EMPRESA DE ACUEDUCTO, ALCANTARILLADO DE SAN JOSÉ DEL GUAVIARE – EMPOAGUAS E.S.P.

NIT: 822.001.883-3

PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN – PSPI

Instrumento de Planeación Institucional

Integrado al Modelo Integrado de Planeación y Gestión – MIPG

En cumplimiento del Decreto 612 de 2018

Proceso: Gestión de Tecnologías de la Información y las Comunicaciones

Dependencia Responsable:

Subgerencia Administrativa y Financiera

Oficina TIC

San José del Guaviare – Colombia

2026

Tabla de Contenido

1. MARCO NORMATIVO, ARTICULACIÓN MIPG Y CUMPLIMIENTO DEL DECRETO 612 DE 2018

El presente Plan de Seguridad y Privacidad de la Información (PSPI) de EMPOAGUAS E.S.P. se formula en cumplimiento del Decreto 612 de 2018, integrándose al Modelo Integrado de Planeación y Gestión (MIPG) y articulándose con los demás planes institucionales.

Marco normativo aplicable:

- Decreto 612/2018 – Integración Planes al MIPG
- Decreto 1499/2017 – MIPG
- Decreto 1008/2018 – Gobierno Digital
- CONPES 3854/2016 – Seguridad Digital
- Ley 1581/2012 – Protección Datos Personales
- Decreto 1078/2015 – Sector TIC
- ISO/IEC 27001, 27002 – Referencia buenas prácticas

1.1-1.6 Articulación MIPG, Vigencia, Responsables, Cronograma, Indicadores, Seguimiento

El Plan se articula con políticas MIPG (Gobierno Digital, Riesgo, Control, Transparencia). Vigencia 2026. Responsables: Alta Dirección, Comité Institucional, TIC, Control Interno, Usuarios. Cronograma con actividades trimestrales. Indicadores: capacitación ≥90%, cumplimiento 100%, disponibilidad ≥99%. Seguimiento mediante reportes trimestrales, auditorías anuales y reporte en FURAG.

1.7 INTEGRACIÓN CON LOS PLANES INSTITUCIONALES DEL DECRETO 612 DE 2018

CUMPLIMIENTO DEL DECRETO 612 DE 2018:

El artículo 2.2.22.3.14 del Decreto 612 de 2018 establece que las entidades del Estado deben integrar en su Plan de Acción los siguientes doce (12) planes institucionales y estratégicos:

1. Plan Institucional de Archivos – PINAR
2. Plan Anual de Adquisiciones
3. Plan Anual de Vacantes
4. Plan de Previsión de Recursos Humanos
5. Plan Estratégico de Talento Humano
6. Plan Institucional de Capacitación
7. Plan de Incentivos Institucionales
8. Plan de Trabajo Anual en SST
9. Plan Anticorrupción y Atención al Ciudadano
10. Plan Estratégico de TIC – PETI
11. Plan de Tratamiento de Riesgos
12. Plan de Seguridad y Privacidad de la Información

ARTICULACIÓN TRANSVERSAL DEL PLAN DE SEGURIDAD:

• Con PETI: Seguridad en iniciativas tecnológicas desde diseño, arquitectura de seguridad alineada, presupuesto para herramientas seguridad, desarrollo seguro software, gestión vulnerabilidades, controles en cambios y proyectos TIC.

• Con PINAR: Controles seguridad gestión documental electrónica, integridad y confidencialidad documentos, firmas digitales, trazabilidad, retención y eliminación segura, protección datos personales, copias seguridad repositorios.

• Con Adquisiciones: Requisitos seguridad en especificaciones técnicas hardware/software, evaluación proveedores con certificaciones ISO 27001, cláusulas confidencialidad contratos, adquisición servicios auditoría/pentesting, SLAs seguridad.

• Con Talento Humano y Capacitación: Competencias seguridad en perfiles cargo TIC, programa anual capacitación seguridad, sensibilización phishing e ingeniería social, formación protección datos personales, cláusulas confidencialidad contratos.

• Con Riesgos: Gestión riesgos seguridad integrada mapa riesgos institucional, identificación/valoración riesgos confidencialidad/integridad/disponibilidad, controles mitigación, monitoreo KRIs, análisis impacto negocio (BIA), tratamiento diferenciado por nivel riesgo.

• Con Anticorrupción: Trazabilidad y auditoría prevención manipulación datos, protección denunciantes, seguridad plataformas participación ciudadana, protección datos trámites en línea, publicación segura transparencia, registros verificación Ley Transparencia.

• Con SST: Protección datos sensibles salud funcionarios, seguridad sistemas SST, controles acceso información accidentes laborales, ergonomía equipos cómputo, prevención riesgos psicosociales tecnología.

CONCLUSIÓN: Esta integración transversal garantiza que el Plan de Seguridad opera como componente habilitador y protector que permea todos los procesos institucionales, siendo pilar fundamental para objetivos estratégicos, cumplimiento normativo, protección patrimonio público, prestación eficiente servicios y fortalecimiento confianza ciudadana.

Conforme parágrafo 1° artículo 2.2.22.3.14 Decreto 612/2018, actividades Plan 2026 están plenamente integradas Plan de Acción con metas, indicadores, responsables y cronogramas. Seguimiento trimestral por TIC con reportes a Comité Institucional y Alta Dirección. Resultados en FURAG y auditorías.

2. PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

2.1 POLÍTICA DE SEGURIDAD Y PRIVACIDAD

Política formal de EMPOAGUAS E.S.P. estableciendo compromiso con protección integral activos de información: funcionarios, contratistas, terceros, información (todos formatos), procesos institucionales y tecnologías (infraestructura, hardware, software, servicios). Orienta implementación, mantenimiento y mejora continua Sistema Gestión Seguridad Información (SGSI).

OBJETIVOS DE SEGURIDAD:

- Identificar, analizar y mitigar riesgos afectando confidencialidad, integridad, disponibilidad, privacidad
- Garantizar principios seguridad y protección datos en todos procesos y sistemas
- Asegurar principios función administrativa: legalidad, eficiencia, eficacia, transparencia

- Mantener confianza funcionarios, usuarios y terceros
- Apoyar innovación con seguridad desde diseño y por defecto
- Implementar y mejorar SGSI conforme estándares y buenas prácticas
- Proteger activos vs accesos no autorizados, pérdida, alteración, divulgación
- Establecer políticas, procedimientos e instructivos claros
- Promover cumplimiento obligatorio
- Fortalecer cultura seguridad y protección datos
- Garantizar continuidad servicios con planes prevención, respuesta, recuperación

2.2 ALCANCE

Aplicación obligatoria para EMPOAGUAS E.S.P. Cobija: funcionarios, contratistas, proveedores, terceros autorizados, ciudadanía (usuarios y titulares datos). Comprende: todos procesos (estratégicos, misionales, apoyo, control), sistemas información, infraestructura, servicios digitales, información física y electrónica, todas ubicaciones y modalidades operación.

2.3 NIVEL DE CUMPLIMIENTO

OBLIGATORIO para todos en alcance. Acceso/uso información implica aceptación expresa obligaciones. Incumplimiento conlleva: sanciones disciplinarias (funcionarios), terminación contratos (contratistas), penalidades (proveedores), responsabilidad penal (delitos informáticos), responsabilidad civil (daños). EMPOAGUAS puede suspender/revocar accesos ante incumplimientos.

3. IMPLEMENTACIÓN DE POLÍTICAS DE SEGURIDAD

3.1 JUSTIFICACIÓN

Plan fundamental para prevención, control y mitigación riesgos activos información. Seguridad basada en CONFIDENCIALIDAD (acceso solo autorizados), INTEGRIDAD (exactitud y validez), DISPONIBILIDAD (acceso oportuno autorizados), más AUTENTICIDAD, NO REPUDIO, TRAZABILIDAD, LEGALIDAD, CONFIABILIDAD.

3.2 OBJETIVO

Establecer mecanismos técnicos, lógicos, físicos, administrativos, legales, ambientales para: prevenir accesos no autorizados, detectar intrusiones, responder oportunamente incidentes, recuperar servicios/datos, proteger confidencialidad clasificada, garantizar integridad crítica, asegurar disponibilidad esencial, cumplir obligaciones legales, proteger reputación, minimizar impactos.

3.3 ALCANCE

Todos recursos, procesos, personal EMPOAGUAS E.S.P. Ciclo completo gestión información: creación hasta disposición final.

3.4 ROLES Y RESPONSABILIDADES

Gerente General: Aprobar Plan, asignar recursos, promover cultura seguridad
Comité Gestión: Direccionar SGSI, aprobar excepciones, revisar riesgos críticos
Jefe TIC: Implementar controles, gestionar incidentes, administrar infraestructura
Control Interno: Auditar SGSI, evaluar controles, emitir recomendaciones
Propietarios Activos: Clasificar información, autorizar accesos, definir controles
Usuarios: Cumplir políticas, proteger credenciales, reportar anomalías

3.5 CUMPLIMIENTO

Obligatorio todos. Mecanismos: monitoreo continuo, auditorías periódicas, evaluaciones seguridad apps, pentesting anual, revisiones configuración, sanciones proporcionales.

3.6 COMUNICACIÓN

Difusión: inducción/reinducción, publicación web/intranet, correos institucionales, carteleras, talleres, contratos, campañas concientización trimestrales.

3.7 MONITOREO

Revisión mensual logs, análisis trimestral indicadores, evaluación semestral controles, auditoría anual SGSI, revisiones incidentes, actualización inventario, análisis tendencias amenazas.

4. DESCRIPCIÓN DE LAS POLÍTICAS

4.1 GESTIÓN DE ACTIVOS

Identificar, inventariar, clasificar y proteger todos activos información. Propietario claro cada activo. Inventario semestral. Clasificación: PÚBLICA (sin restricción), CLASIFICADA (uso interno protección), RESERVADA (altamente sensible acceso restringido). Valoración: confidencialidad, integridad, disponibilidad, cumplimiento legal. Documentar: descripción, ubicación, propietario, clasificación, controles. Etiquetado físico/digital. Disposición segura: borrado seguro, destrucción física discos, fragmentación documentos clasificados, certificados destrucción.

4.2 CONTROL DE ACCESO

PRINCIPIOS: Mínimo privilegio, necesidad conocer, segregación funciones, autenticación fuerte, revisión periódica. CONTROLES RED: Segmentación zonas,

firewall restrictivo, IDS/IPS, VPN cifrada, 802.1X inalámbricas, filtrado web, monitoreo tráfico, ACLs. GESTIÓN USUARIOS: Solicitud/aprobación/provisión/revisión/revocación formal. CONTRASEÑAS: 12 caracteres mínimo, complejidad, cambio 90 días, historial 5, bloqueo 5 intentos fallidos, cambio obligatorio primer acceso. SISTEMAS: Autenticación individual, timeout 15 minutos, registro auditoría, cifrado credenciales, ambientes separados, acceso producción limitado.

4.3 SEGURIDAD FÍSICA

PERÍMETROS: Control ingreso instalaciones (vigilancia, torniquetes, CCTV), áreas críticas (servidores, telecom, archivo) acceso restringido, controles físicos (cerraduras electrónicas, tarjetas, biometría), registro visitantes, cámaras grabación 30 días, alarmas intrusión. PROTECCIÓN AMBIENTAL: Detección/extinción incendios, control temperatura/humedad, protección inundaciones, UPS/planta eléctrica, protección descargas, mantenimiento preventivo.

4.4 SEGURIDAD EQUIPOS

CONFIGURACIÓN: SO actualizado parches, antivirus actualizado, firewall host, cifrado disco portátiles, desactivación USB no autorizados, administración remota, bloqueo pantalla 5 min, software solo autorizado por TIC. USO: Responsabilidad usuario asignado, acta entrega, uso laboral exclusivo, prohibido software no autorizado, no compartir, reportar pérdida inmediata, devolución fin vínculo.

4.5 USO ADECUADO INTERNET

PERMITIDO: Información funciones laborales, investigación desarrollo profesional, comunicaciones institucionales, servicios Estado, trámites oficiales. PROHIBIDO: Contenido pornográfico/violento, software no autorizado, redes sociales no autorizadas, contenido derechos autor, apuestas, proxy/VPN eludir controles, difusión información confidencial, actividades ilegales. CONTROLES: Filtrado contenido, monitoreo tráfico, logs 6 meses, bloqueo maliciosos, análisis amenazas real-time, restricción ejecutables, escaneo antimalware descargas.

5. PRIVACIDAD Y CONFIDENCIALIDAD

5.1 Política Tratamiento y Protección Datos Personales

Cumplimiento Ley 1581/2012, Decreto 1377/2013. PRINCIPIOS: Legalidad, Finalidad, Libertad, Veracidad, Transparencia, Acceso restringido, Seguridad, Confidencialidad. DERECHOS TITULARES: Conocer/actualizar/rectificar, solicitar prueba autorización, ser informado uso, quejas SuperIndustria, revocar/suprimir,

acceso gratuito. CANAL: contacto@empoaguas.gov.co. PLAZOS: Consultas 10 días, Reclamos 15 días. MEDIDAS: Cifrado bases datos, control acceso roles, auditoría accesos, transferencia cifrada, anonimización, seudonimización, eliminación segura, acuerdos confidencialidad procesadores.

5.2 Disponibilidad del Servicio

Plan Continuidad Negocio (BCP) anual, Plan Recuperación Desastres (DRP) servicios críticos, Análisis Impacto Negocio (BIA), definición RTO/RPO, pruebas planes anual, equipo respuesta capacitado, SLAs proveedores críticos, sitio alterno. OBJETIVOS: Sistema comercial 99% disponibilidad/RTO 4h/RPO 24h, Correo 99%/2h/4h, ERP financiero 99%/4h/24h, Portal web 95%/8h/24h.

5.3 Política Continuidad, Contingencia y Recuperación

Mecanismos prevenir, responder, recuperar incidentes afectando disponibilidad información y continuidad procesos críticos.

5.4 Política Copias Seguridad (Backups)

ALCANCE: Bases datos críticas diario incremental/semanal completo, archivos servidores diario incremental/semanal completo, configuraciones red semanal, VMs críticas semanal, correo diario. ALMACENAMIENTO: On-site diarias retención 1 semana, Off-site semanales retención 1 mes, cifrado medios, control acceso físico, verificación integridad, registro copias. PRUEBAS: Trimestrales restauración verificando integridad, capacidad recuperación, RTO, RPO, documentación procedimientos.