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 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. 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

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 en la tabla No.1:

No	Actividad	Descripción	Entregable	Meta	Responsable	2024												2025												2026												2027											
						ENE	FEB	MAR	ABR	MAY	JUN	JUL	AGO	SEP	OCT	NOV	DIC	ENE	FEB	MAR	ABR	MAY	JUN	JUL	AGO	SEP	OCT	NOV	DIC	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 actualizar 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	1	Dirección de TIyC y Secretaria General																																																	
2	Actualizar la Guía del Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información	Actualizar el documento guía para el proceso de gestión integral de los riesgos en	Numero de Guías de Administración del Riesgo actualizadas	1	Dirección de TIyC y Secretaria General																																																	

		los activos de información valorados como críticos.																																																			
3	Actualización y acondicionamiento del aplicativo web Registro Único de Activos de la Información - RUACI	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.	Numero de Aplicaciones Web actualizadas	1	Dirección de TIyC																																																
4	Sensibilizar a enlaces de	Creación espacios de	Acta de Reunión	37	Equipo de Enlaces																																																

	activos de información	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.			de gestión activos de la información, Dirección TIyC, Secretaria General
5	Consolidar base de datos de los activos de información de la entidad	Consolidación de la información recolectada por medio del aplicativo del web dispuesto para ello	Base de datos consolidada	1	Secretaria General
6	Identificar los riesgos	La identificaci	Número de Mapas	37	Equipo de

	de seguridad y privacidad de la información de activos de información	ón de los riesgos de Seguridad y Privacidad de la Información se realiza al inventario de activos de información clasificados con impacto / criticidad Alta	de Riesgo que incluya Riesgos de SPI		Enlaces de gestión activos de la informaci ón
7	Evaluar los Riesgos Residuales	Evaluar la aplicación de controles y evaluar los riesgos residuales	Número de Mapas de Riesgo	37	Equipo de Enlaces de gestión activos de la informaci ón
8	Aprobar el Mapa de Riesgos de SPI del	Revisión y verificació n de los Riesgos	Acta de Aprobació n	1	CICCI Comité Institucio nal de

	proceso de Gestión de Informática	de Seguridad y Privacidad de la Información			Coordinación de Control Interno
9	Realizar el Plan de Tratamiento de Riesgos	Identificar acciones de mejora según resultados de la evaluación riesgos residuales.	Número de Planes de Tratamiento Identificados	37	Dirección de TIyC
10	Revisar y Aprobar el Plan de Tratamiento de Riesgos de cada dependencia	Revisar y Aprobar el Plan de Tratamiento de Riesgos de cada dependencia	Actas de Aprobación	37	Dirección de TIyC
11	Monitorear los Planes de Tratamiento de Riesgos	Realización de la verificación de la aplicación y	Informe con estadísticas	1	CICCI Comité Institucional de Coordinación de

		efectividad del Plan de Tratamiento de Riesgos y el cumplimiento de Seguridad y Privacidad de la Información			Control Interno																																																
12	Publicar informe general los Riesgos de Seguridad y Privacidad de la Información de la entidad	Publicación en la Página WEB el informe general los Riesgos de Seguridad y Privacidad de la Información de la entidad.	Publicación en Portal Web de la entidad	1	Dirección de Tecnología, Innovación y Ciencia																																																

Tabla No. 1. Cronograma de actividades del Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información.

6. 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
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

Tabla No. 2. Detalle del tipo de recurso requerido para desarrollo del Plan

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.

7. Control de Cambios

Fecha	Versión Inicial	Identificación del Cambio	Versión Final
22/01/2024	N/A	Creación del documento	01

Proyectó: Crhistian Alberto Muñoz – Profesional especializado - Dirección de Tecnología, Innovación y Ciencia
Revisó: Diego Alejandro Valencia – Profesional especializado - Dirección de Tecnología, Innovación y Ciencia
Aprobó: Andrés Mauricio Hormaza – Director - Dirección de Tecnología, Innovación y Ciencia