

# Plan de seguridad de la información

## 2024-2028

(Versión 1)

Elaborado por:

Ing. Eliany Rocío Montejo Carrascal – Profesional Especializado

Revisado:

Ing. Gustavo Carvajal Millan – Jefe de Oficina TIC

## Tabla de contenido

<b>PLAN DE SEGURIDAD DE LA INFORMACIÓN</b> .....	3
1. Introducción .....	3
2. Alcance.....	3
3. Responsabilidades sobre activos de información .....	3
4. Análisis de riesgos actuales.....	4
5. Proyectos e iniciativas .....	8

## PLAN DE SEGURIDAD DE LA INFORMACIÓN

### 1. Introducción

Para realizar un análisis de riesgos debemos partir de un buen análisis de la situación inicial de la alcaldía municipal de Chía, para así llevar esos activos de Hardware y Software que consideramos de valor para la empresa y así poder crear un análisis de cada uno de los riesgos que lleguen a afectar el buen funcionamiento de la entidad y tratar de mitigar cada uno de los riesgos identificados a un nivel aceptable, por lo cual nos podemos apoyar en un plan de seguridad de la información y a través del cumplimiento de los lineamientos, directrices establecidos en la política de seguridad de la información y la política de seguridad digital, poder contribuir a la continuidad de las operaciones.

### 2. Alcance

El plan de seguridad de la información de la alcaldía municipal de Chía se articulará con los instrumentos de planificación municipal y con el PETIC para garantizar su integración efectiva en la administración pública. Este plan busca conseguir la mejora continua de la seguridad de la información, en la alcaldía, motivo por el cual abarcaremos los siguientes puntos críticos:

- Responsabilidades sobre activos de información
- Análisis de riesgos actuales
- Proyectos de implementación del MSPI, políticas y procedimientos de seguridad de la información

### 3. Responsabilidades sobre activos de información

Todos los activos deben tener un responsable específico, por cada una de las dependencias de la alcaldía, que garantice la protección continua de la información y los datos almacenados, cumpliendo con las políticas y procedimientos establecidos por la alcaldía municipal de Chía.

### 3.1 Identificación y clasificación de activos:

Desde la Oficina TIC, se realiza el levantamiento de la información en corresponsabilidad con cada una de las dependencias de la alcaldía municipal de Chía, con el fin de realizar una identificación sistemática y clasificación de todos los activos de información. Esta clasificación debe basarse en criterios de confidencialidad, integridad, disponibilidad, autenticidad y trazabilidad, considerando también los riesgos identificados y los requerimientos legales de retención.

### 3.2 Asignación de responsabilidades:

Cada activo de información debe tener un responsable designado, típicamente un líder de proceso, jefe de área o director, quien es encargado de asegurar un nivel adecuado de protección y de mantener actualizada la valoración del activo.

## 4. Análisis de riesgos actuales

De acuerdo a los activos de información consolidados de acuerdo a lo relacionado por cada una de las dependencias de la alcaldía municipal de Chía, surgen los siguientes riesgos, que son objeto de actualización, de acuerdo a los cambios y estructura organizacional.

ID del Riesgo	Descripción del Riesgo	Vulnerabilidad	Amenaza	Impacto Potencial	Probabilidad	Acciones de Mitigación	Responsable
R-01	Pérdida de información	Contraseñas predeterminadas no modificadas	Ataques por descifrado de contraseñas	Alta	Media	Establecer políticas de contraseñas seguras	Gobierno TI – Oficina TIC

ID del Riesgo	Descripción del Riesgo	Vulnerabilidad	Amenaza	Impacto Potencial	Probabilidad	Acciones de Mitigación	Responsable
R-02	Robo de información confidencial	Falta de cifrado de discos	Ciberdelincuentes	Muy Alta	Alta	Implementar cifrado en discos y correo electrónico	Oficial de seguridad TIC
R-03	Accesos no autorizados	Usuarios con permisos de administradores	Modificación y acceso no autorizado	Muy Alta	Alta	Control de accesos y aplicación de principio de menor privilegio	Infraestructura / Soporte Técnico / Innovación tecnológica
R-04	Pérdida de información	Falta de planes de contingencia	Desastres naturales	Alta	Media	Diseñar e implementar un plan de continuidad del negocio	Infraestructura y redes – Oficina TIC
R-05	Robo de información	Personal descontento	Compra de información	Alta	Alta	Implementar monitoreo de actividades internas y establecer un proceso	Jefe de función pública

ID del Riesgo	Descripción del Riesgo	Vulnerabilidad	Amenaza	Impacto Potencial	Probabilidad	Acciones de Mitigación	Responsable
						de salida controlado	
R-06	Pérdida de control sobre activos	Cuentas de usuario activas de extrabajadores	Suplantación de identidad	Muy Alta	Alta	Deshabilitar cuentas de extrabajadores inmediatamente	Secretarios y/o jefes de área y/o supervisores
R-07	Interceptación de información	Falta de cifrado en la red	Interceptación de información	Alta	Alta	Implementar cifrado extremo a extremo en la red	Infraestructura y redes – Oficina TIC
R-08	Disrupción de servicios	Falta de infraestructura de respuesta ante desastres	Desastres naturales o ataques internos/externos	Muy Alta	Media	Adquirir infraestructura de respaldo y redundancia geográfica	Alcalde y Jefe de Oficina TIC
R-09	Transmisión de virus informáticos	Acceso de equipos personales a la red	Transmisión de virus y malware	Alta	Alta	Implementar controles de acceso a la red y políticas BYOD	Infraestructura y redes – Oficina TIC

ID del Riesgo	Descripción del Riesgo	Vulnerabilidad	Amenaza	Impacto Potencial	Probabilidad	Acciones de Mitigación	Responsable
R-10	Obsolescencia tecnológica	Insuficiente stock de repuestos	Fallas de equipos informáticos	Media	Alta	Realizar evaluación periódica de tecnologías críticas	Soporte técnico – Oficina TIC
R-11	Desactualización de software	Falta de actualizaciones automáticas	Ataques por vulnerabilidades no parcheadas	Muy Alta	Alta	Implementar sistema de gestión de parches automáticos	Soporte técnico – Oficina TIC
R-12	Falta de capacitación	Conocimientos desactualizados en ciberseguridad	Cambios normativos y tecnológicos	Alta	Media	Implementar capacitación continua en temas de ciberseguridad	Jefes de función pública y Oficina TIC
R-13	Costos elevados de tecnología	Aumento de costos por variación del dólar	Elevados costos de adquisición	Media	Media	Diversificar proveedores	Jefe de Oficina TIC y supervisores
R-14	Falla de la infraestructura TIC	Falta de sistemas de respaldo	Corte de energía y pérdida de	Muy Alta	Alta	Implementar sistemas de	Infraestructura y redes –

ID del Riesgo	Descripción del Riesgo	Vulnerabilidad	Amenaza	Impacto Potencial	Probabilidad	Acciones de Mitigación	Responsable
		eléctrico (UPS)	operatividad			respaldo eléctrico (UPS)	Oficina TIC

## 5. Proyectos e iniciativas

### 5.1. Proyectos 2024-2027:

En el plan de desarrollo de la Oficina TIC, se dejaron establecidos proyectos de inversión, los cuales están alineados a fortalecer la implementación de la seguridad de la información en la alcaldía de Chía, cuyas metas específicas se relacionan a continuación:

Proyecto	Meta	Inversión cuatrienio
Ampliación del acceso seguro y equitativo a la tecnología - Código BPIN: 2024251750010	Elaborar dos (2) documentos de seguimientos técnicos sobre estrategias de seguridad informática con soluciones de alta disponibilidad y redundancia para equipos activos de red y servidores	\$ 470.987.671,00
Proyecto innovación tecnológica y estratégica para la comunidad de Chía - Código BPIN: 2024251750020	Formular dos (2) documentos a partir de la recolección, análisis y procesamiento de información para la generación modelos de analítica de datos acompañados de una herramienta que permita el tratamiento de datos para la toma de decisiones	\$ 224.858.252,00
Transformación digital para el desarrollo	Implementar cuatro (4) documentos metodológicos	\$ 338.697.885,00

Proyecto	Meta	Inversión cuatrienio
socioeconómico en el municipio de Chía - Código BPIN: 2024251750019	asociados a las estrategias de gobierno digital alineadas a la normatividad y buenas prácticas	
	Desarrollar quince (15) productos digitales que atiendan los diferentes sectores del municipio para garantizar la atención, trazabilidad y respuesta a la ciudadanía	\$ 1.112.540.670,00

### 5.2. Iniciativas 2024-2027:

Las iniciativas serán ejecutadas en mayor porcentaje por los funcionarios de carrera administrativa. Sin embargo, algunas de ellas, también serán apoyadas por OPS, cuyos costos están incluidos dentro del presupuesto de inversión asignado en plan de desarrollo municipal.

Nombre iniciativa	Plan asociado
Políticas de Gobierno Digital, Seguridad Digital y Seguridad de la información	<ol style="list-style-type: none"> <li>1. Documentarse con la normatividad vigente</li> <li>2. Conocer el PDM</li> <li>3. Identificar las debilidades, oportunidades, fortalezas y amenazas de la Oficina TIC</li> <li>4. Elaborar las políticas de Gobierno Digital, Seguridad Digital, Seguridad de la Información</li> <li>5. Realizar mesas de trabajo con el jefe de la Oficina TIC para obtener retroalimentación</li> <li>6. Ajustar las políticas de acuerdo a las observaciones dadas por el jefe de la Oficina TIC</li> <li>7. Realizar la presentación de forma ejecutiva para ser expuesta ante el comité de gestión y desempeño</li> <li>8. Exponer las políticas al comité de gestión y desempeño y solicitar aprobación.</li> </ol>
Socialización y apropiación de las políticas de gobierno digital, seguridad digital y seguridad de la información	<ol style="list-style-type: none"> <li>1. Elaborar anualmente el plan de sensibilización, capacitación y comunicaciones:</li> <li>2. Realizar presentación con los puntos más relevantes de cada política</li> <li>3. Resolver dudas en los espacios destinados para las sensibilizaciones</li> </ol>

Nombre iniciativa	Plan asociado
	<ol style="list-style-type: none"> <li>4. Gestionar las firmas de asistencias a las sensibilizaciones</li> <li>5. Compartir las presentaciones con los asistentes</li> <li>6. Gestionar publicación de las políticas en el sitio web de la alcaldía municipal de Chía</li> </ol>
Procedimientos	<ol style="list-style-type: none"> <li>1. Elaborar el documento con los procedimientos alineados a la política de seguridad de la información a ser implementados en la alcaldía municipal de Chía.</li> <li>2. Elaborar procedimiento MDS</li> <li>3. Actualizar protocolo de uso y protección de los recursos tecnológicos</li> <li>4. Elaborar el proceso de valoración los riesgos de seguridad y privacidad de la información de la entidad.</li> </ol>
Documentos de alta disponibilidad	<ol style="list-style-type: none"> <li>1. Realizar levantamiento de inventario de equipos, aplicaciones y servicios críticos que requieren alta disponibilidad.</li> <li>2. Realizar BIA limitándonos a los Sistemas de información on-premises de la entidad, en donde se identifiquen los tiempos máximos de indisponibilidad tolerables (RTO) y el punto objetivo de recuperación (RPO).</li> <li>3. Redactar documento DRP en donde se visualice la arquitectura de respaldo, redundancia en almacenamiento, backup, roles y responsabilidades, árbol de llamadas.</li> <li>4. Redactar documento en donde se desarrolle redundancia para equipos activos de red y seguridad perimetral, el cual contenga diseño de arquitectura redundante para la red, topología de red, redundancia en enlaces WAN, procedimientos para implementación y puesta en operación de redundancia en enlaces y pruebas.</li> <li>5. Realizar las configuraciones en materia de infraestructura de redes, seguridad perimetral y servidores que permitan las réplicas descritas en el DRP</li> </ol>
Soporte y configuración de dispositivos de seguridad	<ol style="list-style-type: none"> <li>1. Incluir en inventario de activos de información los dispositivos de seguridad informática actualmente utilizados en la entidad.</li> <li>2. Configurar en los dispositivos de seguridad las políticas establecidas en el documento de Políticas de Seguridad y Privacidad de la Información.</li> <li>3. Analizar reportes de alertas generadas por los dispositivos de seguridad.</li> </ol>

Nombre iniciativa	Plan asociado
	<p>4. Realizar configuraciones en los dispositivos de seguridad que subsanen los hallazgos encontrados en la etapa anterior.</p> <p>5. Realizar actualización de los dispositivos posterior al análisis de la compatibilidad</p>
Configuración de acceso controlado a internet	<p>1. Establecer las políticas de conexión permitidas, como limitación en velocidad, tiempo de conexión, restricción en visualización de contenido.</p> <p>2. Realizar configuración de portal cautivo</p> <p>3. Realizar pruebas de conexión y consulta de contenido en internet.</p>
Desarrollo de la metodología de gestión de datos y gobernanza	<p>Elaborar e implementar un documento metodológico que establezca directrices claras para la gestión y gobernanza de datos en el ámbito del gobierno digital. La metodología abordará políticas de manejo de datos, calidad, protección y gestión de metadatos, garantizando el cumplimiento de las normativas vigentes y alineándose con las mejores prácticas internacionales</p>