ALCALDÍA MUNICIPAL DE PALMIRA VALLE DEL CAUCA

PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

DIRECCIÓN DE TECNOLOGÍA INNOVACIÓN Y CIENCIA

PALMIRA VALLE 2024-2027

1. INTRODUCCIÓN

La gestión de riesgos de seguridad y privacidad de la información tiende a establecer procesos, procedimientos y actividades encaminados a lograr un equilibrio entre la prestación de servicios y los riesgos asociados a los activos de información que dan apoyo y soporte en el desarrollo de la misionalidad de la entidad. Por lo tanto, se deben implementar los controles necesarios para dar un adecuado tratamiento a los riesgos, generando una estrategia de seguridad digital efectiva que controle y administre la materialización de eventos o incidentes, mitigando los impactos adversos o considerables al interior de la entidad.
Lo anterior, dando cumplimiento a la normativa establecida por el estado colombiano, CONPES 3854 de 2016, Modelo de Seguridad y Privacidad de MINTIC y lo establecido en el decreto 1008 de 14 de junio 2018, adoptando las buenas prácticas y los lineamientos de los estándares ISO 27001:2013, ISO 27005:2018 y la *guía para la administración del riesgo y el diseño de controles en entidades públicas - Riesgos de gestión, corrupción y seguridad digital*, en particular el capítulo No.6 Lineamientos riesgos de seguridad de la información, emitida por el Departamento Administrativo de la Función Pública.

2. OBJETIVOS

2.1. Objetivo General

Desarrollar estrategias e implementar actividades y controles que permitan minimizar los riesgos basados en la disponibilidad, confidencialidad e integridad de activos de la información en la Alcaldía Municipal de Palmira.

2.2. Objetivos Específicos

- **a.** Plantear modelos de gestión de la información para evaluar la incidencia presentada en la Alcaldía municipal.
- **b.** Gestionar los eventos de seguridad de la información y darle una clasificación debida a la incidencia.
- **c.** Determinar el alcance del Plan de tratamiento de riesgos de la seguridad y privacidad de la información.
- **d.** Definir los activos de la información calificados en riesgo alto a proteger en la Alcaldía de Palmira.
- **e.** Identificar las principales amenazas que afectan a los activos de la información.
- **f.** Proponer soluciones para minimizar los riesgos a los que está expuesto cada activo de la información.
- **g.** Evaluar y comparar el nivel de riesgo actual con el impacto generado después de implementar el Plan de tratamiento de seguridad de la información.

3. ALCANCE

El presente plan es aplicable a todos los procesos que conforman el Sistema Integrado de Gestión de la Alcaldía de Palmira y a todas las actividades realizadas por los servidores públicos durante el ejercicio de sus funciones contemplando riesgos de seguridad y privacidad de la información.

4. RESPONSABILIDADES

El suministro de la información base para la ejecución del presente plan, es de responsabilidad de la Secretaría General, de acuerdo a su proceso de identificación y valoración de activos de información e índice de información reservada y clasificada, el cual deberá realizarse sobre la plataforma Registro Único de Activos de Información - RUACI.
La actualización con frecuencia anual de los activos de información, es responsabilidad de cada dependencia de la entidad en conjunto con la Secretaría General.
La Dirección de Tecnología, Innovación y Ciencia del Municipio de Palmira, es responsable de realizar el seguimiento a la implementación de los controles a los activos de información de tipo digital de la entidad con el fin de minimizar la materialización de riesgos de seguridad y privacidad de la información.

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.

5. DESCRIPCIÓN DE ACTIVIDADES

ITEM	ACTIVIDAD	CICLO PHVA	RESPONSABLE	REGISTRO
1	Verificar que la guía para la administración del riesgo se encuentre alineada con los requerimientos de Riesgos de seguridad digital	P	Director(a) Contratistas Profesional Universitario Profesional Especializado	Actas de reunión

2	Actualizar el documento guía para el proceso de gestión integral de los riesgos en los activos de información valorados como críticos.	H	Contratistas Profesional Universitario Profesional Especializado	-Presentaciones realizadas -Listados de asistencia a capacitaciones y mesas de trabajo
3	Aplicar actualizaciones y/o mejoras al aplicativo web RUACI para integrar las etapas de identificación de los riesgos y asignación de controles a los activos de la información.	H	Contratistas Profesional Universitario Profesional Especializado	-Presentaciones realizadas -Listados de asistencia a capacitaciones y mesas de trabajo -Actas de Reuniones
4	Creación espacios de sensibilización, en coordinación con la secretaria general, con las dependencias de la entidad para el registro y valoración de los activos de la información de cada proceso.	A	Contratistas Profesional Universitario Profesional Especializado	-Manual de Usuario RUACI -Actualizaciones del Registro Único de Inventarios
5	Consolidación de la información recolectada por medio del aplicativo del web dispuesto para ello	H	Contratistas Profesional Universitario Profesional Especializado	-Matriz de Valoración de activos -Informe del Registro Único de Inventarios
6	La identificación de los riesgos de Seguridad y Privacidad de la Información se realiza al inventario de activos de información clasificados con impacto / criticidad Alta	A	Contratistas Profesional Universitario Profesional Especializado	-Matriz de Riesgos -Matriz de Valoración de activos -Informe del Registro Único de Inventarios
7	Evaluar la aplicación de controles y evaluar los riesgos residuales	V	Contratistas Profesional Universitario Profesional Especializado	-Informes de Evaluación

8	Revisión y verificación de los Riesgos de Seguridad y Privacidad de la Información	A	Contratistas Profesional Universitario Profesional Especializado	-Actas de reunión -Listados de asistencia
9	Identificar acciones de mejora según resultados de la evaluación riesgos residuales.	A	Contratistas Profesional Universitario Profesional Especializado	-Actas de reunión -Listados de asistencia
10	Revisar y Aprobar el Plan de Tratamiento de Riesgos de cada dependencia	A	Contratistas Profesional Universitario Profesional Especializado	-Actas de reunión -Listados de asistencia
11	Realización de la verificación de la aplicación y efectividad del Plan de Tratamiento de Riesgos y el cumplimiento de Seguridad y Privacidad de la Información	V	Contratistas Profesional Universitario Profesional Especializado	-Actas de reunión -Listados de asistencia
12	Publicación en la Página WEB el informe general los Riesgos de Seguridad y Privacidad de la Información de la entidad.	A	Contratistas Profesional Universitario Profesional Especializado	-Publicación en la Página WEB institucional

Enlace de Plan de Acción del Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información: https://docs.google.com/spreadsheets/d/1KZ-5ffQzRzT7SoVofKqF2PUwK5EIyBz3WjjVpobXbls/edit?gid=374957487#gid=374957487

6. DEFINICIONES

- Activo: [Según ISO 27000]: En relación con la seguridad de la información, se refiere a cualquier información o elemento relacionado con el tratamiento de esta (sistemas, soportes, edificios, personas) que tenga valor para la organización.

- Amenaza: [Según ISO 27000]: Causa potencial de un incidente no deseado, que puede provocar daños a un sistema o a la organización.

- Análisis del riesgo: [NTC ISO 31000:2011]: Proceso sistemático para comprender la naturaleza del riesgo y determinar el nivel de riesgo.

- Apetito de riesgo: Es el nivel máximo de riesgo que la entidad está dispuesta a asumir.

- Consecuencia: [NTC ISO 31000:2011]: Resultado o impacto de un evento que afecta a los objetivos.

- Controles: [Según ISO 27000]: Las políticas, los procedimientos, las prácticas y las estructuras organizativas concebidas para mantener los riesgos de seguridad de la información por debajo del nivel de riesgo asumido. Control es también utilizado como sinónimo de salvaguarda o contramedida. En una definición más simple, es una medida que modifica el riesgo.

- Criterios del riesgo: [Según NTC ISO 31000:2011]: Términos de referencia frente a los cuales se evalúa la importancia de un riesgo.

- Evaluación del riesgo: [Según NTC ISO 31000:2011]: Proceso de comparación de los resultados del análisis del riesgo, con los criterios del riesgo, para determinar si el riesgo, su magnitud o ambos son aceptables o tolerables.

- Identificación del riesgo: [Según NTC ISO 31000:2011]: Proceso para encontrar, reconocer y describir el riesgo.

- Impacto: [Según ISO 27000]: El coste para la empresa de un incidente de la escala que sea, que puede o no ser medido en términos estrictamente financieros -p.ej., pérdida de reputación, implicaciones legales, etc.

- Inventario de activos: [Según ISO 27000.ES]: Sigla en inglés: Assets inventory. Lista de todos aquellos recursos (físicos, de información, software, documentos, servicios, personas, intangibles, etc.) dentro del alcance del SGSI, que tengan valor para la organización y necesiten, por tanto, ser protegidos de potenciales riesgos.

- Nivel de riesgo: [Según NTC ISO 31000:2011]: Magnitud de un riesgo o de una combinación de riesgos expresada en términos de la combinación de las consecuencias y su probabilidad.
- Perfil del riesgo: [Según NTC ISO 31000:2011]: Descripción de cualquier conjunto de riesgos.
- Política: [Según ISO/IEC 27000:2016]: Intenciones y dirección de una organización como las expresa formalmente su alta dirección.
- Política: para la gestión del riesgo [Según NTC ISO 31000:2011]: Declaración de la dirección y las intenciones generales de una organización con respecto a la gestión del riesgo.
- Reducción del riesgo: [Según NTC ISO 31000:2011]: Acciones que se toman para disminuir la posibilidad, las consecuencias negativas o ambas, asociadas con un riesgo.
- Riesgo: [Según ISO 27000]: Posibilidad de que una amenaza concreta pueda explotar una vulnerabilidad para causar una pérdida o daño en un activo de información. Suele considerarse como una combinación de la probabilidad de un evento y sus consecuencias.
- Riesgo Residual: [Según ISO 27000]: El riesgo que permanece tras el tratamiento del riesgo.
- Vulnerabilidad: [Según ISO 27000]: Debilidad de un activo o control que puede ser explotada por una o más amenazas.

7. METODOLOGÍA

La Dirección de Tecnología, Innovación y Ciencia - DTIyC de la Alcaldía de Palmira siguiendo los lineamientos trazados por el Gobierno Nacional con lo expuesto en la Ley de transparencia 1712 de 2014, la Estrategia Gobierno Digital establece el PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN en el cual se identifiquen las amenazas, las vulnerabilidades, el impacto y el nivel de riesgo asociados a los activos de información de la entidad.

En el tratamiento de riesgos de seguridad y privacidad de la información resulta importante lograr una aceptación de los riesgos con base en las posibles consecuencias de afectación; establecer una estrategia de mitigación adecuada que logre un entendimiento y aceptación del riesgo residual así como de los recursos empleados en relación costo beneficio con el fin de emplear medidas para salvaguardar, proteger y custodiar los activos de información de las aplicaciones, servicios tecnológicos, bases de datos, redes de comunicaciones, equipos de cómputo y documentos físicos garantizando la disponibilidad, confidencialidad e integridad de la información. Por consiguiente,

resulta indispensable definir actividades que de manera articulada permitan implementar medidas de control que ayuden a la prevención, contención y mitigación de amenazas a las que se encuentran expuestos los activos de información de la entidad por medio de la metodología descrita a continuación:

8. RECURSOS

Tipo de Recurso	Descripción
Humanos	La Dirección de Tecnología, Innovación y Ciencia a través de seguridad de la información es responsable de coordinar, implementar, modificar y realizar seguimiento a las políticas, estrategias y procedimientos en la Entidad en lo concerniente a la seguridad y privacidad de la información lo cual contribuye a la mejora continua.
Técnicos	- Guía para la administración del riesgo y el diseño de controles en entidades públicas - Riesgos de gestión, corrupción y seguridad digital del DAFP. -Guía de Administración del Riesgo de la Alcaldía Municipal de Palmira -Guía para la Gestión Integral del Riesgo en Entidades Públicas Versión 2025 DAFP
Logísticos	Gestión de recursos para realizar socializaciones, transferencia de conocimientos y seguimiento a la gestión de riesgos.
Financieros	Recursos para la adquisición de conocimiento, recursos humanos, técnicos, y desarrollo de auditorías

La estimación y asignación del presupuesto para el plan de tratamiento de riesgos de Seguridad y Privacidad de la información identificados en la entidad, corresponderá al dueño del riesgo, quien es el responsable de contribuir con el seguimiento y control de la gestión, además de la implementación de los controles definidos en el plan de tratamiento.

La entidad pública debe utilizar medidas de desempeño (indicadores) para la gestión de los riesgos de seguridad y privacidad de la información, las cuales deben reflejar el cumplimiento de los objetivos propuestos.

9. DOCUMENTOS RELACIONADOS

- ISO/IEC 27001:2022, Tecnología de la información — Técnicas de seguridad — Sistemas de gestión de seguridad de la información — Requisitos.

10. DOCUMENTOS ASOCIADOS

- AIFPR-015 PROCEDIMIENTO DE GESTIÓN Y RECUPERACIÓN DE DESASTRES DE LOS SERVICIOS CRÍTICOS DE TI

11. CONTROL DE CAMBIOS

Fecha	Versión Inicial	Identificación del Cambio	Versión Final
28/01/2026	N/A	Creación del documento. Adición de la Guía para la Gestión Integral del Riesgo en Entidades Públicas Versión 2025 DAFP	01

12. CONTROL DE REVISIONES Y APROBACIÓN

Elaborado por:		Revisado por:		Aprobado por:	
Nombre:	Cristian Alberto Muñoz Perdomo	**Nombre:**	Ángela María Valencia Brand	**Nombre:**	Andrés Mauricio Hormaza Tobón
Cargo:	Profesional especializado 3	**Cargo:**	Profesional especializado 3	**Cargo:**	Director TIyC