1. INFORMACIÓN GENERAL

Campo	Descripción
Nombre del Plan	Plan de Tratamiento de riesgos de seguridad y privacidad de la información
Vigencia	2025
Proceso	APOYO
Dependencia Responsable	Sistemas
Líder del Plan	Profesional Especializado en Sistemas
Fecha de Elaboración	02/01/2025
Fecha de Aprobación	24/01/2025
Estado	Aprobado

2. MARCO ESTRATÉGICO

2.1 Articulación Estratégica

Nivel	Descripción
Dimensión MIPG	Fortalecimiento organizacional y simplificación de procesos.
Política MIPG	Gestión del conocimiento y la innovación
Objetivo Plan de Desarrollo	Promover sociedades pacificas e inclusivas para el desarrollo sostenible, facilitar el acceso a la justicia para todos y construir a todos los niveles instituciones eficaces e inclusivas que rindan cuentas.
Meta Plan de Desarrollo	"Integrando territorio, ciudad y naturaleza"

2.2 Marco Normativo

Tipo de Norma	Número	Año	Descripción
Políticas técnicas de seguridad de la información Función Pública		2020	La declaración de la Política de Seguridad de la Información institucional busca proteger los activos de información (grupos de valor, información, procesos, tecnologías de información incluido el hardware y el software), mediante el establecimiento de lineamientos generales para la aplicación de la seguridad de la información en la gestión de los procesos internos, bajo el marco del Modelo Integrado de Planeación y Gestión, consolidada en los procedimientos, guías, instructivos y publicaciones, así como la asignación de roles y responsabilidades
Decreto	103	2015	Compendio de políticas aplican para todos los servidores públicos y contratistas de Función Pública que procesan y/o manejan información de la entidad.
Decreto	1494	2015	Por el cual se reglamenta parcialmente la Ley 1712 de 2014 y se dictan otras disposiciones
Decreto	1008	2018	Por el cual se establecen los lineamientos generales de la política de Gobierno Digital.
Ley	1712	2014	Para la Implementación de la Estrategia de Gobierno en Línea, entidades del orden nacional; Modelo de Seguridad de la Información para la Estrategia de Gobierno en Línea.
Decreto	2573	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	1377	2013	Por el cual se establecen los lineamientos generales de la Estrategia de Gobierno en línea, se reglamenta parcialmente la Ley 1341 de 2009 y se dictan otras disposiciones.
Ley	527	2015	Por la cual se dictan las disposiciones generales del hábeas data y se regula el manejo de la información contenida en bases de datos personales.
Ley	1266	2008	Habeas Data

1. DIAGNÓSTICO

Con el fin de cumplir con este plan EMPODUITMA se compromete al cumplimiento de los siguientes puntos, por parte de todos los integrantes del equipo de trabajo de la entidad.

- Garantizar al Titular, en todo tiempo, el pleno y efectivo ejercicio del derecho de hábeas data;
- Conservar la información bajo las condiciones de seguridad necesarias para impedir su adulteración, pérdida, consulta, uso o acceso no autorizado o fraudulento.

- Garantizar que la información que se suministre al Encargado del Tratamiento sea veraz, completa, exacta, actualizada, comprobable y comprensible.
- Abstenerse de circular información que esté siendo controvertida por el Titular y cuyo bloqueo haya sido ordenado por la Superintendencia de Industria y Comercio.
- Permitir el acceso a la información únicamente a las personas que pueden tener acceso a ella.
- Suministrar al Encargado del Tratamiento, según el caso, únicamente datos cuyo Tratamiento esté previamente autorizado de conformidad con lo previsto en la presente ley.
- Exigir al Encargado del Tratamiento en todo momento, el respeto a las condiciones de seguridad y privacidad de la información del Titular.
- Tramitar las consultas y reclamos formulados en los términos señalados en la presente ley.
- Adoptar un manual interno de políticas y procedimientos para garantizar el adecuado cumplimiento de la presente ley y en especial, para la atención de consultas y reclamos.
- Registrar en la base de datos la leyenda “reclamo en trámite” en la forma en que se regula en la presente ley.
- Informar a solicitud del Titular sobre el uso dado a sus datos.
- Informar a la Superintendencia de Industria y Comercio cuando se presenten violaciones a los códigos de seguridad y existan riesgos en la administración de la información de los Titulares;
- Cumplir las instrucciones y requerimientos que imparta la Superintendencia de Industria y Comercio.

Para el cumplimiento de los puntos anteriores la dirección debe destinar los recursos necesarios en cuanto a los recursos humanos (Técnico de sistemas de información, técnico Seguridad informática), financieros y tecnológicos, y garantizar el plan de seguimiento y evaluación.

Análisis DOFA:

Aspecto	Descripción	Impacto
Fortalezas	Compromiso institucional con la seguridad de la información	Proporciona una base sólida para implementar y mantener medidas de seguridad efectivas.
	Disponibilidad de guías y metodologías, como las proporcionadas por el MinTIC, para la administración del riesgo.	Apoya la implementación de prácticas estandarizadas y efectivas en la gestión de riesgos
Debilidades	El personal carece de formación actualizada en prácticas de tratamiento de seguridad y privacidad de la información	Posibles brechas en la implementación y mantenimiento de medidas de seguridad efectivas
	Falta de Manuales para Empoduitama de tratamiento de seguridad y privacidad de la información	Compromete la integridad y disponibilidad de la información
Oportunidades	La sociedad demanda mayor protección de sus datos personales, impulsando a las organizaciones a mejorar sus prácticas de seguridad.	Fortalecer la confianza pública y cumplir con normativas vigentes.
	La adopción de manejo de herramientas de software que posee la Empresa de una manera adecuada.	Mejora la detección y respuesta a amenazas, optimizando la protección de datos
Amenazas	Las amenazas cibernéticas evolucionan constantemente, volviéndose más difíciles de detectar y mitigar	Posible compromiso de datos sensibles y afectación de la continuidad operativa

4. OBJETIVOS Y METAS

4.1 Objetivo General

Establecer para Empoduitama directrices para identificar y evaluar los riesgos relacionados con el tratamiento de seguridad y privacidad de la información, asegurando la protección de la confidencialidad, integridad, disponibilidad, privacidad y autenticidad de la información

4.2 Objetivos Específico

- Reconocer y documentar los posibles riesgos que puedan afectar la seguridad y privacidad de la información, considerando amenazas internas y externas
- Determinar la probabilidad de ocurrencia y el impacto potencial de cada riesgo identificado, priorizando aquellos que requieren atención inmediata.
- Promover la formación y sensibilización del personal en materia de tratamiento de seguridad y privacidad de la información, fomentando una cultura organizacional orientada a la protección de los datos

4.3 Metas e Indicadores

Meta	Indicador	Fórmula	Meta 2025	Frecuencia	Responsable
Implementar tres controles para mitigar riesgos identificados	Porcentaje de controles implementados	(Número de controles implementados / Número total de controles planificados) × 100	100	Cuatrimestral	Sistemas
Capacitar al personal en tratamiento de seguridad y privacidad de la información	Porcentaje de personal capacitado	(Número de empleados capacitados / Número total de empleados) × 100	100	Semestral	Sistemas
Realizar auditorías internas de tratamiento de seguridad de la información	Número de auditorías realizadas	auditorías por dependencia / total dependencias	100	Semestral	Sistemas, Control Interno
Crear políticas de tratamiento de seguridad y privacidad de la información	Porcentaje de políticas actualizadas	(Número de políticas actualizadas / Número total de políticas) × 100	100	Anual	Sistemas

5. PLAN DE ACCIÓN

Objetivo	Actividad	Evidencia	% Avance
Fortalecer los controles de seguridad en los servidores (UTM, Bases de Datos)	Identificar y evaluar los controles existentes en los servidores	Informes de evaluación de controles.	
	Implementar controles adicionales donde se identifiquen brechas de seguridad.	Registros de implementación de nuevos controles.	
	Bloqueo de equipos cada minuto y cambio de contraseña cada 30 dias	Verificación usuarios de active directory	
	Configuración de roles de acceso a los diferentes aplicativos de software y Red LAN.	Formato de registro	
Mejorar la capacidad de identificación, respuesta y recuperación frente a incidentes bajo el marco del NIST	Desarrollar e implementar un plan de respuesta a incidentes basado en el Marco de Ciberseguridad del NIST	Documento del plan de respuesta a incidentes	
	Realizar simulacros periódicos de respuesta a incidentes.	Registros de simulacros y lecciones aprendidas.	
	Establecer un técnico en gestión de incidentes de seguridad.	Técnico de gestión de incidentes de seguridad	
Implementar un Programa de Revisión y Actualización de Políticas de tratamiento de riesgos de seguridad y privacidad de la información	Establecer un calendario para la revisión periódica de políticas de seguridad de la información	Calendario de revisiones establecido.	
	Asignar un técnico para la actualización de cada política	Técnico de gestión de incidentes y sus roles.	
	Comunicar y capacitar al personal sobre las actualizaciones realizadas.	Listas de asistencia a capacitaciones sobre nuevas políticas.	

Objetivo	Actividad	Evidencia	% Avance
Desarrollar un Plan de Recuperación de Desastres (DRP)	Identificar los sistemas y procesos críticos de la entidad	Listado de sistemas y procesos críticos.	
	Elaborar un DRP que incluya procedimientos para la recuperación de cada sistema crítico.	Documento del Plan de Recuperación de Desastres.	
	Realizar pruebas periódicas del DRP para asegurar su eficacia	Informes de pruebas y simulacros del DRP.	
Actualizar el Licenciamiento de Software	Realizar un inventario de todo el software utilizado en la entidad.	Inventario de software con estado de licenciamiento.	
	Verificar el estado de licenciamiento y actualizaciones de cada software	Registros de adquisición de licencias.	
	Adquirir las licencias necesarias y actualizar los Softwares a sus versiones más recientes	Documento de licenciamiento	

6. GESTIÓN DE RIESGOS

Riesgo	Probabilidad	Impacto	Nivel	Controles	Responsable	Plan de Contingencia
Insuficiente capacitación del personal	Media	Medio	Media	Capacitaciones esporádicas	sistemas	Programa continuo de formación en seguridad de la información
Posible obsolescencia tecnológica	Alta	Alto	Crítico	Actualizaciones periódicas de software	sistemas	Plan de renovación tecnológica
Riesgo de ciberataques	Alta	Alto	Crítico	Firewalls y antivirus	sistemas	Implementación de sistemas avanzados de detección y respuesta a incidentes

7. SEGUIMIENTO Y CONTROL

7.1 Mecanismos de Seguimiento

Aspecto	Periodicidad	Responsable	Metodología
Revisión de Políticas de Seguridad	Anual	Sistemas	Evaluación y actualización de políticas según normativas vigentes y mejores prácticas.
Monitoreo de Incidentes de Seguridad	Permanente	Sistemas	Implementación de sistemas de detección y respuesta a incidentes, con reportes mensuales de eventos.
Actualización de Inventario de Activos de Información	Semestral	Sistemas	Revisión y actualización del inventario de activos para asegurar su protección adecuada.

7.2 Control de Cambios

Versión	Fecha	Descripción del Cambio	Responsable
0	06/11/2024	Versión inicial	Dir. Planeación

FIRMAS DE APROBACIÓN

Rol	Cargo
Elaboró	Profesional Especializado en Sistemas
Revisó	Jefe Oficina Asesora Planeación y Profesional SGC
Aprobó	Comité de desempeño Institucional

CONTROL DOCUMENTAL

- **Fecha próxima revisión:** 03/04/2025
- **Ubicación digital:** Sistema de Gestión Documental/Planes Institucionales MIPG/2025
- **Copias controladas:** Gerencia, Planeación, Control Interno

Nota: se menciona que si bien todas las actividades contempladas en este plan se desarrollaran en la vigencia 2025 las mismas tendrán un monitoreo trimestral conforme a lo descrito en la Res. No. 196 del 26 de agosto de 2018.