Tabla de Contenido

INTRODUCCIÓN

La información es un activo estratégico para la Alcaldía Municipal de Palmira, esencial para el cumplimiento de su misión de servicio público y el desarrollo de la comunidad. La protección de este activo, asegurando su confidencialidad, integridad y disponibilidad, es fundamental para garantizar la continuidad de las operaciones, mantener la confianza de los ciudadanos y cumplir con los mandatos legales.

Consciente de la importancia de la seguridad y privacidad de la información, la Alcaldía Municipal de Palmira, a través de la Dirección de Tecnología, Innovación y Ciencia, ha asumido el compromiso de establecer un marco sólido y completo para la gestión de la seguridad de la información. Este compromiso se cristaliza en el presente Manual de Políticas de Seguridad y Privacidad de la Información, que establece las reglas, directrices y procedimientos necesarios para proteger la información en todas sus formas, tanto en entornos físicos como digitales.

Este manual se ha desarrollado en alineación con las mejores prácticas internacionales, como la norma ISO 27001:2022, que proporciona un marco de referencia para la implementación de un Sistema de Gestión de Seguridad de la Información (SGSI). Además, se han tenido en cuenta las regulaciones nacionales relevantes, como la Política de Gobierno Digital y el Modelo de Seguridad y Privacidad de la Información (MSPI), garantizando así el cumplimiento de los requisitos legales y normativos aplicables.

La Dirección de Tecnología Innovación y Ciencia TIyC se compromete a mantener este manual actualizado y a revisarlo periódicamente para asegurar su adecuación a las necesidades cambiantes de la organización y al entorno tecnológico en constante evolución.

1. OBJETIVO GENERAL:

Establecer las políticas de seguridad de la información que deben ser conocidas y cumplidas por todos los miembros de la comunidad de la Alcaldía Municipal de Palmira, incluyendo directivos, funcionarios, contratistas y terceros.

2. ALCANCE:

El presente manual es de aplicación a todas las personas: servidores públicos, funcionarios, contratistas, proveedores y cualquier otra persona que tenga acceso a la información (tanto física como digital) de la Alcaldía Municipal de Palmira. El cumplimiento de estas políticas es responsabilidad

de todos los miembros de la entidad, y su aplicación efectiva es fundamental para garantizar la protección de la información y la continuidad de las operaciones.

3. RESPONSABILIDADES:

Las Políticas de Seguridad y Privacidad de la Información son de aplicación obligatoria para todo el personal de la Alcaldía Municipal de Palmira, cualquiera sea su situación contractual, la dependencia a la cual se encuentre adscrito y el nivel de las tareas que desempeñe.

- **Alta Gerencia:** Liderar la implementación y seguimiento de esta política, establecer controles de seguridad y privacidad, y promover la concienciación sobre estos temas.
- **Líderes de Proceso:** Identificar y evaluar los riesgos de seguridad y privacidad en sus áreas, implementar controles y reportar incidentes.
- **Todos los empleados:** Cumplir con esta política, proteger la información, reportar incidentes y participar en capacitaciones.
- **Comité de Gestión y Desempeño Institucional:** Revisa y aprueba la Política de Seguridad y Privacidad de la Información, define estrategias de capacitación y supervisa la implementación del SGSI.
- **Propietarios de Activos de Información:** Clasifican, protegen y gestionan el acceso a la información bajo su responsabilidad.
- **Encargado de Talento Humano:** Comunica la política a todo el personal y gestiona la firma de los compromisos de confidencialidad.
- **Encargado de la Dirección de Tecnología Innovación y Ciencia:** Actualiza, implementa y mantiene los controles de seguridad informática, siguiendo los lineamientos de la presente política.
- **Oficina de Control Interno:** Realiza auditorías periódicas para verificar el cumplimiento de las políticas y las medidas de seguridad.

4. DEFINICIONES:

DEFINICIONES

A continuación, se presentan las definiciones de los términos clave utilizados en el presente Manual de Políticas de Seguridad de la Información, ordenados alfabéticamente para facilitar su consulta:

- **Acceso:** Capacidad de interactuar con un activo de información, utilizarlo o consumirlo. Puede ser físico (a instalaciones) o lógico (a sistemas y datos).
- **Activo de Información:** Cualquier elemento que tiene valor para la Alcaldía Municipal de Palmira, incluyendo información, software, hardware, servicios y personas.

- **Administrador de Información:** Usuario responsable de la gestión, control y protección de un activo de información específico.
- **Alta Gerencia:** Nivel directivo superior de la Alcaldía Municipal de Palmira, responsable de liderar y aprobar las políticas de seguridad de la información.
- **Amenaza:** Causa potencial de un incidente no deseado que puede resultar en daño a los sistemas o a la información.
- **Ancho de Banda:** Cantidad de datos que se pueden transmitir a través de una conexión de red en un período de tiempo determinado.
- **Aplicación:** Programa informático diseñado para realizar una tarea específica.
- **Archivo:** Conjunto organizado de información, que puede ser digital o físico.
- **Activo de Terceros:** Bienes o recursos de propiedad de entidades externas (proveedores, contratistas, visitantes) que ingresan a las instalaciones de la Alcaldía.
- **Auditoría:** Proceso sistemático, independiente y documentado para obtener evidencias y evaluarlas de manera objetiva con el fin de determinar el grado en que se cumplen los criterios establecidos.
- **Autenticación:** Proceso de verificar la identidad de un usuario, dispositivo o proceso.
- **Autorización:** Proceso de conceder a un usuario, dispositivo o proceso el derecho de acceder a recursos específicos.
- **Aviso de Privacidad:** Documento informativo mediante el cual la Alcaldía informa a los titulares de datos personales sobre el tratamiento que se dará a su información.
- **Backup (Respaldo):** Copia de seguridad de la información que se realiza para poder recuperarla en caso de pérdida o daño.
- **Bitácora:** Registro cronológico de eventos relevantes, como accesos a sistemas o incidentes de seguridad.
- **Bloqueo de Pantalla:** Mecanismo de seguridad que impide el acceso a un dispositivo sin la autenticación del usuario.
- **Cifrado:** Proceso de convertir información legible (texto plano) en un formato ilegible (texto cifrado) para proteger su confidencialidad.
- **Clasificación de la Información:** Proceso de asignar un nivel de sensibilidad a la información según su valor y la necesidad de protección.
- **Claves de Acceso:** Combinación única de caracteres (contraseñas, PINs, etc.) utilizada para autenticar y autorizar el acceso a sistemas y recursos.
- **Código Malicioso (Malware):** Software diseñado para infiltrarse en un sistema informático y dañarlo, alterarlo o robar información.
- **Comunicaciones Unificadas:** Integración de diferentes métodos de comunicación (voz, video, mensajería instantánea, correo electrónico) en una única plataforma.

- **Compromiso de Confidencialidad (Acuerdo de No Divulgación - NDA):** Acuerdo legal mediante el cual las partes se obligan a no revelar información confidencial.
- **Concienciación:** Actividades destinadas a informar y sensibilizar al personal sobre los riesgos de seguridad de la información y sus responsabilidades.
- **Confidencialidad:** Propiedad de la información de no ser puesta a disposición ni revelada a individuos, entidades o procesos no autorizados.
- **Contingencia:** Planificación para responder y recuperarse de eventos inesperados que puedan interrumpir las operaciones.
- **Contratista:** Persona o empresa externa que presta servicios a la Alcaldía bajo un contrato.
- **Control de Acceso:** Mecanismos y procedimientos implementados para garantizar que solo los usuarios autorizados puedan acceder a los activos de información.
- **Controles Criptográficos:** Uso de técnicas de cifrado para proteger la confidencialidad, integridad y autenticidad de la información.
- **Controles de Seguridad:** Medidas técnicas, administrativas y físicas implementadas para mitigar los riesgos de seguridad de la información.
- **Copia de Seguridad:** Duplicación de la información para su recuperación en caso de pérdida o daño.
- **Credenciales de Acceso:** Información utilizada para verificar la identidad de un usuario (por ejemplo, nombre de usuario y contraseña).
- **Data Center:** Instalación que alberga los equipos informáticos críticos de la Alcaldía, como servidores y sistemas de almacenamiento.
- **Debida Diligencia:** Investigación y evaluación exhaustiva de un tercero (proveedor, contratista) antes de establecer una relación comercial.
- **Detección de Intrusos (IDS):** Sistema que monitorea el tráfico de red en busca de actividades sospechosas o maliciosas.
- **Dirección de Tecnología, Innovación y Ciencia (DTIyC):** Área de la Alcaldía responsable de la gestión de la infraestructura tecnológica y la seguridad de la información.
- **Disponibilidad:** Propiedad de estar accesible y utilizable a petición de una entidad autorizada.
- **Dispositivos Móviles:** Equipos portátiles como teléfonos inteligentes y tabletas utilizados para acceder a información y servicios de la Alcaldía.
- **Disco de Red:** Espacio de almacenamiento compartido en la red de la Alcaldía.
- **Documento:** Información registrada en cualquier medio (papel, digital, etc.).
- **Doble Factor de Autenticación (2FA):** Proceso de autenticación que requiere dos o más métodos de verificación para acceder a un sistema o recurso.
- **Drive Institucional:** Servicio de almacenamiento en la nube proporcionado por Google Workspace para la Alcaldía.

- **Eliminación Segura de Información:** Proceso de borrar o destruir información de manera que sea irrecuperable.
- **Empleado:** Persona que trabaja para la Alcaldía bajo una relación laboral.
- **Encriptación:** Ver **Cifrado**.
- **Estación Cliente:** Equipo de cómputo utilizado por los usuarios finales (computador de escritorio o portátil).
- **Firewall:** Dispositivo de seguridad de red que controla el tráfico entrante y saliente, bloqueando accesos no autorizados.
- **Gestión de Activos de Información:** Proceso de identificación, valoración, control y protección de los activos de información de la Alcaldía.
- **Gestión de Incidentes:** Proceso para identificar, analizar, responder y recuperarse de eventos que comprometen la seguridad de la información.
- **Gestión de Riesgos:** Proceso sistemático para identificar, evaluar y tratar los riesgos de seguridad de la información.
- **Gestión de Vulnerabilidades:** Proceso de identificación, evaluación y mitigación de debilidades en los sistemas y aplicaciones.
- **Hardware:** Componentes físicos de un sistema informático.
- **Herramientas Tecnológicas:** Software, hardware y otros recursos tecnológicos utilizados para gestionar la seguridad de la información.
- **Incidente de Seguridad:** Evento que compromete la confidencialidad, integridad o disponibilidad de la información o los sistemas.
- **Índice de Transparencia y Acceso a la Información Pública:** Indicador utilizado para medir el cumplimiento de las entidades públicas en materia de transparencia y acceso a la información.
- **Infraestructura:** Conjunto de componentes físicos y lógicos necesarios para el funcionamiento de los sistemas de información.
- **Información:** Conjunto de datos organizados y procesados que tienen significado o relevancia.
- **Información Confidencial:** Información cuyo acceso no autorizado podría tener consecuencias adversas para la Alcaldía o terceros.
- **Información Institucional:** Información generada, gestionada o custodiada por la Alcaldía en el ejercicio de sus funciones.
- **Información Personal:** Cualquier información vinculada o que pueda asociarse a una o varias personas naturales determinadas o determinables.
- **Información Pública:** Información que puede ser divulgada libremente sin restricciones.

- **Información Pública Clasificada:** Información pública que requiere un tratamiento especial debido a su sensibilidad.
- **Información Pública Reservada:** Información pública cuyo acceso está restringido por disposición legal o razones de interés público.
- **Integridad:** Propiedad de proteger la exactitud y completitud de la información y los métodos de procesamiento.
- **Inteligencia Artificial (IA):** Campo de la informática que busca crear sistemas capaces de realizar tareas que normalmente requieren inteligencia humana.
- **Inventario de Activos de Información:** Registro detallado de los activos de información de la Alcaldía.
- **ISO 27001:** Norma internacional para la gestión de la seguridad de la información.
- **LAN (Red de Área Local):** Red informática que conecta los equipos dentro de un área geográfica limitada (por ejemplo, un edificio).
- **Lecciones Aprendidas:** Conocimiento adquirido a partir del análisis de incidentes o eventos, utilizado para mejorar los procesos.
- **Ley 1273 de 2009 (Ley de Delitos Informáticos):** Ley colombiana que tipifica los delitos relacionados con la informática y la protección de la información.
- **Ley 1581 de 2012 (Ley de Protección de Datos Personales):** Ley colombiana que establece el régimen general de protección de datos personales.
- **Ley 1712 de 2014 (Ley de Transparencia y del Derecho de Acceso a la Información Pública Nacional):** Ley colombiana que regula el derecho de acceso a la información pública.
- **Líderes de Proceso:** Funcionarios responsables de la gestión y ejecución de los procesos dentro de la Alcaldía.
- **Mantenimiento:** Actividades realizadas para asegurar el correcto funcionamiento y la actualización de los sistemas y equipos.
- **Marco Legal y Regulatorio:** Conjunto de leyes, decretos, resoluciones y otras normas aplicables a la seguridad de la información y la protección de datos.
- **Medidas Correctivas:** Acciones tomadas para eliminar la causa de una no conformidad y prevenir su recurrencia.
- **Medidas de Seguridad:** Ver **Controles de Seguridad**.
- **Mesa de Ayuda:** Servicio de soporte técnico para atender consultas e incidentes relacionados con la tecnología y la seguridad de la información.
- **MinTIC (Ministerio de Tecnologías de la Información y las Comunicaciones de Colombia):** Entidad gubernamental colombiana encargada de formular, dirigir y coordinar las políticas en materia de tecnologías de la información y las comunicaciones.

- **Modelo de Seguridad y Privacidad de la Información (MSPI):** Marco de referencia para la gestión de la seguridad y privacidad de la información en entidades públicas colombianas.
- **Monitoreo:** Supervisión continua de los sistemas, redes y actividades para detectar posibles incidentes o anomalías.
- **Normas y Estándares:** Directrices y especificaciones técnicas reconocidas a nivel nacional o internacional en materia de seguridad de la información.
- **No Repudio:** Capacidad de asegurar que una transacción o acción no pueda ser negada por la entidad que la realizó.
- **Parcheo:** Proceso de aplicar actualizaciones de software para corregir vulnerabilidades o errores.
- **Política de Gobierno Digital:** Conjunto de lineamientos y estrategias para el uso y aprovechamiento de las TIC en el sector público.
- **Política de Seguridad de la Información:** Conjunto de directrices de alto nivel que definen los objetivos y principios de la seguridad de la información en la Alcaldía.
- **Privacidad:** Derecho de los individuos a controlar la recopilación y el uso de su información personal.
- **Propietario de la Información:** Persona o área responsable de un activo de información específico.
- **Protección de Datos:** Conjunto de medidas destinadas a garantizar la privacidad y seguridad de los datos personales.
- **Proveedor:** Empresa o persona que suministra bienes o servicios a la Alcaldía.
- **Pruebas de Penetración (Ethical Hacking):** Simulación de ataques cibernéticos para identificar vulnerabilidades en los sistemas.
- **Recuperación ante Desastres (DRP):** Plan para restaurar los sistemas y la información crítica después de un incidente o desastre.
- **Red de Invitados:** Red Wi-Fi con acceso limitado para visitantes y personal externo.
- **Red Wi-Fi:** Red inalámbrica que permite la conexión de dispositivos a internet.
- **Recursos Informáticos:** Hardware, software, redes y otros elementos tecnológicos utilizados por la Alcaldía.
- **Registro de Acceso:** Archivo que documenta quién accedió a qué recurso, cuándo y qué acciones realizó.
- **Reporte de Incidentes:** Comunicación formal de un evento que compromete o podría comprometer la seguridad de la información.
- **Responsabilidad:** Obligación de rendir cuentas por las acciones realizadas y por la protección de los activos de información.
- **Restauración:** Proceso de recuperar la información de una copia de seguridad.

- **Retención de Documentos:** Período de tiempo durante el cual los documentos deben ser conservados, de acuerdo con la normativa archivística.
- **Riesgo:** Medida de la probabilidad de que una amenaza explote una vulnerabilidad y cause daño.
- **Roles y Responsabilidades:** Definición clara de las funciones y obligaciones de cada persona en relación con la seguridad de la información.
- **Sanciones:** Medidas disciplinarias o legales aplicadas por el incumplimiento de las políticas de seguridad.
- **Seguridad de Redes:** Medidas implementadas para proteger la infraestructura de red y la información que se transmite a través de ella.
- **Seguridad Física:** Medidas para proteger las instalaciones y los activos de información contra amenazas físicas.
- **Seguridad Informática:** Conjunto de medidas técnicas y organizativas destinadas a proteger los sistemas y la información digital.
- **Servidor:** Equipo informático centralizado que proporciona servicios a otros equipos en una red.
- **SGSI (Sistema de Gestión de Seguridad de la Información):** Marco de políticas y procedimientos para gestionar los riesgos de seguridad de la información.
- **Software:** Conjunto de programas informáticos que permiten el funcionamiento de un sistema.
- **Software Antivirus:** Programa diseñado para detectar, prevenir y eliminar software malicioso.
- **Software Autorizado:** Software cuya instalación y uso ha sido aprobado por la Dirección de Tecnología, Innovación y Ciencia (DTIyC).
- **Software con Licencia:** Software cuyo uso está permitido bajo los términos de una licencia legal.
- **Soporte Técnico:** Asistencia proporcionada para resolver problemas relacionados con la tecnología y la seguridad de la información.
- **Tabla de Retención Documental (TRD):** Instrumento archivístico que establece los criterios de conservación y disposición final de los documentos.
- **Talento Humano:** Área de la Alcaldía responsable de la gestión del personal.
- **Teletrabajo:** Modalidad de trabajo a distancia que permite a los empleados realizar sus funciones fuera de las instalaciones de la Alcaldía.
- **Tercerización (Outsourcing):** Contratación de servicios externos para realizar actividades que no son core del negocio de la Alcaldía.
- **Titular de los Datos Personales:** Persona natural cuyos datos personales son objeto de tratamiento.

- **Token de 2FA:** Dispositivo físico o virtual que genera códigos de un solo uso para la autenticación de doble factor.
- **Trazabilidad:** Capacidad de rastrear el origen, las modificaciones y el destino de la información o las acciones realizadas en un sistema.
- **Tratamiento de Datos Personales:** Cualquier operación o conjunto de operaciones realizadas sobre datos personales.
- **Transparencia:** Principio de informar de manera clara y accesible sobre las prácticas de seguridad y privacidad de la información.
- **UPS (Sistema de Alimentación Ininterrumpida):** Dispositivo que proporciona energía eléctrica de respaldo en caso de fallo del suministro principal.
- **Uso Aceptable:** Políticas que definen cómo se deben utilizar los recursos informáticos de la Alcaldía.
- **Usuario:** Persona autorizada para acceder a los sistemas y recursos de información de la Alcaldía.
- **VPN (Red Privada Virtual):** Conexión segura y cifrada a través de una red pública como internet, que permite acceder a recursos de red remota.
- **Vulnerabilidad:** Debilidad en un activo que puede ser explotada por una amenaza.
- **Web Master:** Persona responsable de la administración y mantenimiento de las páginas web de la Alcaldía.
- **Wi-Fi:** Tecnología inalámbrica que permite la conexión de dispositivos a una red local o a internet.
- **Trabajo en Casa:** Modalidad de trabajo a distancia similar al teletrabajo.

5. POLÍTICAS

5.1 POLÍTICA DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN DE LA ALCALDÍA DE PALMIRA

1. Objetivo

Adoptar la Política de Seguridad y Privacidad de la Información, la cual se encuentra articulada con el Sistema Integrado de Gestión Institucional de la Alcaldía de Palmira.

Política de Seguridad y Privacidad de la Información. La Alcaldía de Palmira se compromete a proteger la confidencialidad, integridad y disponibilidad de la información que gestiona, reconociendo que los

riesgos pueden afectar el cumplimiento de su misión y el desarrollo social. Para ello, implementará un sistema de gestión de seguridad y privacidad de la información basado en la identificación, evaluación y control continuo de los riesgos, asegurando la mejora continua en la protección de los datos y la privacidad de los ciudadanos y partes interesadas.

Este compromiso se alinea con los objetivos institucionales y busca generar confianza en la gestión de la información, promoviendo la transparencia y el uso responsable de los datos en beneficio de la comunidad.

2. Principios Rectores

- **Confidencialidad:** Garantizar que la información solo sea accesible para personas autorizadas.
- **Integridad:** Proteger la exactitud y completitud de la información y los métodos de procesamiento.
- **Disponibilidad:** Asegurar que la información esté disponible y accesible cuando sea necesario.
- **Privacidad:** Proteger la información personal de acuerdo con la legislación vigente.
- **Responsabilidad:** Establecer roles y responsabilidades claras en la gestión de la seguridad y privacidad de la información.
- **Transparencia:** Informar de manera clara y accesible sobre las prácticas de seguridad y privacidad de la información.

3. Alcance

Esta política aplica a:

- **Todas las personas:** Funcionarios, contratistas, proveedores y cualquier persona que interactúe con la información de la Alcaldía.
- **Toda la información:** Independientemente de su formato (digital, físico, verbal) y ubicación (en sistemas, dispositivos, documentos, etc.).
- **Todos los procesos:** Relacionados con la recolección, almacenamiento, procesamiento, transmisión y eliminación de información.
- **Toda la infraestructura:** Sistemas, redes, aplicaciones, dispositivos y cualquier tecnología utilizada para gestionar la información.
- **Todas las sedes físicas:** Oficinas, instalaciones y cualquier lugar donde se almacene o procese información.

4. Responsabilidades:

- **Alta Gerencia:** Liderar la implementación y seguimiento de esta política, establecer controles de seguridad y privacidad, y promover la concienciación sobre estos temas.
- **Líderes de Proceso:** Identificar y evaluar los riesgos de seguridad y privacidad en sus áreas, implementar controles y reportar incidentes.
- **Todos los empleados:** Cumplir con esta política, proteger la información, reportar incidentes y participar en capacitaciones.

5. Gestión de Riesgos: La Alcaldía implementará un proceso continuo de gestión de riesgos que incluya:

- **Identificación de activos:** Determinar la información crítica y los sistemas que la procesan.
- **Evaluación de riesgos:** Analizar las amenazas, vulnerabilidades y posibles impactos.
- **Tratamiento de riesgos:** Implementar controles para mitigar los riesgos identificados (prevención, detección, respuesta y recuperación).
- **Monitoreo y revisión:** Evaluar periódicamente la efectividad de los controles y actualizar el plan de gestión de riesgos.

6. Controles de Seguridad y Privacidad: La Alcaldía implementará controles técnicos, administrativos y físicos para proteger la información, incluyendo:

- **Controles de acceso:** Autenticación, autorización y gestión de identidades.
- **Protección de datos:** Cifrado, copias de seguridad, recuperación ante desastres.
- **Seguridad de redes:** Firewalls, detección de intrusos, protección contra malware.
- **Gestión de vulnerabilidades:** Escaneo, parcheo, actualizaciones de software.
- **Concienciación y capacitación:** Programas de formación sobre seguridad y privacidad.

7. Gestión de Incidentes: La Alcaldía establecerá un proceso para gestionar los incidentes de seguridad y privacidad, que incluya:

- **Detección y reporte:** Mecanismos para identificar y reportar incidentes.
- **Análisis y contención:** Investigación de incidentes y acciones para limitar el daño.
- **Recuperación:** Restauración de sistemas y datos afectados.
- **Lecciones aprendidas:** Análisis de incidentes para prevenir futuros eventos.

8. Cumplimiento Legal: La Alcaldía se asegurará de cumplir con todas las leyes y regulaciones aplicables en materia de protección de datos y seguridad de la información.

9. Revisión y Actualización: Esta política será revisada y actualizada al menos una vez al año, o con mayor frecuencia si es necesario debido a cambios en la legislación, la tecnología o las prácticas de la industria.

10. Instrumentos para operar. La Alcaldía de Palmira implementará y mantendrá un Sistema de Gestión de Seguridad de la Información (SGSI) para garantizar la aplicación efectiva de esta política. El SGSI se basará en los siguientes instrumentos:

- **Documentos del proceso Gestión de Informática:** Estos documentos, incluidos en el Listado Maestro de Documentos del Sistema Integrado de Gestión Institucional, establecerán los lineamientos, procedimientos y controles específicos para la protección de la información.
- **Normas y estándares:** La Alcaldía adoptará normas y estándares nacionales e internacionales reconocidos en materia de seguridad de la información, como la ISO 27001, para asegurar la alineación con las mejores prácticas.
- **Herramientas tecnológicas:** Se implementarán soluciones tecnológicas adecuadas para la gestión de riesgos, control de acceso, protección de datos, detección de incidentes y otras medidas de seguridad necesarias.
- **Capacitación y concienciación:** Se desarrollarán programas de capacitación y sensibilización para que todo el personal conozca y comprenda sus responsabilidades en la protección de la información y la privacidad.
- **Auditorías y revisiones:** Se realizarán auditorías internas y externas periódicas para evaluar la eficacia del SGSI y asegurar el cumplimiento de esta política y la normativa aplicable.

La Dirección de Tecnología, Innovación y Ciencia será responsable de liderar la implementación y mantenimiento del SGSI, así como de actualizar los instrumentos operativos en función de los cambios en la tecnología, la legislación y las necesidades de la organización.

11. Tratamiento de Riesgos de Seguridad Digital o de la Información: La Alcaldía de Palmira reconoce que la gestión proactiva de los riesgos de seguridad digital es fundamental para proteger la información y garantizar la continuidad de sus operaciones. Por lo tanto, se establece el siguiente proceso:

- **Identificación de riesgos:** Los líderes de cada proceso, en colaboración con la Dirección de Tecnología, Innovación y Ciencia, realizarán un análisis exhaustivo para identificar los riesgos de seguridad digital que puedan afectar sus áreas. Esto incluye amenazas internas y externas, vulnerabilidades en sistemas y procesos, y posibles impactos en la confidencialidad, integridad y disponibilidad de la información.
- **Clasificación de riesgos:** Los riesgos identificados se clasificarán según su probabilidad de ocurrencia y su impacto potencial en las operaciones y la seguridad de la información. Se utilizará una metodología de evaluación de riesgos alineada con la Política de Administración de Riesgos de la entidad.

Tratamiento de riesgos: Una vez clasificados, se implementarán medidas de control para mitigar los riesgos identificados. Estas medidas pueden incluir:

- **Prevención:** Acciones para evitar que los riesgos se materialicen, como la implementación de políticas de seguridad, capacitación del personal y el uso de tecnologías de protección.
- **Detección:** Mecanismos para identificar rápidamente los incidentes de seguridad, como sistemas de detección de intrusos, monitoreo de logs y análisis de vulnerabilidades.
- **Respuesta:** Procedimientos para responder a los incidentes de seguridad de manera efectiva, incluyendo la contención, erradicación y recuperación de los sistemas y datos afectados.
- **Recuperación:** Planes para restaurar las operaciones y la información a su estado normal después de un incidente de seguridad.
- **Monitoreo y revisión:** El proceso de gestión de riesgos será continuo y se revisará periódicamente para asegurar su eficacia. Los líderes de proceso y la Dirección de Tecnología, Innovación y Ciencia evaluarán la efectividad de las medidas de control implementadas y realizarán los ajustes necesarios para mantener un nivel adecuado de seguridad.
- **Parágrafo:** La documentación de las evidencias de los controles implementados para la mitigación de riesgos se realizará de acuerdo con lo establecido en la Guía para la Administración del Riesgo de la entidad, documentada en el Sistema Integrado de Gestión Institucional.

12. Comunicación y Transparencia: La Alcaldía comunicará esta política a todas las partes interesadas y publicará un aviso de privacidad que explique cómo se recopila, utiliza y protege la información personal.

13. Sanciones: El incumplimiento de esta política puede resultar en sanciones disciplinarias de acuerdo con las normas internas de la Alcaldía y la legislación aplicable.

La Política de Seguridad de la Información se basa en los siguientes principios rectores fundamentales:

- **Confidencialidad:** La información solo será accesible para aquellos autorizados.
- **Integridad:** La información se mantendrá completa, precisa y protegida contra modificaciones no autorizadas.
- **Disponibilidad:** La información estará accesible y utilizable cuando sea necesario.
- **Privacidad:** La información personal será protegida de acuerdo con la legislación vigente.
- **Autenticidad:** La información será generada y custodiada por usuarios autorizados y su contenido será verificable.
- **Responsabilidad:** Se establecerán roles y responsabilidades claras en la gestión de la seguridad y privacidad de la información.
- **Transparencia:** Se informará de manera clara y accesible sobre las prácticas de seguridad y privacidad de la información.
- **No repudio:** Se garantizará que las acciones realizadas sobre la información no puedan ser negadas por quienes las realizaron.

5.2 POLÍTICA DE ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN PARA LA ALCALDÍA MUNICIPAL DE PALMIRA

Objetivo: Establecer una estructura organizativa clara y eficiente para la gestión de la seguridad y privacidad de la información en la Alcaldía Municipal de Palmira, incluyendo la gestión de riesgos asociados al uso de Inteligencia Artificial (IA), alineada con los lineamientos del Ministerio de Tecnologías de la Información y las Comunicaciones (MinTIC).

Directrices:

a. Coordinación de la Seguridad de la Información:

El Alcalde Municipal es el máximo responsable de la seguridad y privacidad de la información en la entidad.

La Dirección de Tecnología, Innovación y Ciencia (TIyC):

- Es responsable de la implementación y operación del SGSI, en coordinación con los líderes de proceso.

- Deberá coordinar la implementación de las políticas y procedimientos de seguridad y privacidad de la información.
- Deberá gestionar los riesgos de seguridad y privacidad, incluyendo los relacionados con IA.
- Deberá supervisar la respuesta a incidentes de seguridad y privacidad.
- Deberá promover la cultura de seguridad y privacidad en la entidad.

b. Asignación de Responsabilidades:

- Se definirán y documentarán las responsabilidades de cada rol en relación con la seguridad y privacidad de la información, incluyendo las responsabilidades específicas relacionadas con el uso de IA.
- Se establecerán mecanismos de comunicación y coordinación entre los diferentes roles para garantizar una gestión efectiva de la seguridad y privacidad de la información.

c. Propietarios de la Información:

- Cada activo de información tendrá un propietario claramente identificado, responsable de su clasificación, protección y gestión de riesgos, incluyendo los riesgos asociados a la IA.

d. Autorización para Nuevos Servicios de Procesamiento de la Información:

- Se establecerá un proceso formal para la evaluación y autorización de nuevos servicios de procesamiento de la información, incluyendo aquellos que utilizan IA, para garantizar que cumplan con los requisitos de seguridad y privacidad establecidos.

e. Compromiso de Confidencialidad:

- Se implementará compromiso de confidencialidad (Acuerdos de No Divulgación - NDA) para todos los empleados, contratistas y terceros que tengan acceso a información sensible o confidencial, incluyendo datos utilizados en sistemas de IA. (Formato AIFF0-015 del proceso: Gestión de Informática).

f. Revisión Independiente de la Seguridad de la Información:

- Se realizarán auditorías internas y/o externas de seguridad y privacidad de la información de forma periódica, incluyendo la evaluación de los controles de seguridad de los sistemas de IA.

g. Gestión de Riesgos de IA:

- Se implementará un proceso específico para la gestión de riesgos asociados a la IA, incluyendo la identificación, evaluación y tratamiento de riesgos como el sesgo algorítmico, la discriminación, la falta de transparencia y la seguridad de los modelos.

- Se establecerán mecanismos de seguimiento y control para garantizar que los sistemas de IA se utilicen de manera ética y responsable.

h. Capacitación y Concientización en Seguridad y Privacidad de la Información, incluyendo IA:

- Se implementará un programa continuo de capacitación y concientización para todos los empleados, contratistas y terceros sobre los riesgos de seguridad y privacidad de la información, incluyendo los riesgos específicos de la IA, y las medidas de protección necesarias.

I. Marco Legal y Regulatorio:

- Se asegurará el cumplimiento de todas las leyes y regulaciones aplicables en materia de seguridad y privacidad de la información, incluyendo la Ley 1581 de 2012 (Habeas Data), el Decreto 1377 de 2013 y los lineamientos del Min TIC.
- Se mantendrá un monitoreo constante de los cambios en la legislación y las regulaciones para garantizar la actualización y adecuación de la presente política.

5.3 POLÍTICA DE USO DEL DRIVE INSTITUCIONAL EN GOOGLE WORKSPACE PARA LA ALCALDÍA MUNICIPAL DE PALMIRA

Objetivo: La presente política tiene como objetivo establecer los lineamientos y directrices para el uso adecuado del Drive institucional en Google Workspace, garantizando la gestión eficiente, segura y transparente de la información de la Alcaldía Municipal de Palmira, en cumplimiento de la normativa vigente y las mejores prácticas internacionales.

5.3.1 Lineamientos Generales

a) Clasificación de la Información: Toda la información almacenada en el Drive institucional debe ser clasificada de acuerdo con su nivel de confidencialidad, siguiendo las directrices establecidas en el Modelo de Seguridad y Privacidad de la Información (MSPI) y la Ley 594 de 2000.

b) Estructura Documental: La información se organizará en una estructura jerárquica y coherente, facilitando su consulta y recuperación. Se establecerán carpetas y subcarpetas por áreas, procesos y tipos documentales, utilizando nomenclaturas claras y descriptivas.

c) Versionamiento y Formatos: Los documentos se almacenarán en dos versiones: editable (formato original) y definitiva (PDF/A). Se mantendrá un control de versiones para garantizar la trazabilidad de los cambios.

d) Vigencia: Se establecerán períodos de retención y disposición final de los documentos, de acuerdo con las Tablas de Retención Documental (TRD) y la Ley 594 de 2000.

e) Seguridad: Se aplicarán medidas de seguridad para proteger la información contra accesos no autorizados, pérdida, alteración o divulgación indebida. Se utilizarán contraseñas robustas, autenticación de dos factores y se restringirá el acceso a la información según los roles y responsabilidades de cada usuario.

f) Privacidad: Se protegerá la información personal de acuerdo con la Ley 1581 de 2012 y el Decreto 1377 de 2013. Solo se recopilará y utilizará la información personal estrictamente necesaria para los fines legítimos de la entidad, Privacidad de la Información (MSPI) y la Ley 594 de 2000.

5.3.2 Responsabilidades

- **Dirección de Tecnología, Innovación y Ciencia:** Responsable de la creación, administración de credenciales de acceso al Drive institucional, así como de la implementación y seguimiento de esta política.
- **Jefes de Área:** Responsables de garantizar que la información de su área se gestione adecuadamente en el Drive institucional, siguiendo los lineamientos de esta política.
- **Usuarios:** Responsables de utilizar el Drive institucional de manera responsable, ética y cumpliendo con las disposiciones de esta política.

5.3.3 Referencias Normativas

- Ley 594 de 2000 (Ley General de Archivos).
- Acuerdo 001 de 2024 (Alcaldía Municipal de Palmira).
- ISO 27001:2022 (Sistema de Gestión de Seguridad de la Información).
- Modelo de Seguridad y Privacidad de la Información (MSPI).
- Ley 1581 de 2012 (Protección de Datos Personales).
- Decreto 1377 de 2013 (Reglamentación de la Ley 1581 de 2012).

5.4 POLÍTICA DE CLASIFICACIÓN DE LA INFORMACIÓN PARA LA ALCALDÍA MUNICIPAL DE PALMIRA

Objetivo: Garantizar la protección adecuada de la información de la Alcaldía Municipal de Palmira, asignando niveles de clasificación según su sensibilidad y valor, de acuerdo con la Guía para la Gestión y Clasificación de Activos de Información del MinTIC y las mejores prácticas internacionales (ISO 27001:2022 y el Modelo de Seguridad y Privacidad de la Información - MSPI).

5.4.1 Definiciones:

- **Información:** Cualquier tipo de dato, registro o conocimiento generado o gestionado por la Alcaldía Municipal de Palmira, independientemente del medio en que se encuentre (documentos, bases de datos, sistemas informáticos, comunicaciones orales, etc.).
- **Activo de Información:** Elemento identificable que almacena información y es considerado valioso para la Alcaldía Municipal de Palmira por su importancia para el cumplimiento de sus funciones, su dificultad para ser reemplazado o su impacto en caso de pérdida, robo o modificación no autorizada.

5.4.2 Niveles de Clasificación de la Información:

- **Información Pública:** Información que puede ser divulgada libremente sin restricciones, ya que su conocimiento no afecta los intereses de la Alcaldía ni los derechos de terceros.
- **Información Pública Clasificada:** Información que, aunque es de carácter público, requiere un tratamiento especial debido a su sensibilidad. Su divulgación debe ser controlada y autorizada por el responsable de la información.
- **Información Pública Reservada:** Información que, por disposición legal o por razones de interés público, no puede ser divulgada o su acceso está restringido a personas autorizadas.

5.4.3 Procedimiento de Clasificación:

- **Identificación:** Determinar qué información es relevante para la Alcaldía.
- **Evaluación:** Analizar el impacto que tendría la divulgación, modificación o pérdida de la información.
- **Clasificación:** Asignar el nivel de clasificación adecuado (Pública, Pública Clasificada o Pública Reservada).
- **Etiquetado:** Marcar la información con su nivel de clasificación.
- **Protección:** Aplicar las medidas de seguridad correspondientes a cada nivel.

5.5 POLÍTICA DE GESTIÓN DE ACTIVOS DE INFORMACIÓN PARA LA ALCALDÍA MUNICIPAL DE PALMIRA

Objetivo: Garantizar la protección, control y uso adecuado de los activos de información de la Alcaldía Municipal de Palmira, alineándolos con los roles y responsabilidades de los usuarios, así como con las mejores prácticas internacionales (ISO 27001:2022) y las regulaciones nacionales (Ley 1712 de 2014, MSPI).

Directrices Generales:

- La Dirección de Tecnología, Innovación y Ciencia (DTIyC) mantendrá un inventario actualizado (previa entrega de la información completa por parte de la Secretaría General, encargada de recolectar esta información) de los activos de información, accesible públicamente en la página web de la Alcaldía, cumpliendo con la Ley 1712 de 2014.
- Cada activo de información tendrá un propietario designado, responsable de su gestión.
- Los administradores de información utilizarán los activos exclusivamente para fines laborales y de acuerdo con sus roles y responsabilidades.

5.5.1 Política de uso de los activos:

- **Propiedad:** Los activos de información son propiedad de la Alcaldía y su uso se limita a fines laborales.
- **Autorización:** Los usuarios solo utilizarán software y hardware autorizado por la Dirección de Tecnología, Innovación y Ciencia (Dirección de Tecnología, Innovación y Ciencia (DTIyC).
- **Respaldo:** Los usuarios podrán respaldar únicamente archivos personales, no información pública. La copia de información clasificada o reservada requiere autorización.
- **Software no autorizado:** La descarga, instalación o uso de software no autorizado está prohibido.
- **Requerimientos:** Todos los requerimientos de software, hardware o sistemas deben ser canalizados a través de la Dirección de Tecnología, Innovación y Ciencia (DTIyC).
- **Custodia:** La Dirección de Tecnología, Innovación y Ciencia (DTIyC) custodiará los medios de instalación, licencias y contraseñas de software y hardware.
- **Acceso de la Dirección de Tecnología, Innovación y Ciencia (DTIyC):** La Dirección de Tecnología, Innovación y Ciencia (DTIyC) podrá acceder a los activos de información de los usuarios cuando sea necesario.
- **Uso indebido:** Se prohíbe el uso de recursos informáticos para fines no autorizados, como envío de correo masivo no institucional, juegos en línea, o difusión de contenido inapropiado.
- **Restricciones:** Los usuarios no podrán instalar, descargar, modificar o distribuir software sin autorización de la Dirección de Tecnología, Innovación y Ciencia (DTIyC).
- **Responsabilidad:** Los usuarios son responsables de informar sobre cualquier violación de las políticas de seguridad y del uso adecuado de sus cuentas de usuario.
- **Seguridad en redes externas:** Los usuarios deben garantizar que el uso de redes externas no comprometa la seguridad de los recursos informáticos.
- **Protección antivirus:** Todo archivo proveniente de fuentes externas debe ser escaneado en busca de virus antes de su uso.

- **Respaldo de información:** La información será respaldada regularmente y almacenada de forma segura para su recuperación en caso de incidentes.

5.6 POLÍTICA DE SEGURIDAD DE RECURSOS HUMANOS PARA LA ALCALDÍA MUNICIPAL DE PALMIRA

Objetivo: Garantizar que todos los miembros del personal de la Alcaldía Municipal de Palmira (funcionarios, contratistas y colaboradores) comprendan y cumplan con sus responsabilidades en materia de seguridad y privacidad de la información, minimizando así los riesgos de incidentes de seguridad y protegiendo los activos de información de la entidad.

Directrices Generales:

- **Concienciación y Capacitación:** Se proporcionará capacitación continua y actualizada sobre seguridad de la información a todo el personal, incluyendo temas como políticas de seguridad, identificación de riesgos, manejo seguro de contraseñas, protección de datos y respuesta ante incidentes.
- **Responsabilidad Individual:** Cada miembro del personal es responsable de proteger la información a la que tiene acceso y de cumplir con las políticas y procedimientos de seguridad establecidos.
- **Gestión de Acceso:** El acceso a los sistemas y datos se otorgará en función de los roles y responsabilidades de cada individuo, aplicando el principio de mínimo privilegio.
- **Confidencialidad:** El personal debe mantener la confidencialidad de la información sensible a la que tiene acceso, incluso después de finalizar su relación laboral con la Alcaldía.
- **Uso Aceptable:** El uso de los recursos informáticos de la Alcaldía debe limitarse a fines laborales autorizados y cumplir con las políticas de uso aceptable establecidas.
- **Incidentes de Seguridad:** Cualquier incidente de seguridad, sospecha o violación de las políticas debe ser reportado de inmediato a la Dirección de Tecnología, Innovación y Ciencia (DTIyC).

5.6.1 Políticas específicas para usuarios de la Dirección de Tecnología, Innovación y Ciencia

- **Almacenamiento de Información:** La Dirección de Tecnología, Innovación y Ciencia (DTIyC) proporcionará un drive institucional denominado [drive.nombre del área] en la plataforma de gestión Google Workspace. Los usuarios deben copiar la información relevante a este drive según lo definido en la Política de Uso del Drive Institucional en Google Workspace.
- **Software Autorizado:** Sólo se utilizará software con licencia y autorizado por la Dirección de Tecnología, Innovación y Ciencia (DTIyC). El uso de software sin licencia está prohibido.

- **Responsabilidad por Software:** La Dirección de Tecnología, Innovación y Ciencia (DTIyC) no se hace responsable por copias no autorizadas de software en los equipos de los usuarios.
- **Uso de Dispositivos Externos:** El uso de dispositivos de almacenamiento externo está permitido bajo ciertas condiciones y con autorización previa, debido al riesgo de transmisión de virus y pérdida de información.
- **Propiedad del Software:** El software instalado en los equipos es propiedad de la Dirección de Tecnología, Innovación y Ciencia (DTIyC). La copia no autorizada está prohibida y sujeta a sanciones.
- **Auditorías:** La Dirección de Tecnología, Innovación y Ciencia (DTIyC) realizará auditorías periódicas para garantizar el cumplimiento de las políticas de software.
- **Responsabilidad por Equipos:** Los usuarios son responsables del cuidado y uso adecuado de los equipos y software asignados.
- **Acceso a Datos:** Los usuarios solo tendrán acceso a los datos autorizados por la Dirección de Tecnología, Innovación y Ciencia (DTIyC) y serán responsables de su confidencialidad.
- **Protección de la Información:** Los usuarios deben proteger la información en documentos, formatos, listados, etc., tanto en formato físico como digital.
- **Uso de Dispositivos Electrónicos:** Los dispositivos electrónicos sólo se utilizarán para fines autorizados.
- **Reporte de Incidentes:** Cualquier incidente de seguridad debe ser reportado de inmediato a la Dirección de Tecnología, Innovación y Ciencia (DTIyC) a través de la mesa de ayuda https://mesadeayuda.palmira.gov.co/.
- **Intercambio de Datos:** El intercambio de datos debe realizarse a través de los canales seguros proporcionados por los sistemas de información, no mediante archivos compartidos o dispositivos externos.

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

- **Uso de Claves de Usuario:** Las claves de usuario son personales e intransferibles y deben ser de alta complejidad.
- **Confidencialidad de las Claves:** Las claves no deben ser compartidas con terceros.
- **Custodia de Claves:** Los funcionarios asignados por el Director de la Dirección de Tecnología, Innovación y Ciencia, custodiarán las claves de forma segura, con acceso restringido.
- **Custodia de Documentos**: Los documentos confidenciales deben ser custodiados para evitar el acceso no autorizado.

- **Eliminación Segura de Información: Al** cambiar o retirar equipos, se deben aplicar prácticas de eliminación segura de la información.
- **Instalación de Software:** Solo se instalará software autorizado y con licencia.
- **Privilegios Especiales:** Los privilegios especiales en estaciones de trabajo sólo se otorgarán con autorización del Director de la Dirección de Tecnología, Innovación y Ciencia (DTIyC).
- **Confidencialidad de la Información:** Los funcionarios y contratistas deben mantener la confidencialidad de la información a la que tienen acceso.
- **Uso Adecuado de la Información:** La información no debe ser utilizada para fines comerciales o personales.
- **Protección de Licencias de Software:** Las licencias de software deben ser protegidas y almacenadas adecuadamente.
- **Control de Acceso al Datacenter:** Se llevará un registro de las personas autorizadas a ingresar al datacenter.
- **Bloqueo de Protocolos y Servicios:** Se bloquearán los protocolos y servicios no necesarios en la infraestructura de la Alcaldía a través de la plataforma de seguridad perimetral fortinet.
- **Configuración Mínima de Servidores:** Los servidores se configurarán con el mínimo de servicios necesarios.
- **Pruebas de Software:** Las pruebas de software deben ser autorizadas y realizadas en entornos aislados.

5.7 POLÍTICA DE TELETRABAJO Y TRABAJO EN CASA PARA LA ALCALDÍA MUNICIPAL DE PALMIRA

Objetivo: Establecer las directrices y requisitos para el acceso remoto seguro a la infraestructura tecnológica de la Alcaldía Municipal de Palmira, garantizando la protección de la información y el cumplimiento de las funciones laborales en modalidades de teletrabajo y trabajo en casa, de acuerdo con las regulaciones del Ministerio de Tecnologías de la Información y las Comunicaciones de Colombia, la política de gobierno digital, la norma ISO 27001:2022 y el modelo de seguridad y privacidad de la información MSPI.

Directrices:

- **Acceso Condicionado:** El acceso remoto se otorgará únicamente a aquellos servidores públicos y contratistas cuyas funciones lo requieran, previa autorización y verificación de cumplimiento de los requisitos técnicos y de seguridad.

- **Alistamiento de Equipos:** Antes de la entrega de cualquier equipo para teletrabajo o trabajo en casa, la Dirección de Tecnología, Innovación y Ciencia (DTIyC) realizará un alistamiento que incluya la instalación y configuración del software necesario, la verificación de la seguridad y la actualización de los sistemas operativos y antivirus.
- **Confidencialidad y Privacidad:** Los tele trabajadores y trabajadores en casa deben mantener la confidencialidad de la información a la que acceden y cumplir con las políticas de privacidad de la Alcaldía.
- **Conexiones Seguras:** Se utilizarán conexiones seguras y cifradas para el acceso remoto, como VPNs (Virtual Private Networks) u otros mecanismos aprobados por la Dirección de Tecnología, Innovación y Ciencia (DTIyC).
- **Evaluación de Riesgos:** La Dirección de Tecnología, Innovación y Ciencia (DTIyC) realizará evaluaciones periódicas de riesgos para identificar y mitigar las vulnerabilidades asociadas al acceso remoto.
- **Monitoreo y Control:** La Dirección de Tecnología, Innovación y Ciencia (DTIyC) implementará mecanismos de monitoreo y control para detectar y prevenir accesos no autorizados, uso indebido de recursos y posibles incidentes de seguridad.
- **Préstamo de Equipos:** El préstamo de equipos de cómputo para teletrabajo o trabajo en casa se realizará a través de un proceso formal, con registro y seguimiento por parte del área de recursos físicos y la Dirección de Tecnología, Innovación y Ciencia (DTIyC). El equipo debe ser devuelto en las mismas condiciones en que fue entregado.
- **Requisitos Técnicos:** La Dirección de Tecnología, Innovación y Ciencia (DTIyC) definirá y mantendrá actualizados los requisitos técnicos mínimos para las conexiones remotas, incluyendo software, hardware, seguridad de redes y protocolos de comunicación.
- **Seguridad de Dispositivos:** Los dispositivos utilizados para el acceso remoto deben cumplir con los estándares de seguridad establecidos por la Dirección de Tecnología, Innovación y Ciencia (DTIyC), incluyendo software antivirus actualizado, contraseñas robustas y cifrados de datos.
- **Uso Responsable de la Información:** La información accedida remotamente debe ser utilizada exclusivamente para fines laborales y en cumplimiento de las obligaciones contractuales. Se prohíbe el uso de información institucional para fines personales o no autorizados.

5.8 POLÍTICA ESPECÍFICA PARA WEB MASTER DE LA ALCALDÍA MUNICIPAL DE PALMIRA

Objetivo: Garantizar la integridad, confidencialidad y disponibilidad de las páginas web institucionales de la Alcaldía Municipal de Palmira, así como la protección del software y la información contenida en ellas, en cumplimiento de la Ley 1712 de 2014, la política de gobierno digital, la norma ISO 27001:2022 y el modelo de seguridad y privacidad de la información MSPI.

Directrices:

5.8.1 Responsabilidades de los Webmasters:

- Preparar y depurar la información de su área o dependencia antes de su publicación.
- Reportar a la Dirección de Tecnología, Innovación y Ciencia (DTIyC) los requerimientos de actualización del software del sitio web.
- Mantener un archivo actualizado con la información de la página inicial.
- Registrar la autorización de publicación por parte del funcionario responsable.
- Coordinar con el administrador web de la Dirección de Tecnología, Innovación y Ciencia (DTIyC) los lineamientos de diseño y estructura del sitio.

5.8.2 Cumplimiento de la Ley 1712 de 2014:

- Asegurar que la publicación y modificación de información oficial en las páginas web cumpla con los parámetros del Índice de Transparencia y Acceso a la Información Pública, establecidos por la Procuraduría General de la República.
- Mantener un registro detallado de todas las publicaciones y modificaciones realizadas en el sitio web, incluyendo fecha, hora, autor y contenido.

5.8.3 Gestión de Claves de Acceso:

- Las claves de acceso de los web masters son estrictamente confidenciales, personales e intransferibles.
- Los web masters deben utilizar contraseñas robustas y cambiarlas periódicamente.
- Se prohíbe compartir las claves de acceso con terceros.

Seguridad del Contenido Web:

- Implementar medidas de seguridad para proteger el contenido web de accesos no autorizados, modificaciones malintencionadas y pérdida de datos.
- Realizar copias de seguridad periódicas del contenido web y almacenarlas en un lugar seguro.

- Utilizar herramientas de detección y prevención de vulnerabilidades para proteger el sitio web de ataques cibernéticos.

5.8.4 Actualización del Software:

- Mantener el software del sitio web actualizado con las últimas versiones y parches de seguridad.
- Realizar pruebas exhaustivas antes de implementar cualquier actualización en el sitio web.

5.9 POLÍTICA DE SEGURIDAD FÍSICA Y AMBIENTAL PARA ESTACIONES CLIENTE EN LA ALCALDÍA MUNICIPAL DE PALMIRA

Objetivo: Garantizar la seguridad, integridad y uso adecuado de las estaciones cliente (computadores de escritorio y portátiles) de la Alcaldía Municipal de Palmira, protegiendo los activos de información y asegurando su disponibilidad y funcionamiento óptimo, en cumplimiento de la norma ISO 27001:2022 y el modelo de seguridad y privacidad de la información MSPI.

Directrices:

- **Gestión de usuario tipo Administrador:** La Dirección de Tecnología, Innovación y Ciencia (DTIyC) deberá establecer contraseñas tipo administrador para los equipos de cómputo e impresoras, y estas serán de uso exclusivo de la Dirección de Tecnología, Innovación y Ciencia (DTIyC).
- **Control de Cambios y Traslados:** Cualquier cambio o traslado de equipos tecnológicos debe ser autorizado y registrado por la Dirección de Tecnología, Innovación y Ciencia (DTIyC), y reflejado en el inventario de bienes muebles.
- **Instalación de Software:** La instalación de software en las estaciones cliente es exclusiva de la Dirección de Tecnología, Innovación y Ciencia (DTIyC). Se mantendrá un inventario actualizado del software autorizado.
- **Almacenamiento de Archivos Personales:** Se prohíbe almacenar archivos de video, música y fotos no institucionales en los discos duros de las estaciones cliente o en discos virtuales de red.
- **Protección del Sistema Operativo:** El disco C:\ contiene el sistema operativo, aplicaciones y perfil de usuario, los usuarios no deben modificar estos archivos.
- **Almacenamiento de Documentos Institucionales:** Los usuarios deben almacenar los documentos institucionales finales en las carpetas virtuales asignadas en Google Drive, y utilizar las estaciones cliente solo para trabajar en borradores.

- **Préstamo de Equipos:** El préstamo de equipos de cómputo debe ser solicitado formalmente al área de recursos físicos, quien coordinará con la Dirección de Tecnología, Innovación y Ciencia (DTIyC) el alistamiento previo.
- **Equipos de Terceros:** Los equipos de terceros que ingresen temporalmente a la Alcaldía deben ser registrados en las porterías. La Dirección de Tecnología, Innovación y Ciencia (DTIyC) no se responsabiliza por su pérdida o daño.
- **Soporte Técnico:** La Dirección de Tecnología, Innovación y Ciencia (DTIyC) no proporcionará soporte técnico a equipos que no pertenezcan a la Alcaldía.

5.9.1 Responsabilidades:

- **Dirección de Tecnología, Innovación y Ciencia (DTIyC):**
  - Autorizar y controlar los cambios y traslados de equipos.
  - Mantener un inventario actualizado del software autorizado.
  - Realizar el alistamiento de equipos para préstamo.
  - Implementar medidas de seguridad para proteger las estaciones cliente.
- **Usuarios:**
  - Cumplir con las políticas de uso de las estaciones cliente.
  - Reportar cualquier incidente de seguridad o mal funcionamiento de los equipos.
  - No instalar software no autorizado.
  - No almacenar archivos personales en los equipos de la Alcaldía.
  - Utilizar las carpetas del drive institucional del área para almacenar documentos institucionales finales.
  - Registrar los equipos de terceros en las porterías.

5.10 POLÍTICA DE SEGURIDAD INFORMÁTICA PARA EQUIPOS DE LA ALCALDÍA MUNICIPAL DE PALMIRA

Objetivo: Garantizar la protección, disponibilidad e integridad de los equipos informáticos y la información que contienen, en cumplimiento de la norma ISO 27001:2022 y el modelo de seguridad y privacidad de la información MSPI.

Directrices:

5.10.1 Protección de la Energía:

- Solo se conectarán a la red eléctrica regulada los equipos autorizados (computadores, pantallas).
- Otros dispositivos se conectarán a la red no regulada, bajo supervisión del área administrativa.

5.10.2 Seguridad del Cableado:

- Los cables estarán claramente identificados para evitar desconexiones erróneas.
- Se mantendrán planos actualizados de las conexiones de cableado.
- El acceso a los centros de cableado (racks) estará restringido.

5.10.3 Mantenimiento de Equipos:

- La Dirección de Tecnología, Innovación y Ciencia (DTIyC) mantendrá contratos de soporte y mantenimiento para equipos críticos.
- Se registrarán todas las actividades de mantenimiento (preventivo y correctivo).
- Se llevará una hoja de vida de cada equipo.
- El mantenimiento de servidores y equipos críticos será programado y aprobado por el Director de TIyC.

5.10.4 Traslado de Equipos:

- La salida de equipos de las instalaciones requiere autorización de la oficina de Recursos Físicos y la Dirección de Tecnología, Innovación y Ciencia (DTIyC).
- Se verificará que los equipos no contengan información clasificada como crítica antes de su salida.
- Los equipos trasladados fuera de las instalaciones deben cumplir con los requisitos mínimos de seguridad.

5.10.5 Retiro de Servicio y Reasignación de Equipos:

- Antes de retirar o reasignar un equipo, se eliminará toda la información almacenada en él, utilizando métodos de borrado seguro o destrucción física.

5.10.6 Ingreso y Retiro de Activos de Terceros:

- El ingreso y retiro de activos personales de los usuarios se realizará según los procedimientos establecidos por la Administración del Edificio.

- La Dirección de Tecnología, Innovación y Ciencia (DTIyC) no se responsabiliza por daños o problemas en equipos personales conectados a la red eléctrica.
- El ingreso y retiro de activos de visitantes se registrará y controlará en las porterías.

5.10.7 Traslado Interno de Activos:

- El traslado de activos entre dependencias será gestionado por el equipo de funcionarios encargado de la administración para el control de inventarios.

5.10.8 Responsabilidades:

- **Dirección de Tecnología, Innovación y Ciencia (DTIyC):**
  - Implementar y mantener esta política.
  - Supervisar el cumplimiento de las directrices.
  - Gestionar el mantenimiento y seguridad de los equipos.
  - Autorizar el traslado y salida de equipos.
- **Usuarios:**
  - Cumplir con las directrices de la política.
  - Reportar cualquier incidente de seguridad o mal funcionamiento de los equipos.
  - No instalar software no autorizado.
  - No almacenar archivos personales en los equipos de la Alcaldía.
  - Seguir los procedimientos de ingreso y retiro de activos personales.

5.11 POLÍTICAS DE SEGURIDAD INFORMÁTICA DEL DATA CENTER Y CENTROS DE CABLEADO DE LA ALCALDÍA MUNICIPAL DE PALMIRA

Objetivo: Garantizar la protección física y lógica de la información y la infraestructura del Data Center y centros de cableado, siguiendo el procedimiento de administración de data center versión 02, la norma ISO 27001:2022 y el modelo de seguridad y privacidad de la información MSPI.

Directrices:

Control de Acceso:

- Solo personal autorizado puede ingresar al Data Center.
- Se llevará un registro de entrada y salida en una bitácora física.
- Se implementarán dispositivos electrónicos de autenticación o sistemas biométricos.

Respaldo de Energía:

- Todos los equipos del Data Center contarán con sistemas de respaldo de energía (UPS).

Limpieza y Aseo:

- La limpieza se realizará bajo supervisión del personal de la Dirección de Tecnología, Innovación y Ciencia (DTIyC), siguiendo protocolos específicos.
- Se restringirá el ingreso de elementos innecesarios para la limpieza.

Condiciones Ambientales:

- Se prohíbe fumar, comer o beber en el Data Center.
- Se mantendrá el orden y la limpieza, evitando acumulación de materiales inflamables.

Infraestructura del Data Center:

- Señalización clara de equipos y salidas de emergencia.
- Pisos de materiales no combustibles.
- Sistema de refrigeración redundante.
- UPS con capacidad adecuada.
- Alarmas de detección de humo y sistema de extinción de incendios.
- Extintores adecuados para fuegos eléctricos y químicos.
- Cableado de red y potencia protegidos y separados según normas técnicas.

Grabación de Video:

- La grabación de video requiere autorización del Director(a) de la Dirección de Tecnología, Innovación y Ciencia, y se limita a fines institucionales.

5.11.1 Supervisión de Actividades:

Las actividades de soporte y mantenimiento serán supervisadas por personal autorizado de la Dirección de Tecnología, Innovación y Ciencia (DTIyC).

Control de Puertas y Armarios:

- Las puertas del Data Center permanecerán cerradas.
- Los armarios (racks) se mantendrán cerrados y con llave.

Iluminación:

- Las luces se apagarán cuando no haya personal presente.

Uso de Comunicaciones Unificadas:

- Se utilizarán de forma responsable, evitando contenido inapropiado o malicioso.
- Se verificará la ausencia de malware antes de enviar cualquier contenido.

Publicación de Información:

- La información publicada o divulgada debe cumplir con las medidas de seguridad según su clasificación.

Responsabilidad Individual:

- Cada usuario es responsable del uso adecuado de las herramientas y de los daños que pueda causar.

Monitoreo de Equipos:

- Los equipos del Data Center serán monitoreados para detectar fallas.

5.11.2 Responsabilidades:

Dirección de Tecnología, Innovación y Ciencia:

- Implementar y mantener esta política.
- Supervisar el cumplimiento de las directrices.
- Gestionar el acceso, seguridad y mantenimiento del Data Center.

Personal Autorizado:

- Cumplir con las directrices de la política.
- Reportar cualquier incidente de seguridad.
- Mantener la confidencialidad de la información.

Dependencia Administrativa:

- Coordinar la limpieza del Data Center bajo supervisión de la Dirección de Tecnología, Innovación y Ciencia (DTIyC).

5.12 POLÍTICA DE GESTIÓN DE COMUNICACIONES Y OPERACIONES PARA LA ALCALDÍA MUNICIPAL DE PALMIRA

Objetivo: Establecer lineamientos claros y seguros para el uso de las tecnologías de la información y comunicación (TIC) en la Alcaldía Municipal de Palmira, garantizando la protección de la información, el cumplimiento de la normativa vigente (Ley 1712 de 2014, política de gobierno digital, ISO 27001:2022, MSPI), y la eficiencia en las operaciones, considerando los avances en inteligencia artificial.

Directrices:

5.12.1. Procedimientos y Responsabilidades de Operación:

- La Dirección de Tecnología, Innovación y Ciencia (DTIyC) es responsable de la gestión, mantenimiento y seguridad de la infraestructura TIC, así como de la definición y actualización de esta política.
- Los usuarios son responsables del uso adecuado y ético de los recursos TIC, cumpliendo con las normas y procedimientos establecidos.

5.12.2. Política de Uso de Internet:

- El uso de internet debe ser exclusivamente para fines laborales y en cumplimiento de las funciones asignadas.
- Se prohíbe el acceso a sitios web con contenido ilegal, inapropiado o que represente un riesgo para la seguridad de la información.
- La descarga de archivos debe ser moderada y justificada.
- Se permite el acceso a plataformas de streaming con fines laborales y previa autorización.
- La Dirección de Tecnología, Innovación y Ciencia (DTIyC) realizará controles periódicos para verificar el cumplimiento de esta política.

5.12.3. Política de Uso de Mensajería Instantánea y Redes Sociales:

- El uso de mensajería instantánea (WhatsApp) y redes sociales se limita a funcionarios autorizados y para fines específicos de comunicación con la ciudadanía.
- Se prohíbe el envío de contenido inapropiado, ofensivo o que ponga en riesgo la seguridad de la información.
- La Alcaldía no se responsabiliza por el uso personal de redes sociales por parte de funcionarios o contratistas.

5.12.4. Política de Uso de Discos de Red y Carpetas Virtuales:

- El acceso a discos de red y carpetas virtuales en el drive institucional se otorgará según los roles y funciones de cada usuario.
- La información almacenada debe ser de carácter institucional y relevante para las funciones laborales.
- Se prohíbe almacenar contenido inapropiado o ilegal.
- Se prohíbe la divulgación no autorizada de información almacenada en estos recursos.
- La Dirección de Tecnología, Innovación y Ciencia (DTIyC) es responsable de las copias de seguridad y custodia de la información (a demanda).

5.12.5. Política de Uso de Impresoras y Servicio de Impresión:

- La impresión de documentos debe limitarse a fines institucionales.
- Los usuarios son responsables del uso adecuado de las impresoras.
- Cualquier falla debe ser reportada a la Dirección de Tecnología, Innovación y Ciencia (DTIyC).
- Se debe minimizar el uso de papel, promoviendo la digitalización de documentos.

5.12.6. Política de Uso de Dispositivos Móviles:

- Los dispositivos móviles son herramientas de trabajo y su uso debe limitarse a fines laborales.
- Los dispositivos deben estar integrados a una plataforma de administración de la Dirección de Tecnología, Innovación y Ciencia (DTIyC).
- Solo se pueden instalar aplicaciones autorizadas por la Dirección de Tecnología, Innovación y Ciencia (DTIyC).
- Los dispositivos deben tener contraseña de ingreso y bloqueo.
- Los dispositivos deben permanecer encendidos y cargados durante la jornada laboral.
- La instalación de aplicaciones adicionales requiere autorización del Director(a) de la Dirección de Tecnología, Innovación y Ciencia (DTIyC).

5.13 POLÍTICA DE PROTECCIÓN CONTRA CÓDIGO MALICIOSO (MALWARE) PARA LA ALCALDÍA MUNICIPAL DE PALMIRA

Objetivo: Esta política establece los controles y directrices para proteger los sistemas y la información de la Alcaldía Municipal de Palmira contra software malicioso (malware), garantizando la confidencialidad, integridad y disponibilidad de los activos de información.

Directrices:

5.13.1 Prevención

- **Análisis de archivos:** Antes de abrir, ejecutar o compartir cualquier archivo o enlace recibido por correo electrónico, mensajería instantánea o cualquier otro medio, es obligatorio analizarlo con el software antivirus institucional.
- **Actualizaciones de seguridad:** Mantener el sistema operativo, aplicaciones y software antivirus actualizados con los últimos parches de seguridad proporcionados por los fabricantes.
- **Contraseñas seguras:** Utilizar contraseñas robustas y únicas para cada servicio, cambiándolas periódicamente.
- **Copias de seguridad:** Realizar copias de seguridad periódicas de la información crítica, almacenándolas en ubicaciones seguras y verificando su integridad.
- **Concientización:** La Dirección de Tecnología, Innovación y Ciencia (DTIyC) implementará un programa de concientización y capacitación continua para el personal sobre los riesgos del malware y las mejores prácticas para prevenir infecciones.
- **Navegación segura:** Evitar visitar sitios web sospechosos o de dudosa reputación, así como hacer clic en enlaces o anuncios emergentes (pop-ups) no confiables.
- **Software autorizado:** Únicamente el personal de la Dirección de Tecnología, Innovación y Ciencia (DTIyC), con previa autorización del jefe inmediato, podrá instalar software en los equipos institucionales.

5.13.2 Detección y respuesta

- **Monitoreo:** La Dirección de Tecnología, Innovación y Ciencia (DTIyC) implementará mecanismos de monitoreo para detectar posibles infecciones de malware y actividades sospechosas en los sistemas.
- **Plan de respuesta a incidentes:** La Alcaldía contará con un plan de respuesta a incidentes de seguridad, que incluirá procedimientos para contener, erradicar y recuperar los sistemas afectados por malware.
- **Software antivirus:** Todos los equipos institucionales deben contar con software antivirus actualizado, configurado para realizar análisis periódicos y en tiempo real.
- **Reporte de incidentes:** Cualquier sospecha de infección o incidente de seguridad debe ser reportado inmediatamente a la Dirección de Tecnología, Innovación y Ciencia (DTIyC) para su análisis y respuesta.

5.13.3 Referencias

- ISO/IEC 27001:2022 - Tecnologías de la información - Técnicas de seguridad - Sistemas de gestión de la seguridad de la información - Requisitos
- Política de Gobierno Digital de la Alcaldía Municipal de Palmira
- Ley 1581 de 2012 - Protección de Datos Personales

5.14 POLÍTICA DE RESPALDO Y RESTAURACIÓN DE INFORMACIÓN PARA LA ALCALDÍA MUNICIPAL DE PALMIRA

Objetivo: Esta política establece los lineamientos y procedimientos para garantizar la protección, respaldo y recuperación oportuna de la información crítica de la Alcaldía Municipal de Palmira, asegurando la continuidad de las operaciones en caso de incidentes o desastres.

Directrices:

5.14.1 Planificación y responsabilidades

- **Análisis de impacto al negocio (BIA):** Se realizará un BIA para identificar los sistemas y datos críticos, así como el tiempo máximo tolerable de interrupción (RTO) y la pérdida máxima tolerable de datos (RPO).
- **Estrategia de respaldo:** La Dirección de Tecnología, Innovación y Ciencia (DTIyC) definirá una estrategia de respaldo adecuada, considerando los requisitos del BIA, la criticidad de la información y los recursos disponibles.
- **Inventario de información:** La Dirección de Tecnología, Innovación y Ciencia (DTIyC) mantendrá un inventario actualizado de la información crítica, clasificándola según su importancia y nivel de confidencialidad.
- **Responsabilidad de los propietarios de la información:** Definir los requisitos de respaldo y restauración, así como aprobar los planes de recuperación.
- **Responsabilidad de la Dirección de Tecnología, Innovación y Ciencia:** Implementar y mantener los sistemas de respaldo, realizar las copias de seguridad, verificar su integridad y ejecutar las restauraciones cuando sea necesario.

5.14.2 Procedimientos de respaldo:

- **Frecuencia:** Los respaldos se realizarán con la frecuencia establecida en la estrategia de respaldo, considerando la criticidad de la información y los cambios realizados.
- **Tipos de respaldo:** Se utilizarán diferentes tipos de respaldo (completo, incremental, diferencial) para optimizar el uso de los recursos y minimizar el tiempo de recuperación.

- **Medios de almacenamiento:** Los respaldos se almacenarán en medios seguros y confiables, tanto dentro como fuera de las instalaciones de la Alcaldía, para garantizar su disponibilidad en caso de desastre.
- **Encriptación:** La información sensible será encriptada antes de ser respaldada, utilizando algoritmos robustos y claves seguras.
- **Verificación:** Se verificará periódicamente la integridad de los respaldos y su capacidad de restauración.

5.14.3 Procedimientos de restauración:

- **Plan de recuperación ante desastres (DRP):** La Alcaldía contará con un DRP que incluya procedimientos detallados para restaurar los sistemas y la información en caso de incidentes o desastres.
- **Pruebas de restauración:** Se realizarán pruebas periódicas de restauración para verificar la eficacia del DRP y asegurar la recuperación oportuna de la información.
- **Aprobación:** Las restauraciones en ambientes de producción requerirán la aprobación del propietario de la información y la Dirección de Tecnología, Innovación y Ciencia (DTIyC).

5.14.4 Gestión de medios de respaldo:

- **Almacenamiento seguro:** Los medios de respaldo se almacenarán en un lugar seguro, con acceso restringido y condiciones ambientales adecuadas.
- **Rotación de medios:** Se establecerá un esquema de rotación de medios para garantizar la disponibilidad de copias de respaldo actualizadas y minimizar el riesgo de pérdida o deterioro.
- **Eliminación segura:** Los medios de respaldo que ya no sean necesarios serán eliminados de forma segura, utilizando métodos que garanticen la destrucción completa de la información.

5.15 POLÍTICA DE GESTIÓN DE INFORMACIÓN EN ESTACIONES DE TRABAJO DE USUARIO PARA LA ALCALDÍA MUNICIPAL DE PALMIRA

Objetivo: Esta política establece los lineamientos y procedimientos para la gestión segura y eficiente de la información almacenada en las estaciones de trabajo de los usuarios finales de la Alcaldía Municipal de Palmira, garantizando su protección, disponibilidad y cumplimiento de la normativa vigente.

Directrices:

5.15.1 Propiedad de la información

- **Derechos de autor:** De acuerdo con la Ley 23 de 1982, los derechos de autor sobre las obras creadas por los empleados y funcionarios en el ejercicio de sus funciones pertenecen a la Alcaldía, con las excepciones establecidas por la ley.

5.15.2 Respaldo y retención de información

- **Respaldos automáticos:** La Dirección de Tecnología, Innovación y Ciencia (DTIyC) implementará mecanismos de respaldo automático de la información almacenada en las estaciones de trabajo, utilizando soluciones de almacenamiento en la nube o servidores centralizados.
- **Frecuencia de respaldo:** Los respaldos se realizarán con la frecuencia establecida por la Dirección de Tecnología, Innovación y Ciencia (DTIyC), considerando la criticidad de la información y los cambios realizados.
- **Retención de respaldos:** Los respaldos se conservarán durante el tiempo establecido en la tabla de retención de documentos de la Alcaldía, cumpliendo con los requisitos legales y regulatorios.

5.15.3 Acceso y uso de la información

- **Información institucional:** La información almacenada en las estaciones de trabajo es propiedad de la Alcaldía y solo debe ser utilizada para fines laborales.
- **Información personal:** Los usuarios finales no deben almacenar información personal sensible en las estaciones de trabajo, salvo que sea estrictamente necesario para el desempeño de sus funciones.
- **Dispositivos extraíbles:** El uso de dispositivos extraíbles (USB, discos duros externos, etc.) está restringido, excepto para aquellos usuarios autorizados por la Dirección de Tecnología, Innovación y Ciencia (DTIyC).

5.15.4 Retiro o traslado de personal

- **Copia de seguridad:** En caso de retiro o traslado de un usuario, la Dirección de Tecnología, Innovación y Ciencia (DTIyC) realizará una copia de seguridad de la información almacenada en su estación de trabajo antes de su entrega.
- **Acceso a la copia:** El acceso a la copia de seguridad estará restringido al jefe inmediato del usuario y a la Dirección de Tecnología, Innovación y Ciencia (DTIyC), quienes podrán solicitarla justificando su necesidad y presentando un acuerdo de confidencialidad firmado por el usuario retirado.

5.15.5 Borrado seguro de información

- **Equipos en desuso:** Antes de desechar o reutilizar un equipo, la Dirección de Tecnología, Innovación y Ciencia (DTIyC) realizará un borrado seguro de la información almacenada en el disco duro, utilizando métodos que garanticen la imposibilidad de recuperar los datos.

5.16 POLÍTICA DE USO GESTIÓN DE SEGURIDAD DE RED (RED DE ÁREA LOCAL – LAN) PARA LA ALCALDÍA MUNICIPAL DE PALMIRA

Objetivo: Esta política establece los lineamientos y controles para garantizar la seguridad, disponibilidad y uso adecuado de la red de área local (LAN) de la Alcaldía Municipal de Palmira, protegiendo la información y los sistemas de posibles amenazas internas y externas.

Directrices:

5.16.1 Acceso a la red

- **Equipos autorizados:** Solo los equipos de cómputo estándar de propiedad de la Alcaldía podrán conectarse a la red LAN.
- **Equipos personales:** Los equipos personales podrán conectarse a una red de invitados separada, con acceso limitado a servicios específicos y previa autenticación.
- **Puntos de acceso:** Los equipos solo podrán conectarse a los puntos de acceso autorizados y definidos por la Dirección de Tecnología, Innovación y Ciencia (DTIyC).

5.16.2 Gestión de la red

- **Responsabilidad:** La Dirección de Tecnología, Innovación y Ciencia (DTIyC) es responsable de la instalación, configuración, monitoreo y mantenimiento de la infraestructura de red, incluyendo switches, routers, firewalls y puntos de acceso.
- **Segmentación de red:** La red LAN se segmentará en diferentes zonas de seguridad, de acuerdo con la criticidad de la información y los requisitos de acceso.
- **Control de acceso:** Se implementarán mecanismos de control de acceso basados en roles y privilegios, para garantizar que los usuarios solo puedan acceder a los recursos necesarios para el desempeño de sus funciones.
- **Seguridad perimetral:** Se implementará un firewall para proteger la red LAN de amenazas externas, controlando el tráfico entrante y saliente.
- **Detección de intrusos:** Se implementará un sistema de detección de intrusos (IDS) para monitorear la red en busca de actividades sospechosas y generar alertas.

5.16.3 Uso aceptable de la red

- **Fines laborales:** La red LAN debe utilizarse exclusivamente para fines laborales, evitando actividades que puedan comprometer la seguridad o el rendimiento de la red.
- **Política de uso aceptable:** Los usuarios deben cumplir con la política de uso aceptable de la Alcaldía, que establece las normas y restricciones para el uso de los recursos informáticos.
- **Software malicioso:** Está prohibido descargar, instalar o ejecutar software malicioso en la red LAN.
- **Uso de ancho de banda:** El uso del ancho de banda debe ser responsable, evitando la descarga de archivos grandes o el uso excesivo de aplicaciones que consuman recursos de red.

5.17 POLÍTICA DE CONTROL DE ACCESO A LA INFRAESTRUCTURA TECNOLÓGICA DE LA ALCALDÍA MUNICIPAL DE PALMIRA

Objetivo: Garantizar un acceso seguro y controlado, tanto físico como lógico, a la información y recursos tecnológicos de la Alcaldía Municipal de Palmira, en cumplimiento de la norma ISO 27001:2022, el modelo de seguridad y privacidad de la información MSPI, la política de gobierno digital y las regulaciones del Ministerio de Tecnologías de la Información y las Comunicaciones de Colombia.

Directrices:

Recursos Tecnológicos Proporcionados:

- La Dirección de Tecnología, Innovación y Ciencia (DTIyC) proporcionará los recursos tecnológicos necesarios para el desempeño de las funciones laborales. No se permite conectar dispositivos no autorizados a la red.

Gestión de Claves de Acceso:

- La Dirección de Tecnología, Innovación y Ciencia (DTIyC) asignará claves de acceso únicas y personales a cada usuario autorizado.
- Las claves son intransferibles y los usuarios son responsables de su confidencialidad y uso adecuado.
- Las claves deben cumplir con los requisitos de complejidad establecidos por la Dirección de Tecnología, Innovación y Ciencia (DTIyC).

Instalación de Software y Hardware:

- Solo el personal autorizado por la Dirección de Tecnología, Innovación y Ciencia (DTIyC) puede instalar software licenciado o hardware en la infraestructura tecnológica de la Alcaldía.

Trabajo Remoto:

- Todo trabajo con información institucional debe realizarse en las instalaciones de la Alcaldía, a menos que se cuente con autorización expresa de la Dirección de Tecnología, Innovación y Ciencia (DTIyC).
- El acceso remoto a la red de la Alcaldía se realizará exclusivamente a través de una conexión VPN segura proporcionada por la Dirección de Tecnología, Innovación y Ciencia (DTIyC).

Monitoreo y Control de Acceso:

- La Dirección de Tecnología, Innovación y Ciencia (DTIyC) implementará mecanismos de monitoreo y registro de acceso para detectar y prevenir accesos no autorizados y actividades sospechosas.
- Se realizarán auditorías periódicas para verificar el cumplimiento de esta política.

Gestión de Identidades y Accesos:

- Se implementará un sistema de gestión de identidades y accesos que permita controlar y administrar los permisos de los usuarios de forma centralizada y eficiente.
- Se aplicará el principio de mínimo privilegio, otorgando a cada usuario solo los permisos necesarios para desempeñar sus funciones.
- Seguridad en Dispositivos Móviles:
- Los dispositivos móviles utilizados para acceder a los recursos de la Alcaldía deben cumplir con las políticas de seguridad establecidas, incluyendo el uso de contraseñas seguras, cifrado de datos y software de seguridad actualizado.

Concientización y Capacitación:

- Se proporcionará capacitación continua a los usuarios sobre las mejores prácticas de seguridad, incluyendo el manejo seguro de contraseñas, la identificación de ataques de phishing y la protección de datos confidenciales.

5.18 POLÍTICA DE ESTABLECIMIENTO, USO Y PROTECCIÓN DE CLAVES DE ACCESO PARA LA ALCALDÍA MUNICIPAL DE PALMIRA

Objetivo: Garantizar la seguridad de la información de la Alcaldía Municipal de Palmira mediante el control efectivo del acceso a los sistemas y recursos informáticos, promoviendo una cultura de ciberseguridad y cumpliendo con la norma ISO 27001:2022, el modelo de seguridad y privacidad de la información MSPI, la política de gobierno digital y las regulaciones del Ministerio de Tecnologías de la Información y las Comunicaciones de Colombia.

Directrices:

Concienciación y Buenas Prácticas:

- Se promoverá la cultura de ciberseguridad mediante capacitación y sensibilización sobre la importancia de las contraseñas seguras y las buenas prácticas de gestión de acceso.
- Los usuarios son responsables de proteger sus claves de acceso y de cumplir con las políticas establecidas.

Gestión de Contraseñas:

Las contraseñas deben cumplir con los siguientes requisitos:

- Mínimo de 8 caracteres alfanuméricos.
- Al menos un carácter especial (!@#$%^&*).
- No contener información personal (nombres, fechas, etc.).
- No ser palabras comunes ni secuencias fáciles de adivinar.
- Las contraseñas deben cambiarse obligatoriamente cada 3 meses o según lo indique la Dirección de Tecnología, Innovación y Ciencia (DTIyC).
- Las nuevas contraseñas deben ser diferentes de las últimas tres utilizadas.
- Las contraseñas deben cambiarse inmediatamente si se sospecha de una brecha de seguridad.

Uso de Contraseñas:

- Las contraseñas son personales e intransferibles.
- No se deben compartir contraseñas con nadie, ni siquiera con personal de la Dirección de Tecnología, Innovación y Ciencia (DTIyC).
- Se debe cerrar sesión al finalizar el uso de un sistema o recurso.
- Se debe utilizar el bloqueo de pantalla cuando se deja el equipo desatendido.

Bloqueo de Cuentas:

- Las cuentas de usuario se bloquearán automáticamente después de tres intentos fallidos de inicio de sesión.
- El desbloqueo de cuentas se realizará únicamente por la Dirección de Tecnología, Innovación y Ciencia (DTIyC), previa solicitud formal del usuario o su jefe inmediato.

Doble Factor de Autenticación (2FA):

- Se recomienda encarecidamente el uso de 2FA para añadir una capa adicional de seguridad al proceso de autenticación.

5.18.1. Responsabilidades del Usuario:

- Cumplir con las directrices de esta política.
- Crear y mantener contraseñas seguras.
- No compartir contraseñas con terceros.
- Reportar cualquier incidente de seguridad relacionado con las claves de acceso.

5.18.2. Responsabilidades de la Dirección de Tecnología, Innovación y Ciencia (DTIyC):

- Establecer y comunicar las políticas de contraseñas.
- Proporcionar herramientas y recursos para la gestión segura de contraseñas.
- Monitorear el cumplimiento de las políticas.
- Investigar y responder a incidentes de seguridad.
- Promover la adopción de 2FA.

5.19 POLÍTICA DE CONTROL DE ACCESO A LA RED CON DOBLE AUTENTICACIÓN PARA LA ALCALDÍA MUNICIPAL DE PALMIRA

Objetivo: Establecer los lineamientos y directrices para el uso seguro y controlado del mecanismo de doble autenticación (2FA) implementado por la Dirección de Tecnología, Innovación y Ciencia (DTIyC) para acceder a los servicios de red de la Alcaldía Municipal de Palmira, incluyendo VPN, conexión inalámbrica y autenticación de equipos institucionales, en cumplimiento con la norma ISO 27001:2022, el modelo de seguridad y privacidad de la información MSPI y la política de gobierno digital.

Directrices:

Asignación de Credenciales:

La Dirección de Tecnología, Innovación y Ciencia (DTIyC) asignará las credenciales de acceso (usuario y contraseña) y tokens de 2FA a los usuarios autorizados, previa solicitud y justificación de necesidad.

La asignación de credenciales para VPN y tokens se basará en los requerimientos de las funciones del usuario y la necesidad de acceso remoto a los servicios informáticos de la Alcaldía.

Uso Responsable:

- Los usuarios son responsables del uso adecuado y confidencial de sus credenciales de acceso y tokens de 2FA.
- El uso de los servicios de red debe ser exclusivamente para fines laborales y en cumplimiento de las funciones asignadas.
- Las conexiones VPN deben realizarse desde entornos seguros y confiables.

Gestión de Tokens:

- Los usuarios deben mantener sus tokens de 2FA en buen estado y reportar inmediatamente cualquier pérdida o robo a la Dirección de Tecnología, Innovación y Ciencia (DTIyC).
- Al finalizar la relación laboral o al no requerir más el token, este debe ser devuelto a la Dirección de Tecnología, Innovación y Ciencia (DTIyC) en las mismas condiciones en que fue entregado.

Monitoreo y Control:

- La Dirección de Tecnología, Innovación y Ciencia (DTIyC) implementará mecanismos de monitoreo y registro de los accesos a la red para detectar y prevenir actividades sospechosas o no autorizadas.
- Se realizarán auditorías periódicas para verificar el cumplimiento de esta política.

5.19.1. Responsabilidades:

Dirección de Tecnología, Innovación y Ciencia:

- Asignar y gestionar las credenciales de acceso y tokens de 2FA.
- Implementar y mantener los mecanismos de doble autenticación.
- Monitorear y controlar el acceso a la red.
- Brindar capacitación y soporte a los usuarios sobre el uso de la doble autenticación.

Usuarios:

- Utilizar los servicios de red de manera responsable y ética.

- Proteger la confidencialidad de sus credenciales de acceso y tokens.
- Reportar cualquier incidente de seguridad o pérdida de tokens a la Dirección de Tecnología, Innovación y Ciencia (DTIyC).
- Cumplir con las políticas y procedimientos de seguridad de la información.

5.20 POLÍTICA DE CONTROL DE ACCESO AL SISTEMA OPERATIVO Y APLICACIONES DE LA ALCALDÍA MUNICIPAL DE PALMIRA

Objetivo: Garantizar la protección de la información y los sistemas de la Alcaldía Municipal de Palmira mediante el control de acceso al sistema operativo, aplicaciones y datos, minimizando el riesgo de acceso no autorizado, pérdida o daño de información, en cumplimiento con la norma ISO 27001:2022, el modelo de seguridad y privacidad de la información MSPI y la política de gobierno digital.

5.20.1 Directrices para el Control de Acceso al Sistema Operativo:

a) Escritorio Limpio: Mantener el escritorio libre de documentos o información confidencial que pueda ser accedida por personas no autorizadas.

b) Bloqueo de Pantalla: Bloquear la pantalla del computador cuando no se esté utilizando o al ausentarse del puesto de trabajo.

c) Impresión Segura: Retirar inmediatamente los documentos confidenciales de la impresora y no dejarlos desatendidos.

d) Equipos Desatendidos: No dejar fotocopiadoras, escáneres, equipos de fax u otros dispositivos desatendidos.

5.20.2 Directrices para el Control de Acceso a Aplicaciones e Información:

Cuentas de Usuario y Contraseñas:

- Las cuentas de usuario y contraseñas son personales, únicas e intransferibles.
- Los usuarios son responsables del uso adecuado de sus credenciales.
- Las contraseñas deben cumplir con los requisitos de complejidad establecidos por la Dirección de Tecnología, Innovación y Ciencia (DTIyC) (longitud mínima, combinación de caracteres, etc.).

- Las contraseñas deben cambiarse periódicamente según las políticas de la Dirección de Tecnología, Innovación y Ciencia (DTIyC).

Gestión de Sesiones:

- Cerrar sesión al finalizar el uso de un sistema o aplicación.
- Bloquear la sesión al ausentarse del puesto de trabajo.
- Bloqueo y Desbloqueo de Cuentas:
- La Dirección de Tecnología, Innovación y Ciencia (DTIyC) es la única entidad autorizada para bloquear y desbloquear cuentas de usuario.
- El desbloqueo se realizará previa solicitud formal del usuario o su jefe inmediato.

Gestión de Privilegios:

- Los privilegios de acceso se otorgarán en función del rol y responsabilidades de cada usuario, siguiendo el principio de mínimo privilegio.
- La Dirección de Tecnología, Innovación y Ciencia (DTIyC) revisará y actualizará periódicamente los privilegios de acceso.

Autenticación de Dos Factores (2FA):

- Se implementará 2FA para fortalecer la seguridad del acceso a sistemas y aplicaciones críticas.

5.20.3 Responsabilidades:

Dirección de Tecnología Innovación y Ciencia:

- Establecer y mantener esta política.
- Implementar y gestionar los controles de acceso.
- Monitorear el acceso a los sistemas y aplicaciones.
- Capacitar a los usuarios sobre las políticas y procedimientos de seguridad.

Usuarios:

- Cumplir con las directrices de esta política.
- Proteger sus credenciales de acceso.
- Reportar cualquier incidente de seguridad.
- Utilizar los sistemas y aplicaciones de forma responsable.

5.21 POLÍTICA DE USO DEL SERVICIO DE WI-FI DE LA ALCALDÍA MUNICIPAL DE PALMIRA

Objetivo: Establecer las directrices, términos y condiciones para el uso seguro y responsable del servicio de Wi-Fi provisto por la Alcaldía Municipal de Palmira, en cumplimiento de la Ley 1712 de 2014, la política de gobierno digital, la norma ISO 27001:2022 y el modelo de seguridad y privacidad de la información MSPI.

5.21.1 Condiciones Generales del Servicio:

Al conectarte a nuestras redes Wi-Fi, aceptas los siguientes términos y condiciones, así como las políticas de seguridad y privacidad de datos de la Alcaldía.

Tipos de acceso:

- **Red de invitados:**
  - Acceso limitado a 2 horas para visitantes y personal externo.
  - Capacidad de navegación restringida.

- **Red de empleados:**
  - Acceso ilimitado para funcionarios y contratistas autorizados.
  - Es obligatorio solicitar el registro de la dirección MAC de tu dispositivo ante la Dirección de Tecnología, Innovación y Ciencia (DTIyC).
  - Mayor ancho de banda para optimizar tu desempeño laboral.

- **Términos de Uso para Visitantes:**
  - **Ancho de Banda:** El ancho de banda de la red de invitados es limitado y compartido, por lo que se espera un uso racional y eficiente por parte de los usuarios.
  - **Disponibilidad del Servicio:** La Alcaldía no garantiza la disponibilidad ininterrumpida del servicio, pudiendo haber limitaciones o interrupciones por mantenimiento o causas de fuerza mayor.
  - **Reconocimiento de Riesgos:** Los visitantes reconocen los riesgos potenciales de utilizar una red Wi-Fi pública y deben tomar precauciones al transmitir información sensible.
  - **Restricciones:** La Alcaldía puede establecer límites de uso, bloquear contenidos inapropiados o restringir el acceso a ciertos servicios para proteger la red.
  - **Requisitos Técnicos:** Los dispositivos deben ser compatibles con los estándares 802.11 b/g/n y WPA2.

5.21.2 Prohibiciones:

Uso Ilegal o Inapropiado:

- Se prohíbe el uso de la red Wi-Fi para actividades ilegales, inmorales, ofensivas o que violen los derechos de terceros.

Actividades Específicamente Prohibidas:

- Compartir contenido ilegal, ofensivo o que viole derechos de autor.
- Realizar ataques de hacking o intrusión a sistemas.
- Difundir virus, malware u otro software malicioso.
- Interferir con el uso de la red por otros usuarios.
- Utilizar la red para fines comerciales no autorizados.
- Violar las políticas de uso aceptable de correo electrónico o plataformas colaborativas.
- Realizar cualquier actividad prohibida por la Ley 1273 de 2009 (Ley de Delitos Informáticos).

5.21.3 Responsabilidad y Soporte:

- **Responsabilidad de la Dirección de Tecnología, Innovación y Ciencia (DTIyC):** Mantener la infraestructura de red y brindar soporte técnico a través de la mesa de ayuda.
- **Responsabilidad del Usuario:** Proteger sus dispositivos con software de seguridad actualizado y utilizar la red de forma responsable. La Alcaldía no se hace responsable por daños a los equipos personales ni por el uso indebido de la red.

5.21.4 Suspensión del Servicio:

- La Dirección de Tecnología, Innovación y Ciencia (DTIyC) puede suspender temporal o definitivamente el acceso a la red Wi-Fi en caso de incumplimiento de esta política, uso indebido de los recursos o actividades que pongan en riesgo la seguridad de la red.

5.22 POLÍTICA DE ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS DE INFORMACIÓN PARA LA ALCALDÍA MUNICIPAL DE PALMIRA

Objetivo: Garantizar la seguridad, integridad y disponibilidad de los sistemas de información a lo largo de su ciclo de vida (adquisición, desarrollo y mantenimiento), en cumplimiento de la norma ISO 27001:2022, el modelo de seguridad y privacidad de la información MSPI, la política de gobierno digital y las regulaciones del Ministerio de Tecnologías de la Información y las Comunicaciones de Colombia.

Directrices:

5.22.1 Requerimientos de Seguridad de los Sistemas de Información:

- **Análisis de Seguridad:** Se realizarán análisis de seguridad periódicos para identificar y mitigar vulnerabilidades en los sistemas de información.
- **Baja de Software:** El software será dado de baja siguiendo los lineamientos establecidos por la Alcaldía.
- **Controles de Seguridad:** Todos los sistemas de información deben incorporar controles de seguridad adecuados para proteger la confidencialidad, integridad y disponibilidad de la información, de acuerdo con las políticas de seguridad informática de la Alcaldía.
- **Documentación y Registro:** Los sistemas desarrollados internamente deben estar debidamente documentados, con versiones controladas y copias de seguridad almacenadas externamente. Además, deben ser registrados ante la Dirección Nacional de Derechos de Autor.
- **Gestión de Adquisiciones:** Toda adquisición de hardware y software debe ser gestionada por la Dirección de Tecnología, Innovación y Ciencia (DTIyC) para garantizar su compatibilidad, seguridad y cumplimiento de las políticas de la Alcaldía.
- **Instalación de Software:** La instalación de software en los equipos de la Alcaldía es exclusiva de la Dirección de Tecnología, Innovación y Ciencia (DTIyC).
- **Licencias de Software:** La compra de licencias de software permite a la Dirección de Tecnología, Innovación y Ciencia (DTIyC) realizar una copia de seguridad. Cualquier otra copia se considera no autorizada y su uso está sujeto a sanciones.
- **Restricciones de Uso:** Se prohíbe la copia o distribución de software a terceros, así como la instalación y uso de juegos en los equipos de la Alcaldía.

5.22.2 Controles Criptográficos:

- **Protección de Información Sensible:** La Dirección de Tecnología, Innovación y Ciencia (DTIyC) verificará que los sistemas que transmiten información clasificada utilicen herramientas de cifrado de datos.
- **Herramientas de Cifrado:** La Dirección de Tecnología, Innovación y Ciencia (DTIyC) proporcionará herramientas de cifrado a los usuarios que las soliciten formalmente.
- **Uso de Criptografía:** Se utilizarán controles criptográficos para proteger claves de acceso, información clasificada transmitida fuera de la Alcaldía, y cualquier otra información que el Comité de Seguridad de la Información considere necesaria.

5.22.3 Gestión de Vulnerabilidades Técnicas:

- **Pruebas de Penetración:** La Dirección de Tecnología, Innovación y Ciencia (DTIyC) coordinará con un tercero especializado la realización de pruebas de Ethical Hacking cada 12 meses para identificar vulnerabilidades técnicas.
- **Planes de Acción:** La Dirección de Tecnología, Innovación y Ciencia (DTIyC) generará, ejecutará y monitoreará planes de acción para mitigar las vulnerabilidades detectadas en las pruebas.
- **Actualización de Software:** Se mantendrá el software actualizado con los últimos parches de seguridad para minimizar el riesgo de explotación de vulnerabilidades conocidas.
- **Monitoreo Continuo:** Se implementarán herramientas de monitoreo continuo de vulnerabilidades para detectar nuevas amenazas y aplicar medidas de mitigación de forma proactiva.

5.22.4 Responsabilidades:

Dirección de Tecnología, Innovación y Ciencia (DTIyC):

- Implementar y mantener esta política.
- Gestionar la adquisición, desarrollo y mantenimiento de los sistemas de información.
- Asegurar el cumplimiento de los requisitos de seguridad.
- Realizar análisis de riesgos y vulnerabilidades.
- Proporcionar herramientas de seguridad y capacitación a los usuarios.

Usuarios:

- Utilizar los sistemas de información de forma responsable y ética.
- Reportar cualquier incidente de seguridad.
- Cumplir con las políticas y procedimientos de seguridad.

5.23 POLÍTICA DE GESTIÓN DISCIPLINARIA DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN PARA LA ALCALDÍA MUNICIPAL DE PALMIRA

Objetivo: Asegurar la detección, comunicación y gestión oportuna de eventos e incidentes de seguridad que afecten los activos de información de la Alcaldía Municipal de Palmira, siguiendo los procedimientos establecidos y aplicando medidas correctivas y disciplinarias según corresponda, en cumplimiento de la norma ISO 27001:2022, el modelo de seguridad y privacidad de la información MSPI, la política de gobierno digital y las regulaciones del Ministerio de Tecnologías de la Información y las Comunicaciones de Colombia.

5.23.1 Proceso de Gestión de Incidentes:

a) Detección: Identificar y reportar de inmediato cualquier evento o incidente de seguridad a la Dirección de Tecnología, Innovación y Ciencia (DTIyC).

b) Análisis: La Dirección de Tecnología, Innovación y Ciencia (DTIyC) evaluará el impacto y la gravedad del incidente, determinando las acciones a tomar.

c) Contención: Implementar medidas para limitar el daño y evitar la propagación del incidente.

d) Erradicación: Eliminar la causa del incidente y restaurar los sistemas afectados.

e) Recuperación: Restaurar la normalidad de las operaciones y la disponibilidad de los servicios.

f) Lecciones Aprendidas: Documentar el incidente, analizar las causas y tomar medidas para prevenir futuros incidentes.

5.23.2 Actuaciones que Constituyen Violación de la Seguridad de la Información:

- No firmar los acuerdos de confidencialidad.
- No reportar incidentes de seguridad.
- No actualizar la información de los activos a cargo.
- Clasificar o almacenar información de forma inadecuada.
- Dejar información confidencial desprotegida.
- Permitir el acceso no autorizado a instalaciones o información.
- Utilizar recursos tecnológicos para fines personales o no autorizados.
- Divulgar información confidencial sin autorización.
- Utilizar software no autorizado o realizar modificaciones no permitidas en los sistemas.
- No seguir los procedimientos de eliminación segura de información.
- No cumplir con las medidas de protección de activos de información.
- Cualquier otra acción que ponga en riesgo la seguridad de la información.

5.23.3 Responsabilidades:

- **Todos los usuarios:** Cumplir con las políticas de seguridad de la información y reportar cualquier incidente o sospecha de violación.
- **Dirección de Tecnología, Innovación y Ciencia (DTIyC):** Gestionar los incidentes de seguridad, aplicar medidas correctivas y colaborar con Talento Humano en el proceso disciplinario.
- **Talento Humano:** Llevar a cabo el proceso disciplinario de acuerdo con la normativa vigente.

5.24 POLÍTICA DE TERCERIZACIÓN U OUTSOURCING DE SERVICIO PARA LA ALCALDÍA MUNICIPAL DE PALMIRA

Objetivo: Esta política establece los lineamientos y controles para gestionar de forma segura y eficiente la tercerización de servicios que involucren el acceso, procesamiento, almacenamiento o transmisión de información institucional de la Alcaldía Municipal de Palmira, garantizando la protección de los activos de información y el cumplimiento de los requisitos legales y regulatorios.

5.24.1 Evaluación y selección de proveedores

a) Análisis de riesgos: Antes de iniciar cualquier proceso de tercerización, se realizará un análisis de riesgos exhaustivo para identificar y evaluar los posibles impactos en la seguridad, confidencialidad, integridad y disponibilidad de la información institucional.

b) Criterios de selección: Se establecerán criterios de selección rigurosos para los proveedores, considerando su experiencia, reputación, capacidad técnica, financiera y cumplimiento de estándares de seguridad y privacidad de la información (ISO 27001 u otros equivalentes).

c) Debida diligencia: Se realizará una debida diligencia de los proveedores seleccionados, verificando su historial, referencias, certificaciones y cumplimiento de las leyes y regulaciones aplicables.

5.24.2 Formalización de acuerdos

- **Contratos:** Todos los servicios tercerizados se formalizarán mediante contratos que incluyan cláusulas específicas sobre seguridad de la información, confidencialidad, niveles de servicio, responsabilidades, gestión de incidentes, auditorías y terminación del contrato.
- **Acuerdos de confidencialidad:** Se firmarán acuerdos de confidencialidad (NDA) con todos los proveedores que tengan acceso a información clasificada como sensible o confidencial, de acuerdo con la guía para la calificación de la información de la Alcaldía.
- **Acuerdos de nivel de servicio (SLA):** Se establecerán SLA claros y medibles para garantizar el cumplimiento de los niveles de servicio acordados y la continuidad de las operaciones.

5.24.3 Gestión y supervisión de proveedores

- **Monitoreo continuo:** La Dirección de Tecnología, Innovación y Ciencia (DTIyC) realizará un monitoreo continuo del desempeño de los proveedores, verificando el cumplimiento de los acuerdos contractuales y los niveles de servicio.

- **Auditorías:** Se realizarán auditorías periódicas a los proveedores para evaluar la efectividad de sus controles de seguridad y privacidad de la información.
- **Gestión de incidentes:** Se establecerán procedimientos para la gestión de incidentes de seguridad que involucren a proveedores, incluyendo la notificación, investigación y respuesta oportuna.

5.24.4 Terminación de contratos

- **Devolución de información:** Al finalizar el contrato, el proveedor deberá devolver toda la información institucional en su poder, en un formato acordado y de forma segura.
- **Borrado seguro:** El proveedor deberá garantizar el borrado seguro de toda la información institucional de sus sistemas y dispositivos.

5.25 POLÍTICA DE RESPALDO Y RECUPERACIÓN DE INFORMACIÓN EN GOOGLE WORKSPACE

Objetivo

Definir los **lineamientos para la generación y gestión de copias de seguridad** de la información institucional de la Alcaldía Municipal de Palmira, específicamente la almacenada en **Google Workspace (Drive y Correo electrónico)**. El objetivo principal es **garantizar la disponibilidad, integridad y recuperabilidad** de dicha información para todo el personal que utilice estos servicios, así como para las áreas involucradas en su supervisión, asegurando la continuidad operacional y el cumplimiento de la normativa de seguridad y privacidad.

5.25.1 Principios Generales

- La información institucional almacenada en Google Workspace es un activo crítico que debe ser protegido mediante **copias de seguridad periódica y verificable**.
- Se deben establecer **procedimientos claros y responsabilidades definidas** para la generación, almacenamiento y recuperación de las copias de seguridad.
- Las copias de seguridad deben ser almacenadas en un **lugar seguro y con acceso restringido**, garantizando su confidencialidad e integridad.
- Se deben realizar **pruebas periódicas de restauración** para verificar la efectividad de las copias de seguridad y los procedimientos de recuperación.
- Todo el personal debe ser consciente de la importancia de la seguridad de la información y cumplir con las políticas y procedimientos establecidos.

Referirse al **AIFIT-009 INSTRUCTIVO COPIAS DE SEGURIDAD DEL DRIVE GOOGLE.**

5.25.2 Directrices

Respaldo Completo (Correo y Drive)

Para realizar copias de seguridad completas de tu correo electrónico y archivos de Google Drive, se **debe usar Google Takeout**.

- **Accede a Google Takeout:** Ve a https://takeout.google.com/ e inicia sesión con su cuenta institucional de Google.
- **Selecciona Datos:** Desmarca todas las opciones predeterminadas y selecciona específicamente **"Correo" y "Drive"** para la exportación.
- **Selección Opcional de Carpetas de Drive:** Si necesitas respaldar menos información, puedes seleccionar carpetas específicas dentro de Google Drive en lugar de descargar todo el contenido.
- **Configura la Exportación:** Elige "Enviar enlace de descarga por correo electrónico" como tipo de entrega y ".zip" como formato de archivo. El tamaño máximo del archivo de exportación se debe configurar según tus necesidades o las directrices de la DTIC.
- **Inicia la Exportación y Descarga:** Una vez que inicies la exportación, recibirás un enlace de descarga por correo electrónico. **Es obligatorio que descargues los archivos antes de que el enlace expire** (normalmente en una semana) y los guardes en una ubicación segura y bajo tu control o el de tu área.

5.25.3 Respaldo Manual de Google Drive (Parcial)

Para descargar archivos y carpetas de Google Drive de forma selectiva, sigue estos pasos:

- **Accede a Google Drive:** Ve a tu Google Drive institucional a través de https://drive.google.com/.
- **Selecciona Contenido:** Elige los archivos y carpetas que deseas respaldar (usa Ctrl o Cmd para seleccionar múltiples elementos, o simplemente selecciona una carpeta para incluir todo su contenido).
- **Descarga Archivos:** Haz clic derecho sobre los elementos seleccionados y elige la opción **"Descargar"**. Google Drive comprimirá los archivos en formato .zip para la descarga.
- **Almacenamiento Local: Debes guardar** los archivos .zip descargados en una ubicación segura en tu equipo local o en un dispositivo de almacenamiento externo.

- **Capacidad de Almacenamiento:** Es responsabilidad del usuario o del área asegurar que se dispone de suficiente espacio de almacenamiento en el equipo local o en dispositivos externos para guardar las copias de seguridad.
- **Seguridad del Respaldo:** Las copias de seguridad descargadas deben ser almacenadas en un lugar seguro y protegido contra accesos no autorizados. Se recomienda el uso de contraseñas para proteger los archivos .zip si la información es sensible.
- **Verificación de Integridad:** Posterior a la descarga, es mandatorio que el personal verifique la integridad del archivo .zip y que los archivos y carpetas esperados estén presentes y sean accesibles. Esta verificación es crucial para garantizar que el respaldo se realizó correctamente.
- **Frecuencia de los Respaldos:** La frecuencia de los respaldos será definida por la DTIC en coordinación con cada dependencia, basándose en la criticidad y la volatilidad de la información.

5.25.4 Responsabilidades

Dirección de Tecnología, Innovación y Ciencia (DTIC)

La DTIC será la responsable principal de la implementación y supervisión de esta política, incluyendo, pero no limitándose a:

- **Establecer y actualizar** los procedimientos técnicos para la generación, verificación y restauración de las copias de seguridad.
- **Asegurar el cumplimiento** de las políticas de seguridad y privacidad de la información durante todo el ciclo de vida de las copias de seguridad.
- **Diseñar y ejecutar** programas de capacitación para el personal encargado de la generación y gestión de las copias de seguridad.
- **Supervisar y controlar** la correcta ejecución del proceso de generación de copias de seguridad.
- **Gestionar los recursos tecnológicos** necesarios para el almacenamiento seguro de las copias de seguridad.

Personal Encargado de la Generación de Copias de Seguridad

Este rol será asignado por la DTIC y será responsable de:

- **Ejecutar los procedimientos** establecidos para la generación de copias de seguridad, utilizando las herramientas y métodos definidos.
- **Verificar la integridad y consistencia** de las copias de seguridad generadas.

- **Reportar de forma inmediata** cualquier anomalía, incidente o error detectado durante el proceso de generación de copias.
- **Mantener actualizados** los registros y la documentación relacionada con el proceso de generación de copias de seguridad.

Secretarios, Directores y Jefes de Dependencia

Estos roles serán responsables de:

- **Colaborar con la DTIC** en la identificación y clasificación de la información crítica de sus respectivas áreas que requiera respaldo.
- **Asegurar que el personal a su cargo** conozca y cumpla con los procedimientos establecidos para la generación de copias de seguridad.
- **Participar activamente** en las pruebas de restauración de las copias de seguridad cuando sea requerido.

Usuarios Finales

Todos los usuarios del Drive institucional y del correo electrónico de la Alcaldía Municipal de Palmira son responsables de:

- **Cumplir estrictamente** con las políticas de uso del Drive institucional.
- **Reportar a la DTIC** cualquier incidente o problema relacionado con la información almacenada en el Drive institucional que pueda afectar su disponibilidad o integridad.
- **Colaborar con la DTIC** en el proceso de restauración de la información en caso de ser necesario.

5.25.5 Auditoría y Cumplimiento

La DTIC realizará auditorías periódicas para asegurar el cumplimiento de esta política. El incumplimiento de las disposiciones aquí establecidas puede acarrear sanciones de acuerdo con el régimen disciplinario interno de la Alcaldía Municipal de Palmira y la normativa legal vigente en materia de seguridad de la información y protección de datos personales.

5.26 POLÍTICA PARA GUARDAR INFORMACIÓN INSTITUCIONAL EN EL PC

Objetivo

Establecer los lineamientos para el almacenamiento seguro y adecuado de la información institucional en los computadores de escritorio y portátiles (PC) de la Alcaldía Municipal de Palmira, garantizando la **confidencialidad**, **integridad** y **disponibilidad** de los datos, y cumpliendo con las políticas de seguridad y privacidad de la entidad.

5.26.1 Directrices Generales

- **Uso exclusivo de recursos institucionales**: La información institucional, sin importar su formato (documentos, bases de datos, imágenes, etc.), debe almacenarse únicamente en los sistemas y dispositivos de almacenamiento provistos por la Alcaldía. Esto incluye el **Drive institucional en Google Workspace** y otros servidores o repositorios designados por la Dirección de Tecnología, Innovación y Ciencia (DTIyC).
- **Prohibición de almacenamiento en local**: Se prohíbe el almacenamiento de información institucional de manera permanente en el disco duro local de los computadores. Los usuarios podrán guardar archivos temporalmente en el PC solo para la ejecución de sus funciones laborales inmediatas, pero deberán moverlos al Drive institucional tan pronto como finalicen su tarea.
- **Responsabilidad del usuario**: Cada usuario es responsable de la información que genera y maneja. Esto incluye clasificarla correctamente, protegerla del acceso no autorizado y asegurarse de que se almacene en los sistemas designados por la DTIyC para garantizar su respaldo y seguridad.
- **Información personal**: Queda prohibido almacenar información personal, como documentos privados, fotos, música o videos, en los equipos de la Alcaldía. El uso del PC es exclusivamente para fines laborales.
- **Respaldo y recuperación**: La DTIyC no se hace responsable del respaldo de la información almacenada en los discos duros locales de los PC, ya que el respaldo oficial y seguro se realiza únicamente en los sistemas de almacenamiento institucionales. La pérdida de información guardada en el PC local será responsabilidad del usuario.

Procedimiento para el Almacenamiento

1. **Generación y edición**: Los usuarios pueden crear o editar documentos y archivos institucionales en su PC, utilizando software autorizado.
2. **Almacenamiento temporal**: Durante la creación o edición, el archivo puede permanecer en el disco duro local, por ejemplo, en la carpeta "Documentos" o en el escritorio.
3. **Transferencia al Drive institucional**: Una vez que el trabajo en el archivo haya finalizado, o al terminar la jornada laboral, el usuario debe mover el documento a la carpeta correspondiente dentro del **Drive institucional**.

4. **Clasificación de la información**: Al guardar la información en el Drive, se debe seguir la estructura documental y clasificar los archivos según su nivel de confidencialidad (Pública, Pública Clasificada o Pública Reservada), tal como lo define la **Política de Clasificación de la Información**.

6. DOCUMENTOS RELACIONADOS

- Política de Seguridad y Privacidad de la Información.
- AIFMN-005 Manual de Políticas de Seguridad y Privacidad de la Información del Municipio de Palmira.
- AIFPR-018 Procedimiento lineamientos para la formulación de proyectos de sistemas de información y proyectos de innovación.
- 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.
- AIFIT-008 Instructivo para guardar información institucional digital en los pc
- AIFIT-009 Instructivo copias de seguridad del drive.
- AIFFO-015 Compromiso de Confidencialidad, Integridad Y Disponibilidad de La Información

7. ANEXOS

- Anexo 01 AIFFO-015 Compromiso de Confidencialidad, Integridad Y Disponibilidad de La Información.

8. CONTROL DE CAMBIOS

Fecha	Versión Inicial	Identificación del Cambio	Versión Final
24/10/2017	N.A	Creación del documento	01
19/07/2019	01	Actualización y Estructuración ISO 27001	02

17/09/2021	02	Actualización	03
26/12/2022	03	Actualización	04
24/09/2025	04	De acuerdo a la actualización de la política de seguridad y privacidad de la información, se cambia todo el documento del manual	05

9. CONTROL DE REVISIÓN Y APROBACIÓN

Elaborado por:		Revisado por:		Aprobado por:	
Nombre:	Darwin Vélez López	**Nombre:**	Ángela María Valencia Bránd	**Nombre:**	Andrés Mauricio Hormaza Tobón
Cargo:	Profesional Especializado G03	**Cargo:**	Profesional Especializado G03	**Cargo:**	Director de Tecnología, Innovación y Ciencia