COMITE DE TRATAMIENTO DE Riesgos

Actualización, Diciembre de 2024

ALCALDÍA DE CHÍA

1. INTRODUCCION

El objetivo fundamental del Plan de tratamiento de riesgos de Seguridad de la Información, es evaluar las posibles acciones que se deben tomar para mitigar los riesgos existentes teniendo en cuenta los criterios de aceptación de riesgos definidos por la Alcaldía de Chía. Dichas acciones deben ser conocidas, tratadas y ejecutadas por las secretarias y/o dependencias de la Administración Municipal de una forma documentada, sistemática, estructurada y eficiente.

En la medida que se tenga una visión de los riesgos que puedan afectar la seguridad de la información, la Oficina TIC puede establecer controles y medidas efectivas, viables y transversales, con el propósito de preservar la disponibilidad, integridad y confidencialidad de su información, para lo cual es necesario definir los lineamientos que se deben seguir para el análisis y evaluación de los riesgos de seguridad de la información de la Entidad.

Lo anterior dando cumplimiento a la normativa establecida por el estado colombiano y adoptando las buenas prácticas y los lineamientos de los estándares ISO/IEC 27001:2013, ISO 31000:2018 y la guía para la administración del riesgo y el diseño de controles en entidades públicas emitida por el DAFP (Departamento Administrativo de la Función Pública).

2. ALCANCE

El plan de tratamiento de riesgos de seguridad de la información es aplicable a todos los procesos de la Alcaldía Municipal de Chía, con alcance a los colaboradores de todos los niveles; desde la identificación de los riesgos de seguridad de la información que se encuentran en los niveles “Alto” y “Extremo” en la Matriz de riesgos de Seguridad de la información de la Alcaldía Municipal de Chía hasta la definición del plan de tratamiento, responsables y fechas de implementación.

3. JUSTIFICACIÓN

Este documento busca preservar la confidencialidad, integridad y disponibilidad de la información, permitiendo garantizar la privacidad de los datos, mediante la aplicación del proceso de gestión del riesgo, brindando confianza a las partes interesadas acerca de la adecuada gestión de riesgos y apoyando el “Modelo de Seguridad y Privacidad de la Información – MSPI”

4. OBJETIVO

4.1 Objetivo General

Detallar el plan de tratamiento de riesgos que hace parte del Sistema de Gestión de Seguridad de la Información – SGSI de la Unidad Nacional para la gestión del Riesgo de Desastres, mediante el cual se definen los controles que permiten mitigar la materialización de los riesgos de seguridad de la información en la Alcaldía Municipal de Chía.

4.2 Objetivos Específicos

- Identificar los riesgos asociados a los procesos y los activos de información que hacen parte del alcance del SGSI
- Calcular el nivel del riesgo
- Establecer seguimiento y control a la eficacia del plan de tratamiento de riesgos

5. TERMINOS Y DEFINICIONES

- **Activos de Información:** aquello que es de alta validez y que contiene información vital de la Alcaldía Municipal de Chía que debe ser protegida.
- **Amenaza:** es un ente o escenario interno o externo que puede hacer uso de una vulnerabilidad para generar un perjuicio o impacto negativo en la Entidad (materialización del riesgo).
- **Asumir/Aceptar:** la Entidad acepta el riesgo en relación con sus objetivos, el marco legal y las disposiciones de la alta dirección y lo asume conociendo los efectos de su posible materialización.
- **Control o Medida:** acciones o mecanismos definidos para prevenir o reducir el impacto de los eventos que ponen en riesgo, la adecuada ejecución de las actividades y tareas requeridas para el logro de objetivos de los procesos de una entidad.
- **Evaluación del Riesgo:** Proceso de comparar los resultados del análisis de riesgo con los criterios de riesgo para determinar si el riesgo y/o su magnitud es aceptable o tolerable. La evaluación de riesgos ayuda en la decisión sobre el tratamiento de riesgos.
- **Impacto:** son las consecuencias que genera un riesgo una vez se materialice.
- **Probabilidad:** es la probabilidad de la amenaza aproveche la vulnerabilidad para materializar el riesgo.
- **Reducir/Mitigar:** el riesgo se trata mediante la transferencia o la implementación de acción que mitiguen su nivel. No necesariamente es un control adicional.

- **Riesgo:** es un escenario bajo el cual una amenaza puede explotar una vulnerabilidad generando un impacto negativo al negocio evitando cumplir con sus objetivos.
- **Vulnerabilidad:** es una falencia o debilidad que puede estar presente en la tecnología, las personas o en las políticas y procedimientos.
- **Seguridad de la Información:** este principio busca crear condiciones de uso confiable en el entorno digital, mediante un enfoque basado en la gestión de riesgos, preservando la confidencialidad, integridad y disponibilidad de la información de las entidades del Estado, y de los servicios que prestan al ciudadano.

SIGLAS

ISO: International Standard Organization.

MINTIC: Ministerio de Tecnología de la Información y las Comunicaciones.

MOP: Modelo de operación por procesos.

MSPI: Modelo de Seguridad y Privacidad de la Información. SGSI: Sistema de Gestión de Seguridad de la Información. TI: Tecnología de información.

TIC: Tecnologías de la información y la comunicación.

6. NORMOGRAMA

- Ley 909 de 2004: "Por la cual se expiden normas que regulan el empleo público, la carrera administrativa, gerencia pública y se dictan otras disposiciones".
- Ley 1581 de 2012: "Por la cual se dictan disposiciones generales para la protección de datos personales".
- Ley 1712 de 2014: "Por medio de la cual se crea la Ley de Transparencia y del Derecho de Acceso a la Información Pública Nacional y se dictan otras disposiciones".
- Decreto Ministerial 1078 de 2015: "Por medio del cual se expide el Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones".
- Decreto Presidencial 1083 de 2015: "Por medio del cual se expide el Decreto Único Reglamentario del Sector de Función Pública", el cual establece las políticas de Gestión y Desempeño Institucional, entre las que se encuentran las de "11. Gobierno Digital, antes Gobierno en Línea" y "12. Seguridad Digital".

- Decreto Municipal 883 de 2015: "Por el cual se adecúa la Estructura de la Administración Municipal de Medellín, las funciones de sus organismos, dependencias y entidades descentralizadas, se modifican unas entidades descentralizadas y se dictan otras disposiciones".
- Decreto Presidencial 612 de 2018: "Por el cual se fijan directrices para la integración de los planes institucionales y estratégicos al Plan de Acción por parte de las entidades del Estado".
- Decreto Presidencial 767 de 2022: "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".
- Resolución Ministerial 00500 de 2021: "Por la cual se establecen los lineamientos y estándares para la estrategia de seguridad digital y se adopta el modelo de seguridad y privacidad como habilitador de la política de gobierno digital".
- ISO/IEC 27001:2013: Tecnología de la información-Técnicas de seguridad
- Ley 1273 de 2009, "Por medio de la cual se modifica el código penal, se crea un nuevo bien jurídico tutelado – denominado "de la protección de la información y de los datos" y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones".

7. PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE ACTIVOS DE INFORMACIÓN POR CATEGORÍAS

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 cada una de las secretarias y/o dependencias de la administración, para lo cual se proponen 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:

Carrera 7 N° 12-100
PBX: (601) 884 4444 Ext. 2300-2301
oficinatic@chia.gov.co
www.chia-cundinamarca.gov.co

Actividad	Responsable	1 Semestre						2 Semestre					
		2025						2025					
		E	F	M	A	M	J	J	A	S	O	N	D
Realizar la Adquisición e implementación de controles de seguridad de la información para abordar los riesgos de seguridad y privacidad de la información identificados, analizados, valorados y priorizados sobre los activos de información bajo la responsabilidad de cada dependencia a nivel central.	Todas las Secretarías, departamentos Administrativos y Gerencias a nivel central del Municipio.					X	X	X	X	X	X	X	X
Realizar los procesos requeridos para el seguimiento a la operación de los controles de seguridad de la información para abordar los riesgos de seguridad y privacidad de la información identificados, analizados, valorados y priorizados sobre los activos de información bajo la responsabilidad de cada dependencia a nivel central.	Todas las Secretarías, Departamentos Administrativos y Gerencias a nivel central del Municipio.					X	X	X	X	X	X	X	X
Realizar el seguimiento a las actividades de identificacion y operación de controles de seguridad de la información para abordar los riesgos de seguridad y privacidad de la información identificados, analizados, valorados y priorizados sobre los activos de información bajo la responsabilidad de cada dependencia a nivel central.	Oficina TIC					X		X			X		X

Tabla 1. Actividades tratamiento de riesgos de seguridad.
Semestre – mes correspondiente

Carrera 7 N° 12-100
PBX: (601) 884 4444 Ext. 2300-2301
oficinatic@chia.gov.co
www.chia-cundinamarca.gov.co

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 afán de riesgo institucional y a las orientaciones de la alta dirección, en cuanto al afán de riesgo institucionales que han adoptado para afrontar el desarrollo y cumplimiento de las actividades planificadas.

Para el desarrollo de las actividades, la Oficina TIC contará con un equipo humano dispuesto para adelantar actividades de sensibilización, capacitación y atención de inquietudes a las dependencias de la Administración Municipal a nivel central a través de cronogramas definidos.

La Oficina TIC ha establecido unos tiempos en los cuales se brindará y apoyará el seguimiento al desarrollo de los planes de seguridad y privacidad de la información que las dependencias presenten y así tratar las actividades pertinentes a los procesos relacionados al diligenciamiento de los planes de seguridad y privacidad de la información.

8. POLITICA DE ADMINISTRACION DE RIESGOS

La Oficina TIC de la Alcaldía Municipal de Chía, a través de su Modelo Integrado de Gestión, se compromete a mantener una cultura de la gestión del riesgo TIC, asociados con la responsabilidad de diseñar, adoptar y promover las políticas, programas y proyectos del sector TIC, regulando los riesgos de los procesos y proyectos luchando continuamente contra la corrupción, mediante mecanismos, sistemas y controles enfocados a la prevención y detección de hechos asociados a este fenómeno y fortaleciendo las medidas de control y la eficiencia a lo largo del ciclo de vida del proyecto para optimizar de manera continua y oportuna la respuesta a los riesgos además de los de seguridad y privacidad de la información y seguridad digital de manera integral.

La política identifica las opciones a tratar y manejar los riesgos basados en su valoración, permiten tomar decisiones adecuadas y fijar los lineamientos para la administración de estos; a su vez transmiten la posición de la dirección y establecen las guías de acción necesarias a todos los colaboradores de la Alcaldía Municipal de Chía. Se deben tener en cuenta algunas de las siguientes opciones, las cuales pueden considerarse independientemente, interrelacionadas o en un conjunto:

- Evitar: es eliminar la probabilidad de ocurrencia o disminuir totalmente el impacto, lo que requiere la eliminación de la actividad o fuente de riesgo, eliminar la exposición y su expresión máxima es dejar una actividad. Por ejemplo, para evitar perdida de documentación se prohíbe el ingreso a un área.

Carrera 7 N° 12-100
PBX: (601) 884 4444 Ext. 2300-2301
oficinatic@chia.gov.co
www.chia-cundinamarca.gov.co

• Prevenir: corresponde al área de planeación, esto es, planear estrategias conducentes a que el evento no ocurra o que disminuya su probabilidad. Un ejemplo de ello son las inspecciones el mantenimiento preventivo, las políticas de seguridad o las revisiones periódicas a los procesos

• Reducir o mitigar: corresponde a la protección en el momento en que se presenta el riesgo se encuentra en esta categoría los planes de emergencia planes de contingencia equipos de protección personal, ambiental, de acceso mantener copias de respaldo

• Dispersar: es dividir una actividad en diferentes componentes operativos, de manera que las actividades no se concentren en un mismo sitio o bajo una sola responsabilidad. Este es el caso de los contratos de suministro de partes, la ubicación de nodos, plantas alternas, equipos paralelos, contratar obras por tramos

• Compartir: es involucrar a un tercero para que responda en todo o en parte por el riesgo que genera una actividad. Dentro de los mecanismos de transferencia se encuentran los siguientes: contratos de seguro, transferencia explicita por medio de cláusulas contractuales, derivados financieros.

Los riesgos detectados deberán ser analizados de tal forma que se pueda determinar cuál va a ser su tratamiento. Así mismo, teniendo en cuenta lo expuesto en la Guía de Gestión de Riesgos de Seguridad y Privacidad de la Información (MinTIC:2016), en los " riesgos no se debe olvidar que dentro del análisis de los controles se debe tener en cuenta al dueño del riesgo (dueño del proceso), ya que la definición de los controles es el resultado de los análisis realizados a través del seguimiento y aplicación de los pasos descritos anteriormente en el tratamiento del riesgo y los cuales deben tener el concurso de todos los interesados".

Carrera 7 N° 12-100
PBX: (601) 884 4444 Ext. 2300-2301
oficinatic@chia.gov.co
www.chia-cundinamarca.gov.co

9. METODOLOGIA

El plan de tratamiento de riesgos contempla la definición de las actividades a desarrollar en aras de mitigar los riesgos sobre los activos, estas actividades se estructuraron de la siguiente manera, siguiendo las recomendaciones de la Guía de Gestión de Riesgos de Seguridad y Privacidad de la Información.

GESTION	ACTIVIDAD	TAREA	RESPONSABLE	FECHA DE INICIO	FECHA DE FIN
Gestión de Riesgos	Actualización de lineamientos de riesgo TIC	Actualizar política y metodología de gestión de riesgos TIC	Equipo de Gestión de Riesgos	Marzo 2024	Marzo 2027
	Sensibilización	Socialización guía y herramienta de gestión de riesgo de seguridad y privacidad de la información, seguridad digital y continuidad de la operación	Equipo de Gestión de Riesgos	Marzo 2024	Marzo 2027
	Identificación de riesgos de seguridad y privacidad de la información, seguridad digital y continuidad de la operación	Identificación, análisis y evaluación de riesgos – seguridad y privacidad de la información, seguridad digital y continuidad de la operación.	Equipo de Gestión de Riesgos	Marzo 2024	Marzo 2027
		Realimentación, revisión y verificación de los riesgos TIC, identificados (Ajustes)	Equipo de Gestión de Riesgos	Marzo 2024	Marzo 2027
	Aceptación de riesgos identificados	Aceptación, aprobación riesgos TIC identificados y planes de tratamiento	Equipo de Gestión de Riesgos	Marzo 2024	Marzo 2027
	Publicación	Publicación matriz de riesgos TIC	Equipo de Gestión de Riesgos	Marzo 2024	Marzo 2027

	Seguimiento fase de tratamiento	Seguimiento estado planes de tratamiento de riesgos TIC identificados y verificación de evidencias	Equipo de Gestión de Riesgos	Marzo 2024	Marzo 2027
	Evaluación de riesgos residuales	Evaluación de riesgos TIC residuales	Equipo de Gestión de Riesgos	Marzo 2024	Marzo 2027
	Mejoramiento	Identificación de oportunidades de mejora acorde a los resultados obtenidos durante la evaluación de riesgos TIC residuales	Equipo de Gestión de Riesgos	Marzo 2024	Marzo 2027
		Actualización Guía gestión de Riesgos Seguridad de la información, de acuerdo con los cambios solicitados	Equipo de Gestión de Riesgos	Marzo 2024	Marzo 2027
	Monitoreo y Revisión	Generación, presentación y reporte de indicadores	Equipo de Gestión de Riesgos	Marzo 2024	Marzo 2027

9.1 DESARROLLO METODOLOGICO

• Fase 1: Análisis de la información

En esta etapa se evaluarán los resultados de las entrevistas con los colaboradores del proceso de TI, se desarrollarán las siguientes actividades:

- Aplicar las políticas de tratamiento de riesgos.
- Determinar los controles (se desprenden de las medidas) según los lineamientos del Ministerio TIC.
- Determinar los riesgos que van a ser incluidos en el Plan de Tratamiento de Riesgos TIC.

• Fase 2: Desarrollo de los proyectos

En esta fase se realizarán las actividades que permitan la estructuración de las medidas.

- Determinar el nombre de la medida.

- Definir los responsables de cada medida.
- Establecer el objetivo de cada medida.
- Elaborar la justificación de la medida.
- Definir las actividades a realizar para el desarrollo de la medida.

• Fase 3: Análisis de los proyectos

- Definición de los controles relacionados con cada medida.
- Validar los riesgos TIC mitigados por cada medida.
- Análisis de la aplicabilidad de las medidas.
- Priorización de las medidas.

• Fase 4: Definición del organigrama de responsabilidad

En esta fase se realizará un organigrama y se definirán responsabilidades respecto a la administración y gestión del riesgo, esta etapa deberá ser definida por la Alcaldía Municipal de Chía, teniendo en cuenta su estructura organizacional para la gestión de riesgos.

- Identificación de las funciones de la Alcaldía Municipal de Chía en materia de seguridad de la información.
- Definición del grupo de trabajo de gestión de riesgo por parte de la Alcaldía Municipal de Chía.
- Definición de las funciones del grupo de trabajo referentes a la aplicación y gestión de las medidas.

• Fase 5: Ciclo de vida del tratamiento de riesgos

Definir las actividades a realizar por cada uno de los elementos del ciclo de vida del Plan de Tratamiento de Riesgos.

Planear: Dentro de esta etapa se desarrollan las actividades definidas en la fase 1 de la metodología de tratamiento de riesgos.

Hacer: En este paso del ciclo de vida se desarrollarán las actividades enmarcadas en la fase 2 de la metodología del tratamiento de riesgos.

Verificar: En esta etapa se desarrollarán las actividades que permiten hacer seguimiento o auditorías a la ejecución de cada una de las medidas.

Actuar: Dentro de esta etapa se realizarán las mejoras teniendo en cuenta el seguimiento y los resultados de las auditorías de la ejecución de los proyectos.

Carrera 7 N° 12-100
PBX: (601) 884 4444 Ext. 2300-2301
oficinatic@chia.gov.co
www.chia-cundinamarca.gov.co

9.2. OPORTUNIDAD DE MEJORA

La Oficina TIC no sólo deberá centrarse en los riesgos identificados, sino que este análisis o apreciación del riesgo TIC debe ser la base para identificar oportunidades. Por lo anterior la oportunidad deberá entenderse como la consecuencia positiva frente al resultado del tratamiento del Riesgo.

Teniendo en consideración la guía metodológica gestión de riesgos para SGSI de la Alcaldía Municipal de Chía, en la definición del plan de tratamiento de riesgos de seguridad de la información se realizaron las siguientes actividades en conjunto con los colaboradores asignados para cada proceso de la entidad:

Identificación de los riesgos, que superan los niveles aceptables definido por los riesgos de seguridad de la información y la zona del riesgo.

Riesgo Estratégico: Se asocia con la forma en que se administra la Entidad. El manejo del riesgo estratégico se enfoca a asuntos globales relacionados con la misión y el cumplimiento de los objetivos estratégicos, la clara definición de políticas, diseño y conceptualización de la entidad por parte de la alta gerencia.

Riesgos de Imagen: están relacionados con la percepción y la confianza por parte d la ciudadanía hacia la entidad.

Riesgos Operativos: Comprenden riesgos provenientes del funcionamiento y operatividad de los sistemas de información institucional, de la definición de los procesos, de la estructura de la entidad, de la articulación entre dependencias.

Riesgos Financieros: se relacionan con el manejo de los recursos de la entidad que incluyen: la ejecución presupuestal, la elaboración de los estados financieros, los pagos, manejos de excedentes de tesorería y el manejo sobre los bienes.

Riesgos de cumplimiento: se asocian con la capacidad de la entidad para cumplir con los requisitos legales, contractuales, de ética pública y en general con su compromiso ante la comunidad.

Riesgos de Tecnología: Están relacionados con la capacidad tecnológica de la entidad para satisfacer sus necesidades actuales y futuras y el cumplimiento de la misión.

- Identificación de los Activos: Un activo es todo aquello que tiene valor para la administración municipal y que, por lo tanto, requiere de protección. La realización de un inventario y clasificación de activos hace parte de la diligencia que a nivel estratégico se ha definido en el Modelo de seguridad y Privacidad de la información (MSPI) con respecto a la seguridad de los activos de información de los procesos de la Alcaldía.

En la creación del inventario de activos realizada en la Alcaldía de Chía se establecieron criterios específicos y lineamientos para el tratamiento adecuado del activo, con el fin

identificar qué valor tiene activos. La siguiente tabla define los criterios del activo.

Criterios de clasificación

CONFIDENCIALIDAD	INTEGRIDAD	DISPONIBILIDAD
INFORMACION PUBLICA RESERVADA	ALTA (A)	ALTA (1)
INFORMACION PUBLICA CLASIFICADA	MADIA (M)	MEDIA (2)
INFORMACION PUBLICA	BAJA (B)	BAJA (3)
NO CLASIFICADA	NO CLASIFICADA	NO CLASIFICADA

Fuente: Guía para gestión y clasificación de activos de información. Min TIC

Niveles de clasificación

ALTA	Activos de información en los cuales la clasificación de la información en dos (2) o todas las propiedades (Confidencialidad, integridad y disponibilidad) es alta.
MEDIA	Activos de información en los cuales la clasificación de la información es alta en una (1) de sus propiedades o al menos una de ellas es de nivel medio.
BAJA	Activos de información en los cuales la clasificación de la información en todos sus niveles es baja.

Fuente: Guía para gestión y clasificación de activos de información. Min TIC

Con la identificación del inventario de activos de información, permite clasificar los activos a los que se les debe brindar mayor protección, pues se identifica claramente sus características y rol al interior de un proceso.

Aspectos importantes a tener en cuenta en los riesgos que se detectaron, son: Mejorar el proceso de contratación con proveedores de desarrollo de software o manejo de bases de datos para que la información como código fuente y silos de información sean entregados a la administración municipal al finalizar el contrato.

Disponer recursos financieros para servidores o repositorios en las secretarias dependencias que manejen volúmenes de información alta, por ejemplo, prensa, planeación (cartografía). Además de salvaguardar la información producida por OPS que manejan computadores personales.

Se tiene la necesidad que el datacenter cuente con redundancia geográfica y en alta disponibilidad o de manera mixta de acuerdo a los activos que maneja cada dependencia/secretaria.

Luego de identificar los activos de información, por lo anterior se identifican las amenazas que pueden ser de origen natural o humano y podrían ser accidentales o deliberadas.

A continuación, se describen una serie de amenazas comunes.

D= Deliberadas, A=Accidentales, E= Ambientales

TIPO	AMENAZA	ORIGEN
Daño Físico	Fuego	A, D, E
	Agua	A, D, E
	Contaminación	A, D, E
	Accidente Importante	A, D, E
	Destrucción del equipo o medios	A, D, E
	Polvo, corrosión, congelamiento	A, D, E
Eventos Naturales	Fenómenos climáticos	E
	Fenómenos sísmicos	E
	Fenómenos volcánicos	E
	Fenómenos meteorológico	E
	Inundación	E
Perdida de los servicios esenciales	Fallas en el sistema de suministro de agua o aire acondicionado	A, D
	Perdida de suministro de energía	A, D
	Falla en equipo de telecomunicaciones	A, D, E
Perturbación debida a la radicación	Radiación electromagnética	A, D, E
	Radiación térmica	A, D, E
	Impulsos electromagnéticos	E
Compromiso de la información	Interceptación de señales de interferencia comprometida	D
	Espionaje remoto	D
	Escucha encubierta	D
	Hurto de medios o documentos	D
	Hurto de equipo	D
	Recuperación de medios reciclados o desechados	D
	Divulgación	D

Carrera 7 N° 12-100
PBX: (601) 884 4444 Ext. 2300-2301
oficinatic@chia.gov.co
www.chia-cundinamarca.gov.co

	Datos provenientes de fuentes no confiables	D, A
	Manipulación con hardware	D, A
	Manipulación con software	D, A
	Detección de la posición	D
Fallas técnicas	Fallas del equipo	D, A
	Mal funcionamiento del equipo	D, A
	Saturación del sistema de información	D
	Mal funcionamiento del software	D, A
	Incumplimiento en el mantenimiento del sistema de información	D
Acciones no autorizadas	Uso no autorizado del equipo	D
	Copia fraudulenta del software	D
	Uso de software falso copiado	D, A
	Corrupción de los datos	D, A
	Procesamiento ilegal de datos	D
Corrupción de las funciones	Error en el uso	D, A
	Abuso de derechos	D
	Falsificación de derechos	D
	Negación de acciones	D
	Incumplimiento en la disponibilidad del personal	D

Carrera 7 N° 12-100
PBX: (601) 884 4444 Ext. 2300-2301
oficinatic@chia.gov.co
www.chia-cundinamarca.gov.co

Amenazas Humanas

FUENTE DE AMENAZA	MOTIVACION	ACCIONES AMENAZANTES
Pirata informático, intruso ilegal	Reto Ego Rebelión Estatus Dinero	• Piratería • Ingeniería Social • Intrusión, accesos forzados al sistema • Acceso no autorizado
Criminal de la computación	Destrucción de la información Divulgación ilegal de la información Ganancia monetaria Alteración no autorizada de los datos	• Crimen por computador • Acto fraudulento • Soborno de la información • Suplantación de identidad • Intrusión en el sistema
Terrorismo	Chantaje Destrucción Explotación Venganza Ganancia política Cubrimiento de los medios de comunicación	• Bomba/Terrorismo • Guerra de la información • Ataques contra el sistema DDoS • Penetración en el sistema • Manipulación en el sistema
Espionaje industrial (inteligencia, empresas, gobiernos extranjeros, otros intereses)	Ventaja competitiva Espionaje económico	• Ventaja de defensa • Ventaja política • Explotación económica

Carrera 7 N° 12-100
PBX: (601) 884 4444 Ext. 2300-2301
oficinatic@chia.gov.co
www.chia-cundinamarca.gov.co

		• Hurto de información • Intrusión en privacidad personal • Ingeniería social • Penetración en el sistema • Acceso no autorizado al sistema
Intrusos (Empleados con entrenamiento deficiente, descontentos, malintencionados, negligentes, deshonestos o despedidos)	Curiosidad Ego Inteligencia Ganancia monetaria Venganza Errores y omisiones no intencionales (ej. Error en el ingreso de datos, error de programación)	• Asalto a un empleado • Chantaje • Observar información reservada • Uso inadecuado del computador • Fraude y hurto • Soborno de información • Ingreso de datos falsos o corruptos • Interceptación • Código malicioso • Venta de información personal • Errores en el sistema • Intrusión al sistema • Sabotaje del sistema • Acceso no autorizado al sistema.

- **Opción de Tratamiento:** según la zona donde se ubica el riesgo residual, se determina la opción o estrategia de tratamiento a seguir para combatir el riesgo, para esta actividad se debe considerar la siguiente tabla:

ZONA DE RIESGO RESIDUAL	NIVEL DE RIESGO ACEPTABLE	OPCION O ESTRATEGIA DE TRATAMIENTO A SEGUIR
Bajo	Aceptable	Asumir/Aceptar
Moderado	Aceptable	Asumir/Aceptar
Alto	No Aceptable	Reducir/Mitigar
Extremo	No Aceptable	Reducir/Mitigar

Carrera 7 N° 12-100
PBX: (601) 884 4444 Ext. 2300-2301
oficinatic@chia.gov.co
www.chia-cundinamarca.gov.co

- **Riesgo del tratamiento del riesgo.** El registro del tratamiento de riesgo de seguridad de la información se realiza en los siguientes campos:
- **Opción de tratamiento:** Campo se calcula automáticamente de acuerdo con la valoración del riesgo residual, teniendo en cuenta el nivel de Riesgo Aceptable.
- **Acciones de mejora:** es la relación del control teniendo en cuenta la siguiente estructura; responsable de la ejecución + acción realizada + complemento.
- **Control Anexo A de la NTC-ISO-IEC 27001:2022:** seleccionar de la lista plegable
- **Soporte:** Registro de la evidencia que deja la implementación de la acción de mejora
- **Responsable:** registrar el rol o cargo responsable de implementar la acción de mejora
- **Fecha de Implementación:** Periodo de tiempo en el cual se implementara la acción de mejora

5.1 RESULTADOS DE VALORACION DE RIESGOS DE SEGURIDAD DE LA INFORMACION

La identificación y valoración de riesgos sobre los activos de información de la entidad se encuentra detallada en la matriz de gestión de riesgos de seguridad de la información identificados por nivel de riesgo residual, tomando también de esta matriz los pesos de la información reportada como critica.

TABLA DE RIESGO VS PESO

N°	RIESGOS	CODIGO	PESO - GB
1	Divulgación de información	R-02	23,5163
2	Perdida de información	R-15, R-16, R-17, R-18, R-44	11,0951
3	Alteración de copias de seguridad	R-03, R-28, R-29, R-30	25,7588
4	Compromiso de la información	R-25, R-33, R-34	0,40356
5	Denegación de los Servicios	R-53, R-54	0,3457
6	Robo de información	R-05, R-06, R-07, R-65, R-67	0,54605
7	Alteración de la información	R-1, R-08, R-09, R-10, R-11, R-49, R-50	2472,60362
8	Manipulación de la información	R-12, R-13, R-14	10,10016

Carrera 7 N° 12-100
PBX: (601) 884 4444 Ext. 2300-2301
oficinatic@chia.gov.co
www.chia-cundinamarca.gov.co

N°	RIESGOS	CODIGO	PESO - GB
9	Fuga de información	R-19, R-20, R-21, R-22	4,25562
10	Permisos de roles mal gestionados	R-27, R-66	39,1155
11	Destrucción de la información	R-39, R-40, R-41	98,99783223
12	perdida de bases de datos	R-32	2,6729
13	Acceso a la información confidencial	R-36, R-37, R-38	211,6766
14	Conexión de red a la base de datos	R-23, R-24, R-25	6,495
15	Alteración de base de datos	R-26, R-42	25,0558
16	destrucción de equipos	R-61	0,3434
17	Acceso no autorizado	R-46, R-62	114,55154
18	No disponibilidad de la información fallas de medio de transmisión	R-63	260,39783
19	Falla de seguridad	R-43	4,56117
20	Alteración de usuarios y contraseñas	R-45	0,3887
21	Perdida económica	R-47, R-48	0,04783
22	Daños del sistema	R-51, R-52	0,5383
23	Código malicioso	R-55, R-56	12,0346
24	Caída de los sistemas	R-57, R-58	38,827964
25	Indisponibilidad de los sistemas	R-59, R-60	26,38059623
26	Daño físico	R-64	0,7743
		Total	3391,484772

La siguiente tabla realiza la identificación del numero de riesgos por cada nivel, destacando el porcentaje del nivel de riesgo para tener en cuenta en el plan de tratamiento de los riesgos identificados en los activos de información reportados.

Nivel del Riesgo	Cantidad de Riesgos	%
Bajo (2)	13	17
Moderado (3)	21	27
Alto (4)	32	41
Extremo (5)	12	15
Total	78	100

Carrera 7 N° 12-100
PBX: (601) 884 4444 Ext. 2300-2301
oficinatic@chia.gov.co
www.chia-cundinamarca.gov.co

	Insignificante(1)	Menor(2)	Moderado(3)	Mayor (4)	Catastrófico (5)
Casi certeza (5)					
Probable (4)	R-01 R-08 R-25	R-02 R-09 R-10 R-11 R-12 R-24 R-25 R-28 R-29	R-05	R-24	R--55
Posible (3)	R-02 R-09 R-13 R-14 R-15 R-16 R-17 R-23	R-04 R-14 R-16 R-17 R-20 R-22 R-25 R-26 R-27 R-28 R-35	Rr-64 R-59 R-60	R-03 R-19 R-37 R-39	R-43 R-54
Improbable (2)	R-16 R-18	R-07 R-27	R-55 R-58 R-56 R-55	R-06 R-21 R-31 R-33 R-36	R-34 R-40 R-47 R-53
Raro (1)	R-32			R-31 R-45 R-51 R-52	R-30 R-38 R-41 R-42 R-44 R-46 R-48 R-49 R-50 R-51 R-52

8. RECURSOS

La oficina TIC, en el marco de la gestión de riesgos de seguridad y Privacidad de la información, Seguridad Digital y Continuidad de la Operación, dispone de los siguientes recursos.

RECURSOS	VARIABLE
Humanos	La Oficina de Tecnologías de la información y comunicaciones, es responsable de coordinar,

Carrera 7 N° 12-100
PBX: (601) 884 4444 Ext. 2300-2301
oficinatic@chia.gov.co
www.chia-cundinamarca.gov.co

RECURSOS	VARIABLE
	implementar, modificar y realizar seguimiento a las políticas, estrategias y procedimientos en la Alcaldía Municipal de Chía 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 - Versión 4 - octubre de 2018 del DAFP. Herramienta para la gestión de riesgos (Matriz de Riesgos SGSI)
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, físicos, y desarrollo de auditorías

9. 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.

10. CONCLUSIONES Y RECOMENDACIONES

En el proceso de gestión de riesgos de seguridad de la información se logró definir el plan de tratamiento para los cuarenta y cuatro (44) riesgos de seguridad de la

información ubicados en la zona de riesgo “Alto” y “Extremo” (equivalentes al 56% del total de riesgos identificados).

En el proceso se logró la participación de todos los procesos y personal asignado para la identificación de riesgos y plan de tratamiento de riesgos.

Se recomienda comunicar los riegos identificados, aprobar y aplicar las acciones definidas para su tratamiento con el objetivo de:

• Compartir los resultados de la evaluación del riesgo y presentar el plan para el tratamiento del riesgo.

• Evitar o reducir tanto la ocurrencia como la consecuencia de las brechas en la seguridad de la información debidas a la falta de comprensión mutua entre quienes toman las decisiones y las partes involucradas.

• Brindar soporte para la toma de decisiones.

• Obtener conocimientos nuevos sobre la seguridad de la información.

• Coordinar con otras partes y planificar las respuestas para reducir las consecuencias de cualquier incidente.

• Facilitar a quienes toman las decisiones y a las partes involucradas un sentido de responsabilidad acerca de los riesgos.

• Mejorar la concienciación.

Es importante que se realice seguimiento y monitoreo a las acciones definidas en el Plan de tratamiento de riesgos a través de varios mecanismos como seguimiento periódico y cumpliendo con la metodología y directrices aprobadas para la gestión de riesgos de seguridad de la información.

La Oficina TIC no sólo deberá centrarse en los riesgos identificados, sino que este análisis o apreciación del riesgo debe ser la base para identificar oportunidades. Por lo anterior la oportunidad deberá entenderse como la consecuencia positiva frente al resultado del tratamiento del Riesgo.

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

11. DOCUMENTOS ASOCIADOS

Constitución Política de Colombia 1991. Artículo 15. Reconoce como Derecho Fundamental el Habeas Data y Artículo 20. Libertad de Información.

- Decreto 612 de 4 de abril de 2018, Por el cual se fijan directrices para la integración de los planes institucionales y estratégicos al Plan de Acción por parte de las Entidades del Estado.
- Decreto 1008 de 14 de junio de 2018, Por el cual se establecen los lineamientos generales de la política de Gobierno Digital.
- Norma Técnica Colombiana NTC/ISO 27001:2022 Sistemas de gestión de la seguridad de la información.
- RG-1300-SIPG-84 Política de Administración de Riesgos de la UNGRD.
- RG-1101-GTI-04 Matriz de Riesgos de Seguridad de la Información
- G-1101-GTI-01 Guía Metodológica Gestión de Riesgos para SGSI
- Plan tratamiento de Riesgos vigencia 2020 - MIN TIC
- Ley 1273 de 2009, "Por medio de la cual se modifica el código penal, se crea un nuevo bien jurídico tutelado – denominado "de la protección de la información y de los datos" y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones".
- https://www.mintic.gov.co/gestionti/615/articles-5482_G7_Gestion_Riesgos.pdf
- https://www.mintic.gov.co/gestionti/615/articles-5482_G21_Gestion_Incidentes.pdf
- Articles-61854_documento – Modelo Nacional de Riesgos de Seguridad Digital, Gobierno de Colombia
- https://www.mintic.gov.co/portal/715/articles-135830_plan_tratamiento_riesgos_seguridad_privacidad_informacion_vi gencia_2023.pdf

12. CONTROL DE CAMBIOS

Fecha	Versión	Descripción del cambio
28/09/2023	1	Elaboración del plan
30/12/2024	2	Actualización del Plan

Carrera 7 N° 12-100
PBX: (601) 884 4444 Ext. 2300-2301
oficinatic@chia.gov.co
www.chia-cundinamarca.gov.co