## TABLA DE CONTENIDO

# 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.

| RIESGOS | TRATAMIENTO |
|---|---|
| No se tiene UPS en la entidad que salvaguarde los equipos ante la baja de energía | Compra de Ups |
| No cuenta con un sistema de Backup centralizado. | Compra de disco duro para backup de la información general (jurídica, contable, dirección, archivo) |
| Daño locativo a (software y hardware) | Cumplir el plan de mantenimientos preventivos |
| Digitales (externos e internos) | Cumplimiento a la Política de Seguridad Digital. |
| Daño al archivo físico | Custodia adecuada |

### 4.1. Plan de Gestión de Riesgos de Seguridad y Privacidad de la Información

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

| 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. |

| | |
|---|---|
| **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 |

## 5. VIGENCIA

Tiene vigencia permanente y será revisada como mínimo una vez al año con el fin de realizar actualizaciones o mejoras que se consideren pertinentes si aplica.

Se debe publicar con una frecuencia anual, y en caso de modificaciones o actualizaciones, se realizará una nueva publicación por los medios dispuestos.

Se aprueba y adopta por medio del comité de gestión y desempeño

## 6. CONTROL DE CAMBIOS

| VERSIÓN | FECHA | ÍTEM MODIFICADO | DESCRIPCIÓN DEL CAMBIO |
|---|---|---|---|
| 1 | 25/01/2022 | | Creación del documento |