ALCALDÍA MUNICIPAL DE PALMIRA

VALLE DEL CAUCA

PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

DIRECCION DE TECNOLOGIA INNOVACION Y CIENCIA

PALMIRA VALLE
2024-2027

Tabla de contenido

INTRODUCCIÓN

Los grandes volúmenes de información institucionales se originan desde diversas fuentes y con estándares tecnológicos heterogéneos en hardware, software, comunicaciones que requieren de una infraestructura de red adecuada, funcional y confiable para su transmisión y almacenamiento. En el caso del Municipio de Palmira, las soluciones de conectividad y servicios informáticos fueron diseñadas fundamentalmente para soportar aplicaciones de procesamiento de datos.

El crecimiento exponencial de nuevos servicios y aplicaciones ha generado un conjunto de necesidades en la operación de la red y en la gestión de la seguridad de la información, elementos que han estado en una arriesgada prioridad en el dimensionamiento tecnológico institucional. En el marco de las TI se hace necesaria la implementación de estrategias de seguridad para preservar los servicios disponibles y garantizar la confidencialidad e integridad de los datos en las aplicaciones.

Existen algunos estándares de seguridad informática que sugieren, como primera medida realizar análisis de vulnerabilidades para responder corrigiendo posibles fallos y apuntando a modelos preventivos. Estos esfuerzos son inocuos, sin la implementación de un Sistema Integral de la Seguridad de la Información.

El presente documento pretende exponer una serie de lineamientos para implementar las mejores prácticas de Seguridad Informática en la Alcaldía Municipal de Palmira, con el fin de optimizar la disponibilidad, la integridad, la confidencialidad/privacidad, entre otros principios relevantes, teniendo en cuenta la infraestructura y limitaciones actuales.

1. POLÍTICA DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

La Política de Seguridad y Privacidad de la Información es la declaración general que representa la posición del Municipio de Palmira con respecto a la protección de los activos de información (los funcionarios, contratistas, terceros, la información, los procesos, las tecnologías de información incluido el hardware y el software), que soportan los procesos de la Entidad y apoyan la implementación del Sistema de Gestión de Seguridad de la Información, por medio de la generación y publicación de sus políticas, procedimientos e instructivos, así como de la asignación de responsabilidades generales y específicas para la gestión de la seguridad de la información.

El Municipio de Palmira, para asegurar el direccionamiento estratégico de la Entidad, establece la compatibilidad de la política y de los objetivos de seguridad de la información.

a) Mitigar el riesgo de la entidad.

b) Cumplir con los principios de seguridad de la información.

c) Cumplir con los principios de la función administrativa.

d) Mantener la confianza de los funcionarios, contratistas y terceros.

e) Apoyar la innovación tecnológica.

f) Implementar el sistema de gestión de seguridad de la información.

g) Proteger los activos de información.

h) Establecer las políticas, procedimientos e instructivos en materia de seguridad de la información.

j) Fortalecer la cultura de seguridad de la información en los funcionarios y clientes externos del municipio.

k) Garantizar la continuidad del servicio frente a incidentes.

1.1.Nivel de cumplimiento

A continuación, se establecen los doce (12) Lineamientos de la Política de Seguridad que soportan el Modelo de Seguridad y Protección de la Información - MSPI de la Administración Central del Municipio de Palmira, conforme a las orientaciones del Ministerio de Tecnologías de la Información y las Comunicaciones -MINTIC.

1. La Administración Central del Municipio de Palmira ha decidido definir, implementar, operar y mejorar de forma continua un Modelo de Seguridad y Privacidad de la Información, soportado en lineamientos claros alineados a las necesidades del negocio y a los requerimientos regulatorios que le aplican a su naturaleza.

2. Las responsabilidades frente a la seguridad de la información serán definidas, compartidas, publicadas y aceptadas por cada uno de los empleados, contratistas o terceros.
3. La Administración Central del Municipio de Palmira protegerá la información generada, procesada o resguardada por los procesos de negocio y activos de información que hacen parte de los mismos.
4. La Administración Central del Municipio de Palmira protegerá la información creada, procesada, transmitida o resguardada por sus procesos de negocio, con el fin de minimizar impactos financieros, operativos o legales debido a un uso incorrecto de esta. Para ello es fundamental la aplicación de controles de acuerdo con la clasificación de la información de su propiedad o en custodia.
5. La Administración Central del Municipio de Palmira protegerá su información de las amenazas originadas por parte del personal.
6. La Administración Central del Municipio de Palmira protegerá las instalaciones de procesamiento y la infraestructura tecnológica que soporta sus procesos críticos.
7. La Administración Central del Municipio de Palmira controlará la operación de sus procesos de negocio garantizando la seguridad de los recursos tecnológicos y las redes de datos.
8. La Administración Central del Municipio de Palmira implementará control de acceso a la información, sistemas y recursos de red.
9. La Administración Central del Municipio de Palmira garantizará que la seguridad sea parte integral del ciclo de vida de los sistemas de información.
10. La Administración Central del Municipio de Palmira garantizará una adecuada gestión de debilidades, eventos e incidentes de seguridad de la información asociada con los sistemas de información de la entidad
11. La Administración Central del Municipio de Palmira garantizará la disponibilidad de sus procesos de negocio y la continuidad de su operación considerando el impacto que pueden generar los eventos.
12. La Administración Central del Municipio de Palmira garantizará el cumplimiento de las obligaciones legales, regulatorias y contractuales establecidas.

El incumplimiento a la política de seguridad y privacidad de la información traerá consigo las consecuencias legales y/o disciplinarias que apliquen a la normativa de la Entidad, incluyendo lo establecido en las normas que competen al gobierno nacional y territorial que estén relacionadas con la seguridad y privacidad de la información.

2. IMPLEMENTACIÓN DE POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN

2.1. Justificación.

El Municipio de Palmira con el propósito de salvaguardar la información de la entidad en todos sus aspectos, garantizando la seguridad de los datos y el cumplimiento de las normas legales, ha establecido realizar un Plan de Seguridad y Privacidad de la información con el ánimo de que no se presenten pérdidas, robos, accesos no autorizados y duplicación de la misma, igualmente promueve una política de seguridad de la información física y digital de acuerdo a la caracterización de los usuarios tanto internos como externos.

La seguridad de la información se entiende como la preservación de las siguientes características:

a) **Confidencialidad**: se garantiza que la información sea accesible sólo a aquellas personas autorizadas a tener acceso a la misma.

b) **Integridad**: se salvaguarda la exactitud y totalidad de la información y los métodos de procesamiento.

c) **Disponibilidad**: se garantiza que los usuarios autorizados tengan acceso a la información y a los recursos relacionados con la misma, toda vez que lo requieran.

Adicionalmente, debe considerarse los conceptos de:

a) **Auditabilidad**: define que todos los eventos de un sistema deben poder ser registrados para su control posterior.

b) **Protección a la duplicación:** consiste en asegurar que una transacción sólo se realiza una vez, a menos que se especifique lo contrario. Impedir que se grabe una transacción para luego reproducirla, con el objeto de simular múltiples peticiones del mismo remitente original.

c) **No repudio:** se refiere a evitar que una entidad que haya enviado o recibido información alegue ante terceros que no la envió o recibió.

d) **Legalidad:** referido al cumplimiento de las leyes, normas, reglamentaciones o disposiciones a las que está sujeto el Organismo.

e) **Confiabilidad de la Información:** es decir, que la información generada sea adecuada para sustentar la toma de decisiones y la ejecución de las misiones y funciones.

A los efectos de una correcta interpretación del presente Plan, se realizan las siguientes definiciones:

a) **Información:** se refiere a toda comunicación o representación de conocimiento como datos, en cualquier forma, con inclusión de formas textuales, numéricas, gráficas, cartográficas, narrativas o audiovisuales,

y en cualquier medio, ya sea magnético, en papel, en pantallas de computadoras, audiovisual u otro.

b) **Sistema de Información:** se refiere a un conjunto independiente de recursos de información organizados para la recopilación, procesamiento, mantenimiento, transmisión y difusión de información según determinados procedimientos, tanto automatizados como manuales.

c) **Tecnología de la Información:** se refiere al hardware y software operados la entidad o por un tercero que procese información en su nombre, para llevar a cabo una función propia del Organismo, sin tener en cuenta la tecnología utilizada, ya se trate de computación de datos, telecomunicaciones u otro tipo.

2.2. Objetivo

Definir los mecanismos y todas las medidas necesarias por parte del Municipio de Palmira, tanto técnica, lógica, física, legal y ambiental para la protección de los activos de información, los recursos y la tecnología de la entidad, con el propósito de evitar accesos no autorizados, divulgación, duplicación, interrupción de sistemas, modificación, destrucción, pérdida, robo, o mal uso, que se pueda producir de forma intencional o accidental, frente a amenazas internas o externas, asegurando el cumplimiento de la confidencialidad, integridad, disponibilidad, legalidad y confiabilidad de la información.

2.3.Alcance

Este Plan de Seguridad y Privacidad de la Información y su política, son aplicables a todos los funcionarios del Municipio de Palmira, a sus recursos, procesos y procedimientos tanto internos como externos, así mismo al personal vinculado a la entidad y terceras partes, que usen activos de información que sean propiedad de la entidad.

2.4.Roles y Responsabilidades

Es responsabilidad de la Dirección de Tecnología, Innovación y Ciencia, del Municipio de Palmira, la implementación, aplicación, seguimiento y autorizaciones de la Política y las Políticas del Plan de Seguridad y Privacidad de la información en las diferentes áreas y procesos de la entidad, además garantiza el apoyo y el uso de la Política y las Políticas de Seguridad de la Información como parte de su herramienta de gestión, las cuales deberán ser aplicada de forma obligatoria por todos los funcionarios para el cumplimiento de los objetivos. Para tal efecto, todos los funcionarios, contratistas y terceros que intervengan en la producción y administración de información, deberán firmar el Compromiso de Confidencialidad, Integridad y Disponibilidad de la información, establecido en la Administración central del Municipio de Palmira. (Ver Anexo 001).

Es responsabilidad de la Dirección de Tecnología, Innovación y Ciencia, del Municipio de Palmira, la

actualización y seguimiento a las actividades del presente plan.

El Comité Institucional de Gestión y Desempeño deberá revisar y aprobar este plan anualmente.

2.5.Descripción de Actividades

ITEM	ACTIVIDAD	CICLO PHVA	RESPONSABLE	REGISTRO
1	Actualizar y formalizar el compromiso de la alta dirección, con los objetivos y política de seguridad.	A	Director(a)	Actas de reunión
2	1.1 Analizar la información relacionada con modelo de seguridad y privacidad de la información (MSPI)	H	Contratistas Profesional Universitario Profesional Especializado	-Informes -Seguimientos mediante Instrumentos de Evaluación
3	1.2 Analizar y Actualizar la Política de Seguridad y Privacidad de la Información	A	Director(a) Contratistas Auxiliar Administrativo Profesional Universitario Profesional Especializado	-Manual de Políticas de Seguridad y Privacidad de la Información -AIFFO-015 Formato de Compromiso de Confidencialidad, Integridad y disponibilidad de la Información -Resolución No.094 del 03 de Septiembre de 2025 - "POR MEDIO DE LA CUAL SE DEROGA LA RESOLUCIÓN 012 DEL 22 DE ABRIL DE 2022 Y SE ESTABLECEN NUEVOS LINEAMIENTOS DE LA POLÍTICA DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN"

4	1.3 Revisar y actualizar el Manual de Políticas de Seguridad y Privacidad de la Información	A	Director(a) Contratistas Profesional Universitario Profesional Especializado	-Manual de Políticas de Seguridad y Privacidad de la Información -AIFFO-015 Formato de Compromiso de Confidencialidad, Integridad y disponibilidad de la Información -Resolución No.094 del 03 de Septiembre de 2025 - "POR MEDIO DE LA CUAL SE DEROGA LA RESOLUCIÓN 012 DEL 22 DE ABRIL DE 2022 Y SE ESTABLECEN NUEVOS LINEAMIENTOS DE LA POLÍTICA DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN"
5	6.1 Identificar los sistemas de información, plataformas y servicios que requieren la renovación del soporte, actualización y mantenimiento del licenciamiento	P	Director(a) Contratistas Profesional Universitario Profesional Especializado	-Matriz de licencias -Servicios Tercerizados
6	6.2 Garantizar el soporte, actualización y mantenimiento del licenciamiento de las herramientas, plataformas, servicios y sistemas de información que hacen parte de la infraestructura tecnológica de la entidad	A	Director(a) Contratistas Profesional Universitario Profesional Especializado	-Seguimiento a la Matriz de licencias -Seguimiento a los Servicios Tercerizados
7	7.1 Realizar acciones encaminadas al mejoramiento de la plataforma de seguridad perimetral - Firewall	P	Director(a) Contratistas Profesional Universitario	-Informes de afinamientos y actualizaciones de políticas de Firewall

			Profesional Especializado	
8	7.2 Presentación de informe relacionado con la implementación de Políticas de Seguridad en la nueva plataforma de seguridad perimetral	A	Contratistas Operador Profesional Universitario Profesional Especializado	-Informes de afinamientos y actualizaciones de políticas de Firewall
9	7.3 Parametrización y generación de informes de seguridad producto de la plataforma fortianalyzer	A	Contratistas Operador Profesional Universitario Profesional Especializado	-Informes Firewall
10	7.4 Realizar técnicas de Ethical Hacking	A	Contratistas Operador Profesional Universitario Profesional Especializado	- Informe Pentesting_Externo - Informe Pentesting segmento Red
11	7.5 Aplicación de sugerencias/mejoras/correcciones del ejercicio de Ethical Hacking	A	Contratistas Profesional Universitario Profesional Especializado	-Informes sobre Remediaciones Ethical Hacking
12	7.6 Realizar pruebas de ingeniería social	V	Contratistas Profesional Universitario Profesional especializado Profesional Especializado	-Listados de Asistencia a capacitaciones -Evidencias Fotográficas -Informe Phishing

13	8.1 Revision y actualizacion de Guia de gestion y clasificación de incidentes de seguridad	A	Contratistas Profesional Universitario Profesional Especializado	-Gestión de incidentes de seguridad
14	8.2 Registro de comunicaciones enviadas y recibidas con el Colcert	H	Contratistas Profesional Universitario Profesional Especializado	-Consultas y comunicaciones realizadas
15	9.1 Actualizar los Activos de Información de la dirección de tecnología (Aplicación RUACI)	H	Contratistas Profesional Universitario Profesional especializado	-Aplicativo RUACI
16	9.2 Aprobar por el inventario de activos de información de cada área	H	Contratistas Profesional Universitario Profesional Especializado	-Aplicativo RUACI -Reporte generado del Aplicativo RUACI
17	9.3 Publicar los activos de información de la administración municipal.	A	Contratistas Profesional Universitario Profesional Especializado	-Publicación en la página web institucional
18	11 Proceso de identificación de infraestructura crítica	P	Contratistas Profesional Universitario Profesional Especializado	- informe infraestructura critica actualizado
19	12.1 Identificar, valorar, evaluar y formular el Plan de Tratamiento de Riesgo de Seguridad Digital de Dirección de TIyC	P	Contratistas Profesional Universitario Profesional Especializado	-Aplicativo RUACI -Plan de Tratamiento de Riesgos de Seguridad de la Información
20	12.2 Realizar Seguimiento a la implementación de Planes de Tratamiento de Riesgos de Seguridad Digital	V	Contratistas Profesional Universitario	-Aplicativo RUACI -Plan de Tratamiento de Riesgos de Seguridad de la Información

			Profesional Especializado	
21	14.1 Sensibilización en Privacidad y Seguridad de la Información en Ingeniería Social	H	Contratistas Profesional Universitario Profesional Especializado	-Actas de reuniones -Listados de Asistencia -Evidencias Fotográficas
22	14.2 Publicar en los medios oficiales de la Administración la Política de Seguridad y Privacidad de la Información y Manual de Políticas de Seguridad y Privacidad de la Información	A	Contratistas Profesional Universitario Profesional Especializado	-Publicación en la página web institucional, correo institucional, Intranet.
23	14,3 Realizar actividades/campañas de socialización de la Política de Seguridad y Privacidad de la Información y Manual de Políticas de Seguridad y Privacidad de la Información	H	Contratistas Profesional Universitario Profesional Especializado	-Actas de reuniones -Listados de Asistencia -Evidencias Fotográficas
24	14.4 Realizar actividades/campañas de socialización de estrategia de administración de la data institucional encaminadas en el marco de la Política de Seguridad y Privacidad de la Información y Manual de Políticas de Seguridad y Privacidad de la Información	H	Contratistas Profesional Universitario Profesional Especializado	-Actas de reuniones -Listados de Asistencia -Evidencias Fotográficas
25	15.3 Implementación del esquema de gestión y almacenamiento de backups seleccionado en la actividad 15.1	H	Contratistas Profesional Universitario Profesional Especializado	- AIFIT-009 Instructivo Copias de Seguridad del Drive Google

				- AIFIT-xx Instructivo copias de seguridad del PC
26	16.1 Realizar una auditoría de seguridad de la información, con el objetivo de medir el nivel de maduración del MSPI	V	Oficina de Control Interno	-Informe de auditoría

2.6.Cumplimiento

El cumplimiento de la Política y las Políticas de Seguridad y Privacidad de la Información es obligatorio. Si los funcionarios de la entidad o terceros violan este plan, el Municipio de Palmira se reserva el derecho de tomar las medidas correspondientes.

2.7.Comunicación

Mediante socialización a todos los funcionarios de la Administración Central de Palmira se dará a conocer el contenido del documento de la política, las políticas de seguridad Compromiso de Confidencialidad de información de información, así mismo se deberá informar a los contratistas y/o terceros en el momento que se requiera con el propósito de realizar los ajustes y la retroalimentación necesaria para dar cumplimiento efectivo al plan.

Todos los funcionarios, contratistas y/o terceros de la entidad deben conocer la existencia de la política, las políticas, el compromiso de confidencialidad de información y la obligatoriedad de su cumplimiento; la ubicación física del documento estará a cargo del Sistema de Gestión Integrado para que sean consultados en el momento que se requieran, igualmente estarán alojados en la página de la entidad www.palmira.gov.co

2.8. Monitoreo

Se crearán los mecanismos y los indicadores correspondientes a la política de seguridad con el fin de determinar el cumplimiento de las mismas para establecer qué modificaciones o adiciones deben hacerse, este monitoreo debe realizarse como mínimo una vez al año o cuando sea necesario.

3. DESCRIPCIÓN DE ACTIVIDADES (POLÍTICAS)

Generalidades

El Municipio de Palmira en todas sus áreas y procesos cuenta con información, reservada, relevante, privilegiada e importante, es decir que esta información es el principal activo de la entidad para el desarrollo de todas sus actividades por lo que se hace necesario y se debe proteger conforme a los criterios y principios de los sistemas de información, como son integridad, disponibilidad y confidencialidad de la información.

De acuerdo a esta Política se divulgan los objetivos y alcances de seguridad de la información de la entidad, que se logran por medio de la aplicación de controles de seguridad, con el fin de mantener y gestionar el riesgo como lo establece la política de riesgos institucional. Este documento tiene el objetivo de garantizar la continuidad de los servicios, minimizar la probabilidad de explotar las amenazas, y asegurar el eficiente cumplimiento de los objetivos institucionales y de las obligaciones legales conforme al ordenamiento jurídico vigente y los requisitos de seguridad destinados a impedir infracciones y violaciones de seguridad.

3.1. ESTRUCTURACIÓN DE LAS ACTIVIDADES DEL PLAN DE SEGURIDAD

3.1.1. Plan de implementación

Ver Plan de seguridad y Privacidad de la información Anexo, en formato Excel, el cual detalla mes a mes las actividades.

COMPONENTE	No.	ACTIVIDAD
0. COMPROMISO DE LA ALTA DIRECCIÓN	0	Actualizar y formalizar el compromiso de la alta dirección, con los objetivos y política de seguridad.
1. DIAGNÓSTICO DE SEGURIDAD INFORMÁTICA	1.1	Analizar la información relacionada con modelo de seguridad y privacidad de la información (MSPI)
	1.2	Analizar y Actualizar la Política de Seguridad y Privacidad de la Información
	1.3	Revisar y actualizar el Manual de Políticas de Seguridad y Privacidad de la Información
2. ELABORACIÓN PLAN DE SEGURIDAD	2.1	Elaboración de documento de Plan de Seguridad y Privacidad de la Información 2020-2023 a version 2024-2027
3. EJECUTAR EL PROYECTO PARA MIGRACIÓN IPV4 - IPV6 FASE 01 DIAGNÓSTICO DE LA SITUACIÓN ACTUAL	3.1	Construcción del plan de Diagnóstico
	3.2	Inventario de TI (Hardware, Software)
	3.3	Análisis de la nueva topología de la infraestructura actual y su funcionamiento
	3.4	Protocolo de pruebas de validación de aplicativos, comunicaciones, plan de seguridad y coexistencia de los protocolos
	3.5	Planeación de la transición de los servicios tecnológicos de la Entidad

	3.6	Validación de estado actual de los sistemas de información, los sistemas de comunicaciones, las interfaces y revisión de los RFC correspondientes.(Request for Comments (RFC) es un documento numérico en el que se describen y definen protocolos, conceptos, métodos y programas de Internet)
	3.7	Identificación de esquemas de seguridad de la información y las comunicaciones
4. EJECUTAR EL PROYECTO PARA MIGRACIÓN IPV4 - IPV6 FASE 02 DESARROLLO PLAN DE IMPLEMENTACIÓN	4.1	Habilitación direccionamiento IPv6 para cada uno de los componentes de hardware y software de acuerdo al plan de diagnóstico de la Primera Fase.
	4.2	Configuración de servicios de DNS, DHCP, Seguridad, VPN, servicios WEB, entre otros.
	4.3	Configuración del protocolo IPv6 en aplicativos, sistemas de Comunicaciones, sistemas de almacenamiento y en general de los equipos Susceptibles a emplear direccionamiento IP.
	4.4	Activación de políticas de seguridad de IPv6 en los equipos de seguridad y comunicaciones que posea cada entidad de acuerdo con los RFC de seguridad en IPv6
	4.5	Coordinación con el proveedor (es) de servicios de Internet ISP, para establecer el enrutamiento y la conectividad integral en IPv6 hacia el exterior.
5. EJECUTAR EL PROYECTO PARA MIGRACIÓN IPV4 - IPV6 FASE 03 PRUEBAS DE FUNCIONALIDAD	5.1	Pruebas de funcionalidad y monitoreo de IPv6 en los servicios de la Entidad.
	5.2	Análisis de información y pruebas de funcionalidad frente a las políticas de seguridad perimetral de la infraestructura de TI.
	5.3	Afinamiento de las configuraciones de hardware, software y servicios de la Entidad
6. RENOVACIÓN DE LICENCIAMIENTOS	6.1	Identificar los sistemas de información, plataformas y servicios que requieren la renovación del soporte, actualización y mantenimiento del licenciamiento

	6.2	Garantizar el soporte, actualización y mantenimiento del licenciamiento de las herramientas, plataformas, servicios y sistemas de información que hacen parte de la infraestructura tecnológica de la entidad
7. SEGURIDAD PERIMETRAL	7.1	Realizar acciones encaminadas al mejoramiento de la plataforma de seguridad perimetral - Firewall
	7.2	Presentación de informe relacionado con la implementación de Políticas de Seguridad en la nueva plataforma de seguridad perimetral
	7.3	Parametrización y generación de informes de seguridad producto de la plataforma fortianalyzer
	7.4	Realizar técnicas de Ethical Hacking
	7.5	Aplicación de sugerencias/mejoras/correcciones del ejercicio de Ethical Hacking
	7.5	Realizar pruebas de ingeniería social
8. GESTIÓN DE INCIDENTES DE SEGURIDAD (SGSI)	8.1	Revision y actualizacion de Guia de gestion y clasificación de incidentes de seguridad
	8.2	Registro de comunicaciones enviadas y recibidas con el Colcert
9. ACTIVOS DE INFORMACIÓN	9.1	Actualizar los Instrumentos de Activos de Información de la dirección de tecnología
	9.2	Aprobar por el inventario de activos de información de cada área
	9.3	Publicar los activos de información de la administración municipal.
10. ESQUEMA DE GESTIÓN DE INFORMACIÓN (Data Institucional)	10.1	Realizar análisis/diagnóstico de alternativas para implementación de esquema de gestión de la información
	10.2	Realizar análisis/diagnóstico de alternativas para implementación de esquema de gestión backup de la información

	10.3	Realizar reunión con Secretaria General para estructurar la estrategia a seguir relacionada con la implementación de políticas de manejo, gestión y administración de la data institucional
11. INFRAESTRUCTURA CRÍTICA	11.1	Proceso de identificación de infraestructura crítica
12. IDENTIFICAR RIESGOS DE SEGURIDAD DE LA INFORMACIÓN	12.1	Identificar, valorar, evaluar y formular el Plan de Tratamiento de Riesgo de Seguridad Digital de Dirección de TIyC
	12.2	Realizar Seguimiento a la implementación de Planes de Tratamiento de Riesgos de Seguridad Digital
13. TRANSFORMACIÓN DIGITAL	13.1	Elaborar Plan Estratégico de Tecnologías de la Información (PETI)
	13.2	Implementación de proyectos que le permitan generar soluciones novedosas y creativas haciendo uso de TIC, con la participación de los grupos de interés (ciudadanía, academia, sector privado, sector público)
	13.3	Utilización de tecnologías emergentes de la cuarta revolución industrial para desarrollar procesos de innovación pública digital
14. ESTRATEGIA DE SOCIALIZACIÓN Y PUBLICACIÓN SENSIBILIZACIÓN	14.1	Sensibilización en Privacidad y Seguridad de la Información en Ingeniería Social
	14.2	Publicar en los medios oficiales de la Administración la Política de Seguridad y Privacidad de la Información y Manual de Políticas de Seguridad y Privacidad de la Información
	14.3	Realizar actividades/campañas de socialización de la Política de Seguridad y Privacidad de la Información y Manual de Políticas de Seguridad y Privacidad de la Información
	14.4	Realizar actividades/campañas de socialización de estrategia de administración de la data institucional encaminadas en el marco de la Política de Seguridad y Privacidad de la Información y Manual de Políticas de Seguridad y Privacidad de la Información
15. ACTUALIZACIÓN DISEÑO, DESARROLLO E	15.1	Revisar y actualizar el Plan de Recuperación de desastres, continuidad, contingencia y recuperación de la información

IMPLEMENTACIÓN DEL PLAN DE RECUPERACIÓN DE DESASTRES PARA EL PROCESO DE GESTIÓN DE TECNOLOGÍAS DE LA INFORMACIÓN	15.6	Realizar diagnóstico para establecer un esquema de almacenamiento y gestión de backups
	15.7	Revisar y actualizar el Plan de Recuperación de desastres, continuidad, contingencia y recuperación de la información
16. AUDITORÍA INTERNA DE SEGURIDAD DE LA INFORMACIÓN, CON EL OBJETIVO DE MEDIR EL NIVEL DE MADURACIÓN DEL MSPI	15.1	Realizar una auditoría de seguridad de la información, con el objetivo de medir el nivel de maduración del MSPI

4. DOCUMENTOS RELACIONADOS

- Ley 44 de 2093. Por la cual se modifica y adiciona la Ley 23 de 2082 y se modifica la Ley 29 de 2044 y Decisión Andina 351 de 2015 (Derechos de autor).
- Ley 527 de 2099. Por la cual se define y reglamenta el acceso y uso de los mensajes de datos, del comercio electrónico y de las firmas digitales y se establecen las entidades de certificación y se dictan otras disposiciones.
- Ley 594 de 2000. Por medio de la cual se expide la Ley General de Archivos.
- Ley 850 de 2003. Por medio de la cual se reglamentan las veedurías ciudadanas
- Ley 1266 de 2008. Por la cual se dictan las disposiciones generales del Hábeas data y se regula el manejo de la información contenida en bases de datos personales, en especial la financiera, crediticia, comercial, de servicios y la proveniente de terceros países y se dictan otras disposiciones.
- Ley 1221 de 2008. Por la cual se establecen normas para promover y regular el Teletrabajo y se dictan otras disposiciones.
- Ley 1273 de 2009. Por medio de la cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado - denominado "de la protección de la información y de los datos"- y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones.
- Ley 1341 de 2009. Por la cual se definen principios y conceptos sobre la sociedad de la información y la organización de las tecnologías de la información y las comunicaciones - TIC- Se crea la agencia Nacional de espectro y se dictan otras disposiciones.
- Ley 1437 de 2011. Por la cual se expide el código de procedimiento administrativo y de lo contencioso administrativo.
- Ley 1474 de 2011. Por la cual se dictan normas orientadas a fortalecer los mecanismos de prevención, investigación y sanción de actos de corrupción y la efectividad del control de la gestión pública.
- Ley 1581 de 2012. Por la cual se dictan disposiciones generales para la protección de datos personales.
- Ley 1712 de 2014. Por medio de la cual se crea la Ley de Transparencia y del Derecho de Acceso a la Información Pública Nacional y se dictan otras disposiciones.

- Ley 2015 de 2018. Por la cual se modifica la Ley 23 de 2082 y se establecen otras disposiciones en materia de derecho de autor y derechos conexos.
- Ley 2052 de 2020. Por medio de la cual se expide el código general disciplinario
- Ley 2055 de 2020. Por el cual se expide el Plan Nacional de Desarrollo 2018-2022. "Pacto por Colombia, Pacto por la Equidad".
- Decreto 2609 de 2012. Por el cual se reglamenta el Título V de la Ley 594 de 2000, parcialmente los artículos 58 y 59 de la Ley 1437 de 2011 y se dictan otras disposiciones en materia de Gestión Documental para todas las Entidades del Estado.
- Decreto 0884 de 2012. Por el cual se reglamenta parcialmente la Ley 1221 de 2008.
- Decreto 1377 de 2013. Por el cual se reglamenta parcialmente la Ley 1581 de 2012.
- Decreto 886 de 2014. Por el cual se reglamenta el Registro Nacional de Bases de Datos.
- Decreto 103 de 2015. Por medio del cual se reglamenta parcialmente la Ley 1712 de 2014 y se dictan otras disposiciones.
- Decreto 1074 de 2015. Por medio del cual se expide el Decreto Reglamentario del Sector Comercio, Industria y Turismo. Reglamenta parcialmente la Ley 1581 de 2012 e imparte instrucciones sobre el Registro Nacional de Bases de Datos. Artículos 25 y 26.
- Decreto 1078 de 2015. Por medio del cual se expide el Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones.
- Decreto 1080 de 2015. Por medio del cual se expide el Decreto Reglamentario del Sector Cultura.
- Decreto 1081 de 2015. Por medio del cual se expide el Decreto Reglamentario del Sector Presidencia.
- Decreto 728 de 2017. Por el cual se adiciona el capítulo 2 al título 9 de la parte 2 del libro 2 del Decreto Único Reglamentario del sector TIC, Decreto 1078 de 2015, para fortalecer el modelo de Gobierno Digital en las entidades del orden nacional del Estado colombiano, a través de la implementación de zonas de acceso público a Internet inalámbrico
- Decreto 1499 de 2017. Por medio del cual se modifica el Decreto 1083 de 2015, Decreto Único Reglamentario del Sector Función Pública, en lo relacionado con el Sistema de Gestión establecido en el artículo 133 de la Ley 1753 de 2015.

- Decreto 1008 del 2018. Por el cual se establecen los lineamientos generales de la política de Gobierno Digital y se subroga el capítulo 1 del título 9 de la parte 2 del libro 2 del Decreto 1078 de 2015, Decreto Único Reglamentario del sector de Tecnologías de la Información y las Comunicaciones.
- Decreto 2106 de 2019. Por el cual se dictan normas para simplificar, suprimir y reformar trámites, procesos y procedimientos innecesarios existentes en la administración pública. Resolución 2999 del 2008. Por el cual se adoptan las políticas de seguridad para el manejo de la información y se dictan otras normas para el uso y administración de los bienes y servicios informáticos del Ministerio TIC.
- Resolución 2034 de 2016. Por la cual se adoptó el Modelo de Responsabilidad Social Institucional en el Ministerio TIC.
- Resolución 2007 de 2018. Por la cual se actualiza la política de tratamiento de datos personales del Ministerio/Fondo TIC.
- Resolución 2133 de 2018. Por la cual se establecen las condiciones especiales del Teletrabajo en el Ministerio de Tecnologías de la Información y las Comunicaciones, y se derogan las resoluciones No 3559 y 4950 de 2013, 2313 y 494 de 2014 y 2787 de 2016.
- Resolución 512 de 2019. Por la cual se adopta la Política General de Seguridad y Privacidad de la Información, Seguridad Digital y Continuidad de los servicios del Ministerio/Fondo de Tecnologías de la Información y las Comunicaciones y se definen lineamientos frente al uso y manejo de la información
- Resolución 2005 de 2019. Por la cual se actualiza el Modelo Integrado de Gestión (MIG) del Ministerio/Fondo de Tecnologías de la Información y las Comunicaciones y se deroga la Resolución 911 de 2018
- CONPES 3701 de 2011. Lineamientos de Política para Ciberseguridad y Ciberdefensa.
- CONPES 3854 de 2016. Política Nacional de Seguridad Digital.

5. DOCUMENTOS ASOCIADOS

- AIFPR-015 PROCEDIMIENTO DE GESTIÓN Y RECUPERACIÓN DE DESASTRES DE LOS SERVICIOS CRÍTICOS DE TI
- AIFPR-005 PROCEDIMIENTO ADMINISTRACIÓN DATA-CENTER Y SEGURIDAD INFORMÁTICA

- AIFIT-007 INSTRUCTIVO RECUPERACIÓN Y BACKUPS DEL PORTAL WEB MUNICIPAL
- AIFFO-01 CAPACITACIÓN INFORMÁTICA
- AIFPR-003 PROCEDIMIENTO GESTIÓN USUARIO DE DOMINIO PLATAFORMAS ERP Y CORREO ELECTRÓNICO INSTITUCIONAL
- AIFMN-005 MANUAL DE POLÍTICAS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN DEL MUNICIPIO DE PALMIRA

6. CONTROL DE CAMBIOS

Fecha	Versión Inicial	Identificación del Cambio	Versión Final
28/01/2026	N/A	Creación del documento. Actualización del Anexo 01 Acuerdo de Confidencialidad de información, se reemplaza por el Formato de Compromiso de Confidencialidad, Integridad y Disponibilidad de la Información	01

7. CONTROL DE REVISIONES Y APROBACIÓN

Elaborado por:	Revisado por:	Aprobado por:
Nombre: Oscar Guio	**Nombre:** Ángela María Valencia Brand	**Nombre:** Andrés Mauricio Hormaza Tobón
Cargo: Profesional especializado 3	**Cargo:** Profesional especializado 3	**Cargo:** Director TIyC

COMPROMISO DE CONFIDENCIALIDAD, INTEGRIDAD Y DISPONIBILIDAD DE LA INFORMACIÓN

LA ALCALDÍA MUNICIPAL DE PALMIRA, entidad pública del orden territorial, representada legalmente por el señor Alcalde Municipal de Palmira, o por quien éste delegue, identificada con el NIT 891.380.007-3, con domicilio principal en la ciudad de Palmira, en adelante "**La Alcaldía de Palmira**" y, **[Nombre completo del empleado/contratista]**, identificado(a) con la cédula de ciudadanía número [Número de identificación], mayor de edad y vecino de [Ciudad], en adelante "**El Colaborador**", quien se desempeña como [Cargo o rol] en el área de [Área o dependencia].

CONSIDERANDO QUE:

La Alcaldía maneja información confidencial y sensible en el desarrollo de sus funciones y actividades. **El Colaborador**, en virtud de su relación laboral o contractual con **La Alcaldía**, tendrá acceso a dicha información. **Ambas partes** reconocen la importancia de proteger la confidencialidad, integridad y disponibilidad de la información y desean establecer los términos y condiciones para su manejo adecuado.

1. Objeto

El presente compromiso tiene como objeto establecer los términos y condiciones bajo los cuales **El Colaborador** se compromete a proteger la confidencialidad, integridad y disponibilidad de la información a la que tenga acceso en el desarrollo de sus funciones o actividades en relación con **La Alcaldía de Palmira**, de conformidad con la Ley 1581 de 2012, el Decreto Único Reglamentario 1074 de 2015, la Ley 1712 de 2014, el Decreto 1494 de 2015, la Política de Gobierno Digital adoptada mediante el Decreto 1008 de 2018 (compilado en el Decreto 1078 de 2015 del Sector TIC), y la norma ISO/IEC 27001:2022.

2. Definiciones

- **Información Confidencial:** Cualquier información no pública, oral, visual, escrita, electrónica o en cualquier otro formato, relacionada con **La Alcaldía de Palmira**, sus actividades, proyectos, clientes, proveedores, empleados u otros terceros, que no sea de conocimiento público y cuya divulgación no autorizada pueda causar perjuicio a **La Alcaldía de Palmira** o a terceros.
- **Datos Personales:** Cualquier información vinculada o que pueda asociarse a una o varias personas naturales determinadas o determinables.

3. Obligaciones de El Colaborador

- **Confidencialidad:**
  - Mantener en estricta confidencialidad la Información Confidencial a la que tenga acceso.
  - No divulgar la Información Confidencial a terceros no autorizados, ni utilizarla para fines distintos a los autorizados por **La Alcaldía de Palmira**.
  - No utilizar la Información Confidencial para obtener beneficios personales o para terceros.

- **Autenticidad:**
  - Asegurar la autenticidad de la información generada, recibida o transmitida durante el desarrollo de sus funciones, garantizando su veracidad, trazabilidad y atribución al autor legítimo, especialmente mediante el uso de credenciales, mecanismos de control de acceso o firma digital cuando aplique.
- **Integridad:**
  - Proteger la integridad de la Información Confidencial, evitando su alteración, modificación o destrucción no autorizada.
  - Notificar de inmediato a **La Alcaldía de Palmira** sobre cualquier pérdida, robo o acceso no autorizado a la Información Confidencial.
- **Disponibilidad:**
  - Garantizar la disponibilidad de la Información Confidencial para su uso legítimo por parte de **La Alcaldía de Palmira**.
  - Colaborar con **La Alcaldía de Palmira** en la implementación de medidas de seguridad para proteger la Información Confidencial.
- **Protección de datos personales:**
  - Cumplir con la Ley 1581 de 2012, el Decreto Único Reglamentario 1074 de 2015 y las disposiciones vigentes sobre protección de datos personales a los que tenga acceso en el desarrollo de sus funciones.
  - No recolectar, almacenar, utilizar o divulgar Datos Personales sin la autorización correspondiente.
- **Uso adecuado de recursos informáticos:**
  - Utilizar los recursos informáticos (correo electrónico, internet, equipos de cómputo, etc.) proporcionados por **La Alcaldía** de manera responsable y exclusivamente para fines laborales.
  - Cumplir con las políticas de uso aceptable de los recursos informáticos de **La Alcaldía de Palmira**.
- **Reporte de incidentes:**
  - Informar de inmediato a **La Alcaldía** sobre cualquier incidente de seguridad que pueda comprometer la confidencialidad, integridad o disponibilidad de la Información Confidencial o los Datos Personales.
- **Devolución de información:**
  - Al finalizar la relación laboral o contractual, devolver a **La Alcaldía de Palmira** toda la Información Confidencial en su poder, en cualquier formato o medio.

4. Propiedad de la información

La Información Confidencial es propiedad exclusiva de **La Alcaldía de Palmira**. **El Colaborador** reconoce que no adquiere ningún derecho de propiedad sobre dicha información y que su acceso está limitado a los fines establecidos en este acuerdo.

5. Excepciones a la confidencialidad

El Colaborador podrá divulgar la Información Confidencial únicamente en los siguientes casos:

- Cuando sea requerido por ley, orden judicial o autoridad competente.
- Cuando sea necesario para proteger los derechos o intereses legítimos de **La Alcaldía de Palmira**.
- Cuando **La Alcaldía de Palmira** autorice expresamente la divulgación.

6. Vigencia y terminación

Este COMPROMISO DE CONFIDENCIALIDAD, INTEGRIDAD Y DISPONIBILIDAD DE LA INFORMACIÓN será continuo desde la fecha de su firma y no vencerá aún finalizada la vinculación laboral del empleado público con la Alcaldía de Palmira, cumpliendo con la clasificación y el tiempo de reserva de los activos de información establecidos en los instrumentos de gestión documental y en la Política de Seguridad y Privacidad de la Información adoptada por la Alcaldía de Palmira, conforme a la Ley 1581 de 2012, la Ley 1712 de 2014 (arts. 18 a 22), el Decreto 1494 de 2015 y demás normas concordantes.

7. Incumplimiento y sanciones

El incumplimiento de las obligaciones establecidas en este acuerdo dará lugar a las acciones legales y sanciones que correspondan, de acuerdo con la legislación vigente, las políticas internas de **La Alcaldía** y los términos del contrato laboral o de prestación de servicios.

8. Jurisdicción y ley aplicable

Este acuerdo se rige por las leyes de la República de Colombia y cualquier disputa que surja de su interpretación o aplicación será resuelta por los tribunales competentes de la ciudad de Palmira.

9. Aceptación

Declaro haber leído, entendido y aceptado la totalidad de los términos y condiciones contenidos en el presente documento, en prueba de lo cual lo suscribo en la ciudad de Palmira, a los [Día] días del mes de [Mes] de [Año].

Firma: _____
Nombre: _____
Cédula: _____
Cargo: _____
Número de contrato: _____
Dependencia: _____