CONCEJO MUNICIPAL DE CARTAGO

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

CARTAGO, VIGENCIA 2024-2027

INTRODUCCION

El Concejo Municipal de Cartago -Valle presenta a los grupos de interés y a la ciudadanía el Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información para la vigencia 2024. Este plan, fundamentado en el ciclo PHVA (Planear-Hacer-Verificar-Actuar), tiene como objetivo establecer una serie de actividades que generarán condiciones de uso confiable tanto en el entorno digital como físico de la información.

La implementación de este enfoque, basado en la gestión de riesgos, busca preservar la confidencialidad, integridad y disponibilidad de la información del Concejo Municipal. Esto se realiza con la finalidad de mitigar cualquier posible afectación a los activos que respaldan la gestión pública en todos sus niveles, así como las investigaciones relacionadas con factores que influyen en la calidad del servicio al ciudadano.

Este plan se alinea con la guía para la administración del riesgo y el diseño de controles en entidades públicas, así como con lo establecido en el Decreto 1008 de junio 14 de 2018, que regula la política de Gobierno Digital. De acuerdo con dicho decreto, se subroga el capítulo 1 del título 9 de la parte 2 del libro 2 del Decreto 1078 de 2015, el cual es el Decreto Único Reglamentario del sector de Tecnologías de la Información y las Comunicaciones. En este contexto, se resaltan los Habilitadores Transversales para las entidades del estado: Seguridad de la Información, Arquitectura de TI y Servicios Ciudadanos Digitales.

Este documento comprensivo incluye objetivos específicos, generalidades, contexto, contexto normativo, definiciones, metodología de implementación y un detallado mapa de ruta con las actividades a ejecutar, especificando fechas y responsables. Es una herramienta integral diseñada para fortalecer la seguridad y privacidad de la información, garantizando así la confianza y eficacia en el manejo de esta por parte del Concejo.

PLAN DE TRATAMIENTO DE RIESGO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACION

1. OBJETIVOS

1.1 OBJETIVOS GENERALES

Establecer un marco de acción destinado a contribuir al tratamiento de riesgos de seguridad y privacidad de la información, focalizando la atención en los activos de información que respaldan el cumplimiento de los objetivos organizacionales. El objetivo primordial es preservar la confidencialidad, integridad y disponibilidad de la información institucional, considerando el contexto organizacional de la Corporación Edilicia, así como las capacidades y recursos disponibles. Este enfoque tiene como propósito reforzar la confianza de los ciudadanos, usuarios, socios y demás partes interesadas.

La planificación se centrará en fortalecer la implementación de acciones para el tratamiento de riesgos de seguridad y privacidad de la información, alineándonos con los lineamientos establecidos por el Ministerio de Tecnologías de la Información y las Comunicaciones y el Departamento Administrativo de la Función Pública.

1.2 OBJETIVOS ESPECIFICOS.

• Identificar los riesgos asociados a los procesos y los activos de información que hacen parte del alcance del SGSI

• Calcular el nivel de riesgo

• Establecer el plan de tratamiento de riesgos

• Realizar seguimiento y control a la eficacia del plan de tratamiento de riesgos

2. ALCANCE

La gestión de riesgos de seguridad de la información, incluido su tratamiento será aplicado sobre todos los activos de información del Concejo Municipal de Cartago - Valle identificados por cada uno de los procesos y que hacen parte del Registro de Activos de Información del Concejo; con base en las normas vigentes, la metodología definida por la entidad para la gestión del riesgo definida, las pautas y

recomendaciones previstas en la ISO 27001 para su seguimiento, monitoreo y evaluación enfocado al cumplimiento y mejoramiento continuo.

3. MARCO NORMATIVO

Decreto 1078 de 2015: Por medio del cual se expide el Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones.

Decreto 1008 de 2018: Por el cual se establecen los lineamientos generales de la política de Gobierno Digital y se subroga el capítulo 1 del título 9 de la parte 2 del libro 2 del Decreto 1078 de 2015, Decreto Único Reglamentario del sector de Tecnologías de la Información y las Comunicaciones.

NTC / ISO 27001:2013: Tecnología de la información. Técnicas de seguridad. Sistemas de gestión de la seguridad de la información (SGSI).

NTC/ISO 31000:2009: Gestión del Riesgo. Principios y directrices.

Guía para la administración del riesgo y el diseño de controles en entidades públicas – Versión 4. Riesgos de Gestión, Corrupción y Seguridad Digital Función Pública octubre 2018

4. DEFINICIONES

Administración del Riesgo: Conjunto de elementos de control que al Interrelacionarse brindan a la entidad la capacidad para emprender las acciones necesarias que le permitan el manejo de los eventos que puedan afectar negativamente el logro de los objetivos institucionales y protegerla de los efectos ocasionados por su ocurrencia.

Activo de Información: En relación con la seguridad de la información, se refiere a cualquier información o elemento de valor para los procesos de la Organización.

Análisis de Riesgos: Es un método sistemático de recopilación, evaluación, registro y difusión de información necesaria para formular recomendaciones orientadas a la adopción de una posición o medidas en respuesta a un peligro determinado.

Amenaza: Es la causa potencial de una situación de incidente y no deseada por la organización

Causa: Son todo aquello que se pueda considerar fuente generadora de eventos (riesgos). Las fuentes o agentes generadores son las personas, los métodos, las herramientas, el entorno, lo económico, los insumos o materiales entre otros.

Confidencialidad: Propiedad de la información de no ponerse a disposición o ser revelada a individuos, entidades o procesos no autorizados.

Consecuencia: Resultado de un evento que afecta los objetivos.

Criterios del riesgo: Términos de referencia frente a los cuales la importancia de un riesgo se evaluada.

Control: Medida que modifica el riesgo. 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.

Declaración de aplicabilidad: Documento que enumera los controles aplicados por el Sistema de Gestión de Seguridad de la Información – SGSI, de la organización tras el resultado de los procesos de evaluación y tratamiento de riesgos y su justificación, así como la justificación de las exclusiones de controles del anexo A de ISO 27001.

Disponibilidad: Propiedad de la información de estar accesible y utilizable cuando lo requiera una entidad autorizada.

Evaluación de riesgos: 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.

Evento: Un incidente o situación, que ocurre en un lugar particular durante un intervalo de tiempo específico.

Estimación del riesgo. Proceso para asignar valores a la probabilidad y las consecuencias de un riesgo.

Evitación del riesgo. Decisión de no involucrarse en una situación de riesgo o tomar acción para retirarse de dicha situación.

Factores de Riesgo: Situaciones, manifestaciones o características medibles u observables asociadas a un proceso que generan la presencia de riesgo o tienden a aumentar la exposición, pueden ser internos o externos a la entidad.

Gestión del riesgo: Actividades coordinadas para dirigir y controlar una organización con respecto al riesgo, se compone de la evaluación y el tratamiento de riesgos.

Identificación del riesgo. Proceso para encontrar, enumerar y caracterizar los elementos de riesgo.

Incidente de seguridad de la información: Evento único o serie de eventos de seguridad de la información inesperados o no deseados que poseen una probabilidad significativa de comprometer las operaciones del negocio y amenazar la seguridad de la información (Confidencialidad, Integridad y Disponibilidad).

Integridad: Propiedad de la información relativa a su exactitud y completitud.

Impacto. Cambio adverso en el nivel de los objetivos del negocio logrados.

Nivel de riesgo: Magnitud de un riesgo o de una combinación de riesgos, expresada en términos de la combinación de las consecuencias y su posibilidad.

Matriz de riesgos: Instrumento utilizado para ubicar los riesgos en una determinada zona de riesgo según la calificación cualitativa de la probabilidad de ocurrencia y del impacto de un riesgo.

Monitoreo: Mesa de trabajo anual, la cual tiene como finalidad, revisar, actualizar o redefinir los riesgos de seguridad de la información en cada uno de los procesos, partiendo del resultado de los seguimientos y/o hallazgos de los entes de con trol o las diferentes auditorías de los sistemas integrados de gestión.

Plan de tratamiento de riesgos: Documento que define las acciones para gestionar los riesgos inaceptables en el marco de la seguridad de la información e implantar los controles necesarios para proteger la misma.

Parte interesada: Persona u organización que puede afectar a, ser afectada por, o percibirse a sí misma como afectada por una decisión o actividad.

Propietario del riesgo: Persona o entidad con la responsabilidad de rendir cuentas y la autoridad para gestionar un riesgo.

Proceso: Conjunto de actividades interrelacionadas que apuntan a un objetivo o que interactúan para transformar una entrada en salida.

Riesgo en la seguridad de la información: 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 Inherente: Es el nivel de riesgo propio de la actividad, sin tener en cuenta el efecto de los controles.

Riesgo Residual: El riesgo que permanece tras el tratamiento del riesgo o nivel resultante del riesgo después de aplicar los controles.

Reducción del riesgo. Acciones que se toman para disminuir la probabilidad las consecuencias negativas, o ambas, asociadas con un riesgo.

Retención del riesgo: Aceptación de la pérdida o ganancia proveniente de un riesgo particular.

Seguridad de la información: Preservación de la confidencialidad, integridad y disponibilidad de la información.

Seguimiento: Mesa de trabajo semestral, en el cual se revisa el cumplimiento del plan de acción, indicadores y metas de riesgo y se valida la aplicación de los controles de seguridad de la información sobre cada uno de los procesos.

Tratamiento del Riesgo: Proceso para modificar el riesgo" (Icontec Internacional, 2011).

Valoración del Riesgo: Proceso global de identificación del riesgo, análisis del riesgo y evaluación de los riesgos.

Vulnerabilidad: Debilidad de un activo o control que puede ser explotada por una o más amenazas.

5. DESARROLLO DEL PLAN

5.1 IDENTIFICACIÓN Y VALORACIÓN DE RIESGOS

La técnica de análisis de riesgo para activos de información nos permite desde un punto de vista orientado al negocio y sistémico en su naturaleza, comprender claramente los riesgos sobre los activos de información a los que puede estar expuesto el Concejo Municipal de Cartago. Es recomendable contar con técnicas tradicionales para identificar los riesgos específicos asociados a los activos y complementar este proceso en la medida de lo posible con la identificación de puntos críticos de fallas, análisis de disponibilidad, análisis de vulnerabilidad, análisis de confiabilidad y árboles de falla.

El plan propuesto en este documento comprende, como se detallará más adelante, las siguientes actividades principales: establecimiento del contexto, identificación riesgos, estimación de riesgos, evaluación de riesgos, tratamiento de riesgo y aceptación del riesgo, guardando coherencia con la Guía para la administración del riesgo y el diseño de controles en entidades públicas V6, emitida por el Departamento Administrativo de la Función Pública.

La gestión del riesgo dentro de la seguridad de la información se puede también enmarcar dentro del ciclo de planear, hacer, verificar y actuar (PHVA) tal como se muestra en la siguiente ilustración (ISO 27001:2013):

Ilustración 2. Ciclo PHVA y la gestión de riesgos

5.1.1 Programación y Agendamiento de Entrevistas

En esta fase se seleccionan los procesos incluidos en el alcance del SGSI del Concejo y se procede a programar y a agendar a los líderes de las dependencias y

grupos internos de trabajo que conforman los procesos, para la identificación de riesgos.

5.1.2 Entrevista con los Líderes

Se entrevista a cada líder de dependencia o grupo, se presenta la metodología y en conjunto se procede a realizar la identificación de los riesgos sobre los activos de información, los cuales se consignan en la Matriz de Riesgos.

5.1.3 Identificación y Calificación de Riesgos

En esta fase, el líder de proceso evalúa el nivel de impacto vs. Probabilidad y los controles existentes para calcular el nivel de riesgo.

5.1.4 Valoración del Riesgo Residual

En esta fase se hace una proyección de la eficacia de los controles para calcular el riesgo residual.

5.1.5 Mapas De Calor Donde Se Ubican Los Riesgos

Luego se procede a ubicar los riesgos en un mapa de calor para visualizar su comportamiento a medida que se van aplicando los controles.

5.2 TRATAMIENTO DE RIESGOS DE SEGURIDAD DE LA INFORMACION

Una vez ejecutadas las etapas de análisis y valoración de riesgos, y con base en los resultados obtenidos en la determinación real de riesgos, es necesario tomar decisiones aplicando el apetito de riesgos definido por el Concejo Municipal.

Si el riesgo se ubica en una zona no aceptable, cada líder responsable de los riesgos identificados debe definir e implementar los controles necesarios para llevar el riesgo a un nivel aceptable a través del plan de tratamiento de riesgos.

A continuación, se definen las siguientes estrategias de tratamiento, asumir los riesgos bajos y moderados y gestionar el riesgo alto y extremo y se muestra la estrategia para abordar los riesgos y establecer su tratamiento:

PROCESO	ASUMIR EL RIESGO		REDUCIR EL RIESGO		TOTAL
	BAJO	MODERADO	ALTO	EXTREMO	
Gestión Direccionamiento Estratégico	8		4		12
Gestión Pública	5		1		6
Gestión Talento Humano	9		4		13
Gestión TICs	4				4
Gestión Jurídica	9	3			12
Gestión Documental	2		3		5
TOTAL	**37**	**3**	**12**	**0**	**52**

Controles recomendados Frente a los 6 riesgos con estrategia de mitigación, para su gestión se proponen los siguientes controles de la norma ISO 27001 – Anexo A:

CODIGO	PROCESO
P1	Gestión Direccionamiento Estratégico
P2	Gestión Pública
P3	Gestión Talento Humano
P4	Gestión TICs
P5	Gestión Jurídica
P6	Gestión Documental

CONTROLES		PROCESOS DEL CONCEJO MUNICIPAL														TOTAL
COD	NOMBRE	P1	P2	P3	P4	P5	P6	P7	P8	P9	P10	P11	P12	P13	P14	
A.7.1.1	Selección													1	1	2
A.7.2.2	Toma de conciencia, educación y formación de la seguridad de la información										3	3				6
A.9.3	Responsabilidad de los usuarios		3	3	2	2										10
A.10.1.1	Política sobre el uso de controles criptográficos											1				1
A.11.1.1	Perímetro de Seguridad Física										2					2

CONTROLES		PROCESOS DEL CONCEJO MUNICIPAL														TOTAL
COD	NOMBRE	P1	P2	P3	P4	P5	P6	P7	P8	P9	P10	P11	P12	P13	P14	
A.11.1.3	Seguridad de Oficina, Salones e Instalaciones										2					2
A.11.1.4	Protección contra amenazas externas y ambientales						1	3								4
A.11.2.1	Ubicación y protección de los Equipos										3					3
A.11.2.2	Servicios públicos de soportes	1	1						1							3
A.11.2.4	Mantenimiento de Equipos											1				1
A.12.3.1	Copias de respaldo de la información												1	1		2
A.15.2	Gestión de la prestación de servicios de proveedores	2							1	1						4
TOTAL		**3**	**4**	**3**	**2**	**2**	**1**	**3**	**2**	**1**	**10**	**5**	**1**	**2**	**1**	40

En general, el control que más aplica es A.9.3. Responsabilidades de los usuarios, seguido de: A.7.2.2. Toma de conciencia, educación y formación de la Seguridad de la Información, A.11.1.4. Protección contra amenazas externas y ambientales, y A.15.2. Gestión de la prestación de servicios de proveedores.

5.3 SEGUIMIENTO Y CONTROL

El seguimiento y control se realiza de acuerdo con la GUÍA PARA LA ADMINISTRACIÓN DE RIESGO de la Función Pública.

6 CRONOGRAMA

Para dar cumplimiento al ciclo de riesgo, el cronograma se establece anualmente, los riesgos de seguridad digital identificados se reflejarán en el Mapa de Riesgos Institucional, donde se establecerán las acciones de control y las fechas para implementar dichos controles, la oficina de sistemas e informática o el despacho delegado apoyará el proceso de definición de los controles con los líderes de cada uno de los grupos o dependencias.

Según lo expuesto en la Guía para la Administración del Riesgo y el Diseño de Controles en Entidades Públicas emitida por el Departamento Administrativo de la Función Pública, el tratamiento de riesgos es la respuesta establecida por la primera línea de defensa para la mitigación de los diferentes riesgos, por lo tanto dicha

planeación en este caso en particular, hace alusión al tratamiento de riesgos de Seguridad y Privacidad de la Información enfocado en la seguridad de la información sobre los activos de información a cargo de Secretaria General, para lo cual se realizan un conjunto de actividades durante la vigencia orientadas a implementar los controles requeridos y priorizados. En atención a lo anterior, a continuación, se describen las actividades más relevantes orientadas al tratamiento de riesgos de Seguridad y Privacidad de la Información.

La implementación se desarrolla en 4 ciclos, los cuales se definen a continuación:

ACTIVIDADES	FEBRERO – JUNIO 2024		JULIO – NOVIEMBRE 2024	
	CICLO 1		CICLO 2	
	Identificación y Valoración de Riesgos	Tratamiento de Riesgos	Seguimiento y Control	
Programación y Agendamiento de Entrevistas				
Entrevista con los líderes				
Identificación y Calificación de Riesgos				
Valoración del Riesgo Residual				
Mapas de Calor donde se ubican los riesgos				
Identificación y publicación Plan de Tratamiento de Riesgos				
Monitoreo y Seguimiento				

7. RECURSOS

La estimación y asignación de los recursos para el plan de tratamiento de riesgos de Seguridad 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.

Si el establecimiento de los controles implica la adquisición de herramientas tecnológicas bajo la responsabilidad del funcionario delegado de las TICs o el despacho delegado, los recursos de inversión se tomarán del proyecto.

“Fortalecimiento de las tecnologías de la información y la comunicación del plan desarrollo”.

8. INDICADORES

La medición se realiza con un indicador de gestión que está orientado principalmente a disminuir el número de riesgos identificados con nivel alto y externo a través de la implementación y evaluación de controles.

El número de riesgos identificados como no aceptables no debe ser superior al 20% del total de riesgos identificados.

9. CONSIDERACIONE GENERALES

El desarrollo de las actividades para lograr su consecución estará sujeto a la disponibilidad de recursos (humanos, técnicos, tecnológicos, financieros) que faciliten el cumplimiento de las actividades; de acuerdo con la disponibilidad presupuestal oportuna, al apetito de riesgo institucional y a las orientaciones de la alta dirección, en cuanto al apetito de riesgo institucionales que han adoptado para afrontar el desarrollo y cumplimiento de las actividades planificadas.

Para el desarrollo de las actividades, la Secretaría encargada del desarrollo de este Plan contará con un equipo humano dispuesto para adelantar actividades de sensibilización, capacitación y atención de inquietudes a las dependencias adscritas al Concejo a nivel central a través de cronogramas definidos.