



Alcaldía Municipal de
Palmira Nit.: 891.380.007-3

República de Colombia Departamento
del Valle del Cauca Alcaldía
Municipal de Palmira
**DIRECCIÓN DE TECNOLOGÍA, INNOVACIÓN Y
CIENCIA**

**ALCALDÍA MUNICIPAL DE PALMIRA
VALLE DEL CAUCA**

**PLAN DE TRATAMIENTO DE RIESGOS EN SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN
DIRECCION DE TECNOLOGIA INNOVACION Y CIENCIA**

**PALMIRA VALLE
2021-2023**



Alcaldía Municipal de
Palmira Nit.: 891.380.007-3

República de Colombia Departamento
del Valle del Cauca Alcaldía
Municipal de Palmira
**DIRECCIÓN DE TECNOLOGÍA, INNOVACIÓN Y
CIENCIA**

Tabla de contenido

1.	Introducción	3
2.	Objetivos	3
2.1.	General	3
2.2.	Específicos	3
3.	Alcance	3
4.	Definiciones	4
5.	Metodología	5
5.1.	Plan de Gestión de Riesgos de Seguridad y Privacidad de la Información	5
6.	Recursos	15
7.	Presupuesto	15
8.	Medición	15
9.	CONTROL DE CAMBIOS	16
10.	CONTROL DE REVISIONES Y APROBACIÓN DE DOCUMENTOS	16



Alcaldía Municipal de
Palmira Nit.: 891.380.007-3

1. Introducción

La gestión de riesgos de seguridad y privacidad de la información establece 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 emitida por el DAFP.

2. Objetivos

2.1. General

Desarrollar estrategias que permitan minimizar los riesgos de pérdida de activos de la información en la Alcaldía Municipal de Palmira.

2.2. Específicos

- Plantear modelos de gestión de la información para evaluar la incidencia presentada en la Alcaldía municipal.
- Gestionar los eventos de seguridad de la información y darle una clasificación debida a la incidencia.
- Determinar el alcance del Plan de tratamiento de riesgos de la seguridad y privacidad de la información.
- Definir los principales activos a proteger en la Alcaldía de Palmira.
- Identificar las principales amenazas que afectan a los activos.
- Proponer soluciones para minimizar los riesgos a los que está expuesto cada activo.
- 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.



Alcaldía Municipal de
Palmira Nit.: 891.380.007-3

4. 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.



Alcaldía Municipal de
Palmira Nit.: 891.380.007-3

República de Colombia Departamento
del Valle del Cauca Alcaldía
Municipal de Palmira
**DIRECCIÓN DE TECNOLOGÍA, INNOVACIÓN Y
CIENCIA**

- 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.

5. Metodología

5.1. Plan de Gestión de Riesgos de Seguridad y Privacidad de la Información

La Dirección de Tecnología, Innovación y Ciencia - DTlyC 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 un PLAN DE GESTIÓN 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.

En la gestión 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:



Alcaldía Municipal de
Palmira Nit.: 891.380.007-3

República de Colombia Departamento
del Valle del Cauca Alcaldía
Municipal de Palmira
**DIRECCIÓN DE TECNOLOGÍA, INNOVACIÓN Y
CIENCIA**

6. Recursos

RECURSOS	VARIABLE
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
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

7. Presupuesto

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.

8. Medición

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.





Alcaldía Municipal de
Palmira Nit.: 891.380.007-3

República de Colombia Departamento
del Valle del Cauca Alcaldía
Municipal de Palmira
**DIRECCIÓN DE TECNOLOGÍA, INNOVACIÓN Y
CIENCIA**

9. CONTROL DE CAMBIOS

Fecha	Versión Inicial	Identificación del Cambio	Versión Final
15/08/2018	N/A	Creación del documento	01
12/12/2018	01	Cambios de forma de acuerdo con el procedimiento información documentada que reglamenta el SIG.	02
15/01/2020	02	Actualización de acuerdo con el Modelo de Planeación y Gestión (MIPG).	03
22/01/2021	03	Actualización de acuerdo con el Modelo de Planeación y Gestión (MIPG)	04
14/01/2022	04	Actualización de acuerdo con el Modelo de Planeación y Gestión (MIPG)	05
16/01/2023	05	Actualización y reprogramación de actividades	06

10. CONTROL DE REVISIONES Y APROBACIÓN DE DOCUMENTOS

Elaborado por:	Revisado por	Aprobado por:
Nombre: Christian Muñoz P.	Nombre: Diego A. Valencia	Nombre: Juan David Escobar García
Cargo: Profesional especializado	Cargo: Profesional especializado	Cargo: Director TlyC
Fecha: 16/01/2023	Fecha: 16/01/2023	Fecha: 16/01/2023
Firma 	Firma 	Firma 