EMPRESA DE ACUEDUCTO Y ALCANTARILLADO

DE SAN JOSÉ DEL GUAVIARE

EMPOAGUAS E.S.P

NIT: 822.001.883-3

PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

Vigencia 2026

En cumplimiento del Decreto 612 de 2018

SUBGERENCIA ADMINISTRATIVA Y FINANCIERA

Oficina de Tecnologías de la Información y las Comunicaciones (TIC)

SAN JOSÉ DEL GUAVIARE, 2026

Tabla de Contenido

1. INTRODUCCIÓN

La seguridad de la información constituye un pilar fundamental para la continuidad operacional y el cumplimiento de los objetivos misionales de las entidades públicas. En el contexto actual, donde las amenazas cibernéticas evolucionan constantemente y los datos personales requieren protección rigurosa, es imperativo contar con un marco de gestión integral que permita identificar, evaluar y tratar los riesgos asociados a los activos de información.

El presente Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información se desarrolla en cumplimiento del Decreto 612 de 2018, que establece directrices para la integración de los planes institucionales y estratégicos al Plan de Acción de las entidades del Estado. Este decreto, en su artículo 2.2.22.3.14, incluye el Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información como uno de los doce planes institucionales que deben ser publicados a más tardar el 31 de enero de cada año.

EMPOAGUAS E.S.P., como empresa de servicios públicos domiciliarios, maneja información sensible relacionada con usuarios, procesos operativos, infraestructura crítica y datos personales. La gestión adecuada de los riesgos asociados a esta información es esencial para garantizar la confidencialidad, integridad y disponibilidad de los datos, así como para proteger los derechos de los titulares de la información y cumplir con las obligaciones legales vigentes.

Este plan se articula con otros instrumentos de planeación institucional establecidos en el Decreto 612 de 2018, tales como el Plan Estratégico de Tecnologías de la Información y las Comunicaciones (PETI), el Plan de Seguridad y Privacidad de la Información, el Plan Anticorrupción y de Atención al Ciudadano, y el Plan de Acción institucional, garantizando coherencia con los objetivos estratégicos de la entidad y el Modelo Integrado de Planeación y Gestión (MIPG).

La implementación de este plan permitirá a EMPOAGUAS E.S.P. fortalecer su capacidad de respuesta ante amenazas y vulnerabilidades, cumplir con los estándares internacionales de seguridad de la información (ISO/IEC 27001), y garantizar el adecuado tratamiento de los datos personales en cumplimiento de la Ley 1581 de 2012 y sus decretos reglamentarios.

2. MARCO NORMATIVO

2.1. Decreto 612 de 2018

Articulación con el Plan de Acción Institucional

El Decreto 612 del 4 de abril de 2018 fija directrices para la integración de los planes institucionales y estratégicos al Plan de Acción por parte de las entidades del Estado. Este decreto adiciona el artículo 2.2.22.3.14 al Decreto 1083 de 2015, Único Reglamentario del Sector de Función Pública.

Según el artículo 2.2.22.3.14, las entidades del Estado, de acuerdo con el ámbito de aplicación del Modelo Integrado de Planeación y Gestión (MIPG), deberán integrar al Plan de Acción institucional doce planes específicos y publicarlos en su página web a más tardar el 31 de enero de cada año. El Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información aparece en el numeral 11 de este listado, junto con:

- Plan Institucional de Archivos de la Entidad - PINAR
- Plan Anual de Adquisiciones
- Plan Anual de Vacantes
- Plan de Previsión de Recursos Humanos
- Plan Estratégico de Talento Humano
- Plan Institucional de Capacitación
- Plan de Incentivos Institucionales
- Plan de Trabajo Anual en Seguridad y Salud en el Trabajo
- Plan Anticorrupción y de Atención al Ciudadano
- Plan Estratégico de Tecnologías de la Información y las Comunicaciones - PETI
- Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información
- Plan de Seguridad y Privacidad de la Información

El parágrafo 1 del artículo 2.2.22.3.14 establece que cuando se trate de planes de duración superior a un año, se integrarán al Plan de Acción las actividades que correspondan a la respectiva anualidad. Además, el parágrafo 2 indica que harán parte del Plan de Acción las acciones y estrategias a través de las cuales las entidades facilitarán y promoverán la participación de las personas en los asuntos de su competencia, en los términos de la Ley 1757 de 2015.

2.2. Normativa Complementaria

NORMA	DESCRIPCIÓN
Ley 1581 de 2012	Protección de datos personales. Establece el régimen general de protección de datos personales en Colombia.
Decreto 1377 de 2013	Reglamenta parcialmente la Ley 1581 de 2012 en lo relacionado con el tratamiento de datos personales.
Ley 1712 de 2014	Transparencia y acceso a la información pública nacional. Define las categorías de información pública.
ISO/IEC 27001:2013	Estándar internacional para Sistemas de Gestión de Seguridad de la Información (SGSI).
Decreto 1078 de 2015	Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones. Establece la Estrategia de Gobierno Digital.
CONPES 3854 de 2016	Política Nacional de Seguridad Digital. Define los lineamientos de seguridad digital para el país.
Decreto 1083 de 2015	Único Reglamentario del Sector de Función Pública. Desarrolla el Modelo Integrado de Planeación y Gestión (MIPG).
Ley 594 de 2000	Ley General de Archivos. Establece las normas sobre conservación de documentos.

3. GLOSARIO DE TÉRMINOS

Para efectos del presente plan, se adoptan las siguientes definiciones:

Activo de Información: Cualquier información o elemento relacionado con el tratamiento de la misma (sistemas, soportes, edificios, personas) que tenga valor para la organización. (ISO/IEC 27000)

Amenaza: Causa potencial de un incidente no deseado, que puede provocar daños a un sistema o a la organización. (ISO/IEC 27000)

Análisis de Riesgo: Proceso para comprender la naturaleza del riesgo y determinar el nivel de riesgo. (ISO/IEC 27000)

Control: Medida que modifica el riesgo. Comprende las políticas, procedimientos, prácticas y estructuras organizativas concebidas para mantener los riesgos de seguridad de la información por debajo del nivel de riesgo asumido.

Datos Personales: Cualquier información vinculada o que pueda asociarse a una o varias personas naturales determinadas o determinables. (Ley 1581 de 2012)

Datos Personales Sensibles: Aquellos que afectan la intimidad del titular o cuyo uso indebido puede generar su discriminación, tales como los que revelen el origen racial o étnico, la orientación política, las convicciones religiosas o filosóficas, la pertenencia a sindicatos, así como los datos relativos a la salud, a la vida sexual y los datos biométricos.

Información Pública Clasificada: Información que estando en poder o custodia de un sujeto obligado, pertenece al ámbito propio, particular y privado o semiprivado de una persona natural o jurídica, por lo que su acceso podrá ser negado o exceptuado. (Ley 1712 de 2014)

Información Pública Reservada: Información que estando en poder o custodia de un sujeto obligado, es exceptuada de acceso a la ciudadanía por daño a intereses públicos. (Ley 1712 de 2014)

Plan de Tratamiento de Riesgos: Documento que define las acciones para gestionar los riesgos de seguridad de la información inaceptables e implantar los controles necesarios para proteger la misma. (ISO/IEC 27000)

Privacidad: Derecho que tienen todos los titulares de la información en relación con la información que involucre datos personales y la información clasificada que estos hayan entregado o esté en poder de la entidad.

Riesgo: Posibilidad de que una amenaza concreta pueda explotar una vulnerabilidad para causar una pérdida o daño en un activo de información. Se considera como una combinación de la probabilidad de un evento y sus consecuencias. (ISO/IEC 27000)

Seguridad de la Información: Preservación de la confidencialidad, integridad y disponibilidad de la información. (ISO/IEC 27000)

Sistema de Gestión de Seguridad de la Información (SGSI): Conjunto de elementos interrelacionados (estructura organizativa, políticas, planificación de actividades, responsabilidades, procesos, procedimientos y recursos) que utiliza una organización para establecer una política y objetivos de seguridad de la información, basado en un enfoque de gestión y mejora continua. (ISO/IEC 27000)

Vulnerabilidad: Debilidad de un activo o control que puede ser explotada por una o más amenazas. (ISO/IEC 27000)

4. OBJETIVOS

4.1. Objetivo General

Diseñar, implementar, operar y mejorar continuamente el Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información, como instrumento institucional integrado al Plan de Acción en cumplimiento del Decreto 612 de 2018, que permita identificar, evaluar, tratar y monitorear los riesgos asociados a los procesos, activos, sistemas de información e infraestructura tecnológica de EMPOAGUAS E.S.P., en el marco del Modelo Integrado de Planeación y Gestión (MIPG), la Política de Gobierno Digital, la normativa de protección de datos personales y el Sistema de Control Interno.

4.2. Objetivos Específicos

Identificación y Clasificación de Activos

Identificar, inventariar y clasificar los activos de información y TIC de EMPOAGUAS E.S.P., determinando su nivel de criticidad y los responsables de su custodia y tratamiento.

Gestión del Riesgo de Seguridad de la Información

Implementar una metodología de gestión del riesgo que permita identificar amenazas, vulnerabilidades e impactos sobre los activos de información, definiendo controles adecuados para su tratamiento, conforme a ISO/IEC 27001 e integración con el Mapa de Riesgos Institucional.

Protección de Datos Personales y Privacidad

Garantizar la adecuada recolección, almacenamiento, uso, circulación y disposición de los datos personales, en cumplimiento de la Ley 1581 de 2012, el Decreto 1377 de 2013 y las políticas internas de tratamiento de la información.

Implementación de Controles de Seguridad

Definir e implementar controles técnicos, administrativos y físicos que mitiguen los riesgos de seguridad de la información, incluyendo control de accesos, seguridad en redes, respaldo de información y gestión de incidentes.

Continuidad y Disponibilidad de la Información

Establecer medidas que aseguren la continuidad de los servicios TIC críticos, minimizando la interrupción de los procesos misionales y administrativos de la entidad.

Gestión de Incidentes de Seguridad

Diseñar e implementar procedimientos para la detección, reporte, análisis, respuesta y recuperación ante incidentes de seguridad de la información.

Cultura y Sensibilización Organizacional

Fortalecer la cultura de seguridad de la información mediante programas de capacitación, sensibilización y buenas prácticas dirigidas a funcionarios, contratistas y terceros.

Cumplimiento Normativo y Mejora Continua

Asegurar el cumplimiento de los lineamientos del Modelo Integrado de Planeación y Gestión (MIPG), la Política de Gobierno Digital, el Decreto 612 de 2018 y demás normas aplicables, promoviendo la mejora continua del plan a través de seguimiento, auditorías y evaluación periódica.

5. ALCANCE

El presente Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información aplica a:

- Todos los procesos misionales, estratégicos, de apoyo y de evaluación de EMPOAGUAS E.S.P.
- Todos los activos de información (físicos, digitales, documentales) de la entidad.
- La infraestructura tecnológica, sistemas de información, redes y telecomunicaciones.
- Datos personales de usuarios, funcionarios, contratistas y terceros.
- Información pública clasificada y reservada según la Ley 1712 de 2014.
- Todos los funcionarios, contratistas y terceros que interactúan con los activos de información de la entidad.
- Todas las sedes y ubicaciones donde se procesa, almacena o transmite información de la entidad.

Exclusiones:

El presente plan no abarca la gestión de riesgos operacionales, financieros o estratégicos que no estén directamente relacionados con la seguridad y privacidad de la información, los cuales son tratados en el Mapa de Riesgos Institucional y otros instrumentos de planeación específicos.

Vigencia:

El Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información tiene vigencia anual, comprendida entre el 1 de enero y el 31 de diciembre de 2026, en cumplimiento del Decreto 612 de 2018. Su aprobación y publicación se realizará a más tardar el 31 de enero de 2026.

6. RESPONSABLES Y LIDERAZGO

En cumplimiento del Decreto 612 de 2018 y el Modelo Integrado de Planeación y Gestión (MIPG), la formulación, ejecución, seguimiento y control del presente Plan corresponde a:

RESPONSABLE FUNCIONES Y RESPONSABILIDADES

Gerencia

- Aprobar el Plan de Tratamiento de Riesgos.
- Garantizar los recursos necesarios para su implementación.
- Promover la cultura de seguridad de la información en la entidad.

Subgerencia Administrativa y Financiera

- Articular el Plan con el Plan Estratégico Institucional y el MIPG.
- Coordinar la integración con los demás planes institucionales del Decreto 612 de 2018.
- Garantizar la asignación de recursos para la ejecución del plan.

Oficina de Tecnologías de la Información y las Comunicaciones (TIC)

- Formular y actualizar el Plan de Tratamiento de Riesgos.
- Ejecutar las actividades programadas.
- Realizar seguimiento periódico y generar reportes de avance.
- Coordinar con los líderes de proceso la identificación y valoración de riesgos.
- Implementar controles de seguridad de la información.

Oficina de Control Interno

- Realizar seguimiento independiente a la ejecución del plan.
- Evaluar la efectividad de los controles implementados.
- Emitir recomendaciones de mejora.
- Verificar el cumplimiento normativo.

Líderes de Proceso

- Identificar y reportar riesgos de seguridad en sus procesos.
- Participar en la valoración de riesgos.
- Implementar controles en sus áreas de responsabilidad.
- Reportar incidentes de seguridad de la información.

Funcionarios, Contratistas y Terceros

- Cumplir las disposiciones establecidas en el presente Plan.
- Adoptar buenas prácticas de seguridad de la información.
- Reportar incidentes o vulnerabilidades identificadas.
- Participar en las capacitaciones y sensibilizaciones.

7. METODOLOGÍA DE IMPLEMENTACIÓN DEL SGSI (ISO/IEC 27001)

Para el establecimiento, implementación, operación, monitoreo, revisión, mantenimiento y mejora continua del Sistema de Gestión de la Seguridad de la Información (SGSI), se adopta el ciclo de mejora continua PDCA (Plan–Do–Check–Act), ampliamente reconocido en los sistemas de gestión y base fundamental de la norma ISO/IEC 27001.

Planificar (Plan) – Establecimiento del SGSI

En esta fase se define el marco estratégico y operativo del SGSI, asegurando su alineación con los objetivos institucionales y los requisitos legales y normativos aplicables. Incluye:

- Definición del alcance del SGSI, considerando procesos, activos de información, sistemas, sedes y partes interesadas.
- Identificación y clasificación de los activos de información.
- Análisis y evaluación de riesgos de seguridad de la información, incluyendo amenazas, vulnerabilidades e impactos.
- Definición de la política de seguridad de la información.
- Selección de controles de seguridad apropiados (Anexo A de ISO/IEC 27001) y elaboración del Plan de Tratamiento de Riesgos.
- Asignación de roles, responsabilidades y recursos necesarios.

Hacer (Do) – Implementación y Operación del SGSI

En esta etapa se ejecuta lo planificado, asegurando que los controles y procedimientos definidos se apliquen de manera efectiva:

- Implementación de controles técnicos, administrativos y físicos de seguridad.
- Desarrollo y divulgación de procedimientos, normas y guías de seguridad.
- Capacitación y sensibilización del personal en seguridad de la información.
- Gestión de incidentes de seguridad de la información.
- Operación continua de los procesos definidos en el SGSI.

Verificar (Check) – Seguimiento y Revisión del SGSI

Se evalúa el desempeño del SGSI para verificar su eficacia y conformidad con los requisitos establecidos:

- Monitoreo y medición de los controles de seguridad implementados.
- Revisión del cumplimiento de políticas, procedimientos y requisitos legales.
- Ejecución de auditorías internas del SGSI.
- Análisis de incidentes, no conformidades y resultados de auditorías.
- Revisión por la dirección.

Actuar (Act) – Mantenimiento y Mejora Continua del SGSI

Con base en los resultados de la fase de verificación, se implementan acciones para corregir desviaciones y mejorar continuamente el SGSI:

- Definición e implementación de acciones correctivas y preventivas.
- Actualización del análisis de riesgos y del plan de tratamiento.
- Ajuste de políticas, controles y procedimientos.
- Incorporación de mejoras tecnológicas, organizacionales y normativas.
- Fortalecimiento continuo de la cultura de seguridad de la información.

8. ACTIVIDADES

1. Realizar el diagnóstico inicial de seguridad y privacidad de la información

Identificar el estado actual de los procesos, activos de información, controles existentes, brechas y nivel de madurez en seguridad de la información, conforme a los lineamientos del SGSI.

2. Definir y documentar el alcance del Plan de Tratamiento de Riesgos

Establecer los procesos, activos, áreas, sistemas de información y partes interesadas que serán objeto del tratamiento de riesgos, alineados con los objetivos estratégicos de la entidad.

3. Realizar la identificación y valoración de riesgos

Analizar amenazas, vulnerabilidades e impactos sobre la confidencialidad, integridad y disponibilidad de la información, determinando el nivel de riesgo inherente y el riesgo residual posterior a la aplicación de controles.

4. Elaborar mapas de calor de riesgos

Representar gráficamente los niveles de riesgo identificados, clasificándolos según su probabilidad e impacto, con el fin de priorizar el tratamiento y facilitar la toma de decisiones.

5. Formular y formalizar el Plan de Tratamiento de Riesgos

Definir las acciones de mitigación, aceptación, transferencia o eliminación de riesgos, asignando responsables, recursos, cronogramas e indicadores, y someter el plan a aprobación por parte de los líderes y la alta dirección.

6. Implementar controles de seguridad

Ejecutar las acciones definidas en el plan de tratamiento, implementando controles técnicos, administrativos y físicos para reducir los riesgos a niveles aceptables.

7. Capacitar y sensibilizar al personal

Desarrollar programas de formación en seguridad de la información dirigidos a todos los niveles de la organización, fortaleciendo la cultura de seguridad.

8. Realizar seguimiento y monitoreo continuo

Evaluar periódicamente la efectividad de los controles implementados y el nivel de riesgo residual, ajustando el plan según sea necesario.

9. CRONOGRAMA DE EJECUCIÓN

ACTIVIDAD	RESPONSABLE	PERIODO
Aprobación y publicación del Plan	Gerencia / Oficina TIC	Enero 2026
Diagnóstico inicial de seguridad	Oficina TIC	Enero - febrero 2026
Identificación de riesgos con líderes de proceso	Oficina TIC / Líderes de Proceso	Enero - abril 2026
Valoración y análisis de riesgos	Oficina TIC	Enero - abril 2026
Elaboración de mapas de calor	Oficina TIC	Marzo - abril 2026
Diseño de controles y establecimiento de indicadores	Oficina TIC	Enero - abril 2026
Implementación de controles de seguridad	Oficina TIC / Líderes de Proceso	Mayo - noviembre 2026
Capacitación y sensibilización	Oficina TIC / Talento Humano	Marzo - octubre 2026
Seguimiento y control (primera revisión)	Oficina TIC / Control Interno	Junio 2026
Seguimiento y control (segunda revisión)	Oficina TIC / Control Interno	Diciembre 2026
Evaluación y mejora continua	Oficina TIC / Control Interno	Permanente

10. SEGUIMIENTO Y EVALUACIÓN

En cumplimiento del Decreto 612 de 2018 y el Modelo Integrado de Planeación y Gestión (MIPG), el seguimiento y evaluación del Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información se realizará de la siguiente manera:

Reuniones de Seguimiento

Al cierre de cada fase del proyecto se realizará una reunión formal de seguimiento, con participación de:

- Responsables de las diferentes áreas de la empresa
- Oficina de Tecnologías de la Información y las Comunicaciones (TIC)
- Oficina de Control Interno
- Líderes de proceso involucrados

Informes de Avance

Durante las sesiones de seguimiento se presentarán informes que incluirán:

- Estado de cumplimiento de las actividades planificadas
- Hitos alcanzados y pendientes
- Desviaciones identificadas y causas raíz
- Nivel de avance frente al cronograma establecido
- Indicadores de gestión y desempeño
- Evaluación de la eficacia de los controles implementados
- Análisis del riesgo residual

Indicadores de Gestión

Se establecen los siguientes indicadores para medir el cumplimiento y efectividad del plan:

INDICADOR	FÓRMULA	META
Cumplimiento del plan	(Actividades ejecutadas / Actividades programadas) x 100	≥ 90%
Efectividad de controles	(Controles efectivos / Controles implementados) x 100	≥ 85%
Reducción del riesgo	(Riesgo residual / Riesgo inherente) x 100	≤ 40%
Personal capacitado	(Personal capacitado / Total personal) x 100	≥ 95%
Incidentes gestionados	(Incidentes resueltos / Incidentes reportados) x 100	≥ 90%

Acciones de Mejora

Como resultado de la evaluación, se definirán:

- Acciones correctivas para atender desviaciones identificadas
- Acciones preventivas para mitigar riesgos potenciales
- Acciones de mejora para optimizar procesos y controles
- Asignación de responsables y plazos de ejecución
- Documentación para garantizar trazabilidad y control

La evaluación se realizará en coherencia con los requisitos de la norma ISO/IEC 27001, verificando la conformidad con el alcance del SGSI y la adecuada aplicación del ciclo de mejora continua (Plan–Do–Check–Act).

11. ENTREGABLES

Como resultado de la implementación del Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información, en cumplimiento del Decreto 612 de 2018 y el Modelo Integrado de Planeación y Gestión (MIPG), se generarán los siguientes entregables:

1. Actas de reunión

Evidencian la socialización, análisis y toma de decisiones relacionadas con la gestión de riesgos de seguridad y privacidad de la información.

2. Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información

Documento debidamente revisado, validado y aprobado por los líderes de proceso y la Alta Dirección, publicado en la página web institucional.

3. Política de Seguridad y Privacidad de la Información

Formalmente adoptada y divulgada en la entidad, alineada con el MIPG y la normativa vigente.

4. Matriz de Riesgos de Seguridad y Privacidad

Incluye la identificación, valoración, tratamiento y monitoreo de riesgos asociados a los activos de información.

5. Mapas de Calor de Riesgos

Representación gráfica de los niveles de riesgo por proceso y activo de información.

6. Registro de Controles Implementados

Documentación de los controles técnicos, administrativos y físicos implementados para mitigar riesgos.

7. Informes de Seguimiento

Reportes periódicos (semestrales) sobre el avance en la ejecución del plan, cumplimiento de actividades e indicadores de gestión.

8. Plan de Capacitación en Seguridad de la Información

Programa de formación y sensibilización para funcionarios, contratistas y terceros.

9. Registro de Incidentes de Seguridad

Documentación de incidentes reportados, análisis realizados y acciones correctivas implementadas.

10. Declaración de Aplicabilidad (SOA)

Listado de controles del Anexo A de ISO/IEC 27001 que aplican a EMPOAGUAS E.S.P., con justificación de inclusiones y exclusiones.

11. Informe de Auditoría Interna del SGSI

Resultado de las auditorías internas realizadas para verificar la conformidad del sistema de gestión.

12. Plan de Mejora Continua

Acciones correctivas, preventivas y de mejora identificadas durante el seguimiento y evaluación.

Todos estos documentos servirán como evidencia de cumplimiento ante entes de control, en el marco del FURAG (Formulario Único de Reporte de Avances de la Gestión) y las evaluaciones del MIPG.

12. APROBACIÓN Y PUBLICACIÓN

Aprobación

En cumplimiento del Decreto 612 de 2018, el presente Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información es aprobado por:

GERENTE GENERAL

EMPOAGUAS E.S.P.

Publicación

De conformidad con el artículo 2.2.22.3.14 del Decreto 1083 de 2015, adicionado por el Decreto 612 de 2018, el presente Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información será publicado en la página web institucional de EMPOAGUAS E.S.P. a más tardar el 31 de enero de 2026, como parte integral del Plan de Acción institucional.

Vigencia

El presente plan tiene vigencia anual, del 1 de enero al 31 de diciembre de 2026, y será objeto de seguimiento semestral por parte de la Oficina de TIC y la Oficina de Control Interno, en articulación con el Sistema de Control Interno y el proceso de autoevaluación del MIPG.

Articulación con el MIPG

Este plan hace parte integral del Modelo Integrado de Planeación y Gestión (MIPG) de EMPOAGUAS E.S.P. y se articula con:

- Plan de Acción Institucional
- Plan Estratégico de Tecnologías de la Información y las Comunicaciones (PETI)
- Plan de Seguridad y Privacidad de la Información
- Plan Anticorrupción y de Atención al Ciudadano
- Mapa de Riesgos Institucional
- Política de Gobierno Digital
- Sistema de Control Interno