**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**

## 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

## 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.

**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.

- 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 - 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 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:

| N° | Actividad | Descripción | Entregable | Meta | Responsable | 2021 | | | | | | | | | | | | 2022 | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | | | | | ENE | FEB | MAR | ABR | MAY | JUN | JUL | AGO | SEP | OCT | NOV | DIC | ENE | FEB | MAR | ABR | MAY | JUN | JUL | AGO | SEP | OCT | NOV | DIC |
| 1 | Analizar y revisar la guía de Gestión de Riesgos de la entidad | Verificar que la guía para la administración del riesgo se encuentre alineada con los requerimientos de Riesgos de seguridad digital | Número de Informes de lineamientos actualizados | 2 | Dirección de TIyC y Secretaria General | | | | | | | | | | | | | | | | | | | | | | | | |
| 2 | Capacitar al equipo de base de SPI en Gestión de los riesgos de seguridad en la información | Apropiar el conocimiento sobre ISO 27000 en capacitación oficial considerada para este proceso | Número de Personas Capacitadas | 6 | Control Interno | | | | | | | | | | | | | | | | | | | | | | | | |

| | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 3 | Determinar guía de tratamiento de riesgos de seguridad de la información para la entidad | Generación documento guía para instruir a equipo de enlaces en el tratamiento de riesgos de seguridad de la información | Acta de comité de técnico o herramienta | 1 | Dirección TIyC | | | | | | | | | | | | | | | | | | | | | | | |
| 4 | Crear Formato de aplicación para riesgos de seguridad de la información | Generación de archivo o plantilla para registro de la información obtenida de la aplicación de la guía | Formato Mapa de Riesgos parametrizado | 1 | Dirección TiyC | | | | | | | | | | | | | | | | | | | | | | | |
| 5 | Sensibilizar el Equipo Gestor de Riesgos de SPI | Determinar con la Secretaria General el Equipo administrador de Riesgos de | Acta de Reunión | 1 | Equipo de Enlaces de gestión de riesgo SPI y/o Enlaces de Identificación | | | | | | | | | | | | | | | | | | | | | | | |

| | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | SPI | | | de Activos de Información | | | | | | | | | | | | | | | | | | | | | | | |
| 6 | Identificar los riesgos de seguridad y privacidad de la información tomado del inventario de activos de información clasificados con impacto / criticidad Alta, además de las amenazas y vulnerabilidades asociadas. | Mesa de trabajo con enlaces, custodios y/o personal con experiencia en identificación de riesgos de cada una de las dependencias realizarán la identificación y el análisis respecto a los activos de información clasificados como alto o crítico según la Guía de Seguridad y Privacidad de la Información. | Número de Mapas de Riesgo que incluya Riesgos de SPI | 37 | Equipo de Enlaces de gestión de riesgo SPI | | | | | | | | | | | | | | | | | | | | | | | | |

| | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 7 | Aprobar la Mapa de Riesgos de SPI de la Entidad | Revision y verificacion de los Riesgos de SPI | Acta de Aprobación | 1 | Comité de Seguridad y Privacidad de la Información | | | | | | | | | | | | | | | | | | | | | | | |
| 8 | Aprobar la Mapa de Riesgos de SPI de la Entidad | Publicación en la Página WEB de los Riesgos de SPI de la Entidad | Publicación en Página WEB | 2 | Dirección de TIyC | | | | | | | | | | | | | | | | | | | | | | | |
| 9 | Capacitar en la elaboración del Plan de Tratamiento de Riesgos de SPI | Jornada de capacitación para sensibilizar en la Metodología de Tratamiento de Riesgos de SPI, donde se definen criterios relevantes a aplicar | Acta de Reunión | 1 | Dirección de TIyC y Secretaria General | | | | | | | | | | | | | | | | | | | | | | | |

| | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 10 | Evaluar los Riesgos Residuales | Evaluar la aplicación de controles y evaluar los riesgos residuales | Número de Mapas de Riesgos de PSI | 37 | Equipo Enlace de Gestión de Riesgo SPI y Dirección de TIyC | | | | | | | | | | | | | | | | | | | | | | | | |
| 11 | Preparar Plan de Tratamiento de Riesgos | Identificar oportunidades de mejora según resultados evaluación riesgos residuales | Número de Planes de Tratamiento Identificados | 37 | Equipo Enlaces gestión de riesgo SPI | | | | | | | | | | | | | | | | | | | | | | | | |
| 12 | Revisar y Aprobar el Plan de Tratamiento de Riesgos de Cada una de las Dependencias | Revisar y Aprobar el Plan de Tratamiento de Riesgos de Cada una de las Dependencias por parte de la Dirección de TIyC | Actas de Aprobación | 37 | Dirección de TIyC | | | | | | | | | | | | | | | | | | | | | | | | |

| | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 13 | Monitorear los Planes de Tratamiento de Riesgos | Se realizará la verificación de la aplicación y efectividad del Plan de Tratamiento de Riesgos y el cumplimiento de Seguridad y Privacidad de la Información | Informe | 1 | Oficina de Control Interno | | | | | | | | | | | | | | | | | | | | | | | | |

## 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.<br><br>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.

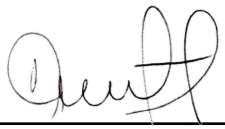
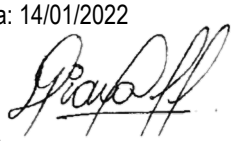
## 8. Medición

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.

## 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 |

## 10. CONTROL DE REVISIONES Y APROBACIÓN DE DOCUMENTOS

| Elaborado por: | Revisado por | Aprobado por: |
|---|---|---|
| Nombre: Crhistian Muñoz P.<br><br>Cargo: Profesional especializado<br><br>Fecha: 14/01/2022<br><br>Firma  | Nombre: Diana Sánchez S<br><br>Cargo: Profesional especializado<br><br>Fecha: 14/01/2022<br><br>Firma  | Nombre: Juan David Escobar García<br><br>Cargo: Director TIyC<br><br>Fecha: 14/01/2022<br><br> <br>Firma |