PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN 2026

La Mesa - Cundinamarca, enero 2026

	ELABORÓ	REVISÓ	APROBÓ
Nombre:	Mauricio Sánchez Herrera	Comité Institucional de Gestión y Desempeño. Acta 002 de 2026	Dr. Nelson Iván García Tarquino
Cargo:	Profesional de apoyo en sistemas		Gerente
Fecha:	Enero de 2026	30 de enero de 2026	30 de enero de 2026

TABLA DE CONTENIDO

INTRODUCCIÓN

La Empresa Regional Aguas del Tequendama S.A. E.S.P. (ERAT), en cumplimiento de su misión de prestar servicios públicos domiciliarios de acueducto y alcantarillado con calidad y eficiencia en la región del Tequendama, reconoce la información como un activo fundamental para su operación.

El presente Plan de Seguridad y Privacidad de la Información (PSPI) para la vigencia 2026 establece la hoja de ruta para garantizar la confidencialidad, integridad y disponibilidad de los activos de información de la entidad. Este plan se alinea con el Modelo Integrado de Planeación y Gestión (MIPG), la Política de Gobierno Digital y la reciente actualización del Modelo de Seguridad y Privacidad de la Información (MSPI) del MinTIC.

1. OBJETIVOS

1.1 Objetivo General

Fortalecer el Sistema de Gestión de Seguridad de la Información (SGSI) de la ERAT durante el año 2026, implementando controles técnicos, legales y administrativos que minimicen los riesgos de seguridad digital y protejan los datos personales de suscriptores, empleados y proveedores.

1.2 Objetivos Específicos

- **Actualizar el esquema de riesgos:** Identificar y tratar nuevas amenazas cibernéticas (Ransomware, Phishing) que puedan afectar la infraestructura crítica de la Entidad.
- **Cumplimiento Normativo:** Garantizar el cumplimiento de la Ley 1581 de 2012 (Protección de Datos) y la Resolución 02277 de 2025 del MinTIC.
- **Cultura de Seguridad:** Capacitar al 100% de los funcionarios y contratistas de las sedes (La Mesa, Anapoima y operativas) en buenas prácticas de seguridad digital.
- **Gestión de Activos:** Mantener actualizado el inventario de activos de información clasificados por criticidad.

2. ALCANCE

Este plan aplica a todos los procesos estratégicos, misionales, de apoyo y de evaluación de la ERAT. Cubre a todos los funcionarios, contratistas, proveedores y terceros que tengan acceso a los sistemas de información o bases de datos de la empresa, tanto en la sede administrativa de La Mesa, como en la sede de Anapoima y de atención al usuario.

3. MARCO NORMATIVO Y REFERENCIAL

El plan se fundamenta en la siguiente normatividad vigente:

- **Constitución Política de Colombia:** Arts. 15 (Habeas Data) y 209 (Función Administrativa).
- **Ley 1581 de 2012:** Disposiciones generales para la protección de datos personales.
- **Decreto 1078 de 2015:** Decreto Único Reglamentario del Sector TIC (Políticas de Gobierno Digital).
- **Resolución MinTIC 02277 de 2025:** Por la cual se actualiza el Modelo de Seguridad y Privacidad de la Información (MSPI).
- **Norma ISO/IEC 27001:2022**: Estándar internacional para Sistemas de Gestión de Seguridad de la Información.

- **Circular Externa Superservicios:** Circulares vigentes de la SSPD relacionadas con la calidad y seguridad del reporte de información al SUI.

3.1 Políticas Institucionales de Seguridad

Para garantizar la operatividad de este plan y el cumplimiento del marco legal descrito anteriormente, la ERAT se rige por las siguientes políticas internas, las cuales son de obligatorio cumplimiento para todos los funcionarios y contratistas:

- **Política General de Seguridad y Privacidad de la Información:** Lineamientos marco para la protección de los activos de la entidad.
- **Política de Control de Acceso y Gestión de Usuarios:** Reglas para la creación, modificación y eliminación de permisos de acceso a los sistemas (MFA, contraseñas seguras).
- **Política de Escritorio Limpio y Pantalla Bloqueada:** Directrices para asegurar la información física y lógica en los puestos de trabajo.
- **Política de Uso Aceptable de Activos Tecnológicos:** Normas sobre el uso adecuado de computadores, correo electrónico e internet corporativo.
- **Política de Copias de Seguridad (Backups):** Procedimientos para la generación y restauración de copias de respaldo de la información crítica.

4. ROLES Y RESPONSABILIDADES

Para la ejecución de este plan, se definen los siguientes roles dentro de la ERAT:

- **Comité Institucional de Gestión y Desempeño:** Aprueba el plan y asigna los recursos financieros y humanos.
- **Líder de TI:** Responsable de diseñar, implementar y monitorear el plan.
- **Líderes de Proceso:** Responsables de identificar los activos de información de su área y reportar incidentes.
- **Gestores de Talento Humano:** Responsables de incluir cláusulas de confidencialidad en los contratos y apoyar las capacitaciones.
- **Todos los funcionarios:** Responsables de cumplir las políticas (ej. no compartir contraseñas, bloquear equipos).

5. DIAGNÓSTICO DE SEGURIDAD

Antes de iniciar el 2026, la ERAT presenta el siguiente estado:

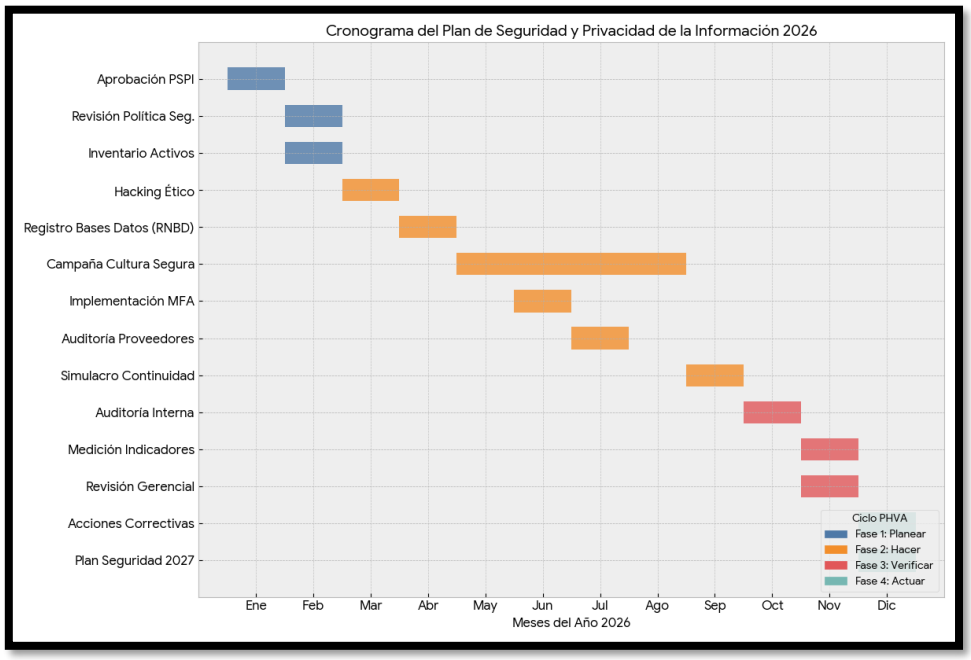
- **Principales riesgos materializados en 2025:** Intentos de phishing a correos corporativos, caída temporal del sistema de facturación,
- **Estado de copias de seguridad:** Se realizan backups diarios, pero falta prueba de restauración trimestral.

Análisis de Contexto (DOFA):

- **Debilidades:** Obsolescencia en algunos equipos de cómputo y falta de cultura de seguridad en personal operativo.
- **Amenazas:** Aumento global de ataques de Ransomware a empresas de servicios públicos y fallas en el suministro de energía que afectan la disponibilidad.
- **Fortalezas:** Compromiso de la Alta Dirección y existencia de herramientas de seguridad perimetral (Firewall).
- **Oportunidades:** Actualización normativa del MinTIC para estandarizar procesos y disponibilidad de nuevas tecnologías de autenticación (MFA).

6. PLAN DE ACCIÓN 2026

A continuación, se detallan las actividades a ejecutar durante la vigencia 2026, divididas por las fases del ciclo PHVA (Planear, Hacer, Verificar, Actuar):



FASE 1: PLANEAR (enero - febrero)

Actividad	Entregable	Responsable	Fecha
Aprobación del PSPI 2026	Acta de Comité	Gerencia / TI	Enero 30
Revisión y actualización de la Política de Seguridad Digital	Política v.2026	Líder TI / Jurídica	Feb 15
Actualización del Inventario de Activos de Información (Clasificación: Confidencial, Público, Interno)	Inventario Actualizado	Líderes de Proceso	Feb 28

FASE 2: HACER (marzo - septiembre)

Actividad	Entregable	Responsable	Fecha
Gestión de Riesgos: Análisis de vulnerabilidades y pruebas de penetración (Ethical Hacking) en infraestructura crítica.	Informe Técnico de Vulnerabilidades	Líder TI	Marzo
Protección de Datos: Actualización del Registro Nacional de Bases de Datos (RNBD) ante la SIC y revisión de cláusulas con terceros.	Constancia RNBD y Contratos actualizados	Jurídica / TI	Abril
Cultura: Campaña "ERAT Segura": Talleres de Ingeniería Social y Phishing.	Listas de asistencia y evaluaciones	Talento Humano / TI	Mayo / Agosto
Control de Acceso: Implementación de Doble Factor de Autenticación (MFA) en correos y VPN.	Reporte de implementación MFA	Líder TI	Junio
Gestión de Proveedores: Auditoría de seguridad a proveedores de software.	Informe de Auditoría a Terceros	Líder TI	Julio
Continuidad: Simulacro de recuperación de desastres (RTO/RPO) del sistema de facturación.	Informe de resultados del simulacro	Líder TI	Septiembre

FASE 3: VERIFICAR (octubre - noviembre)

Actividad	Entregable	Responsable	Fecha
Auditoría Interna al Sistema de Seguridad de la Información	Informe de Auditoría	Control Interno	Octubre
Medición de Indicadores de Seguridad (Incidentes reportados, tiempo de respuesta)	Tablero de Indicadores	Líder TI	Noviembre
Revisión por la Dirección (Gerencia)	Acta de Revisión	Gerencia General	Noviembre

FASE 4: ACTUAR (diciembre)

Actividad	Entregable	Responsable	Fecha

Implementación de Acciones Correctivas y de Mejora	Plan de Mejora	Líder TI	Diciembre
Formulación del Plan de Seguridad 2027	Borrador PSPI 2027	Líder TI	Diciembre

6.1 Indicadores de Gestión

Para evaluar la efectividad del plan, se medirán los siguientes indicadores:

Indicador	Descripción / Fórmula	Meta 2026	Frecuencia
Efectividad de Backups	(N° Backups Exitosos / N° Programados) * 100	100%	Mensual
Cobertura Capacitación	(N° funcionarios Capacitados / Total) * 100	> 90%	Semestral
Gestión de Incidentes	(Incidentes Resueltos / Incidentes Reportados) * 100	100%	Trimestral
Disponibilidad Servicios	(Horas operativas reales / Horas planificadas) * 100	> 99.5%	Mensual

7. GESTIÓN DE RIESGOS DE SEGURIDAD DIGITAL

La ERAT gestionará sus riesgos basándose en la metodología de la Función Pública y la guía de riesgos del MinTIC, enfocándose en:

1. **Riesgo:** Secuestro de información (Ransomware).
   - ***Control:*** Backups inmutables fuera de línea y restricción de puertos remotos.
2. **Riesgo:** Fuga de información de usuarios (Habeas Data).
   - ***Control:*** Cifrado de bases de datos y acuerdos de confidencialidad firmados.
3. **Riesgo:** Indisponibilidad del servicio de facturación.
   - ***Control:*** Servidor de contingencia y planta eléctrica en sede principal.

Para el detalle operativo de los controles, responsables y monitoreo, véase el anexo: Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información 2026, el cual hace parte integral de este documento.

7.1 Protocolo de Gestión y Respuesta a Incidentes

Con el objetivo de minimizar el impacto ante cualquier eventualidad que afecte la confidencialidad, integridad o disponibilidad de la información de la ERAT, se establece el siguiente flujo de respuesta, de obligatorio cumplimiento para todos los funcionarios y contratistas:

a) Detección y Reporte Cualquier funcionario que detecte una anomalía (ej. correos sospechosos, acceso no autorizado, pérdida de equipos, lentitud inusual en el sistema comercial, mensajes de extorsión/ransomware) debe reportarlo de inmediato.

- **Canal de Reporte:** Correo electrónico sistemas@aguasdeltequendama.com, o mesa de ayuda institucional.

- **Tiempo máximo de reporte:** Inmediato (dentro de los primeros 30 minutos tras la detección).

b) Clasificación y Priorización (Triaje) El Líder de TI recibirá el reporte y clasificará el incidente según su severidad:
   - **Nivel Bajo:** Incidentes aislados que no afectan la prestación del servicio (ej. un PC con virus, correo spam).
   - **Nivel Medio:** Afectación parcial de servicios internos o sospecha de acceso no autorizado sin confirmación de exfiltración de datos.
   - **Nivel Alto (Crítico):** Caída de sistemas misionales (Facturación/Recaudo), ataque de Ransomware confirmado, o fuga masiva de datos personales. Requiere escalamiento inmediato a Gerencia.

c) Contención y Erradicación El equipo de TI ejecutará las medidas técnicas para detener la amenaza:
   - Desconexión de la red de los equipos afectados (Aislamiento).
   - Bloqueo de usuarios o IPs sospechosas en el Firewall.
   - Ejecución de herramientas antimalware y cambio forzado de contraseñas administrativas.

d) Recuperación Una vez contenida la amenaza, se procederá a restaurar la operación normal:
   - Restauración de copias de seguridad (Backups) validadas previamente.
   - Reinstalación de sistemas operativos o aplicaciones comprometidas.
   - Verificación de funcionalidad antes de dar servicio a los usuarios.

e) Comunicación y Notificación Legal
   - **Interna:** El Líder de TI informará a las áreas afectadas sobre los tiempos estimados de solución.
   - **Externa (Legal):** En caso de violación de datos personales (Ley 1581 de 2012), la Oficina Jurídica y la Gerencia notificarán a la Superintendencia de Industria y Comercio (SIC) dentro de los 15 días hábiles siguientes a la detección, y a los titulares de los datos si existe riesgo para sus derechos.

f) Lecciones Aprendidas Tras el cierre del incidente, el Comité de Gestión y Desempeño analizará la causa raíz y actualizará la matriz de riesgos o los controles de seguridad para evitar la repetición del evento.

8. TÉRMINOS Y DEFINICIONES

Para efectos de la interpretación e implementación del presente Plan, se adoptan las siguientes definiciones:

- **Activo de Información:** Cualquier información (datos, documentos, bases de datos) o sistema que tenga valor para la ERAT y que requiera protección.
- **Amenaza:** Causa potencial de un incidente no deseado, que puede dañar un sistema o la organización (ej. un virus, un hacker, un terremoto).
- **Autenticación de Múltiples Factores (MFA):** Medida de seguridad que requiere más de un método de verificación para acceder a una cuenta (ej. contraseña + código al celular), dificultando el acceso a atacantes.

- **Backup (Copia de Seguridad):** Copia de datos originales que se realiza para restaurar la información en caso de pérdida, daño o ataque cibernético.
- **Confidencialidad:** Propiedad que garantiza que la información solo sea accesible o revelada a personas o sistemas autorizados.
- **Dato Personal:** Cualquier información vinculada o que pueda asociarse a una o varias personas naturales determinadas o determinables (ej. nombre, cédula, dirección del suscriptor).
- **Dato Sensible:** Aquel dato que afecta la intimidad del titular o cuyo uso indebido puede generar discriminación (ej. datos de salud, biometría/huella digital).
- **Disponibilidad:** Propiedad que garantiza que la información y los sistemas estén accesibles y utilizables por las personas autorizadas cuando lo requieran.
- **Firewall (Cortafuegos):** Dispositivo o software de seguridad de red que monitorea y filtra el tráfico entrante y saliente según las políticas de seguridad establecidas.
- **Habeas Data:** Derecho constitucional que tienen todas las personas a conocer, actualizar y rectificar las informaciones que se hayan recogido sobre ellas en bancos de datos.
- **Incidente de Seguridad:** Evento único o serie de eventos inesperados que tienen una probabilidad significativa de comprometer las operaciones del negocio o amenazar la seguridad de la información (ej. pérdida de una USB, infección por virus).
- **Integridad:** Propiedad que salvaguarda la exactitud y completitud de la información, asegurando que no haya sido modificada sin autorización.
- **Phishing (Suplantación de Identidad):** Técnica de engaño utilizada por ciberdelincuentes mediante correos electrónicos o mensajes falsos para robar información confidencial como contraseñas o datos bancarios.
- **Ransomware (Secuestro de Datos):** Tipo de software malicioso (malware) que cifra los archivos de la víctima y exige un pago (rescate) para devolver el acceso a la información.
- **SGSI (Sistema de Gestión de Seguridad de la Información):** Conjunto de políticas, procedimientos y controles que permiten a la ERAT gestionar los riesgos de su información de manera sistemática.
- **VPN (Red Privada Virtual):** Tecnología que permite extender una red local sobre una red pública (internet) de forma segura, utilizada por funcionarios para trabajar remotamente.
- **Vulnerabilidad:** Debilidad en un sistema, procedimiento o control que puede ser explotada por una amenaza para causar un daño.

BIBLIOGRAFIA

-Plan de seguridad y privacidad de la Información 2025 Empresa Regional Aguas del Tequendama S.A E.S.P. Tomado de: https://aguasdeltequendama.com/

NELSON IVAN GARCIA TARQUINO
Gerente