Contenido

INTRODUCCIÓN

La información es un activo de gran valor para la Alcaldía Municipal de Palmira, por consiguiente debe ser debidamente protegido; garantizado, confiable al cual se deben de minimizar los riesgos de daño o pérdida; por lo tanto, lograr que los principios de Seguridad Informática sean efectivos en la entidad, hace necesario la implementación de Políticas de Seguridad Informática que formen parte de la cultura organizacional y cumplan a cabalidad los estándares aplicables y requeridos para la administración integral de la misma.

La Dirección de Tecnología, Innovación y Ciencia, como agente de gestión y apoyo en materia tecnológica, formula un conjunto de reglas que definen lo que está permitido y lo que está prohibido, igualmente propone prácticas que implican el manifiesto compromiso de todas las personas vinculadas de una manera u otra a la entidad, es por ello, que la Alcaldía Municipal de Palmira se ha puesto a la tarea de implementar sus propias políticas de seguridad informática, basándose en las características establecidas en el Modelo de Política de Seguridad de la Información para Organismos de la Administración Pública Nacional publicado por la Oficina Nacional de Tecnología de Información ONTI y el Modelo de Seguridad y Privacidad de la Información propuesto por Min TIC.
Así pues, con la promulgación de la presente Política de Seguridad de la Información la Alcaldía Municipal de Palmira, formaliza su compromiso con el proceso de gestión responsable de la información que tiene como objetivo garantizar la integridad, confidencialidad y disponibilidad de este importante activo, teniendo como eje el cumplimiento de los objetivos misionales.

“Porque la seguridad informática depende más de las personas que de las máquinas”

La Seguridad de la Información se entiende como la preservación, aseguramiento y cumplimiento de las siguientes características de la información:

CONFIDENCIALIDAD: Los activos de la información solo pueden ser accedidos y custodiados por usuarios que tengan permisos para ello.

INTEGRIDAD: El contenido de los activos de la información debe permanecer inalterado y completo. Las modificaciones realizadas deben ser registradas asegurando su confiabilidad.

DISPONIBILIDAD: Contar con la permanencia del sistema informático, en condiciones de actividad adecuadas para que los usuarios accedan a los datos con la frecuencia y dedicación que requieran, es importante en sistemas informáticos cuyos compromiso con el usuario, es prestar servicio permanente.

1. OBJETIVO

Presentar en forma clara y coherente los elementos que conforman las políticas de seguridad que deben conocer y cumplir todos los directivos, funcionarios contratistas y terceros que presten sus servicios o tengan algún tipo de relación con la Alcaldía de Palmira.

2. ALCANCE

Las Políticas de Seguridad Informática son aplicables para todos los aspectos administrativos y de control que deben ser cumplidos por los directivos, funcionarios, contratistas y terceros que presten sus servicios o tengan algún tipo de relación con la Alcaldía Municipal de Palmira para el cumplimiento de sus funciones y para conseguir un adecuado nivel de protección de las características de calidad y seguridad de la información, aportando con su participación en la toma de medidas preventivas y correctivas, siendo un punto clave para el logro del objetivo y la finalidad del presente manual.

Los usuarios y/o funcionarios tienen la obligación de dar cumplimiento a las presentes políticas emitidas por la Dirección de Tecnología, Innovación y Ciencia (TI y C) y aprobadas por el comité de privacidad y seguridad de la información.

3. RESPONSABILIDADES

3.1 La Política de Seguridad de la Información es de aplicación obligatoria para todo el personal de la Administración Central del Municipio de Palmira, cualquiera sea su situación contractual, la dependencia a la cual se encuentre adscrito y el nivel de las tareas que desempeñe.
3.2 El Comité de Seguridad de la Información de la Alcaldía de Palmira es responsable de revisar y aprobar, el texto de la Política de Seguridad de la Información, las funciones generales en materia de seguridad de la información y la estructuración, recomendación, seguimiento y mejora del Sistema de Gestión de Seguridad de la institución.
3.3 Es responsabilidad de dicho comité definir las estrategias de capacitación en materia de seguridad de la información al interior de la Alcaldía Municipal de Palmira.
3.4 Los propietarios de activos de información son responsables de la clasificación, mantenimiento y actualización de la misma; así como de documentar y mantener actualizada la clasificación efectuada, definiendo qué usuarios deben tener permisos de acceso a la información de acuerdo a sus funciones y competencia. En general, tienen la responsabilidad de mantener íntegro, confidencial y disponible el activo de información mientras que es desarrollado, producido, mantenido y utilizado.
3.5 El jefe de Recursos Humanos cumplirá la función de notificar a todo el personal que se vincula contractualmente con la Alcaldía Municipal de Palmira, de las obligaciones respecto del cumplimiento de la Política de Seguridad de la Información y de todos los estándares, procesos, procedimientos, prácticas y guías que surjan del Sistema de Gestión de la Seguridad de la Información.

3.6 De igual forma, será responsable de la notificación de la presente Política y de los cambios que en ella se produzcan a todo el personal, a través de la suscripción del Compromiso de Confidencialidad.
3.7 El Jefe de la Dirección de Tecnología Innovación y Ciencia debe seguir los lineamientos de la presente política y cumplir los requerimientos que en materia de seguridad informática se establezcan para la operación, administración, comunicación y Política de Seguridad de la Información.
3.8 La Oficina de Control Interno es responsable de practicar auditorías periódicas sobre los sistemas y actividades vinculadas con la gestión de activos de información y la tecnología de información. Es su responsabilidad informar sobre el cumplimiento de las especificaciones y medidas de seguridad de la información establecidas por esta Política y por las normas, procedimientos y prácticas que de ella surjan

4. DEFINICIONES

Para ello es necesario considerar aspectos tales como:

Autenticidad: Los activos de la Información los crean, editan y custodian los usuarios reconocidos quienes validan su contenido.
Autenticación: Los autores, propietarios y custodios de los activos de información se pueden identificar plenamente.
Confiabilidad: Los activos de la información son fiables en su contenido.
Incidente de seguridad: Un incidente de seguridad en informática es la ocurrencia de uno o varios eventos que atentan contra la confidencialidad, la integridad y la disponibilidad de la información y que violan la Política de Seguridad de la Información de la organización, en el caso de que disponga de ella
Outsourcing: Es un término del inglés que podemos traducir al español como 'subcontratación', 'externalización' o 'tercerización'.
Política de escritorio despejado: La política de la empresa que indica a los funcionarios, contratista y demás colaboradores Informáticos, que deben dejar su escritorio libre de cualquier tipo de informaciones susceptibles de mal uso al finalizar el día.
Protección a la duplicidad: La protección de copia, también conocida como prevención de copia, es una medida técnica diseñada para prevenir la duplicación de información. La protección de copia es a menudo tema de discusión y se piensa que en ocasiones puede violar los derechos de copia de los usuarios, por ejemplo, el derecho a hacer copias de seguridad de una videocinta que el usuario ha comprado de manera legal, el instalar un software de computadora en varias computadoras, o al subir la música a reproductores de audio digital para facilitar el acceso y escucharla.
Riesgo: Posibilidad de que una amenaza concreta pueda explotar una vulnerabilidad para causar una pérdida o daño en un activo de información. Según [ISO Guía 73:2009]: combinación de la probabilidad de un evento y sus consecuencias.
Seguridad de la información: Según [ISO/IEC 27002:2013]: Preservación de la confidencialidad, integridad y disponibilidad de la información; además, otras propiedades como autenticidad, responsabilidad, no repudio, trazabilidad y fiabilidad pueden ser también consideradas.
Token: También llamado componente léxico es una cadena de caracteres que tiene un significado coherente en cierto lenguaje de programación.

Usuario: En el presente documento se emplea para referirse a directivos, funcionarios, contratistas, terceros y otros colaboradores Informática, debidamente autorizados para usar equipos, sistemas o aplicativos informáticos disponibles en la red Informática y a quienes se les otorga un nombre de usuario y una clave de acceso.
Valoración de riesgos: Según [ISO/IEC Guía 73:2009]: Proceso completo de análisis y evaluación de riesgos.
Virus: Tiene por objeto alterar el normal funcionamiento de la computadora, sin el permiso o conocimiento del usuario.

5. POLÍTICAS

Organización de la seguridad de la información

Objetivo:

Determinar la manera de organizar la seguridad de la información dentro de la Administración, definiendo las directrices para gestionar la seguridad de la información dentro de la Alcaldía Municipal de Palmira.
Aplicabilidad:

Las directivas de la Alcaldía Municipal, en cabeza del Alcalde, deben asumir activamente la seguridad de la información dentro de la entidad mediante la asignación de recurso humano, tecnológico y económico con un rumbo claro, un compromiso demostrado, una asignación explícita y el conocimiento de las responsabilidades de la seguridad de la información. Este compromiso se verá reflejado a través de:

a. Creación de un comité de privacidad y seguridad de la información.
b. Asignación de un responsable de la seguridad de la información (Oficial de seguridad/Gestor de Seguridad/Profesional de Seguridad)
c. Aprobación del documento Manual de Políticas de Seguridad y Privacidad de la información
d. Velar por el cumplimiento de la política y las políticas de seguridad y privacidad de la información, y la asignación de responsabilidades asociadas al tema de la seguridad de la información.

Directrices:

Funciones del Comité

a. El comité de Seguridad y privacidad de la Información debe estar conformado por el Alcalde, secretarios, jefes o directivos de las dependencias designadas de la alcaldía municipal y tendrá como funciones las siguientes:
b. Debe periódicamente revisar el estado general de la seguridad de la información revisar y monitorear los incidentes de seguridad de la información.
c. Revisar y aprobar los proyectos de seguridad de la información
d. Aprobar las modificaciones o nuevas políticas de seguridad de la información

e. Realizar otras actividades de alto nivel relacionadas con la seguridad de la información
f. Por último, cuando el comité de seguridad de la información se reúna con el propósito de revisar temas de seguridad de la información se incluirá la participación del Oficial de Seguridad.

Coordinación de la Seguridad de la Información

a. Las actividades de la seguridad de la información deben ser coordinadas por los representantes de todas las partes de la Alcaldía Municipal con roles y funciones laborales pertinentes.
b. El Alcalde Municipal es responsable de que todos los funcionarios y contratistas de la Alcaldia Municipal de Palmira, conozcan y apliquen las políticas de seguridad y privacidad de la información.
c. La Alcaldía Municipal deberá contar con un Oficial de Seguridad de la Información (Oficial de seguridad/Gestor de Seguridad/Profesional de Seguridad) que asuma las tareas y responsabilidades que conlleva este rol:
d. Definir y actualizar políticas, normas, procedimientos y estándares definidos en el Comité.
e. Evaluar, seleccionar e implantar herramientas que faciliten la labor de seguridad de la información
f. Dar los lineamientos para controlar el acceso a los sistemas de información y la modificación de privilegios
g. Promover en la Alcaldía Municipal la formación, educación y el entrenamiento en seguridad de la información.
h. Mantenerse actualizado en nuevas amenazas y vulnerabilidades existentes.
i. Recibir capacitación en el tema de seguridad de la información
j. Administrar la gestión de incidentes de seguridad y privacidad de la información de la Alcaldia Municipal de Palmira
k. Coordinar la realización de estudios de penetración y pruebas de seguridad en todos los ambientes (Desarrollo, Pruebas, Producción y Contingencia)
l. Gestionar la aplicación de correcciones a las vulnerabilidades detectadas en los estudios de penetración y pruebas de seguridad en todos los ambientes (Desarrollo, Pruebas, Producción y Contingencia)

Asignación de responsabilidades para la Seguridad de la Información

a. Se deben definir claramente todas las responsabilidades en cuanto a seguridad de la información; en especial las relacionadas a la existencia de un comité de seguridad y privacidad de la información y un oficial de seguridad (Oficial de seguridad/Gestor de Seguridad/Profesional de Seguridad).

b. Oficial de Seguridad de la información
c. La Alcaldía Municipal mantendrá dentro de su planta de empleados un Oficial de Seguridad de la información (Oficial de seguridad/Gestor de Seguridad/Profesional de Seguridad), que será designado por el Director(a) de la Dirección de tecnología, Innovación y Ciencia (TIyC), cuyas funciones estarán caracterizadas y definidas en el documento Políticas de Seguridad de la Información. (Numeral 5, literal b del presente documento)

Comité de seguridad y privacidad de la información

El Oficial de Seguridad (Oficial de seguridad/Gestor de Seguridad/Profesional de Seguridad), podrá convocar a diferentes funcionarios para formar grupos interdisciplinarios, que apoyen la definición e implementación de los diferentes temas de seguridad de la información.

a. Propietarios de la Información
b. Toda la información utilizada por la Alcaldía Municipal de Palmira, debe poseer un propietario. Estos propietarios de la información son responsables de los activos y deben:
c. Definir la clasificación de la información
d. Determinar los niveles de acceso a la información
e. Autorizar la asignación de permisos de acceso
f. Apoyar a la Dirección de Tecnología, Innovación y Ciencia en la generación de los controles necesarios para el almacenamiento, procesamiento, distribución y uso de la información
g. El Alcalde Municipal es responsable de que los empleados y contratistas conozcan y apliquen las políticas de seguridad y privacidad de la información.
h. Los funcionarios, contratistas y terceros son responsables por el cumplimiento de las políticas de seguridad y privacidad de la información.
i. Adicionalmente cada funcionario contratista o tercero está obligado a reportar al Oficial de Seguridad (Oficial de seguridad/Gestor de Seguridad/Profesional de Seguridad) cualquier incidente de seguridad y privacidad de la información del que tenga conocimiento.
j. Los contratistas, proveedores y terceros que tengan acceso a los activos de información, están obligados a cumplir las políticas de seguridad y privacidad de la Información de la Alcaldía Municipal.
k. Los administradores de los diferentes sistemas deben en forma activa implementar las normas, estándares, formatos y procedimientos, para brindar un nivel apropiado de seguridad de la información.

Autorización para nuevos servicios de procesamiento de la Información

a. Se debe definir e implementar un procedimiento de autorización de la Dirección de Tecnología para nuevos servicios de procesamiento de la información.
b. Se debe considerar para esta implementación los siguientes aspectos:
c. La asignación de un propietario para cualquier nuevo servicio a implementar, además incluyendo la definición de las características de la información, tales como clasificación y definición de los diferentes niveles de acceso por usuario.
d. El propietario de la información debe explícitamente dar autorización para usar este nuevo servicio.
e. Se debe contar con la autorización respectiva por parte del Oficial de Seguridad de la Información (Oficial de seguridad/Gestor de Seguridad/Profesional de Seguridad), garantizando que el nuevo servicio cumple con las políticas de seguridad de la información definidas en este documento.
f. Evaluar la compatibilidad a nivel de hardware y software con otros sistemas.

g. Identificar las vulnerabilidades que genere el nuevo servicio y además definir los controles necesarios para mitigarlas.

Acuerdos de confidencialidad

a. Se debe identificar y revisar con regularidad los requisitos de confidencialidad o los acuerdos de no divulgación que reflejan las necesidades de la Alcaldía Municipal, para la protección y seguridad de la información.
b. Todos los empleados de Alcaldía Municipal de Palmira, contratistas, proveedores y terceros, que deban realizar labores dentro de la Alcaldía Municipal, ya sea por medios lógicos o físicos que involucren el manejo de información, deben conocer, entender, firmar y aceptar el correspondiente acuerdo de confidencialidad de la información. Ver AIFF015 Acuerdo de Confidencialidad Versión 001.

c. Revisión independiente de la Seguridad de la Información
d. Las políticas de seguridad de la información, normas, controles, estándares, formatos y procedimientos, deben ser revisados periódica y planificadamente, por la Dirección de Tecnología, Innovación y Ciencia (TI y C) de la Alcaldía Municipal de Palmira. Este periodo debe ser de al menos una vez al año o cada vez que ocurra un cambio sustancial en la infraestructura o activos de información de la organización.
e. Si se hiciere auditoría externa, seguirá los lineamientos ISO 27001, realizada por alguien con las credenciales de AUDITOR LIDER (Lead Auditor) 27001 vigentes o Auditor CISA.

5.1 Políticas de seguridad

Las Políticas de seguridad informática, surgen como una herramienta institucional para sensibilizar a cada uno de los directivos, funcionarios, contratistas y terceros que presten sus servicios o tengan algún tipo de relación con la Alcaldía de Palmira, sobre la importancia y sensibilidad de la información y servicios críticos, de tal forma que le permitan desarrollar adecuadamente sus labores y cumplir con su propósito misional.

Objetivo:

Definir las pautas de propósito general para asegurar una adecuada protección de la información de la Alcaldía Municipal de Palmira.

Directrices:

a. Se debe verificar que se definan, implementen, revisen y actualicen las políticas de seguridad informática.
b. Diseñar, programar y realizar los programas de auditoría del sistema de gestión de seguridad de la información, los cuales estarán a cargo de la Oficina de Control Interno.
c. Todo aplicativo informático o software debe ser comprado o aprobado por la Dirección de Tecnología, Innovación y Ciencia en concordancia con la política de adquisición de bienes de la entidad.

d. La Dirección de Tecnología, Innovación y Ciencia (TI y C) debe contar con un firewall o dispositivo de seguridad perimetral para la conexión a Internet o cuando sea inevitable para la conexión a otras redes en outsourcing o de terceros.
e. La conexión remota a la red de área local de la Alcaldía Municipal de Palmira debe realizarse a través de una conexión VPN segura suministrada por la entidad, la cual debe ser aprobada, registrada y auditada.
f. La alta dirección, secretarios, subsecretarios, directores, jefes de oficina deben asegurarse que todos los procedimientos de seguridad de la información dentro de su Secretaría, Dirección u Oficina de responsabilidad, se realizan correctamente para lograr el cumplimiento de las políticas y estándares de seguridad de la información de la Alcaldía Municipal de Palmira.
g. La Dirección de Tecnología, Innovación y Ciencia (TI y C) en caso de tener un servicio de transferencia de archivos deberá realizarlo empleando protocolos seguros. Cuando el origen sea el de la Dirección de Tecnología, Innovación y Ciencia (TI y C) hacia entidades externas, la Dirección de Tecnología, Innovación y Ciencia (TI y C) establecerá los controles necesarios para preservar la seguridad de la información; cuando el origen de la transferencia sea una entidad externa, se acordarán las políticas y controles de privacidad y seguridad de la información con esa entidad; en todo caso se deben revisar y proponer controles en concordancia con las políticas de privacidad y seguridad informática de la Alcaldía Municipal de Palmira; los resultados de la revisión de requerimientos de seguridad se documentan y preservarán para futuras referencias o para demostrar el cumplimiento con las políticas y con los controles de privacidad y seguridad de la Alcaldía Municipal de Palmira.
h. El comité de privacidad y seguridad de la información definirá de acuerdo a la clasificación de la información, qué datos deben ser cifrados y dará las directrices necesarias para la implementación de los respectivos controles (dispositivos a emplear, mecanismos de administración de claves, políticas de uso de sistemas de cifrado de datos).

5.2 Política de Clasificación de la información

Objetivo:

Asegurar que la información recibe el nivel de protección apropiado de acuerdo al tipo de clasificación establecido por la Guía para la Gestión y Clasificación de Activos de Información - MinTic. Aplicabilidad:

Estas son políticas que aplican para todos los funcionarios, contratistas y terceros y en general a todos los usuarios de la Alcaldía Municipal de Palmira. Directrices:

Se considera información toda forma de comunicación o representación de conocimiento o datos digitales, escritos en cualquier medio, ya sea magnético, papel, visual u otro que genere la Alcaldía Municipal de Palmira, como por ejemplo:

Formularios / comprobantes propios o de terceros.
Información en los sistemas, equipos informáticos, medios magnéticos/electrónicos o medios físicos como papel.

Otros soportes magnéticos/electrónicos removibles, móviles o fijos.
Información transmitida vía oral o por cualquier otro medio de comunicación.

Los usuarios responsables de la información, deben identificar los riesgos a los que está expuesta la información de sus áreas, teniendo en cuenta que la información pueda ser copiada, divulgada, modificada o destruida física o digitalmente por personal interno o externo.

Un activo de información es un elemento definible e identificable que almacena registros, datos o información en cualquier tipo de medio y que es reconocida como "Valiosa" para la Alcaldía Municipal de Palmira; Independiente del tipo de activo, se deben considerar las siguientes características:

El activo de información es reconocido como valioso para Alcaldía Municipal de Palmira
No es fácilmente reemplazable sin incurrir en costos, habilidades especiales, tiempo, recursos o la combinación de los anteriores.

Forma parte de la identidad de la Alcaldía Municipal y sin el cual este puede estar en algún nivel de riesgo.
Los niveles de clasificación de la información que se ha establecido son: INFORMACIÓN PÚBLICA RESERVADA, INFORMACIÓN PÚBLICA CLASIFICADA e INFORMACIÓN PÚBLICA.

5.3 Política de gestión de activos de información

Objetivo:

Establece la forma en que se logra y mantiene la protección adecuada de los activos de información.

Directrices:
La Dirección de Tecnología Innovación y Ciencia (TIyC) mantendrá un inventario o registro actualizado de sus activos de información, bajo la responsabilidad de cada propietario de información. El Registro de Activos de Información deberá ser publicado en la página web de la Entidad, acorde con lo establecido en el literal j) Datos Abiertos, del Artículo 11 de la Ley 1712 de 2014.
Los administradores de la información, son los funcionarios, contratistas, (denominados "usuarios") que estén autorizados y sean responsables por estos activos.

5.3.1 Política de uso de los activos

Objetivo:

Lograr y mantener la protección adecuada de los activos de información mediante la asignación de estos a los usuarios finales que deban administrarlos de acuerdo a sus roles y funciones.

Directrices:

a. Los activos de información pertenecen a la Alcaldía Municipal de Palmira y el uso de los mismos debe emplearse exclusivamente con propósitos laborales.
b. Los usuarios deberán utilizar únicamente los programas y equipos autorizados por la Dirección de Tecnología, Innovación y Ciencia.
c. La Dirección de Tecnología, Innovación y Ciencia proporcionará al usuario los equipos informáticos y los programas instalados en ellos; los Datos/información creados, almacenados y recibidos, serán propiedad de la Alcaldía Municipal, los funcionarios solo podrán realizar Backup de sus archivos personales, no, de información pública, para copiar cualquier tipo de información clasificada o reservada debe pedir autorización a su jefe inmediato, de acuerdo a las normas sobre clasificación de la información de acuerdo a los niveles de seguridad establecidos por la Dirección de Tecnología, Innovación y Ciencia (TI y C); Su copia, sustracción, daño Intencional o utilización para fines distintos a las labores propias de la Alcaldía Municipal, serán sancionadas de acuerdo con las normas y legislación vigentes.
d. Periódicamente, la Dirección de Tecnología, Innovación y Ciencia, efectuará la revisión de los programas utilizados en cada dependencia. La descarga, instalación o uso de aplicativos o programas informáticos no autorizados será considera como una violación a las Políticas de Seguridad Informática.
e. Todos los requerimientos de aplicativos, sistemas y equipos informáticos deben ser solicitados a través la Dirección de Tecnología, Innovación y Ciencia con su correspondiente justificación para su respectiva viabilidad.
f. Estarán bajo custodia de la Dirección de Tecnología de Tecnología, Innovación y Ciencia, los medios magnéticos/electrónicos (CDs, Dvd, nube, unidades de Red u otros) que vengan originalmente con el software y sus respectivos manuales y licencias de uso, adicionalmente las claves para descargar el software de fabricantes de sus páginas web o sitios en internet y los passwords de administración de los equipos informáticos, sistemas de información o aplicativos.
g. En caso de ser necesario y previa autorización del Comité de Seguridad Informática y de Sistemas, los funcionarios de la Dirección de TI y C podrán acceder a revisar cualquier tipo de activo de información y material que los usuarios creen, almacenen, envíen o reciban, a través de Internet o de cualquier otra red o medio, en los equipos informáticos a su cargo.
h. Los recursos informáticos no podrán ser utilizados, sin previa autorización escrita, para divulgar, propagar o almacenar contenido personal o comercial de publicidad, promociones, ofertas, programas destructivos (virus), propaganda política, material religioso o cualquier otro uso que no esté autorizado.
i. Los usuarios no deben realizar intencionalmente actos que impliquen un mal uso de los recursos tecnológicos.
j. Estos actos incluyen, pero no se limitan a: envió de correo electrónico masivo con fines no institucionales y práctica de juegos en línea.
k. Los usuarios no podrán efectuar ninguna de las siguientes labores sin previa autorización de la Dirección de Tecnología, Innovación y Ciencia:
l. Instalar software en cualquier equipo de la Alcaldía de Palmira.
m. Bajar o descargar software de Internet u otro servicio en línea en cualquier equipo de la Alcaldía de Palmira.

n. Modificar, revisar, transformar o adaptar cualquier software propiedad de la Alcaldía de Palmira.
o. Descompilar o realizar ingeniería inversa en cualquier software de propiedad de la Alcaldía de Palmira.
p. Copiar o distribuir cualquier software de propiedad de la Alcaldía de Palmira.
q. El usuario deberá informar al Jefe Inmediato de cualquier violación de las políticas de seguridad informática o uso indebido que tenga conocimiento.
r. El usuario será responsable de todas las transacciones o acciones efectuadas con su "cuenta de usuario".
s. Ningún usuario deberá acceder a la red o a los servicios TIC Informática, utilizando una cuenta de usuario o clave de otro usuario.
t. Cada usuario es responsable de asegurar que el uso de redes externas, tal como Internet, no comprometa la Seguridad de los recursos informáticos.
u. La Dirección de Tecnología, Innovación y Ciencia, es la dependencia responsable de realizar el aseguramiento de los accesos a internet, acceso a redes de terceros y a las redes de la Alcaldía; esta responsabilidad incluye, pero no se limita a prevenir que intrusos tengan acceso a los recursos informáticos y a prevenir la introducción y propagación de virus.
v. Todo archivo o material recibido a través de medio magnético/electrónico o descarga de Internet o de cualquier red externa, deberá ser revisado para detección de virus y otros programas destructivos antes de ser instalados en la infraestructura de la Dirección de Tecnología, Innovación y Ciencia (TI y C).
w. Todos los archivos provenientes de equipos externos a la Dirección de Tecnología, Innovación y Ciencia (TI y C), deben ser revisados para detección de virus antes de su utilización dentro de la red informática.
x. La información debe ser respaldada de forma frecuente, debe ser almacenada en lugares apropiados en los cuales se pueda garantizar que la información esté segura y podrá ser recuperada en caso de un desastre o de incidentes con los equipos de procesamiento.

5.3.2 Política de retención y archivo de datos

Objetivo:

Mantener la integridad y disponibilidad de la información y de los servicios de procesamiento de información.

Directrices:

a. La política de retención de archivos debe establecer cuánto tiempo se deben mantener almacenados los archivos en la Dirección de Tecnología, Innovación y Ciencia (TI y C) de acuerdo a las tablas de retención documental – TRD.
b. Las reglas y los principios generales que regulan la función archivística del Estado, se encuentran definidos por la Ley, la cual es aplicable a la administración pública en sus diferentes niveles producidos en función de su misión y naturaleza.
c. La ley prevé el uso de las tecnologías de la información y las comunicaciones en la administración, conservación de archivos y en la elaboración e implantación de programas de gestión de documentos.

5.4 Seguridad de recursos humanos

Objetivo:

Asegurar que los funcionarios, contratistas y demás colaboradores de la Alcaldía Municipal de Palmira, entiendan sus responsabilidades y las funciones de sus roles y usuarios, con el fin de reducir el riesgo de hurto, fraude, filtraciones o uso inadecuado de la información y de las instalaciones.

Directrices:

Se debe asegurar que los funcionarios, contratistas y demás colaboradores de la Alcaldía Municipal de Palmira, entiendan sus responsabilidades en relación con las políticas de seguridad y privacidad de la información y actúen de manera consistente frente a las mismas, con el fin de reducir el riesgo de hurto, fraude, filtraciones o uso inadecuado de la información o los equipos empleados para el tratamiento de la información.

5.4.1 Políticas específicas para usuarios de la Dirección de TI y C

Objetivo:

Definir las pautas generales para asegurar una adecuada protección de la información y estructura tecnológica por parte de los usuarios de la Alcaldía.

Directrices:

a. La Dirección de Tecnología, Innovación y Ciencia (TI y C) suministra una cuota de almacenamiento de la información en un servidor de archivos con los permisos necesarios para que cada usuario guarde la información que crea importante y sobre ella se garantizará la disponibilidad en caso de un daño en el equipo asignado, esta información será guardada durante un máximo de 2 años; es de aclarar que el usuario final deberá copiar la información necesaria en la carpeta destinada para este fin, la cual tiene un acceso directo.
b. La Dirección de Tecnología, Innovación y Ciencia (TI y C) instalará copia de los programas que han sido adquiridos legalmente en los equipos asignados en las cantidades requeridas para suplir las necesidades. El uso de programas sin su respectiva licencia y autorización Informática (imágenes, vídeos, software o música), obtenidos a partir de otras fuentes (internet, dispositivos de almacenamiento externo), puede implicar amenazas legales y de seguridad de la información para la entidad, por lo que ésta práctica no está autorizada.
c. Todo el software usado en la plataforma tecnológica Informática debe tener su respectiva licencia y acorde con los derechos de autor según ley.

d. La Dirección de Tecnología, Innovación y Ciencia (TI y C) no se hace responsable por las copias no autorizadas de programas instalados o ejecutados en los equipos asignados a sus funcionarios o contratistas.
e. El uso de dispositivos de almacenamiento externo (dispositivos móviles, DVD, CD Discos Duros externos, memorias USB, agendas electrónicas, celulares, etc.) puede ocasionalmente generar riesgos para la entidad al ser conectados a los computadores, ya que son susceptibles de transmisión de virus informáticos o pueden ser utilizados para la extracción de información no autorizada.
f. Los programas instalados en los equipos, son de propiedad de la Dirección de Tecnología, Innovación y Ciencia (TI y C), la copia no autorizada de programas de su documentación, implica una violación a las políticas de seguridad y privacidad de la información de la Alcaldia Municipal de Palmira. Aquellos funcionarios, contratistas o demás colaboradores que utilicen copias no autorizadas de programas o su respectiva documentación, quedarán sujetos a las acciones disciplinarias establecidas o las sanciones que especifique la ley.
g. La Dirección de Tecnología, Innovación y Ciencia (TI y C) se reserva el derecho de proteger su buen nombre y sus inversiones en hardware y software, fomentando controles internos para prevenir el uso o la realización de copias no autorizadas de los programas de propiedad de la entidad. Estos controles pueden incluir valoraciones periódicas del uso de los programas, auditorías anunciadas y no anunciadas.
h. Los recursos tecnológicos y de software asignados a los funcionarios de la Alcaldía Municipal son responsabilidad de cada funcionario y contratista.
i. Los funcionarios usuarios son los responsables de la información que administran en sus equipos personales y deben abstenerse de almacenar en ellos información no institucional, de acuerdo con la guía de clasificación de la información.
j. Los usuarios sólo tendrán acceso a los datos y recursos autorizados por la Dirección de Tecnología, Innovación y Ciencia (TI y C), y serán responsables disciplinaria y legalmente de la divulgación no autorizada de esta información.
k. Es responsabilidad de cada usuario proteger la información que está contenida en documentos, formatos, listados, etc., los cuales son el resultado de los procesos informáticos; adicionalmente se deben proteger los datos de entrada de estos procesos.
l. Los dispositivos electrónicos (computadores, impresoras, fotocopiadoras, escáner, etc.) solo deben utilizarse para los fines autorizados por la entidad.
m. Cualquier evento o posible incidente que afecte la seguridad de la información, debe ser reportado inmediatamente a la Dirección de Tecnología Innovación y Ciencia (TI Y C).
n. Los datos de los sistemas de información y aplicaciones no deben intercambiarse utilizando archivos compartidos en los computadores, discos virtuales, CD, DVD, medios removibles; deben usarse los mismos servicios del sistema de información, los cuales están controlados y auditados.

5.4.2 Políticas específicas para funcionarios y contratistas de la Alcaldía de Palmira

Objetivo:

Definir las pautas generales para asegurar una adecuada protección de la información e infraestructura computacional por parte de los funcionarios y contratistas de la Alcaldía de Palmira.

Directrices:

a. Los usuarios y claves de los funcionarios y contratistas de la Alcaldía de Palmira son de uso personal e intransferible.
b. Los funcionarios y contratistas de la Alcaldía de Palmira no deben dar a conocer su clave de usuario a terceros.
c. Los usuarios y claves de los funcionarios y contratistas de la Alcaldía de Palmira deben emplear obligatoriamente las claves o contraseñas con un alto nivel de complejidad.
d. Los administradores de los sistemas de información deben utilizar procedimientos de salvaguarda o custodia de las claves o contraseñas en un sitio seguro. A este lugar solo debe tener acceso el Jefe de la Dirección de Tecnología, Innovación y Ciencia.
e. Los documentos y en general la información de procedimientos, seriales, software etc. deben mantenerse custodiados en todo momento para evitar el acceso a personas no autorizadas.
f. Para el cambio o retiro de equipos de funcionarios, se debe llevar a cabo mejores prácticas para la eliminación de la información de acuerdo al software disponible en la entidad, Ej: Formateo seguro, destrucción total de documentos o borrado seguro de equipos electrónicos.
g. Los funcionarios encargados de realizar la instalación o distribución de software, sólo instalarán productos con licencia y software autorizado.
h. Los funcionarios de la Dirección de Tecnología, Innovación y Ciencia no deben otorgar privilegios especiales a los usuarios sobre las estaciones de trabajo, sin la autorización correspondiente del Director (a) de TI y C.
i. Los funcionarios y contratistas de la Alcaldía Municipal de Palmira se obligan a no revelar a terceras personas, la información a la que tenga acceso en el ejercicio de sus funciones, en consecuencia, se obligan a mantenerla de manera confidencial y privada y a protegerla para evitar su divulgación.
j. Los funcionarios y contratistas de la Alcaldía Municipal de Palmira no utilizarán la información para fines comerciales o diferentes al ejercicio de sus funciones.
k. Toda licencia de software o aplicativo informático y sus medios, se deben guardar y relacionar de tal forma que asegure su protección y disposición en un futuro.
l. Las copias licenciadas y registradas del software adquirido, deben ser únicamente instaladas en los equipos y servidores de la entidad. Se deben hacer copias de seguridad en concordancia con las políticas del proveedor y de la entidad.

m. La copia de programas o documentación, requiere tener la aprobación escrita de la Dirección de TI y C y del proveedor si éste lo exige.
n. El personal de la Dirección de Tecnología, Innovación y Ciencia debe velar por que se cumpla con el registro en la bitácora de acceso al datacenter, de las personas que ingresen y que hayan sido autorizadas previamente por la jefatura del área o por quien ésta delegue.
o. Por defecto deben ser bloqueados, todos los protocolos y servicios que no se requieran en la infraestructura instalada en la Alcaldía Municipal de Palmira; no se debe permitir ninguno de ellos, a menos que sea solicitado y aprobado oficialmente por la entidad a través del Comité de Seguridad Informática.
p. Todos los servidores deben ser configurados con el mínimo de servicios necesarios y obligatorios para desarrollar las funciones designadas.
q. Las pruebas de software o piloto deben ser autorizadas por el Comité de Seguridad Informática, estas deben ser realizadas sin conexión a la red LAN de la Alcaldía y con una conexión separada de internet o en su defecto con una dirección IP diferente a las direcciones públicas de producción y en servidores de prueba.

5.5 Teletrabajo – trabajo en casa

a. La Dirección de Tecnología Innovación y Ciencia TI y C debe establecer los requerimientos para autorizar conexiones remotas a la infraestructura tecnológica necesaria para la ejecución de las funciones de los servidores públicos, contratistas de la Alcaldía, garantizando las herramientas y controles para proteger la confidencialidad, integridad y disponibilidad de las conexiones remotas.
b. Toda información gestionada por la Alcaldía de Palmira, y que sea accedida remotamente debe ser utilizada solamente para el cumplimiento de las funciones del cargo o de las obligaciones contractuales.
c. El préstamo de equipos de cómputo de escritorio y/o computadores portátiles se debe tramitar a través de oficio, con anticipación al área de recursos físicos, quienes a su vez coordinará con la dirección de Tecnología Innovación y Ciencia (IT y C), para que se realice el respectivo alistamiento previo a la salida del equipo.
d. El literal C es de obligatorio cumplimiento, para garantizar el correcto funcionamiento del equipo.

5.6 Políticas específicas para Web master

Objetivo:

Proteger la integridad de las páginas Web institucionales, el software y la información contenida. En este caso en la Dirección de Comunicaciones de la Alcaldía de Palmira.
Aplicabilidad:

Estas son políticas que aplican para todos los funcionarios, contratistas y terceros y en general a todos los usuarios de la Alcaldía Municipal de Palmira que se encuentren desempeñando el rol de Web master.

Directrices:

a. Los responsables de los contenidos de la página Web, deben preparar y depurar la información de su área o dependencia y reportar a la Dirección de Tecnología, Innovación y Ciencia (TI y C) los requerimientos de actualización de la versión del software; deben disponer de un archivo actualizado con la información de la página inicial del sitio; y deben registrar la autorización de publicación por parte del funcionario autorizado y coordinar con el administrador web del Área de Tecnología, Innovación y Ciencia los lineamientos del sitio.
b. Se deberá seguir los parámetros del Índice de Transparencia y Acceso a la información Pública - Ley 1712 de 2014, delimitada por la procuraduría General de la República que permita auditar la publicación o modificación de información oficial en las páginas web.
c. Las claves de acceso de los responsables de los contenidos de las páginas Web (web masters), son estrictamente confidenciales, personales e intransferibles.

5.7. Seguridad física y ambiental

5.7.1 Política de uso de estaciones cliente

Objetivo:

Garantizar que la seguridad es parte integral de los activos de información y que son bien utilizados por los usuarios finales.

Directrices:

a. Todo cambio o traslado de equipos tecnológicos deberá estar autorizado y controlado por la Dirección de Tecnología, Innovación y Ciencia (TI y C) y actualizado en el inventario de bienes muebles de recursos físicos.
b. La instalación de software en los computadores suministrados por la Dirección de Tecnología, Innovación y Ciencia (TI y C), es una función exclusiva de esta dependencia. Se mantendrá un inventario actualizado del software autorizado para instalar en los computadores de la Alcaldía de Palmira.
c. Los usuarios no deben mantener almacenados en los discos duros, de las estaciones cliente o discos virtuales de red, archivos de vídeo, música y fotos que no sean de carácter institucional.
d. En el Disco C:\ de las estaciones cliente se tiene configurado el sistema operativo, aplicaciones y perfil de usuario.
e. El usuario deberá abstenerse de realizar modificaciones a éstos archivos.
f. Los usuarios podrán trabajar sus documentos institucionales en borrador en la estación cliente asignado por la Dirección de Tecnología, Innovación y Ciencia (TI y C) y deberán ubicar copias y documentos finales en las carpetas virtuales del grive google asignado a cada usuario

g. El préstamo de equipos de cómputo de escritorio y/o computadores portátiles y video proyectores se debe tramitar a través de oficio, con anticipación al área de recursos físicos, quienes a su vez coordinará con la dirección de Tecnología Innovación y Ciencia (IT y C), para que se realice el respectivo alistamiento a los equipos de cómputo.
h. Los equipos que ingresan temporalmente a la Alcaldía Municipal de Palmira que son de propiedad de terceros: deben ser registrados en las porterías de la entidad para poder realizar su retiro sin autorización, la Dirección de Tecnología, Innovación y Ciencia (TI y C) no se hará responsable en caso de pérdida o daño de algún equipo informático de uso personal o que haya sido ingresado a sus instalaciones sin permiso alguno.
i. La Dirección de Tecnología, Innovación y Ciencia (TI y C) no prestará servicio de soporte técnico (revisión, mantenimiento, reparación, configuración y manejo e información) a equipos que no pertenezcan a la Alcaldía Municipal de Palmira.

5.7.2 Políticas de seguridad informática de los Equipos

Objetivo:

Asegurar la protección de la información en los equipos.

Aplicabilidad:

Estas son políticas que aplican para todos los funcionarios, contratistas y terceros y en general a todos los usuarios de la Alcaldía Municipal de Palmira.

Directrices:

a. Protecciones en el suministro de energía
b. A la red de energía regulada de los puestos de trabajo solo se pueden conectar equipos como computadores, pantallas; los otros elementos deberán conectarse a la red no regulada. Esta labor debe ser revisada por la dependencia administrativa encargada.
c. Seguridad del cableado:
d. Los cables deben estar claramente marcados para identificar fácilmente los elementos conectados y evitar desconexiones erróneas.
e. Deben existir planos que describan las conexiones del cableado.
f. El acceso a los centros de cableado (Racks), debe estar protegido.
g. Mantenimiento de los Equipos
h. La Dirección de Tecnología, Innovación y Ciencia (TI y C) debe mantener contratos de soporte y mantenimiento de los equipos críticos.
i. Las actividades de mantenimiento tanto preventivo como correctivo deben registrarse para cada elemento
j. Se debe llevar una hoja de vida de cada equipo de cómputo.

k. Las actividades de mantenimiento de los servidores, elementos de comunicaciones, energía o cualquiera que pueda ocasionar una suspensión en el servicio, deben ser realizadas y programadas por el responsable de infraestructura y aprobadas por el Director de Tecnología.
l. Los equipos que requieran salir de las instalaciones de la Alcaldía Municipal de Palmira para reparación o mantenimiento, deben estar debidamente autorizados por la oficina de Recursos Físicos de la Alcaldía y se debe garantizar que en dichos elementos **no se encuentra información establecida como crítica en la clasificación de la información de acuerdo a los niveles de clasificación de la información**.
m. Para que los equipos puedan salir de las instalaciones de la Alcaldía Municipal de Palmira, se debe suministrar un nivel mínimo de seguridad, que al menos cumpla con los requerimientos internos, teniendo en cuenta los diferentes riesgos de trabajar en un ambiente que no cuenta con las protecciones ofrecidas en el interior de la Alcaldía Municipal de Palmira.
n. Cuando un dispositivo vaya a ser reasignado o retirado de servicio, debe garantizarse la eliminación de toda información residente en los elementos utilizados para el almacenamiento, procesamiento y transporte de la información, utilizando herramientas para realizar sobre-escrituras sobre la información existente o la presencia de campos magnéticos de alta intensidad. Este proceso puede además incluir, una vez realizado el proceso anterior, la destrucción física del medio, utilizando impactos, fuerzas o condiciones extremas.
o. Ingreso y retiro de activos de información de terceros.
p. El retiro e ingreso de todo activo de propiedad de los usuarios, utilizados para fines personales, se realizará mediante los procedimientos establecidos por la Administración del Edificio. La Dirección de Tecnología, Innovación y Ciencia (TI y C) no se hace responsable de los bienes o los problemas que se presenten al conectarse a la red eléctrica de la Alcaldía de Palmira.
q. El retiro e ingreso de todo activo de información de los visitantes que presten servicios a la Alcaldía, (consultores, pasantes, visitantes, etc.) será registrado y controlado en las porterías del edificio. El personal de vigilancia de recepción verificará y registrará las características de identificación del activo de información.
r. El traslado entre dependencias de todo activo de información, está a cargo de la dependencia administrativa, para el control de inventarios.

5.7.3 Políticas de seguridad informática del Data Center y centros de cableado

Objetivo:

Asegurar la protección de la información en las redes y la protección de la infraestructura de soporte, según procedimiento de administración de datacenter versión 02

Directrices:

a. No se permite el ingreso al centro de datos, al personal que no esté expresamente autorizado. Se debe llevar un control de ingreso y salida del personal que visita el centro de datos. En el centro de datos debe

disponerse de una bitácora para el registro, la cual debe ser diligenciada en lapicero de tinta al iniciar y finalizar la actividad a realizar.

b. El Área de Tecnología, Innovación y Ciencia debe garantizar que el control de acceso al centro de datos de la Dirección de Tecnología, Innovación y Ciencia (TI y C), cuenta con dispositivos electrónicos de autenticación o sistema de control biométrico.
c. La Dirección de Tecnología, Innovación y Ciencia deberá garantizar que todos los equipos de los centros de datos cuentan con un sistema alterno de respaldo de energía.
d. La limpieza y aseo del centro de datos estará a cargo de la Dependencia Administrativa y debe efectuarse en presencia de un funcionario o contratista de la Dirección de Tecnología, Innovación y Ciencia (TI y C). El personal de limpieza debe ser ilustrado con respecto a las precauciones mínimas a seguir durante el proceso de limpieza. Debe prohibirse el ingreso de personal de limpieza con maletas o elementos que no sean estrictamente necesarios para su labor de limpieza y aseo.
e. En las instalaciones del centro de datos o centros de cableado, no se debe fumar, comer o beber; de igual forma se debe eliminar la permanencia de papelería y materiales que representen riesgo de propagación de fuego, así como mantener el orden y limpieza en todos los equipos y elementos que se encuentren en este espacio.
f. El centro de datos debe estar provisto de:
g. Señalización adecuada de todos y cada uno de los diferentes equipos y elementos, así como luces de emergencia y de evacuación, cumpliendo las normas de seguridad industrial y de salud ocupacional.
h. Pisos elaborados con materiales no combustibles.
i. Sistema de refrigeración por aire acondicionado de precisión. Este equipo debe ser redundante para que en caso de falla se pueda continuar con la refrigeración.
j. Unidades de potencia ininterrumpida UPS, que proporcionen respaldo al mismo, con el fin de garantizar el servicio de energía eléctrica durante una falla momentánea del fluido eléctrico de la red pública.
k. Alarmas de detección de humo y sistemas automáticos de extinción de fuego, conectada a un sistema central. Los detectores deberán ser probados de acuerdo a las recomendaciones del fabricante o al menos una vez cada 6 meses y estas pruebas deberán estar previstas en los procedimientos de mantenimiento y de control.
l. Extintores de incendios o un sistema contra incendios debidamente probados y con la capacidad de detener el fuego generado por equipo eléctrico, papel o químicos especiales.
m. El cableado de la red debe ser protegido de interferencias por ejemplo usando canaletas que lo protejan.
n. Los cables de potencia deben estar separados de los de comunicaciones, siguiendo las normas técnicas.
o. La grabación de vídeo en las instalaciones del centro de datos debe estar expresamente autorizada por el Comité de Seguridad Informática y de Sistemas y exclusivamente con fines institucionales.
p. Las actividades de soporte y mantenimiento dentro del centro de datos siempre deben ser supervisadas por un funcionario o contratista autorizado por la Dirección de Tecnología, Innovación y Ciencia (TI y C).
q. Las puertas del centro de datos deben permanecer cerradas. Si por alguna circunstancia se requiere ingresar y salir del centro de datos, el funcionario responsable de la actividad se ubicará dentro del centro de datos.

r. Cuando se requiera realizar alguna actividad sobre algún armario (rack), este debe quedar ordenado, cerrado y con llave, cuando se finalice la actividad.
s. Mientras no se encuentre personal dentro de las instalaciones del centro de datos, las luces deben permanecer apagadas.
t. Los equipos del centro de datos que lo requieran, deben estar monitoreados para poder detectar las fallas que se puedan presentar.

5.8 Gestión de comunicaciones y operaciones

Objetivo:

Definir las pautas de uso de las comunicaciones unificadas en un entorno federado, por parte de los usuarios autorizados por la Alcaldía de Palmira.

Directrices:

a. Las comunicaciones unificadas deben ser usadas de forma austera y no se permite el envío de mensajes con contenido que atente contra la integridad de las personas o las instituciones.
b. Antes de enviar cualquier contenido, se debe verificar que no contenga malware (virus, código malicioso, etc.), mediante el uso del antivirus instalado por la Dirección de Tecnología en los equipos institucionales.
c. La información que se publique o divulgue debe guardar las medidas de seguridad exigibles de acuerdo al tipo de calificación que se le haya dado a dicha información y debe corresponder al entorno laboral.
d. Cada usuario será responsable por el adecuado uso que se le dé a las herramientas, a los daños y perjuicios que puedan llegar a causar, serán de completa responsabilidad de la persona que los haya generado.

5.8.1 Procedimientos y responsabilidades de operación

5.8.1.1 Política de uso de Internet

Objetivo:

Establecer unos lineamientos que garanticen la navegación segura y el uso adecuado de la red por parte de los usuarios finales, evitando errores, pérdidas, modificaciones no autorizadas o uso inadecuado de la información en las aplicaciones WEB.

Directrices:

a. El servicio institucional de Internet se constituye en una herramienta tecnológica que facilita el cumplimiento de las funciones y responsabilidades de los servidores de la Institución, invitados, terceros y/o pasantes autorizados, dentro de los procesos institucionales.
b. Se considera como uso aceptable del servicio institucional de Internet, la navegación para realizar tareas y actividades relacionadas a las funciones asignadas a los servidores de la Institución, invitados, terceros y/o pasantes autorizados, siempre y cuando estén involucrados dentro de los procesos institucionales.
c. La navegación en Internet debe realizarse de forma razonable y con propósitos laborales.
d. No se permite la navegación a sitios con contenidos contrarios a la ley o a las políticas Informáticas de navegación o que representen peligro para la alcaldía como: pornografía, terrorismo, hacktivismo, segregación racial u otras fuentes de dudosa procedencia.
e. El acceso a este tipo de contenidos con propósitos de estudio de seguridad o de investigación, debe contar con la autorización expresa del Comité de Seguridad Informática y de Sistemas de la Dirección de Tecnología, Innovación y Ciencia (TI y C).
f. La descarga de archivos de internet debe ser con propósitos laborales y de forma razonable para no afectar el servicio de Internet/Intranet; en forma específica el usuario debe cumplir los requerimientos de la política de uso de internet descrita en este manual.
g. Se deberá tener acceso a páginas de streaming,
h. La Dirección de Tecnología Innovación y Ciencia realizará controles periódicos que permitan verificar el cumplimiento de la presente Política, y sus procedimientos relacionados; los resultados de dichos controles generarán notificaciones a las líneas de supervisión y reportes a nivel directivo

5.8.1.2 Política de uso de mensajería instantánea y redes sociales

Objetivo:

Definir las pautas generales para asegurar una adecuada protección de la información en el uso del servicio de mensajería instantánea y de las redes sociales, por parte de los usuarios autorizados.

Directrices:

a. El uso de servicios de mensajería instantánea y el acceso a redes sociales estarán autorizados solo para un grupo reducido de usuarios, teniendo en cuenta sus funciones y para facilitar canales de comunicación con la ciudadanía.
b. No se permite el envío de mensajes con contenido que atente contra la integridad de las personas o instituciones o cualquier contenido que represente riesgo de código malicioso.
c. La información que se publique o divulgue por cualquier medio de Internet, de cualquier funcionario, contratista, que sea creado a nombre personal, como redes sociales, twitter®, facebook®, youtube®, likedink® o blogs, se considera fuera del alcance del SGSI y por lo tanto su confiabilidad, integridad y disponibilidad y los daños y perjuicios que pueda llegar a causar serán de completa responsabilidad de la persona que las haya generado.

5.8.1.3 Política de uso de discos de red o carpetas virtuales

Objetivo:

Asegurar la correcta y segura operación de los discos de red o carpetas virtuales.

Directrices:

a. Para que los usuarios tengan acceso a la información ubicada en los discos de red, se debe registrar la solicitud a través de servicios compartidos especificando el acceso y permisos, correspondientes al rol y funciones a desempeñar, a la Dirección de Tecnología, Innovación y Ciencia (TI y C). Los usuarios tendrán permisos de escritura, lectura o modificación de información en los discos de red, dependiendo de sus funciones y su rol.
b. La información institucional que se trabaje en las estaciones cliente de cada usuario debe ser trasladada periódicamente a los discos de red por ser información institucional.
c. La información almacenada en cualquiera de los discos de red debe ser de carácter institucional.
d. Está prohibido almacenar archivos con contenido que atente contra la moral y las buenas costumbres de la entidad o las personas, como pornografía, propaganda racista, terrorista o cualquier software ilegal o malicioso, ya sea en medios de almacenamiento de estaciones de trabajo, computadores de escritorio o portátiles, tabletas, celulares inteligentes, etc. o en los discos de red.
e. Se prohíbe extraer, divulgar o publicar información de cualquiera de los discos de red o estaciones de trabajo, sin expresa autorización de su jefe inmediato.
f. Se prohíbe el uso de la información de los discos de red con fines publicitarios, de imagen negativa, lucrativa o comercial.
g. La responsabilidad de generar las copias de respaldo de la información de los discos de red, está a cargo de la Dirección de Tecnología, Innovación y Ciencia (TI y C).
h. La responsabilidad de custodiar la información en copias de respaldo controladas, fuera de las instalaciones de la Alcaldía, estará a cargo de la Dirección de Tecnología, Innovación y Ciencia.

5.8.1.4 Política de uso de impresoras y del servicio de Impresión

Objetivo:
Asegurar la operación correcta y segura de las impresoras y del servicio de impresión.

Directrices:

a. Los documentos que se impriman en las impresoras de la Alcaldía de Palmira deben ser de carácter institucional.

b. Es responsabilidad del usuario conocer el adecuado manejo de los equipos de impresión (escaneo y fotocopiado) para que no se afecte su correcto funcionamiento.
c. Ningún funcionario o contratista debe realizar labores de reparación o mantenimiento de las impresoras. En caso de presentarse alguna falla, ésta se debe reportar a la Dirección de Tecnología, Innovación y Ciencia (TI y C).
d. Se debe optar por minimizar al máximo la impresión de documentos, dando cumplimiento a la directiva 004 de 2012. "Eficiencia administrativa y lineamientos de la política cero papel en la administración pública".

5.8.1.5 Política de uso de dispositivos móviles

Objetivo:

Establecer las directrices de uso y manejo de dispositivos móviles (teléfonos móviles, teléfonos inteligentes (Smartphones, tabletas, entre otros) de la Alcaldía de Palmira.

Directrices:

a. Los dispositivos móviles (teléfonos móviles, teléfonos inteligentes (Smartphones) tabletas, entre otros), son una herramienta de trabajo que se deben utilizar únicamente para facilitar las comunicaciones de los usuarios de la Alcaldía de Palmira.
b. Los dispositivos móviles deben estar integrados a una plataforma de administración controlada por la Dirección de Tecnología, Innovación y Ciencia.
c. Los usuarios deben tener instaladas únicamente las aplicaciones distribuidas y autorizadas por el administrador de la plataforma.
d. Los dispositivos móviles deben tener configurada únicamente la cuenta de correo electrónico de la Alcaldía de Palmira.
e. En el caso del nivel directivo se autoriza el uso de WhatsApp.
f. Los dispositivos móviles deben tener contraseña de ingreso y bloqueo del equipo.
g. Los dispositivos móviles deben tener únicamente la tarjeta sim asignada por la entidad, de igual forma la tarjeta sim únicamente debe instalarse en los equipos asignados por la Alcaldía de Palmira.
h. Los teléfonos móviles y/o teléfonos inteligentes, deben permanecer encendidos y cargados durante las horas laborales o de acuerdo a la responsabilidad y requerimientos propios del cargo.
i. Es responsabilidad del usuario hacer buen uso del dispositivo suministrado por la Alcaldía de Palmira con el fin de realizar actividades propias de su cargo o funciones asignadas en la Alcaldía de Palmira.
j. En caso de requerir instalación de aplicaciones adicionales en el dispositivo móvil se debe solicitar al comité de seguridad informática para su aprobación.

5.8.2 Protección contra el código malicioso

Objetivo:

Establecer directrices para la detección y prevención de la información contra un código no autorizado.
Directrices

a. Antes de enviar cualquier contenido, se debe verificar que no contenga malware (virus, código malicioso, etc.), mediante el uso del antivirus instalado por la Dirección de Tecnología en los equipos institucionales.
b. La instalación de software en los equipos de la Alcaldía Municipal de Palmira solo se realizará por parte de los funcionarios de la Dirección de Tecnología, Innovación y Ciencia, con previa autorización del Jefe inmediato.
c. El acceso a la información debe manejarse desde las directrices establecidas en este mismo documento.
d. Se realizará concientización y socialización del personal mediante el envío de circulares por los medios de comunicación institucionales.
e. Se realizará la instalación y actualización periódica del sistema de antivirus por parte de los funcionarios de la Dirección de tecnología, innovación y ciencia.
f. Se establecen procedimientos para el uso de antivirus, dar formación para su uso y para afrontar ataques.
g. La Alcaldía Municipal de Palmira dispone de licencias individuales para cada uno de los equipos institucionales donde se encuentra instalado el software de antivirus.

5.8.3 Política de respaldo y restauración de información

Objetivo:

Proporcionar medios de respaldo adecuados para asegurar que toda la información esencial y el software, se pueda recuperar después de una falla.

Directrices:

a. La información de cada sistema debe ser respaldada regularmente sobre un medio de almacenamiento como cinta, cartucho, CD, DVD, unidad virtual, unidad de red, Cloud.
b. Los administradores de los servidores, los sistemas de información o los equipos de comunicaciones, son los responsables de definir la frecuencia de respaldo y los requerimientos de seguridad de la información, (Codificación) y el administrador del sistema de respaldo, es el responsable de realizar los respaldos periódicos.
c. Todas las copias de información crítica deben ser almacenadas en un área adecuada y con control de acceso adecuado.
d. Las copias de respaldo se guardarán únicamente con el objetivo de restaurar el sistema luego de un virus informático, defectos en los discos de almacenamiento, problemas de los servidores o computadores, materialización de amenazas, catástrofes y por requerimiento legal.

e. Un plan de emergencia debe ser desarrollado para todas las aplicaciones que manejen información crítica (SIIFWEB), el propietario de la información debe asegurar que el plan es adecuado, frecuentemente actualizado y periódicamente probado y revisado.
f. Ningún tipo de información institucional puede ser almacenada en forma exclusiva en los discos duros de las estaciones de trabajo; por lo tanto, es obligación de los usuarios finales realizar las copias en las carpetas destinadas para este fin (Google drive).
g. Deben existir al menos una copia de la información de los discos de red, la cual deberá permanecer fuera de las instalaciones de la Dirección de Tecnología, Innovación y Ciencia TI y C.
h. La restauración de copias de respaldo en ambientes de producción debe estar debidamente aprobada por el propietario de la información.
i. Semanalmente los administradores de infraestructura informática verificarán la correcta ejecución de los procesos de backup, de acuerdo al medio que se utilice para este propósito y controlarán la vida útil del medio utilizado.
j. La Dirección de Tecnología, Innovación y Ciencia debe exigir a la firma contratista encargada del SIIWEB mantener un inventario actualizado de las copias de respaldo Bases de Datos e información y los aplicativos o sistemas informáticos.
k. Los medios que vayan a ser eliminados deben surtir un proceso de borrado seguro y posteriormente serán eliminados o destruidos de forma adecuada. *(El borrado seguro se ejecuta cuando al borrar un archivo o formatear un dispositivo de almacenamiento, alguna utilidad de borrado escribe ceros (0) sobre el archivo, no permitiendo que éste se pueda recuperar posteriormente.)*
l. Es responsabilidad de cada dependencia mantener depurada la información de las carpetas virtuales establecidas para la optimización del uso de los recursos de almacenamiento que entrega Informática a los usuarios.

5.8.4 Política para realización de copias en estaciones de trabajo de usuario final

Objetivo:

Asegurar la operación de realización de copias de información en estaciones de trabajo de usuario final.

Directrices:

a. De acuerdo a lo previsto por el artículo 91 de la Ley 23 de 1982, los derechos de autor sobre las obras creadas por los empleados y funcionarios en virtud de su vinculación a la Entidad pública correspondiente, son de propiedad de esta con las excepciones que la misma ley ha señalado.
b. En el evento de retiro de un funcionario o traslado de dependencia, previa notificación a la Subsecretaría de Talento Humano, la Dirección de Tecnología, Innovación y Ciencia generará una copia de la información contenida en el equipo asignado al perfil del usuario (C:\usuarios\nombre-usuario), a una unidad de almacenamiento.

c. Una vez esta información se encuentre ubicada en la unidad de almacenamiento, se le realiza copia de seguridad mensual en cinta magnética, la cual es enviada al custodio de medios magnéticos, para conservar esta información en el tiempo.
d. Si el jefe de la dependencia de la cual se retira el usuario requiere copia de esta información, la podrá solicitar a la Dirección de Tecnología de la Información y ciencia (TIyC) quien la podrá hacer teniendo en cuenta la solicitud explicando el motivo del requerimiento y la verificación de la existencia del acuerdo de confidencialidad debidamente diligenciado por el usuario retirado.
e. Se debe seguir el procedimiento de borrado seguro para equipos finales, a fin de garantizar la copia de la información para la Alcaldía de Palmira y la eliminación de la información almacenada en el disco local.
f. Ningún usuario final debe realizar copias de la información contenida en la estación de trabajo a medios extraíbles de información, excepto aquellos que se encuentren habilitados los privilegios de escritura por puertos USB y el cliente DLP instalado el cual mantendrá un registro de los archivos copiados.
g. En caso de presentarse alguna falla en los equipos de cómputo, se debe reportar mediante la plataforma de mesa de ayuda https://mesadeayuda.palmira.gov.co,, en caso de requerirse copia de la información, esta se realizará de manera temporal durante las diferentes labores de reparación o mantenimiento.

5.8.5 Política de uso gestión de seguridad de RED (red de área local – LAN)

Objetivo:

Asegurar la operación correcta y segura de los puntos de red.

Directrices:

a. Los usuarios deberán emplear los puntos de red, para la conexión de equipos informáticos estándar. Los equipos de uso personal, que no son de propiedad de la Alcaldía de Palmira, solo tendrán acceso a servicios limitados destinados a invitados o visitantes, estos equipos deben ser conectados a los puntos de acceso autorizados y definidos por la Dirección de Tecnología, Innovación y Ciencia.
b. La instalación, activación y gestión de los puntos de red es responsabilidad de la Dirección de Tecnología, Innovación y Ciencia TIyC

5.8.6 Política de disposición de información, medios y equipos

Objetivo:

Contrarrestar las interrupciones en las actividades del servicio y proteger sus procesos críticos contra los efectos de fallas importantes en los sistemas de información o contra desastres y propender por su recuperación oportuna.

Directrices:

a. Los medios y equipos donde se almacena, procesa o comunica la información, (servidores, unidades de Red, Discos flexibles, Nube, etc.) deben mantenerse con las medidas de protección físicas y lógicas, que permitan su monitoreo y correcto estado de funcionamiento; para ello se deben realizar los mantenimientos preventivos y correctivos que se requieran.

5.8.7 Política de Intercambio de Información

Objetivo:

Definir las pautas generales para asegurar una adecuada protección de la información, en el uso del servicio de correo electrónico por parte de los usuarios autorizados.

Directrices:

Esta política define y distingue el uso de correo electrónico aceptable/apropiado e inaceptable/inapropiado y establece las directrices para el uso seguro del servicio.

Servicio de correo electrónico:

a. Permite a los usuarios de la Alcaldía, el intercambio de mensajes, a través de una cuenta de correo electrónico institucional, que facilita el desarrollo de sus funciones.
b. Los usuarios del correo electrónico corporativo son responsables de evitar prácticas o usos del correo que puedan comprometer la seguridad de la información.
c. Los servicios de correo electrónico corporativo se emplean para servir a una finalidad operativa y administrativa en relación con la entidad. Todos los correos electrónicos procesados por los sistemas, redes y demás infraestructura de TIC Informática se consideran bajo el control de la Alcaldía de Palmira.
d. Este servicio debe utilizarse exclusivamente para las tareas propias de la función desarrollada en la Alcaldía de Palmira y no debe utilizarse para ningún otro fin.
e. No está autorizado el envío de cadenas de correo, envío de correos masivos con archivos adjuntos de gran tamaño que pueden congestionar la red. No está autorizado, el envío de correos con contenido que atenten contra la integridad y dignidad de las personas y el buen nombre de la entidad.
f. Se debe evitar el Phishing o correo electrónico que tiene la apariencia de ser fiable para saber distinguir los correos “buenos de los malos”, en el que guardamos nuestro trabajo diario abriendo un correo que nos descargará un malware o al que le proporcionaremos toda nuestra información, incluida nuestra cuenta bancaria.
g. No está permitido utilizar la cuenta de correo corporativo en chats, conferencias, promociones, etc., ya que esto conlleva a que al buzón le llegue un posible malware, spam, virus, ramsonware etc, que pueden atentar con la seguridad de la infraestructura de la Alcaldía Municipal La información del buzón corporativo pertenece a la Alcaldía de Palmira y esta podrá utilizarla cuando la requiera no importando que el usuario

dueño del buzón no la autorice, ya que este firmó el compromiso de confidencialidad donde se le indicaba este requerimiento.

Condiciones de uso del servicio:

a. Cuando un funcionario, contratista o colaborador al que le haya sido autorizado el uso de una cuenta de correo electrónico y se retire de la Alcaldía de Palmira, su cuenta de correo:
b. Será desactivada.
c. Pasados 90 días de su desactivación, se procederá a hacer un backup del buzón y la cuenta será eliminada, con el fin de disponer de la licencia.
d. El backup de buzón se conservará según procedimiento de conservación de medios electrónicos (según esté establecido en el sistema de gestión documental.
e. Los correos electrónicos deben contener la siguiente nota respecto al manejo del contenido:
f. El contenido de este mensaje y sus anexos son propiedad del Municipio de Palmira, es únicamente para el uso del destinatario ya que puede contener Información pública reservada o información pública clasificada (privada o semiprivada), las cuales no son de carácter público. Si usted no es el destinatario, se informa que cualquier uso, difusión, distribución o copiado de esta comunicación está prohibido. Cualquier revisión, retransmisión, diseminación o uso del mismo, así como cualquier acción que se tome respecto a la información contenida, por personas o entidades diferentes al propósito original de la misma, es ilegal.
g. Si usted es el destinatario, le solicitamos dar un manejo adecuado a la información; de presentarse cualquier suceso anómalo, por favor informar a la mesa de ayuda https://mesadeayuda.palmira.gov.co/.
h. El tamaño del buzón de correo electrónico estará determinado por el rol tipo de licenciamiento asignado. Cada dependencia deberá solicitar la creación de las cuentas electrónicas, sin embargo la Dirección de Tecnología Innovación y Ciencia (TIyC) podrán inactivar buzones de personal retirado, y después de 90 días se procederá a hacer un backup del buzón y la cuenta será eliminada, con el fin de disponer de la licencia.
i. El backup de buzón se conservará según procedimiento de conservación de medios electrónicos (según esté establecido en el sistema de gestión documental.
j. Las cuentas de correo electrónico son propiedad de la Alcaldía Municipal de Palmira, las cuales son asignadas a personas que tengan algún tipo de vinculación laboral con la Alcaldía Municipal, ya sea como personal de planta, contratistas, asesores, consultores o personal temporal, quienes deben utilizar este servicio única y exclusivamente para las tareas propias de la función desarrollada en la Alcaldía Municipal de Palmira y no debe utilizarse para ningún otro fin.
k. Cada usuario es responsable del contenido del mensaje enviado y de cualquier otra información adjunta al mismo, de acuerdo a la clasificación de la información establecida por la Alcaldía Municipal de Palmira
l. Todos los mensajes pueden ser sujetos a análisis y conservación permanente por parte de la Alcaldía de Palmira.
m. Todo usuario es responsable por la destrucción de los mensajes cuyo origen sea desconocido y por lo tanto asumirá la responsabilidad y las consecuencias que puede ocasionar la ejecución de cualquier archivo adjunto. En estos casos no se debe contestar dichos mensajes, ni abrir los archivos adjuntos y se debe abrir

un caso en la mesa de ayuda https://mesadeayuda.palmira.gov.co/ con la frase "correo sospechoso" en el asunto. Se deben eliminar tanto de la bandeja de entrada como de elementos eliminados.

n. Los grupos de distribución serán creados a través de solicitud expresa del jefe del área, utilizando el formato establecido para tal fin.
o. En dicho formato se debe especificar el área
p. el administrador de la lista
q. los miembros de la lista
r. Todos los grupos de distribución empezaran con la palabra grupo y serán de manejo interno. En caso de que se requiera un grupo de distribución que reciba correos externos, deberá especificarse en la solicitud.
s. Las cuentas de correo electrónico que presenten un lapso de 90 días sin actividad, serán inactivadas para su posterior eliminación, previa copia de seguridad del buzón, la cual reposará en los servidores dispuestos para tal fin. Se exceptúan las cuentas de correo de usuarios que estén en licencias, incapacidades, vacaciones y encargos.
t. El único servicio de correo electrónico autorizado en la Alcaldía de Palmira es el asignado por la Dirección de Tecnología, Innovación y Ciencia (TI y C).

5.8.8 Política de Tercerización u Outsourcing

Objetivo:

Mantener la seguridad de la información y los servicios de procesamiento de información, a los cuales tienen acceso terceras partes, entidades externas o que son procesados, comunicados o dirigidos por estas.

Directrices:

a. **Selección de outsourcing:** se deben establecer criterios de selección que contemplen la historia y reputación de terceras partes, certificaciones y recomendaciones de otros clientes, estabilidad financiera de la compañía, seguimiento de estándares de gestión de calidad y de seguridad y otros criterios que resulten de un análisis de riesgos de la selección y los criterios establecidos por la entidad.
b. **Análisis de riesgos:** se deben identificar los riesgos para la información y los servicios de procesamiento de información que involucren partes externas a la Alcaldía del municipio de Palmira. El resultado del análisis de riesgos será la base para el establecimiento de los controles y debe ser presentado al Comité de Seguridad Informática antes de firmar el contrato de outsourcing.
c. **Acuerdos con terceras partes:** Con el fin de proteger la información de ambas partes, se debe formalizar un acuerdo de confidencialidad el acuerdo deberá definir claramente el tipo de información que intercambiarán las partes, los medios, la frecuencia y los procedimientos a seguir.
d. Si la información intercambiada lo amerita teniendo en cuenta *guía para la calificación de la información de acuerdo con sus niveles de seguridad*[1], se debe preparar y legalizar un acuerdo de confidencialidad entre la

[1] https://www.mintic.gov.co/gestionti/615/articles-5482_G5_Gestion_Clasificacion.pdf

entidad y el outsourcing de acuerdo al objetivo y al alcance del contrato; el cual debe quedar firmado por ambas partes. En todos los casos deben firmarse acuerdos de niveles de servicio que permitan cumplir con las políticas de seguridad informática y con los objetivos de la entidad.

5.9. Política de control de acceso

Objetivo:

Definir las pautas generales para asegurar un acceso controlado, físico o lógico, a la información de la plataforma informática de la Dirección de Tecnología, Innovación y Ciencia (TI y C), así como el uso de medios de computación móvil.

Directrices:

a. La Dirección de Tecnología, Innovación y Ciencia (TI y C) proporcionará a los funcionarios y contratistas (personas naturales) todos los recursos tecnológicos necesarios para que puedan desempeñar las funciones para las cuales fueron contratados, por tal motivo no se permite conectar a la red o instalar dispositivos fijos o móviles, tales como: computadores portátiles, tabletas, enrutadores, agendas electrónicas, celulares inteligentes, Access Point, que no sean autorizados por la Dirección de Tecnología, Innovación y Ciencia (TI y C).
b. La Dirección de Tecnología, Innovación y Ciencia (TI y C) suministrará a los usuarios las claves respectivas para el acceso a los servicios de red y sistemas de información a los que hayan sido autorizados, las claves son de uso personal e intransferible. Es responsabilidad del usuario el manejo que se les dé a las claves asignadas.
c. Solo usuarios designados por la Dirección de Tecnología, Innovación y Ciencia (TI y C), estarán autorizados para instalar software licenciado o hardware en los equipos, servidores e infraestructura de la Alcaldía de Palmira.
d. Todo trabajo que utilice los servidores, sus funcionarios o contratistas, con información de la entidad, se debe realizar en sus instalaciones, no se podrá realizar ninguna actividad de tipo remoto sin la debida aprobación de la Dirección de Tecnología, Innovación y Ciencia (TI y C).
e. La conexión remota a la red de área local de la Alcaldía debe ser hecha a través de una conexión VPN segura suministrada por la Dirección de Tecnología, Innovación y Ciencia (TI y C), la cual debe ser aprobada, registrada y auditada.

5.9.1 Política de establecimiento, uso y protección de claves de acceso

Objetivo:

Controlar el acceso a la información.

Directrices:

a. Se debe concienciar y controlar que los usuarios sigan buenas prácticas de seguridad en la selección, uso y protección de claves o contraseñas, las cuales constituyen un medio de validación de la identidad de un usuario y consecuentemente un medio para establecer derechos de acceso a las instalaciones, equipos o servicios informáticos. Es decir promover la cultura de ciberseguridad en el puesto de trabajo:
b. Los usuarios son responsables del uso de las claves o contraseñas de acceso que se le asignen para la utilización de los equipos o servicios informáticos de la Alcaldía.
c. Los usuarios deben tener en cuenta los siguientes aspectos:
d. El cambio de contraseña sólo podrá ser solicitado por el titular de la cuenta o su jefe inmediato a la Dirección de Tecnología, Innovación y Ciencia (TI Y C).
e. Terminar las sesiones activas cuando finalicen, o asegurarlas con el mecanismo de bloqueo cuando no estén en uso.
f. Se bloqueará el acceso a todo usuario que haya intentado el ingreso, sin éxito, a un equipo o sistema informático, en forma consecutiva por tres veces.
g. La clave de acceso será desbloqueada sólo por la Dirección de Tecnología, Innovación y Ciencia (TI Y C), luego de la solicitud formal por parte del responsable de la cuenta. Para todas las cuentas especiales, la reactivación debe ser documentada y comunicada a la Dirección de Tecnología, Innovación y Ciencia (TI Y C).

5.9.2 Responsabilidades del Usuario

a. Poseer algún grado de complejidad y no deben ser palabras comunes que se puedan encontrar en diccionarios, ni tener información personal, por ejemplo: fechas de cumpleaños, nombre de los hijos, placas de automóvil, etc.
b. Tener mínimo ocho caracteres alfanuméricos.
c. Cambiarse obligatoriamente la primera vez que el usuario ingrese al sistema.
d. Cambiarse obligatoriamente cada 3 meses, o cuando lo establezca la Dirección de Tecnología, Innovación y Ciencia (TI y C).
e. Cada vez que se cambien estas deben ser distintas por lo menos de las últimas tres anteriores.
f. Cambiar la contraseña si ha estado bajo riesgo o se ha detectado anomalía en la cuenta de usuario.
g. No se deben usar caracteres idénticos consecutivos, ni que sean todos numéricos, ni todos alfabéticos.
h. Debe contener mínimo un carácter especial, por ejemplo $%&!>
i. No debe ser visible en la pantalla, al momento de ser ingresada o mostrarse o compartirse.
j. No ser reveladas a ninguna persona, incluyendo al personal de la Dirección de Tecnología, Innovación y Ciencia (TI y C).
k. No registrarlas en papel, archivos digitales o dispositivos manuales, a menos que se puedan almacenar de forma segura y el método de almacenamiento esté aprobado.
l. No incluir contraseñas en ningún proceso de registro automatizado, por ejemplo almacenadas en un macro o en una clave de función, el usar contraseñas cortas y simples, así como fáciles de adivinar como 12345, pedro, maría, le resulta fácil identificarlas a los ciberdelincuentes, utilicen contraseñas como “¡MeENCANTA*leerenlaweb!”.

m. Utilizar doble Factor de Doble factor de autenticación

5.9.3 Política Control de Acceso a la RED

Objetivo:

Establecer las directrices de uso del mecanismo de doble autenticación implementado por Informática, para los diferentes servicios prestados por la entidad (VPN, conexión inalámbrica, autenticación del equipo de cómputo institucional).

Directrices:

a. La Dirección de Tecnología, Innovación y Ciencia asignará las credenciales de acceso de acuerdo a solicitud elevada por los usuarios.
b. La asignación de credenciales de acceso para VPN a los funcionarios dependerá del requerimiento para el desarrollo de sus funciones, de conectarse desde un lugar remoto a los servicios informáticos brindados por la Alcaldía de Palmira.
c. La conexión realizada a través del servicio de VPN se debe realizar desde un equipo en un ambiente seguro.
d. Es responsabilidad del usuario hacer buen uso del dispositivo del acceso suministrado, con el fin de realizar actividades propias de su cargo o funciones asignadas Alcaldía Municipal de Palmira/Proceso asignado.
e. Usos de Token
f. La Dirección de Tecnología, Innovación y Ciencia asignará los Token de acuerdo a solicitud elevada por los usuarios.
g. La asignación de Token a los funcionarios dependerá del requerimiento para el desarrollo de sus funciones de conectarse desde un lugar remoto a los servicios informáticos brindados por la Alcaldía de Palmira o terceros.
h. Es responsabilidad del usuario hacer buen uso del dispositivo entregado, con el fin de realizar actividades propias de su cargo o funciones asignadas en la Alcaldía Municipal de Palmira.
i. La pérdida del Token entregado debe ser reportada de inmediato a la Dirección de Tecnología, Innovación y Ciencia para su debida desactivación y bloqueo.
j. En caso de no requerir más el uso del Token o retiro definitivo de la Alcaldía de Palmira, el funcionario debe realizar la devolución del mismo en las condiciones que le fue entregado.

5.9.4 Control de acceso al sistema operativo

Objetivo:

Definir las pautas generales para reducir el riesgo de acceso no autorizado, pérdida y daño de la información durante y fuera del horario de trabajo normal de los usuarios.

Directrices:

a. El personal de la Alcaldía debe conservar su escritorio libre de información, propia de la entidad, que pueda ser alcanzada, copiada o utilizada por terceros o por personal que no tenga autorización para su uso o conocimiento.
b. Los funcionarios y contratistas de la Alcaldía deben bloquear la pantalla de su computador con el protector de pantalla, en los momentos que no esté utilizando el equipo o cuando por cualquier motivo deba dejar su puesto de trabajo.
c. Al imprimir documentos de carácter confidencial, estos deben ser retirados de la impresora inmediatamente y no se deben dejar en el escritorio sin custodia.
d. No se debe utilizar fotocopiadoras, escáneres, equipos de fax, cámaras digitales y en general equipos tecnológicos que se encuentren desatendidos.

5.9.5 Control de acceso a las aplicaciones y la información

Objetivo:

Impedir el acceso no autorizado a los sistemas de información.

Directrices:

a. Las cuentas de usuario y contraseña de los sistemas de información serán personales, únicos e intransferibles.
b. Los usuarios son responsables del uso de las claves o contraseñas de acceso que se le asignen para la utilización de los equipos o servicios informáticos de la Alcaldía.
c. Los usuarios deben tener en cuenta los siguientes aspectos:
d. El cambio de contraseña sólo podrá ser solicitado por el titular de la cuenta o su jefe inmediato a la Dirección de Tecnología, Innovación y Ciencia (TI Y C).
e. Terminar las sesiones activas cuando finalicen, o asegurarlas con el mecanismo de bloqueo cuando no estén en uso.
f. La clave de acceso será desbloqueada sólo por la Dirección de Tecnología, Innovación y Ciencia (TI y C), luego de la solicitud formal por parte del responsable de la cuenta.

g. 5.10.6 Protocolo uso de la red wifi
h. La Subsecretaría de Gestión Corporativa dando cumplimiento a su función de evaluar la implementación de políticas, programas y proyectos en materia de desarrollo, modernización y tecnología informática administrativa, contrató la adquisición, instalación, configuración y puesta en funcionamiento de un servicio de WiFi para la Secretaria Distrital de Movilidad.
i. El servicio de WiFi permite conectar a Internet usuarios simultáneamente a través de equipos como computadores, tablets, smartphones, celulares, entre otros mediante el uso de radiofrecuencias, lo que representa un ahorro en infraestructura de medios físicos, cableado, puertos, entre otros, brindando un servicio completamente móvil.
j. Esta solución tecnológica ha sido implementada para brindar el servicio de Internet a los visitantes dentro de las instalaciones de la Alcaldía Municipal de Palmira y en sus sedes externas y así permitir la conexión para el intercambio de información y acceso con un servicio de internet óptimo y confiable.

5.9.6.1 Condiciones generales del servicio

Todos los usuarios al acceder a las redes inalámbricas de la Alcaldía Municipal de Palmira aceptan de manera directa las políticas, términos y condiciones de uso descritos a continuación sin ninguna reserva, así como las políticas de seguridad de la Información de la entidad, las de protección de datos personales y cualquier condición adicional que en el futuro se pudiera complementar en estos lineamientos.

El servicio de red inalámbrica se presta bajo las siguientes características y consideraciones:
Invitados : Podrán acceder a la red Wifi de **Invitados Alcaldía de Palmira,** las personas externas a la entidad que eventualmente asistan a las Sedes de la entidad, personal de las empresas contratistas, personas jurídicas tipo interventorías.

Modo de ingreso:

Conectarse a la red Invitados Alcaldía de Palmira

- Diligenciar correctamente los datos solicitados: Nombre - Empresa – Dirección de correo electrónico - Dependencia destino
- Tiempo de conexión 8 horas

Conectarse a la red Empleados:

- Podrán acceder a la red Wifi de Empleados Alcaldía de Palmira, los funcionarios de la entidad.
- Modo de ingreso:
- Debe solicitar a la dirección de tecnología innovación y Ciencia el registro del equipo en la controladora WIFi
- Conectarse a la red Empleados Alcaldía de Palmira
- Diligenciar correctamente los datos solicitados: Nombre - Empresa – Dirección de correo electrónico - Dependencia destino
- Tiempo de conexión ilimitado

5.9.6.2 Términos y condiciones de la red wifi para visitantes

a. El visitante podrá hacer uso de la red de Wifi de la Alcaldía Municipal de Palmira después de leer y verificar los términos y condiciones de uso de la red y las Políticas de Seguridad y protección de datos personales.
b. El siguiente mensaje aparecerá después de encontrar la red de visitantes y empleados
c. "La Alcaldía Municipal de Palmira.
d. De conformidad con lo establecido en la Ley 1581 de 2012 y Decreto 1377 de 2013 la Alcaldía Municipal de Palmira manifiesta que la información solicitada para el acceso a esta red de la Entidad, será utilizada única y exclusivamente para fines estadísticos.
e. La Entidad garantiza la reserva de la información registrada, la cual deberá ser veraz, completa, actualizada y comprensible".

5.9.6.3 Términos de uso de la red de Visitantes:

a. Al acceder y utilizar la red de WIFI de la Alcaldía Municipal de Palmira el visitante declara que ha leído, entendido y acepta los términos y condiciones para su utilización. Si el visitante no está de acuerdo con esta normatividad no podrá acceder a este servicio.
b. El visitante acepta y reconoce que hay riesgos potenciales a través de un servicio WI-FI. Debe tener cuidado al transmitir datos como: número de tarjetas de crédito, contraseñas u otra información personal sensible a través de redes WIFI. La Alcaldía Municipal de Palmira no puede y no garantiza la privacidad y seguridad de sus datos y de las comunicaciones al utilizar este servicio.
c. La Alcaldía Municipal de Palmira no garantiza el nivel de funcionamiento de la red de WIFI. El servicio puede no estar disponible o ser limitado en cualquier momento y por cualquier motivo, incluyendo emergencias, sobrecarga de conexiones, fallo del enlace, problemas de equipos en la red, interferencias o fuerza de señal. La Entidad no se responsabiliza por datos, mensajes o páginas perdidas, no guardadas o retrasos por interrupciones o problemas de rendimiento del servicio.
d. La Entidad puede establecer límites de uso, suspender el servicio o bloquear ciertos comportamientos, acceso a ciertos servicios o dominios para proteger la red de la Entidad de fraudes o actividades que atenten contra leyes nacionales e internacionales.

5.9.6.4 No se podrá utilizar la rede de WIFI de Visitantes con los siguientes fines:

a. El visitante se compromete a usar el servicio de acceso WiFi de forma diligente y correcta y se compromete a no utilizarlo para la realización de actividades contrarias a la ley, a la moral, a las buenas costumbres aceptadas y/o con fines o efectos ilícitos, prohibidos o lesivos de derechos e intereses de terceros, así como a no realizar ningún tipo de uso que de cualquier forma pueda dañar, inutilizar, sobrecargar, deteriorar o impedir la normal utilización del servicio, los documentos, archivos y toda clase de contenidos almacenados en cualquier equipo informático accesible a través de Internet. El establecimiento declina cualquier

responsabilidad que de todo ello pudiera derivarse con toda la extensión que permita el ordenamiento jurídico.

b. Con carácter enunciativo, no se permiten intercambiar contenidos que incluyan material que infrinja derechos de autor no debidamente autorizados, o que infrinja cualquier otro derecho de Propiedad Intelectual o Industrial, material ofensivo para la comunidad y la moral pública material que realice apología del terrorismo, racismo, u otras conductas ilegales, material pornográfico, especialmente el que atente contra menores, materiales amenazadores, difamatorios o que inciten a la violencia contenidos ilegales o ilícitos de cualquier naturaleza. Asimismo, igualmente a título enunciativo pero no limitativo, el Visitante se compromete a no utilizar, transmitir o difundir: lenguaje difamatorio, amenazante o que sea contrario al derecho al honor, a la intimidad personal o familiar o la propia imagen de las personas físicas y jurídicas, acceder ilegalmente o sin autorización a sistemas, o redes que pertenezcan a otra persona, o a tratar de superar medidas de seguridad del sistema de otra persona ("hacking"), cualquier actividad que pueda ser usada como causante de un ataque a un sistema (escaneo de puertos,etc.). Distribución de virus, gusanos, troyanos a través de Internet, o cualquier otra actividad destructiva; Distribuir información acerca de creación o transmisión de virus por Internet, gusanos, troyanos, saturación, "mailbombing", o ataques de denegación de servicio; Creación o gestión de bootnets; También actividades que interrumpan o interfieran en el uso efectivo de los recursos de red de otras personas o la realización de "spamming". Realizar un uso fraudulento de la dirección IP proporcionada en cada acceso, Cualquier otra forma que sea contraria, menosprecie o atente contra los Derechos Fundamentales y las libertades públicas reconocidas en la Constitución, en los Tratados Internacionales.
c. La Entidad se reserva el derecho a suspender y/o bloquear el servicio de forma inmediata y sin previo aviso en caso de detectar usos del servicio incumpliendo lo dispuesto en esta cláusula.
d. **Configuración del servicio en el dispositivo**. Los usuarios son responsables de configurar sus dispositivos con los procedimientos básicos para el funcionamiento dentro de la red inalámbrica y de acuerdo al protocolo creado para el efecto.
e. **Disponibilidad del servicio**. El servicio de conexión a la red inalámbrica estará disponible, excepto en situaciones de fuerza mayor, o por cortes parciales o interrupciones relativas al mantenimiento preventivo o correctivo de los equipos y elementos que componen la infraestructura de red inalámbrica, así como de los relacionados a la prestación del servicio de Internet.
f. El servicio se ha diseñado y desplegado para minimizar el impacto de redes inalámbricas vecinas, debido a las características propias de esta tecnología y su medio de transmisión, es decir la disponibilidad y calidad del servicio está sujeta a la interferencia de redes inalámbricas de terceros y/o a la cantidad de usuarios conectados a la red.
g. Restricciones del servicio:
h. El acceso a Internet está restringido de acuerdo con las políticas de seguridad de la entidad, por lo tanto, se prohíbe el acceso a páginas relacionadas o de contenido inapropiado como pornográfico, juegos, hacking, entre otros. La Alcaldía Municipal de Palmira podrá limitar o negar el acceso a sitios o lugares que considere peligrosos o de dudoso destino sin que esto se considere una disminución o falla del servicio.
i. Sobre la red inalámbrica de invitados se ha habilitado un ancho de banda máximo de 30Mbps , el cual es compartido por los usuarios conectados a ella. Es responsabilidad de los usuarios hacer uso eficiente y racional de este recurso para el aprovechamiento y beneficio de todos los usuarios.

j. Para el acceso a la red inalámbrica, los equipos deberán soportar el estándar de comunicación 802.11 b/g/n y soportar cifrado WPA2.
k. **De la información transportada en la Red**. La Alcaldía Municipal de Palmira no es responsable del contenido y veracidad de la información a la que se accede por medio de la red inalámbrica.

5.10 Responsabilidad frente al servicio

a. La Dirección de Tecnología Innovación y Ciencia TIyC es responsable de mantener en operación la infraestructura que proporciona red a los puntos de acceso a las redes inalámbricas. El soporte a incidentes sobre esta plataforma lo brindará la mesa de ayuda.
b. Es responsabilidad de los usuarios contar con el software y configuración de seguridad en su equipo personal para minimizar el riesgo al que se puede ver expuesto a un ataque informático al encontrarse conectado sobre esta red.
c. De ninguna forma ni caso específico la Alcaldía Municipal de Palmira será responsable por cualquier daño que pueda sufrir el equipo o dispositivo personal usado para establecer conexión a la red inalámbrica.
d. El usuario es responsable de toda actividad que se lleve a cabo desde su equipo o dispositivo mientras esté conectado a la red inalámbrica. Es obligación del usuario informar a la Dirección de Tecnología Innovación y Ciencia TIyC, la violación de alguna de las consideraciones descritas en este documento tanto por personas ajenas o funcionarios de la entidad. Es responsabilidad del usuario estar enterado de los cambios de las presentes indicaciones.
e. Es responsabilidad del usuario la seguridad física de su equipo o dispositivo, por lo que la Alcaldía Municipal de Palmira no es en ninguna forma responsable por robo o daños al equipo del usuario. El usuario acepta y reconoce que la Alcaldía Municipal de Palmira sólo provee el servicio de acceso a internet.

5.11 Prohibiciones

a. El usuario se compromete a hacer uso productivo y seguro de la red inalámbrica, según los niveles de acceso a Internet establecidos por la Alcaldía Municipal de Palmira.
b. Al hacer uso de la red WiFi está estrictamente prohibido:
c. El uso personal de los recursos públicos para fines distintos a los permitidos.
d. El uso para generar ganancias monetarias personales o propósitos comerciales.
e. Transmitir y/o distribuir cualquier material que viole la ley o regulación de derechos de autor u otros derechos de propiedad intelectual, como software sin licencia, música, videos, películas, entre otros.
f. Revelar o ceder las credenciales de autenticación de la red inalámbrica a personal no autorizado.
g. Descargar servicios broadcast como audio y video.
h. Usar programas “peer to peer” (P2P) o alguna otra tecnología que permita el intercambio de archivos en volumen.
i. Extender el alcance de la red por medio de cualquier dispositivo físico o lógico.
j. Manipular los equipos de transmisión de la red inalámbrica.

k. Instalar o realizar labores de recolección o escucha de información en tránsito por la red.
l. El uso del servicio para interferir o molestar a otros usuarios o entorpecer asuntos propios de la Alcaldía Municipal de Palmira.
m. El uso del servicio para violar las políticas de uso aceptable del correo electrónico o plataformas colaborativas.
n. Transgredir cualquier recurso informático, sistema o sitios de telecomunicaciones a los que no le está permitido acceder.
o. Instalar equipos y/o software que genere interrupción o interferencia con la emisión normal de la red inalámbrica.
p. Realizar el escaneo de vulnerabilidades de la red o de cualquier equipo de la misma sin la expresa autorización de la Dirección de Tecnología innovación y Ciencia tiyc.
q. Monitorear los canales de transmisión y comunicación por personas que no pertenezcan a la Dirección de Tecnología innovación y Ciencia tiyc o no estén debidamente autorizadas.
r. Cualquier conducta que viole las normas generalmente aceptadas dentro de la comunidad de Internet.
s. Realizar alguna acción establecida en la Ley 1273 de 2009 – Ley de delitos informáticos

5.12 Suspensión del servicio

La Dirección de Tecnología innovación y Ciencia TIyC podrá definir límites de uso, bloquear, suspender o desactivar temporalmente los servicios o cancelarlos definitivamente a uno o varios usuarios si detecta un uso indebido de la red inalámbrica.

a. Causas de suspensión temporal del servicio:
b. Distribuir malware (virus, troyanos) u otro software malicioso
c. Efectuar descargas de manera desmesurada, que afecten el desempeño del servicio de los demás usuarios de la red inalámbrica.
d. Causas de suspensión definitiva del servicio:
e. Transmisión de contenido inapropiado.
f. Incumplimiento de las políticas de seguridad de la información
g. Generar o distribuir malware (virus, troyanos) u otro software malicioso
h. Realizar actividades delictivas.
i. Envío de mensajes no solicitados (spam).
j. Atentar contra la disponibilidad, integridad, confidencialidad del servicio.
k. Cualquier conducta que viole las normas aceptadas dentro de la comunidad de Internet, esté o no detallada en estas políticas de uso aceptable.
l. Manipular o intentar manipular cualquier componente de la infraestructura de red.

5.13. Política de adquisición, desarrollo y mantenimiento de sistemas de información

5.13.1 Requerimientos de seguridad de los sistemas de información

Objetivo:
Garantizar que la seguridad es parte integral de los sistemas de información.

Directrices:

a. Asegurar que los sistemas de información o aplicativos informáticos incluyen controles de seguridad y cumplen con las políticas de seguridad informática.
b. En caso de desarrollos propios de la Alcaldía se debe verificar que están completamente documentados, que las diferentes versiones se preservan adecuadamente en varios medios y se guarda copia de respaldo externa a la Alcaldía y que sean registrados ante la Dirección General de Derechos de Autor del Ministerio del Interior y de Justicia.
c. Desarrollar estrategias para analizar la seguridad en los sistemas de información.
d. Todo nuevo hardware y software que se vaya a adquirir y conectar a la plataforma tecnológica, por cualquier dependencia o proyecto de la Alcaldía, deberá ser gestionado por la Dirección de Tecnología, Innovación y Ciencia para su correcto funcionamiento.
e. La compra de una licencia de un programa permitirá a la Dirección de Tecnología, Innovación y Ciencia (TI y C) realizar una copia de seguridad (a no ser que esté estipulado de manera distinta), para ser utilizada en caso de que el medio se averíe.
f. Cualquier otra copia del programa original será considerada como una copia no autorizada y su utilización conlleva a las sanciones administrativas y legales pertinentes.
g. La Dirección de Tecnología, Innovación y Ciencia será la única dependencia autorizada para realizar copia de seguridad del software original.
h. La instalación del software en las máquinas de la Alcaldía, se realizará únicamente a través de la Dirección de Tecnología, Innovación y Ciencia (TI y C).
i. El software proporcionado por la Dirección de Tecnología, Innovación y Ciencia (TI y C), no puede ser copiado o suministrado a terceros.
j. En los equipos de la Alcaldía de Palmira se podrá utilizar el software licenciado por la Dirección de Tecnología, Innovación y Ciencia (TI y C) y el adquirido o licenciado por los proyectos o programas.
k. Para la adquisición y actualización de software, es necesario efectuar la solicitud a la Dirección de Tecnología, Innovación y Ciencia (TI y C) con su justificación, quien analizará las propuestas presentadas para su evaluación y aprobación.
l. El software que se adquiera a través de los proyectos o programas, debe quedar a nombre del Municipio de Palmira.
m. Se encuentra prohibido el uso e instalación de juegos en los computadores de la Alcaldía de Palmira.

n. Se presentarán para dar de baja el software de acuerdo con los lineamientos dados por la Entidad.

5.13.2 Controles Criptográficos

Objetivo

Definir las directrices para proteger la confidencialidad, integridad y disponibilidad de la información, mediante el uso y aplicación de técnicas en la Entidad.

Directrices:

a. La Dirección de Tecnología, Innovación y Ciencia (TI y C) debe verificar los sistemas o aplicaciones que realicen y/o permitan la transmisión de información pública reservada o información pública clasificada (privada o semiprivada), lo realicen mediante herramientas de cifrado de datos.
b. La Dirección de Tecnología, Innovación y Ciencia (TI y C).proveerá la herramienta de encripción de datos a los usuarios, previa solicitud formal. La asignación de la clave para el cifrado de la información en la herramienta, debe ser establecida por el usuario que administra dicha información, teniendo siempre presente que en caso de olvidar la clave, la información cifrada no es recuperable
c. Se utilizarán controles criptográficos en los siguientes casos:
d. En la protección de claves de acceso a sistemas, datos y servicios.
e. Para la transmisión de información Reservada o Clasificada, fuera de la Entidad.
f. En la protección de la información a resguardar, cuando así lo establezca el Comité de Seguridad de la Información, el generador de la información o el Administrador de Seguridad de la Información.

5.13.3 Gestión de vulnerabilidad técnica

Objetivo

Definir las directrices para proteger la confidencialidad, integridad y disponibilidad de la información, mediante el uso y aplicación de técnicas en la Entidad.

Directrices

a. La Dirección de Tecnología, Innovación y Ciencia (TI y C), Coordinará con un tercero especializado la aplicación de pruebas de vulnerabilidades técnicas sobre los recursos de la plataforma tecnológica por medio de la realización de pruebas de Ethical Hacking cada doce meses, debidamente programadas, con el objetivo de realizar la corrección sobre los hallazgos arrojados por dichas pruebas.

b. La Dirección de Tecnología, Innovación y Ciencia (TI y C), debe generar, ejecutar y monitorear planes de acción para la mitigación de las vulnerabilidades técnicas detectadas en la plataforma tecnológica con base al informe suministrado por el tercero.

5.14. Gestión disciplinaria de los incidentes de la seguridad de la información

Asegurar que los eventos e incidentes de seguridad que se presenten con los activos de información, sean comunicados y atendidos oportunamente, empleando los procedimientos definidos, con el fin de que se tomen oportunamente las acciones correctivas.

5.14.1 Proceso Disciplinario

a. Dentro de la estrategia de seguridad de la información Informática, está establecido un proceso disciplinario formal para los funcionarios que hayan cometido alguna violación de la Política de Seguridad de la Información. El proceso disciplinario también se debería utilizar como disuasión para evitar que los funcionarios, contratistas y otros
b. Colaboradores violen las políticas y los procedimientos de seguridad de la información, así como para cualquier otra violación de la seguridad. Las investigaciones disciplinarias corresponden a actividades pertenecientes al Proceso de Talento Humano.
c. Actuaciones que conllevan a la violación de la seguridad de la información establecida por la Dirección de Tecnología, Innovación y Ciencia (TI y C):
d. No firmar los acuerdos de confidencialidad o de entrega de información o de activos de información.
e. No reportar los incidentes de seguridad o las violaciones a las políticas de seguridad informática, cuando se tenga conocimiento de ello.
f. No actualizar la información de los activos de información a su cargo.
g. Clasificar y registrar de manera inadecuada la información, desconociendo los estándares establecidos para este fin.
h. No guardar de forma segura la información cuando se ausenta de su puesto de trabajo o al terminar la jornada laboral, de documentos impresos que contengan información pública reservada, información pública clasificada (privada o semiprivada).
i. No guardar la información digital, producto del procesamiento de la información perteneciente a la Alcaldía de Palmira.
j. Dejar información pública reservada, en carpetas compartidas o en lugares distintos al servidor de archivos, obviando las medidas de seguridad.
k. Dejar las gavetas abiertas o con las llaves puestas en los escritorios.
l. Dejar los computadores encendidos en horas no laborables.
m. Permitir que personas ajenas a la Alcaldía de Palmira, deambulan sin acompañamiento, al interior de las instalaciones, en áreas no destinadas al público.

n. Almacenar en los discos duros de los computadores personales de los usuarios, la información de la Alcaldía de Palmira.
o. Solicitar cambio de contraseña de otro usuario, sin la debida autorización del titular o su jefe inmediato.
p. Hacer uso de la red de datos de la entidad, para obtener, mantener o difundir en los equipos de sistemas, material pornográfico (exceptuando el penalizado por la ley) u ofensivo, cadenas de correos y correos masivos no autorizados.
q. Utilización de software no relacionados con la actividad laboral y que pueda degradar el desempeño de la plataforma tecnológica institucional.
r. Recepcionar o enviar información institucional a través de correos electrónicos personales, diferentes a los asignados por la institución.
s. Enviar información pública reservada o información pública clasificada (privada o semiprivada) por correo, copia impresa o electrónica sin la debida autorización y sin la utilización de los protocolos establecidos para la divulgación.
t. Utilizar equipos electrónicos o tecnológicos desatendidos o que a través de sistemas de interconexión inalámbrica, sirvan para transmitir, recepcionar y almacenar datos.
u. Usar dispositivos de almacenamiento externo en los computadores, cuya autorización no haya sido otorgada por la Dirección de Tecnología, Innovación y Ciencia (TI y C).
v. Permitir el acceso de funcionarios a la red corporativa, sin la autorización de la Dirección de Tecnología, Innovación y Ciencia (TI y C).
w. Utilización de servicios disponibles a través de internet, como FTP y Telnet, no permitidos por la Dirección de Tecnología, Innovación y Ciencia (TI y C).o de protocolos y servicios que no se requieran y que puedan generar riesgo para la seguridad.
x. Negligencia en el cuidado de los equipos, dispositivos portátiles o móviles entregados para actividades propias de la Alcaldía de Palmira.
y. No cumplir con las actividades designadas para la protección de los activos de información.
z. Destruir o desechar de forma incorrecta la documentación institucional.
aa. Descuidar documentación con información pública reservada o clasificada de la entidad, sin las medidas apropiadas de seguridad que garanticen su protección.
bb. Registrar información pública reservada o clasificada, en pos-it, apuntes, agendas, libretas, etc. Sin el debido cuidado.
cc. Almacenar información pública reservada o clasificada, en cualquier dispositivo de almacenamiento que no permanezca en la entidad o conectar computadores portátiles u otros sistemas eléctricos o electrónicos personales a la red de datos de la Alcaldía, sin la debida autorización.
dd. Archivar información pública reservada o clasificada, sin claves de seguridad o cifrado de datos.
ee. Promoción o mantenimiento de negocios personales, o utilización de los recursos tecnológicos institucionales para beneficio personal.
ff. El que sin autorización acceda en todo o parte del sistema o se mantenga dentro del mismo en contra de la voluntad de la Alcaldía de Palmira.
gg. El que impida u obstaculice el funcionamiento o el acceso normal al sistema y/o los datos informáticos o las redes de telecomunicaciones, sin estar autorizado.

hh. El que destruya, dañe, borre, deteriore o suprima datos informáticos o un sistema de tratamiento de información.
ii. El que distribuya, envíe, introduzca software malicioso u otros programas de computación de efectos dañinos en la plataforma tecnológica.
jj. El que viole datos personales de las bases de datos.
kk. El que superando las medidas de seguridad informática suplante un usuario ante los sistemas de autenticación y autorización establecidos por la Dirección de Tecnología, Innovación y Ciencia (TI y C).
ll. No mantener la confidencialidad de las contraseñas de acceso a la red de datos, los recursos tecnológicos, los sistemas de información o permitir que otras personas accedan con el usuario y clave del titular a éstos.
mm. Permitir el acceso u otorgar privilegios de acceso a las redes de datos a personas no Autorizadas.
nn. Llevar a cabo actividades fraudulentas o ilegales, o intentar acceso no autorizado a cualquier computador o de terceros.
oo. Ejecutar acciones tendientes a eludir o variar los controles establecidos por de la Dirección de Tecnología, Innovación y Ciencia (TI y C).
pp. Retirar de las instalaciones de la Alcaldía de Palmira, estaciones de trabajo o computadores portátiles que contengan Información institucional sin la autorización pertinente.
qq. Sustraer de las instalaciones de la Alcaldía de Palmira, documentos con información institucional calificada como Información pública reservada o clasificada, o abandonarlos en lugares públicos o de fácil acceso.
rr. Entregar, enseñar y divulgar información institucional, calificada como información pública reservada y Clasificada a personas o entidades no autorizadas.
ss. No realizar el borrado seguro de la información en equipos o dispositivos de almacenamiento, para traslado, reasignación o para disposición final.
tt. Ejecución de cualquier acción que pretenda difamar, abusar, afectar la reputación o presentar una mala Imagen de la Alcaldía de Palmira o de alguno de sus funcionarios.
uu. Realizar cambios no autorizados en la plataforma tecnológica de la Alcaldía de Palmira.
vv. Acceder, almacenar o distribuir pornografía infantil.
ww. Instalar programas o software no autorizados en las estaciones de trabajo o equipos portátiles Institucionales, cuyo uso no esté autorizado por la Dirección de Tecnología, Innovación y Ciencia (TI y C).
xx. Copiar sin autorización los programas o violar los derechos de autor o acuerdos de licenciamiento.

6 REQUISITOS LEGALES y/o REGLAMENTARIOS

- Constitución Política de Colombia 1991.
- Código Penal Colombiano - Decreto 599 de 2000
- Ley 906 de 2004, Código de Procedimiento Penal.
- Ley 87 de 1993, por la cual se dictan Normas para el ejercicio de control interno en las entidades y organismos del Estado, y demás normas que la modifiquen.
- Decreto 1599 de 2005, por el cual se adopta el Modelo Estándar de Control Interno MECI para el Estado Colombiano.
- Ley 734 de 2002, del Congreso de la República de Colombia, Código Disciplinario Único.

- Ley 23 de 1982 de Propiedad Intelectual - Derechos de Autor.
- Ley 594 de 2000 - Ley General de Archivos.
- Ley 80 de 1993, Ley 1150 de 2007 y decretos reglamentarios.
- Ley 527 de 1999, por la cual se define y reglamenta el acceso y uso de los mensajes de datos, del comercio electrónico y de las firmas digitales y se establecen las entidades de certificación y se dictan otras disposiciones.
- Directiva presidencial 02 del año 2000, Presidencia de la República de Colombia, Gobierno en línea.
- Ley 1032 de 2006, por el cual se dictan disposiciones generales del Habeas
- Data y se regula el manejo de la información contenida en base de datos personales.
- Ley 1266 de 2007, por la cual se dictan disposiciones generales del Habeas Data y se regula el manejo de la información contenida en base de datos personales.
- Ley 1273 de 2009, "Delitos Informáticos" protección de la información y los datos.
- Ley 1437 de 2011, "Código de procedimiento administrativo y de lo contencioso administrativo".
- Ley 1581 de 2012, "Protección de Datos personales".
- Decreto 2609 de 2012, por la cual se reglamenta la ley 594 de 200 y ley 1437 de 2011
- Decreto 1377 de 2013, por la cual se reglamenta la ley 1581 de 2012
- Ley 1712 de 2014, “De transparencia y del derecho de acceso a la información pública nacional”
- Norma Técnica Colombiana NTCI/ISO 27001 Sistemas de gestión de la seguridad de la información
- Norma Técnica Colombiana NTC/ISO 17799 Código de práctica para la gestión de la seguridad de la información.
- ISO/IEC 27005 Information technology Systems- Security techniques- information security risk management.
- **Modelo Integrado de Planeación y Gestión – MIPG** en su versión actualizada mediante el Decreto 1499 de 2017 emitido por el Departamento Administrativo de la Función Pública.".
- **Norma Técnica Colombiana NTC - ISO 19011** "Directrices para la Auditoría de los Sistemas de Gestión de la Calidad y/o Ambiental"
- Ley 1221 de 2008: Establece el reconocimiento del Teletrabajo en Colombia como modalidad laboral en sus formas de aplicación, las bases para la generación de una política pública de fomento al teletrabajo y una política pública de teletrabajo para la población vulnerable. Crea la Red Nacional de Fomento al Teletrabajo, con el fin de promover y difundir esta práctica en el país e incluye las garantías laborales, sindicales y de seguridad social para los Teletrabajadores.
- Decreto 884 de 2012: Especifica las condiciones laborales que rigen el teletrabajo en relación de dependencia, las relaciones entre empleadores y teletrabajadores, las obligaciones para entidades públicas y privadas, las ARLs y la Red de Fomento para el teletrabajo. Así mismo establece los principios de voluntariedad, igualdad y reversibilidad que aplican para el modelo.
- Resolución 2886 de 2012: define las entidades que hacen parte de la Red de Fomento del Teletrabajo y las obligaciones que les compete.

7 DOCUMENTOS RELACIONADOS

- Procedimientos:

- AIFMN-005 Manual de Políticas de Seguridad de la Información del Municipio de Palmira
- AIFPR-012 Concepto técnico para viabilidad del sistema de información
- AIFPR-003 Gestión usuario de dominio y correo electrónico institucional
- AIFPR-004 Adquisición de soluciones tic
- AIFPR-005 Administración data center y seguridad informática
- AIFPR-007 Servicios tecnológicos dirigidos a la comunidad
- Realización de mejoras y mantenimiento del sistema de información

8. ANEXOS

Anexo 01 ACUERDO DE CONFIDENCIALIDAD

9. CONTROL DE CAMBIOS

Fecha	Versión Inicial	Identificación del Cambio	Versión Final
01/02/2019	01	Actualización y Estructuración ISO 27001	02
23/02/2021	02	Actualización	03
26/12/2022	03	Actualización	04

10. CONTROL DE REVISIÓN Y APROBACIÓN

Elaborado por:	Revisado por:	Aprobado por:
Nombre: Darwin Vélez López Oscar Guio Ríos	Nombre: Diana Sánchez Sepúlveda	Nombre: Juan David Escobar García
Cargo: Profesional Especializado	Cargo: Profesional Especializado	Cargo: Director de TIyC