	SISTEMA DE GESTIÓN DE CALIDAD	FORMATO PLANES INSTITUCIONALES MIPG	
	PROCESO: PLANEACIÓN ORGANIZACIONAL Y MEJORA CONTINUA	CÓDIGO: F-PMC-25	VERSIÓN: 1
		FECHA: 08-01-2026	PÁGINA: 1 DE 4

## 1. INFORMACIÓN GENERAL

<b>Nombre del Plan:</b>	PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACION
<b>Vigencia:</b>	2026
<b>Proceso / Área:</b>	SISTEMAS
<b>Líder Responsable:</b>	EDGAR GIOVANNI VASQUEZ ROCHA

## 2. MARCO ESTRATÉGICO

### 2.1 Alineación MIPG


Marque con una X la dimensión MIPG a la que contribuye este plan:

<input type="checkbox"/>	Dimensión 1: Talento Humano
<input type="checkbox"/>	Dimensión 2: Direccionamiento Estratégico y Planeación
<input type="checkbox"/>	Dimensión 3: Gestión con Valores para Resultados
<input type="checkbox"/>	Dimensión 4: Evaluación de Resultados
<input type="checkbox"/>	Dimensión 7: Control Interno

### 2.2 Marco Normativo (Principales normas que sustentan este plan)

Tipo	Número/Año	Descripción breve
Resolución	02277 / 2025	(MinTIC) Actualiza los lineamientos del Modelo de Seguridad y Privacidad de la Información (MSPI). Exige controles más estrictos en la nube y autenticación de usuarios. Obligatorio para MIPG.
Ley	2300 / 2023	Establece límites al contacto con los ciudadanos. Impacta las políticas de privacidad y cómo Empoduitama usa los datos de contacto (teléfonos/correos) de los usuarios.
CONPES	4069 / 2021	Política Nacional de Inteligencia Artificial. Define la ética y el manejo de riesgos en el uso de datos automatizados dentro del sector público.
Directiva Presidencial	03 / 2021	Lineamientos para el uso de servicios en la nube y ciberseguridad en el sector público, priorizando la soberanía de los datos de los ciudadanos.
Políticas técnicas de seguridad de la información Función Pública		a 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

<b>Elaboró:</b> Profesional apoyo en SGC	<b>Revisó:</b> Jefe Oficina Asesora Planeación	<b>Aprobó:</b> Gerente General
--	--	--------------------------------

	SISTEMA DE GESTIÓN DE CALIDAD	FORMATO PLANES INSTITUCIONALES MIPG	
	PROCESO: PLANEACIÓN ORGANIZACIONAL Y MEJORA CONTINUA	CÓDIGO: F-PMC-25	VERSIÓN: 1
		FECHA: 08-01-2026	PÁGINA: 2 DE 4

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	527/1999	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


### 3. DIAGNÓSTICO

*Resuma los hallazgos principales que justifican este plan (situación actual, datos clave, necesidades identificadas):*

#### 3.1 Análisis DOFA

FORTALEZAS	DEBILIDADES	OPORTUNIDADES	AMENAZAS
Existe voluntad política desde la Gerencia General (evidenciada en la aprobación de recursos y planes previos) para la modernización institucional.	El resto de la empresa (administrativos, operativos) sigue viendo la seguridad como una "traba" y busca atajos (compartir claves de usuario, uso de redes personales para información sensible), anulando la inversión tecnológica realizada.	Posibilidad de implementar soluciones de seguridad basadas en IA para la detección temprana de anomalías a costos accesibles.	Riesgo con proveedores tecnológicos externos que infrinjan políticas de privacidad con las empresas con datos que sirven como puente para atacar a la entidad.
Se cuenta con controles perimetrales básicos (Firewall, Antivirus) y gestión de usuarios (Directorio Activo) ya implementados.	Los manuales específicos de Empoduitama no han incorporado los capítulos de IA y Biométrica, tratamiento de seguridad y privacidad de la información exigidos por la SIC.	Cumplir anticipadamente con la Ley "Dejen de Fregar" posiciona a Empoduitama como una entidad respetuosa, mejorando la imagen pública y reduciendo las quejas por acoso administrativo.	Aumento exponencial de ataques de ransomware dirigidos a servicios públicos y uso de IA para ingeniería social (Deepfakes, Vishing).
La empresa cuenta con una estrategia de respaldo que garantiza la restauración de la información incluso si la red principal es infectada, asegurando la continuidad	El sistema actual de facturación/PQR no tiene un módulo nativo que permita marcar qué usuarios no deseen ser contactados por WhatsApp o SMS,	El CONPES habilita y promueve el uso de IA en el sector público. Es la oportunidad para implementar chatbots seguros que atiendan 24/7 sin contratar más	Campañas de phishing altamente personalizadas dirigidas a funcionarios con privilegios de acceso crítico (Tesorería,

<b>Elaboró:</b> Profesional apoyo en SGC	<b>Revisó:</b> Jefe Oficina Asesora Planeación	<b>Aprobó:</b> Gerente General
--	--	--------------------------------

	SISTEMA DE GESTIÓN DE CALIDAD		FORMATO PLANES INSTITUCIONALES MIPG	
	PROCESO: PLANEACIÓN ORGANIZACIONAL Y MEJORA CONTINUA		CÓDIGO: F-PMC-25	VERSIÓN: 1
			FECHA: 08-01-2026	PÁGINA: 3 DE 4

del servicio de facturación y operación.	dificultando el cumplimiento automático de la ley.	personal, reduciendo costos operativos.	Operaciones).
Empoduitama cuenta con un proyecto de inversión aprobado y en ejecución para el fortalecimiento tecnológico, garantizando los recursos necesarios para cumplir con los controles técnicos exigidos por el nuevo modelo de seguridad (MSPI). Ya no se depende de presupuestos precarios para la ciberseguridad.	El personal carece de formación especializada y actualizada frente a las nuevas amenazas (IA, Ransomware avanzado). Dependencia de pocos funcionarios con conocimiento técnico.	Si Empoduitama certifica su seguridad bajo los sellos de Gobierno Digital, puede ganar premios de Alta Gerencia o reconocimiento municipal, blindando políticamente la gestión de la dirección actual.	

#### 4. OBJETIVO Y META DEL PLAN

##### Objetivo General (¿Qué queremos lograr en 2026?)

Implementar controles y tratamientos para mitigar los riesgos de seguridad y privacidad de la información identificados en la matriz institucional, mediante capacitación del personal, actualización de políticas y verificación de cumplimiento a través de auditorías externas y pentesting.

##### Meta (¿Cómo mediremos el logro?):


- Pentesting: 4 pruebas de hacking ético realizadas (línea base 2025: 0)
- Riesgos mitigados: 100% de riesgos críticos con controles implementados (línea base 2025: 60%)
- Auditorías: 100% de auditorías externas atendidas oportunamente (línea base 2025: 100%)
- Cumplimiento del plan: ≥90% de las 5 actividades ejecutadas

#### 5. PLAN DE TRABAJO - ACTIVIDADES PRINCIPALES PARA 2026:

**IMPORTANTE:** Las actividades deben estar alineadas con el objetivo. El Indicador de Gestión debe ser uno de los indicadores oficiales de su área.

No.	Actividad	Línea Base	Meta 2026	Fecha de cumplimiento	Indicador de gestión	Evidencia
1	Capacitaciones trimestrales en seguridad informática y políticas de seguridad de la información	0	100%	30/12/2026	(capacitaciones Dictadas /Total Capacitaciones Anuales)	Evidencias de asistencia
2	Implementar controles para mitigar los riesgos identificados	60%	100%	30/12/2026	(Riesgos Mitigados/t	Evidencias de

<b>Elaboró:</b> Profesional apoyo en SGC	<b>Revisó:</b> Jefe Oficina Asesora Planeación	<b>Aprobó:</b> Gerente General
--	--	--------------------------------

	SISTEMA DE GESTIÓN DE CALIDAD		FORMATO PLANES INSTITUCIONALES MIPG	
	PROCESO: PLANEACIÓN ORGANIZACIONAL Y MEJORA CONTINUA		CÓDIGO: F-PMC-25	VERSIÓN: 1
			FECHA: 08-01-2026	PÁGINA: 4 DE 4

					total Riesgos) x100	acciones mitigación
3	Actualizar Políticas de Tratamiento de Seguridad y Privacidad de la Información	10%	100%	28/02/2026	(Políticas Actualizadas/políticas actualizables)	Documento de cambios
4	Responder a auditorías Externas sobre Seguridad de la Información	100%	100%	30/12/2026	(Auditorías Ejecutadas /Auditorías Programadas)	Documento de socialización y cierre
5	Realizar pruebas de hacking ético	0	100%	30/12/2026	(pruebas Realizadas /Pruebas Programadas)	Evidencias de resultados
6	Actualización y socialización de matriz de riesgos de seguridad y privacidad de la información	0	100%	30/12/2026	No aplica	Matriz de riesgos

 **Nota:** La Línea Base es el de la vigencia (2025) del indicador. La Meta 2026 es el valor que quiere alcanzar. Deben estar alineados con el objetivo del plan.

## 6. SEGUIMIENTO Y CONTROL

- ✓ Seguimiento trimestral en Comité de Desempeño Institucional
- ✓ Reporte de indicadores cada 3 meses (marzo, junio, septiembre, diciembre)
- ✓ Revisión de actividades completadas vs. programadas

## FIRMAS

<b>ELABORÓ</b>	Nombre y Cargo
<b>APROBÓ</b>	Comité de Desempeño Institucional Fecha: 30 de enero de 2026

 **IMPORTANTE:** Este plan se revisará trimestralmente. Recuerde enviar su informe de avance a Planeación

<b>Elaboró:</b> Profesional apoyo en SGC	<b>Revisó:</b> Jefe Oficina Asesora Planeación	<b>Aprobó:</b> Gerente General
--	--	--------------------------------