

|  |   |  |                |
|--|---|--|----------------|
|  <p><b>Empoduitama</b><br/>acueducto alcantarillado<br/>Cuida la Vibrante ESENCIA DE LA VIDA</p> | SISTEMA DE GESTIÓN DE CALIDAD                           | FORMATO<br>PLANES INSTITUCIONALES MIPG |                |
|  | PROCESO:<br>PLANEACIÓN ORGANIZACIONAL Y MEJORA CONTINUA | CÓDIGO: F-PMC-25                       | VERSIÓN: 1     |
|  |   | FECHA: 08-01-2026                      | PÁGINA: 1 DE 5 |

## 1. INFORMACIÓN GENERAL

|                    |  |
|--------------------|--|
| Nombre del Plan:   | PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACION |
| Vigencia:          | 2026   |
| Proceso / Área:    | SISTEMAS   |
| Líder Responsable: | 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  |
|--------------|------------|--|
| Ley 1266     | 2008       | Habeas Data: disposiciones generales y manejo de información en bases de datos personales  |
| Ley 1474     | 2011       | Por la cual se dictan disposiciones generales para la protección de datos personales. Congreso de la República.  |
| Ley 1712     | 2014       | Ley de Transparencia y Acceso a la Información Pública   |
| Ley 527      | 1999       | Por Comercio electrónico y firmas digitales  |
| Ley 1273     | 2009       | Delitos informáticos   |
| Ley 1581     | 2012       | Protección de datos personales   |
| Decreto 4632 | 2011       | Por la cual se dictan normas orientadas a fortalecer los mecanismos de prevención, investigación y sanción de actos de corrupción y la efectividad del control de la gestión pública.  |
| Decreto 1377 | 2013       | Reglamenta Ley 1581: tratamiento de datos personales   |
| Decreto 2573 | 2014       | establecen los lineamientos generales de la Estrategia de Gobierno en línea, se reglamenta parcialmente la Ley 1341 de 2009  |
| 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 2609 | 2017       | Reglamenta la gestión documental en Colombia (Título V de la Ley 594 de 2000), estableciendo el marco obligatorio para que entidades públicas y privadas que cumplen funciones públicas gestionen sus documentos físicos y electrónicos. |
| Decreto 1008 | 2018       | Por el cual se establecen los lineamientos generales de la política de Gobierno Digital.   |

|  |   |  |  |                |
|--|---|--|--|----------------|
|  <p><b>Empoduitama</b><br/>acueducto alcantarillado<br/>Cuida la Vibrante ESENCIA DE LA VIDA</p> | SISTEMA DE GESTIÓN DE CALIDAD                           |  | FORMATO<br>PLANES INSTITUCIONALES MIPG |                |
|  | PROCESO:<br>PLANEACIÓN ORGANIZACIONAL Y MEJORA CONTINUA |  | CÓDIGO: F-PMC-25                       | VERSIÓN: 1     |
|  |   |  | FECHA: 08-01-2026                      | PÁGINA: 2 DE 5 |

### 3. DIAGNÓSTICO

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

#### 3.1 Análisis DOFA

| FORTALEZAS   | DEBILIDADES   | OPORTUNIDADES   | AMENAZAS  |
|--|---|---|---|
| Respaldo de la Alta Dirección asignando presupuesto y recursos   | El recurso humano requiere mas conocimiento en seguridad informática y protección de la información   | Adopción de Inteligencia Artificial para la detección temprana de intrusos.   | Aumento de ataques coordinados como Ransomware o Phishing sofisticado.  |
| Control de permisos en equipos clientes a nivel local y por políticas de Servidor AD   | Se debe censurar contenido. Hay aplicaciones como Anydesk que permiten la ejecución sin instalación (sin ser Administrador) y No se puede censurar de tajo por que la usan proveedores de soporte de plataformas. | Disponibilidad de hardware que no es aceptado por Microsoft Windows para Windows 11 para usar con sistemas operativos con software pentesting y/o hacking ético | Cambios Legislativos Agresivos, nuevas multas o requisitos de privacidad que impliquen costos operativos muy altos de implementar rápidamente |
| Adquisición de equipos de computo de buen rendimiento y con software legal   | Faltan crear y/o oficializar Procedimientos en caso de Incidentes de Seguridad de la Información, el responsable y procesos de notificación   | Nuevas Normativas, cambios legales que obligan a la competencia a mejorar, elevando el estándar del sector.   | A pesar de cláusulas de confidencialidad, antiguos proveedores de plataformas pueden acumular información de la empresa                       |
| Cambio gradual a usar la suite de Workspace aprovechando sus características de seguridad                                    | Aunque se tiene la buena práctica, falta crear y/o oficializar la Política de Contraseñas Fuertes   |   |   |
| Política de backup de plataformas no solo en unidades locales, sino en discos extraíbles asegurados físicamente y en la nube | Falta crear y/o oficializar un Plan de Continuidad del Negocio. Falta de hardware redundante en servidores, equipos activos, UTM  |   |   |

|  |   |  |  |                |
|--|---|--|--|----------------|
|  <p><b>Empoduitama</b><br/>acueducto alcantarillado<br/>Cuida la Vibrante ESENCIA DE LA VIDA</p> | SISTEMA DE GESTIÓN DE CALIDAD                           |  | FORMATO<br>PLANES INSTITUCIONALES MIPG |                |
|  | PROCESO:<br>PLANEACIÓN ORGANIZACIONAL Y MEJORA CONTINUA |  | CÓDIGO: F-PMC-25                       | VERSIÓN: 1     |
|  |   |  | FECHA: 08-01-2026                      | PÁGINA: 3 DE 5 |

#### 4. OBJETIVO Y META DEL PLAN

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

Garantizar la confidencialidad, integridad y disponibilidad de la información de EMPODUITAMA mediante el fortalecimiento de la infraestructura tecnológica, la capacitación del personal y la realización de auditorías de seguridad, asegurando el cumplimiento de la Ley 1581/2012 y Resolución MinTIC 02277/2025.

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

- Disponibilidad de servicios TIC: ≥97%
- Capacitación en seguridad: ≥90% del personal capacitado
- Pentesting: 4 pruebas trimestrales de hacking ético realizadas
- Cumplimiento del plan: ≥90% de las 6 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    | Realizar Auditoria Externa en Seguridad Informática   | 0          | 100%      | 30/12/2026            | (Auditoria Ejecutada/ Auditoria Propuesta )         | Documento Cierre e informe Auditoria          |
| 2    | Capacitaciones trimestrales en seguridad informática y políticas de seguridad de la información | 0          | 100%      | 30/12/2026            | (capacitacionesDictadas /TotalCapcitacionesAnuales) | Evidencias de asistencia                      |
| 3    | Realizar pruebas trimestrales de hacking ético (pentesting)                                     | 0          | 100%      | 30/12/2026            | Pruebas Realizadas/s/pruebas Programadas            | Resultados de pruebas                         |
| 4    | Adquirir e instalar un conjunto de routers y access points para asegurar la red de la empresa   | 0          | 100%      | 30/03/2026            | (Equipos instalados /5) × 100%                      | Acta instalación, diagrama de red actualizado |
| 5    | Implementar planes de Continuidad del Negocio y Plan de Recuperación ante desastres             | 0          | 100%      | 30/12/2026            | (planes implementados/2)                            | Documento evidencia de planes                 |
|      |   |            |           | 28/02/2026            |   | Contrato                                      |

Elaboró: Profesional apoyo en SGC

Revisó: Jefe Oficina Asesora Planeación

Aprobó: Gerente General

|  |   |  |                   |                |
|--|---|--|-------------------|----------------|
|  <p><b>Empoduitama</b><br/>acueducto alcantarillado<br/>Cuida la Vibrante ESENCIA DE LA VIDA</p> | SISTEMA DE GESTIÓN DE CALIDAD                           | FORMATO<br>PLANES INSTITUCIONALES MIPG |                   |                |
|  | PROCESO:<br>PLANEACIÓN ORGANIZACIONAL Y MEJORA CONTINUA |  | CÓDIGO: F-PMC-25  | VERSIÓN: 1     |
|  |   |  | FECHA: 08-01-2026 | PÁGINA: 4 DE 5 |

|   |   |   |      |  |                       |                              |
|---|---|---|------|--|-----------------------|------------------------------|
| 6 | Contratar un segundo operador de Internet para hacer failover | 0 | 100% |  | Cumplimiento en fecha | firmado, pruebas de failover |
|---|---|---|------|--|-----------------------|------------------------------|

**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

|         |  |
|---------|--|
| ELABORÓ | Profesional Especializado en sistemas  |
| APROBÓ  | Comité de Desempeño Institucional <i>Escriba de manera clara y concisa el propósito principal de este plan. Enfóquese en el resultado esperado</i> |

Fecha: 30 de enero de 2026

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