGICA

2.1 INVENTARIO TECNOLOGICO

- Se realizará un inventario tecnológico donde se tenga un registro verídico de la cantidad de equipos de cómputo con que cuenta la entidad.
- Se creará un registro de custodia por parte de almacén municipal de los equipos, impresoras u otros dispositivos asignados a cada funcionario y/o contratista (**Anexo 5**).

2.2 USUARIOS, CONTRASEÑAS Y PRIVILEGIOS

- Con base en el registro de custodia responsabilidad de los equipos de cómputo pertenecientes a la administración municipal se crearán usuarios y contraseñas para el inicio de sesión en cada una de las estaciones de trabajo. Estas claves serán administradas por el contratista del área de sistemas.
- Los privilegios que sean asignados a cada funcionario o contratista dependerán de las actividades que le sean asignadas según el manual de funciones de la Administración Municipal o en su contrato, dichos privilegios no excederán ni limitaran el buen desarrollo de las actividades.
- El usuario administrador de todos los equipos de cómputo de la administración municipal será el encargado del área de sistemas, los demás privilegios serán asignados de acuerdo al manual de funciones y/o actividades del contratista.
- Se realizaran revisiones mensuales de las claves de acceso, realizando comprobaciones de cantidad de usuarios, El área de talento humano o quien haga sus veces, al igual que las Secretarías notificaran cambios en el personal por medio escrito.
- Se realizará una base de datos con los usuarios y contraseñas mensuales de los funcionarios y contratistas que tengan bajo su custodia un equipo de cómputo o dispositivo, se realizarán cambios de contraseñas según la periodicidad requerida.
- Cada funcionario deberá limpiar de manera cuidadosa los equipos que tiene a cargo de tal manera que se alargue la vida útil de los dispositivos.

- No se permitirá el uso de equipos de propiedad de la administración municipal a terceros sin previa autorización del secretario o quien haga sus veces y al contratista encargado del área de sistemas.

Pasantes o Practicantes

- Se les permitirá el ingreso de equipos de cómputo u otros dispositivos mediante solicitud y aprobación escrita a la secretaria con copia al área de sistemas y control interno.
- La conexión a internet que se otorgará será por cable y cumplirá con las demás disposiciones que en este documento expresa.
- La administración Municipal no se hará responsable por daño eléctrico, infección por virus, daño a la integridad del equipo hurto o perdida.
- No podrá acceder a la información de la administración municipal sin previa autorización de la Secretaria a la cual el pasante o practicante se encuentre adscrito y deberá ser informado a control interno y al funcionario encargado del área de sistemas.

Las contraseñas de aplicativos, correos electrónicos, equipos de cómputo o cualquier otro sistema de información deberán cumplir las siguientes especificaciones:

- Mínimo 8 caracteres que contenga letras mayúsculas, minúsculas, símbolos y números.
- No deberán contener nombres de los funcionarios, nombre o lema de la administración municipal, nombre de usuario o documento de identidad del contratista.
- El procedimiento para reinicio de contraseñas y/o usuarios de accesos se realizara la solicitud mediante comunicación escrita al encargado de sistemas de la administración municipal.

3. SEGURIDAD DE COMUNICACIONES

3.1 TOPOLOGIA DE RED

- Deberá existir documentación magnética e impresa sobre la tipología de red y diagramas topológicos de la ubicación de los puntos de red.
- Se creará una base de datos con los distintos usuarios y contraseñas de los dispositivos de red (Router, Switch, servidores, etc.)

3.2 CONEXIONES

- La conexión a internet será suministrada únicamente para temas relacionados con el buen desarrollo de las actividades de los funcionarios y/o contratistas según el manual de funciones o contrato.
- Las claves de acceso a internet inalámbrico de la entidad se realizará la solicitud mediante un formato que será firmado por el Secretario o quien haga sus veces dirigido a control interno, una vez control interno haga la solicitud al encargado de sistemas se procederá a facilitar las claves de acceso. (**Anexo 2**).
- Por ningún motivo se permitirán conexiones a internet inalámbrico a terceros a menos que este en el marco de una actividad institucional o sea autorizado por el Alcalde Municipal mediante solicitud escrita.
- Los funcionarios de la administración municipal no podrán acceder a configuraciones del equipo de cómputo impresoras u otros dispositivos.
- Las redes Wi-Fi que estén a nombre del Concejo Municipal, se realizarán las conexiones mediante el filtro de Seguridad por número MAC del dispositivo, para ello se deberá solicitar por escrito al administrador de Sistemas de la Administración municipal por escrito. **(Anexo 07)**

3.3 ANTIVIRUS

- Se deberá adquirir un software antivirus que se ajuste a las necesidades de seguridad de la administración municipal bajo los lineamientos legales y licenciamiento.
- Se realizaran análisis mensuales con el software antivirus instalado en los equipos de cómputo de propiedad de la administración Municipal.
- Se informará a control interno acerca de la incidencia de virus en los equipos asignados a los funcionarios de la administración municipal, con el fin de implementar medidas que eviten la incidencia de esta falla.

4. SEGURIDAD EN APLICACIONES

Sistemas Operativos

- Se instalará el Sistema Operativo del cual se tiene licencias adquiridas
- Se instalara la versión de office 2016 con licenciamiento adquirido el
- Para los equipos que no cuenten con licenciamiento se instalaran sistemas operativos alternos y una versión libre de gestión de documentos, hasta que no sean adquiridas e instaladas nuevas licencias por parte de la administración municipal.

Control de aplicaciones

- Si por algún caso un funcionario o contratista solicita la instalación de aplicativos en los equipos de cómputo para el desarrollo de sus actividades se deberá informar por medio escrito a la oficina de control interno con copia al funcionario del área de sistemas.
- La actualización de aplicativos se realizarán únicamente si presentan fallas e incompatibilidades.
- En caso de reinstalación de un equipo de cómputo el funcionario está obligado a realizar una copia de seguridad de la información.
- El funcionario, contratista o proveedor no está autorizado para instalar o iniciar ningún tipo de software o aplicativo que no esté en el marco del manual de funciones o contrato, en caso de ser necesario enviará la solicitud a Control interno con copia al funcionario encargado del área de sistemas.
- Se establecerán fechas en común acuerdo con las dependencias de la administración municipal para la realización de mantenimientos físicos y lógicos preventivos en los equipos de propiedad de la administración municipal. El área de sistemas y/o contratista encargado del área de sistemas no está en la obligación de reparar, diagnosticar e instalar software en equipos personales.
- Los equipos de cómputo personales de los funcionarios, contratistas o terceros no podrán tener instalado software con licencia de propiedad de la administración municipal, en caso contrario será autorizado por el Alcalde Municipal quien a la vez notificará a Control Interno y al área de sistemas, además, el Secretario o quien haga sus veces, será el responsable de la información que en dicho equipo de cómputo personal tenga acceso.

Control de Cambios

- Se implementarán formatos o planillas para documentar los cambios de software, hardware o aplicativos que se realicen en los equipos de propiedad de la administración municipal.
- La solicitud de cambio de configuraciones, aplicativos, sistemas operativos o hardware deberán ser solicitadas por escrito especificando la siguiente información
  - Sistema, Aplicación o hardware afectado
  - Funcionario que solicita el cambio
  - Descripción general de la solicitud
  - Firma del supervisor o Secretario de la dependencia.
- Se emitirán mensualmente circulares internas con recomendaciones de seguridad informática basados en los hallazgos que se tengan durante la revisión mensual de los equipos, aplicativos o navegación web.
- Los procedimientos para la adquisición de hardware y software por parte de la administración municipal, se deberá tener en cuenta:
  - Análisis Costo – Beneficio
  - Comprobación de adaptabilidad y compatibilidad con los sistemas operativos y/o aplicaciones actualmente instalados.
  - Evaluación de las medidas de seguridad, respaldo y soporte.
  - Solicitud de manuales de uso de cada aplicación y/o herramienta de hardware.
  - Evaluación y diagnóstico por parte del funcionario del área de sistemas de la administración municipal

5. SEGURIDAD FISICA

5.1 Equipamiento

- Deberá existir una adecuada protección física por parte de los funcionarios hacia los equipos y dispositivos de propiedad de la administración municipal, por otra parte, el funcionario del área de sistemas velara por:
  - Mantenimiento de los equipos de cómputo cada 4 meses
  - Mantenimiento correctivo de los equipos de cómputo una vez sea detectado una falla.
  -

5.2 Controles de Acceso

Las siguientes medidas, protocolos y controles serán adoptados para garantizar la seguridad e integridad de los servidores, rack y cuarto de comunicaciones que alojan la configuración e información de la Administración Municipal.

- Solo podrá ingresar el funcionario encargado del área de sistemas y será el único funcionario que tendrá la disposición de autorizar junto con el Alcalde Municipal quien puede ingresar a esta área.
- El cuarto de comunicaciones permanecerá cerrado y bajo llave las cuales estarán a cargo del funcionario del área de sistemas.
- El personal externo a la administración municipal que necesite ingresar al cuarto de comunicaciones deberá solicitar de manera escrita el ingreso justificando el cambio y el procedimiento a seguir de manera escrita, será supervisado el ingreso por el funcionario encargado del área de sistemas y el funcionario de control interno. (**Anexo 4)**

Los siguientes son los procedimientos a seguir para el correcto funcionamiento de las Secretarias y/o dependencias en cuanto al tema de seguridad informática

- Las unidades de CD, DVD serán deshabilitadas en los Equipos de Cómputo de los funcionarios en los cuales no afecte el buen desarrollo de sus actividades que se especifica en el manual de Funciones de la Administración Municipal o actividades del contrato.
- Según sea el caso, se deshabilitaran los parlantes de los equipos de cómputo.
- Los funcionarios, Contratistas y proveedores no están autorizados para trasladar equipos de cómputo sin previa autorización por parte del funcionario de Almacén y el funcionario del área de Sistemas, dicho cambio se registrará en la planilla de control de cambios.

- No se permitirán el traslado de impresoras, escáner u otros dispositivos entre los funcionarios o dependencias, sin previa autorización del Secretario e informar a la oficina de control interno con copia al funcionario encargado del área de sistemas. (**Anexo 4)**
- Los equipos portátiles, Tablets, u otros dispositivos portables a excepción de los GPS´s, deberán permanecer dentro de las instalaciones de la Alcaldía Municipal, si fuese necesario su traslado deberá ser autorizado por el Alcalde Municipal con copia al funcionario de Almacén y al funcionario del área de sistemas.
- Los GPS´s o dispositivos que sean usados para las salidas a campo las Secretarías o dependencias tendrán control exclusivo y serán responsables de dichos dispositivos, el área de sistemas no dispondrá ni tendrá responsabilidad sobre ellos.
- Los funcionarios, contratistas y proveedores de la administración Municipal únicamente podrán imprimir documentos que estén en el marco del desarrollo de sus actividades que el manual de funciones o contrato especifique, para ello se creará e implementará una planilla de control de impresión en la cual tendrán que especificar la cantidad de impresiones o copias, la actividad que se desarrolla, fecha de impresión y firma, se realizarán controles periódicamente por parte del funcionario encargado del área de sistemas, en caso de detectasen impresiones fuera de las actividades anteriormente mencionadas la Secretaría o dependencia podría asumir el costo de los insumos. **(Anexo 8)**

5.3 RIESGOS QUE AFRONTAN LOS SISTEMAS DE INFORMACION E INFRAESTUCTURA TECNOLOGICA

TIPO DE PROCEDIMIENTO	FACTOR DE RIESGO	PREVENCION Y MITIGACION
Fuego o Incendio: Destrucción o pérdida parcial o total de la infraestructura tecnológica	MEDIO	Extintores ubicados estratégicamente según normativa legal vigente
Robo: Perdida de los equipos	MEDIO	Alarmas, Cámaras de Seguridad
Vandalismo: Daño a los equipos e infraestructura de datos	MEDIO	Seguridad Privada, Policial, Alarmas y Copias de Seguridad
Fallas en equipos de Cómputo: Eliminación de información y Configuración.	MEDIO	Garantías de Equipos de Cómputo y dispositivos, Copias de Seguridad, Backup´s de Configuración y

		Mantenimientos lógicos y físicos preventivos.
Errores Humanos: Eliminación de Información, Configuración o Sabotaje	ALTO	Capacitación de Funcionarios, Copias de Seguridad, Revisiones de Acceso a los sistemas de información
Virus Informáticos: Perdida total o parcial de información y/o configuración	ALTO	Actualizaciones de Sistemas Operativos, Actualización de Software Antivirus, Copias de Seguridad, Controles periódicos.
Desastres Naturales: Destrucción de Equipos	MEDIO	Copias de Seguridad
Accesos no Autorizados: Filtración no autorizada de información, ataques cibernéticos.	BAJO	Cambios de Contraseñas 1 vez al Mes, Implementación y seguimiento de las Políticas de seguridad de la Información, Copias de Seguridad.
Robo de Información: Difusión, publicación o reproducción de la información sin autorización	ALTO	Cambio de Contraseñas, Seguimiento de Políticas de Seguridad Informática, Supervisión y Control de Acceso a la Información.
Fraude –Suplantación de Usuarios: Modificación o desvíos de información.	BAJO	Cambio de Contraseñas, Seguimiento de Políticas de Seguridad Informática, Supervisión y Control de Acceso a la Información.

6. SOPORTE TÉCNICO

6.1 REPORTES DE INCIDENCIAS

Los funcionarios y contratistas de la administración municipal podrán realizar la solicitud de soporte técnico una vez se haya presentado una falla repetidamente o afecte el buen desarrollo de sus actividades que el manual de funciones o contrato especifique, para esto deberán:

- Realizar la solicitud por medio del correo electrónico utilizando el correo institucional y enviando dicha solicitud a sistemas@nunchia-casanare.gov.co, en caso de falla de la red de datos (internet) se realizará mediante llamada telefónica, haciendo énfasis en diligenciar la siguiente información:
  - Dependencia
  - Funcionario o Contratista
  - Falla Presentada

  Al momento de la entrega del usuario y contraseña se ingresará a la planilla de entrega de correos institucionales (**Anexo 1 y Anexo 3**)

- El funcionario o contratista encargado del área de Sistemas no está en la obligación de diagnosticar, reparar e instalar software en equipos de cómputo personal.
- Las solicitudes de soporte técnico se definirán y solucionaran de acuerdo al siguiente esquema de escalonamiento de Soporte técnico.

NIVEL	ESCALONAMIENTO
1	Funcionario y/o Contratista encargado del área de sistemas
2	Proveedores de hardware y software de la entidad Municipal

6.2 TIEMPOS DE ATENCION Y RESPUESTA DE SOPORTE TÉCNICO

Los tiempos que en la siguiente tabla se estipulan serán contados una vez se informé que la solicitud ha sido recibida, se agendará y se brindará solución mediante el protocolo de primera en informarse primeras en solucionarse.

INCIDENCIA O FALLA	TIEMPO DE RESPUESTA
NIVEL 1	
Fallas en la red LAN	3 Horas hábiles
Fallas en Herramientas Ofimáticas	4 Horas hábiles
Fallas en Periféricos	3 Horas hábiles
Asesoría en Manejo de herramientas ofimáticas	3 Días hábiles
Asesoría en manejo de herramientas web	3 Días hábiles
Fallas de impresión	3 Horas hábiles
Infección por virus informáticos	3 Horas hábiles
Daño o Perdida de Archivos	3 Horas hábiles
Cambio de Usuarios, privilegios y contraseñas	3 días hábiles
Fallas en Sistemas Operativos	3 Horas hábiles
Falla en rack de comunicaciones	1 día hábil
Falla en Servidores	1 día hábil
Fallas en sistemas de información	1 día hábil
Fallas en red WAN	1 día hábil
Fallas en sistemas de respaldo	1 día hábil
Reinicio de contraseña de correo institucional	3-5 días hábiles según disponga el Ministerio de las TIC
Reinicio de Usuario y Contraseña para control de Acceso	3-5 días hábiles
NIVEL 2	
Se deberán hacer efectivas las garantías con los proveedores	7 Días Hábiles

7. ADMINISTRACION DE DISPOSITIVOS DE RED Y COMUNICACIONES

- Se deberá garantizar la disponibilidad del funcionario y/o encargado de sistemas para el soporte técnico, asesorías, administración y funcionamiento, esto con el fin de suplir las necesidades de control total de las redes y comunicación de la administración municipal.
- El funcionario y/o contratista encargado del área de sistemas coordinará las actividades correspondientes para velar por el estricto cumplimiento del Manual de Procedimiento de Seguridad de la Información (MPSI), proponer nuevas actualizaciones de ser necesarias para integrarlas al Manual de Procedimientos de Seguridad de la Información (MPSI).
- Cada secretaría o dependencia designará a un funcionario y/o contratista quienes se reunirán con el funcionario de Control Interno y el funcionario encargado del área de sistemas y evaluarán los informes de seguridad y cumplimiento del MPSI, estado de equipos y red de datos.
- Se implementará un buzón de sugerencias donde los funcionarios podrán situar sus opiniones respecto a planes de mejoramiento del MPSI.
- El área de Sistemas deberá informar sobre suspensión de los servicios de comunicaciones, en caso de mantenimientos preventivos se deberá informar con anterioridad las fechas y horas de suspensión así como la duración del procedimiento.

7.1 CAPACITACIONES

- Ejecutar un plan de capacitación para los funcionarios y/o contratistas de la Administración Municipal en cuanto al manejo de herramientas ofimáticas e internet, aplicaciones y sistemas de información utilizados en las labores diarias inherentes a las funciones dentro de la administración municipal, con este plan de capacitación se pretende disminuir el número de solicitudes de soporte técnico.
- Los funcionarios, contratistas y proveedores de la Administración Municipal estarán en la obligación de cumplir con los lineamientos que el Manual de Procedimientos de Seguridad de la Información (MPSI) expresa, de tal manera, que las claves de acceso, usuarios y demás configuración sean de uso único de los funcionarios, contratistas y proveedores de la entidad.
- Los funcionarios de la administración municipal deberán solicitar las capacitaciones al área de control interno quien a su vez informará al funcionario y/o contratista encargado del área de sistemas quien establecerá la estrategia de capacitación.

7.2 PLAN DE RESPALDO DE LA INFORMACIÓN

- Los procedimientos de Respaldo de la información deberán estar documentados en el Registro de Copias de Seguridad (**Anexo 6**).

PROCEDIMIENTO	INFORMACION A RESPALDAR	RESULTADO DEL PROCEDIMIENTO
Copias de seguridad de la información alojado en los servidores de propiedad de la Alcaldía Municipal	Documentos PDF Documentos Word Documentos Excel Documentos Multimedia Correos Electrónicos	Copias de seguridad en la nube (Drive de Gmail), este procedimiento se realizará una (1) vez al año, este procedimiento será realizad por el funcionario encargado del área de sistemas.
Copias de Seguridad de Bases de datos, sistemas de información y aplicativos que sean de propiedad de la Alcaldía Municipal	Aplicaciones Web Sistemas de Información Bases de Datos Sistemas de Información Financieros	Se deberá realizar copias de seguridad una (1) vez a la semana, esta información deberá ser almacenada en discos duros externos y/o DVD´s, estas copias de seguridad deberán contar con medidas se seguridad físicas adecuadas para su almacenamiento, quien estará a cargo de la custodia será el funcionario encargado del área de sistemas
Mantenimientos y Revisiones preventivas y correctivas de los equipos de cómputo y sistemas de información.	Equipos de computo Equipos de redes y comunicaciones Sistemas eléctricos UPS	Se realizará una revisión anual de los equipos de contingencia por parte del personal externo a la administración municipal
Actualización de usuarios y contraseñas de acceso a bases de datos, aplicativos y sistemas de información de los equipos de cómputo.	Bases de Datos Sistemas de Información Aplicativos de propiedad de la administración municipal Equipos de cómputo e impresoras de propiedad de la administración municipal.	Se deberá realizar la actualización y revisión de usuarios y contraseñas cada 2 meses, este procedimiento estará a cargo del funcionario encargado del área de sistemas.

ANEXOS

FORMATO ALMACENAMIENTO USUARIOS Y CONTRASEÑAS (Anexo 1)

Sistema de Información y/o equipo de Computo	Usuario	Contraseña	Fecha actualización

Solicitud de Clave WIFI (Anexo 2)

Nunchía, ____ de ____ del _____

Oficina de Control Interno
Soporte técnico, Sistemas y Enlace TIC

Asunto: **Solicitud Clave WIFI**

Yo _____ identificado con cédula de ciudadanía _____ de _____ cuyo número de contrato (si es OPS) _____,me permito solicitar acceso de conexión a la red inalámbrica de nombre _____ de propiedad de la alcaldía Municipal de Nunchía – Casanare, para realizar las funciones y/o actividades de _____ durante _____ horas, los días _____ esta conexión se realizará desde la Secretaria de _____.

Cordialmente:

_____

Supervisor o Secretario

_____

ENTREGA DE CORREO ELECTRONICO (Anexo 3)

Nunchía, Casanare ____ de ____del ____

Señor (a)
_____

Asunto: Creación de Cuenta de Correo

Cordial Saludo

Dando Cumplimiento al Manual de Procedimiento de Seguridad de la Información me permito remitir la cuenta de correo electrónico institucional para comunicaciones internas y externas pertenecientes al buen desarrollo de sus actividades.

Una vez ingrese a su cuenta de correo deberá cambiar la contraseña de acuerdo a los lineamientos del Manual de Procedimiento de Seguridad de la Información, en caso de reposición de contraseña, se cumplirá con los plazos establecidos en el mismo documento.

USUARIO: _____
CONTRASEÑA: _____

Quedaré atento a cualquier solicitud

Atentamente

Web Máster, Sistemas y Enlace TIC
Administración Municipal
Nunchía – Casanare

CONTROL DE CAMBIOS (Anexo 4)

FECHA	ACTIVIDAD REALIZADA	FUNCIONARIO RESPONSABLE	QUIEN RECIBE EL SOPORTE	CARGO	SISTEMA DE INFORMACION O EQUIPO	FIRMA

Control de Salida de Equipos (Anexo 5)

Fecha de Salida	Nombre Funcionario	Dependencia	Cargo	Motivo de Salida	Fecha de Ingreso	#Placa Equipo

Copias de Seguridad (Anexo 6)

Fecha	Sistema de Información-Correo Electrónico-Equipo de Cómputo - Aplicación	Dependencia	Funcionario Responsable	Funcionario quien realizó la copia de seguridad	Observaciones

Anexo 7

Nunchía, ____ de _____ del _____

Cordial Saludo
César Neyith Osorio Molina
Administrador de Sistemas
Administración Municipal

Ref. Solicitud de Acceso a Red Inalámbrica

Cordial Saludo

Por medio de la presente me dirijo a usted para solicitar acceso a la red inalámbrica _____*(nombre de la red wi-fi)*____ durante el periodo de _____Horas para realizar la actividad de _____
Quien se desempeña como _____ en las instalaciones del Concejo Municipal.
(Si el usuario es Concejal, deberá especificar que es concejal)

Atentamente

Julia Elvira Díaz
Presidente del Concejo

Control de Impresiones (Anexo 8)

	DEPARTAMENTO DE CASANARE ALCALDIA MUNICIPAL DE NUNCHIA ALMACEN GENERAL	
NOMBRE:	*Nombre impresora*	**Fotografía de la Impresora**
MODELO:	*Modelo impresora*	
N° SERIE	N° de Serie de la Impresora	
ID TONER	*N° de Toner Instalado*	
N° DE SERIE TONER	*N° de Serie de Toner*	

N°	MOTIVO DE IMPRESION	FECHA	CANTIDAD IMPRESIÓN	COPIA	DEPENDENCIA	NOMBRE FUNCIONARIO

Los Anexos anteriormente mencionados serán proporcionados por el funcionario del área de sistemas y estarán sujetos a cambios una vez sea actualizado el MPSI.