PLAN DE TRATAMIENTO DE RIESGOS 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 3
1. OBJETIVOS 3
1.1. Objetivo General 3
1.2. Objetivos Específicos 3
2. MARCO NORMATIVO Y REFERENCIAL 3
3. ROLES Y RESPONSABILIDADES EN LA GESTIÓN DEL RIESGO 3
4. MATRIZ DETALLADA DE TRATAMIENTO DE RIESGOS 2026 4
5. CRONOGRAMA DE IMPLEMENTACIÓN DE CONTROLES 5
6. MONITOREO E INDICADORES 6
7. GESTIÓN DE RIESGO RESIDUAL (INCIDENTES) 6
8. GLOSARIO DE TÉRMINOS 6
BIBLIOGRAFIA 6

INTRODUCCIÓN

La Empresa Regional Aguas del Tequendama S.A. E.S.P. (ERAT), reconociendo la información como un activo fundamental para la prestación de servicios públicos de acueducto, alcantarillado y aseo, establece el presente Plan de Tratamiento de Riesgos. Este documento se alinea con el Modelo Integrado de Planeación y Gestión (MIPG) y la Política de Gobierno Digital, definiendo las estrategias para modificar el nivel de riesgo de los activos de información mediante controles técnicos y administrativos.

1. OBJETIVOS

1.1. Objetivo General

Implementar controles efectivos durante el año 2026 que minimicen los riesgos de seguridad digital identificados, garantizando la confidencialidad, integridad y disponibilidad de la información de suscriptores, empleados y la infraestructura crítica de la ERAT.

1.2. Objetivos Específicos

- **Tratamiento de Amenazas:** Gestionar proactivamente riesgos como Ransomware y Phishing que afectan los sistemas de la Entidad.
- **Cumplimiento Legal:** Asegurar la conformidad con la Ley 1581 de 2012 (Protección de Datos) y la Resolución 02277 de 2025 del MinTIC.
- **Fortalecimiento Cultural:** Reducir el riesgo humano mediante la capacitación del 100% de los funcionarios y contratistas.

2. MARCO NORMATIVO Y REFERENCIAL

El tratamiento de riesgos se fundamenta en la siguiente normatividad vigente aplicable a la ERAT:

- **Constitución Política:** Arts. 15 (Habeas Data) y 209 (Función Administrativa).
- **Ley 1581 de 2012:** Protección de datos personales.
- **Decreto 1078 de 2015:** Decreto Único Reglamentario del Sector TIC.
- **Resolución MinTIC 02277 de 2025:** Actualización del Modelo de Seguridad y Privacidad (MSPI).
- **Norma ISO/IEC 27001:2022:** Estándar internacional para Sistemas de Gestión de Seguridad.

3. ROLES Y RESPONSABILIDADES EN LA GESTIÓN DEL RIESGO

Para garantizar la ejecución de los controles, se asignan las siguientes responsabilidades:

- **Comité Institucional de Gestión y Desempeño:** Aprueba el plan de tratamiento.
- **Líder de TI:** responsable del diseño, implementación y monitoreo de los controles técnicos descritos en este plan.

- **Líderes de Proceso:** Encargados de identificar activos en sus áreas y reportar incidentes que materialicen riesgos.
- **Gestión de Talento Humano:** Responsable de los controles relacionados con el personal (cláusulas de confidencialidad y capacitación).
- **Funcionarios y Contratistas:** Responsables de aplicar los controles en su día a día (ej. gestión de contraseñas).

4. MATRIZ DETALLADA DE TRATAMIENTO DE RIESGOS 2026

Basado en el diagnóstico de seguridad y la metodología de Función Pública, se definen las siguientes fichas de tratamiento para los riesgos priorizados:

RIESGO N.º 1: SECUESTRO DE DATOS (RANSOMWARE)

- **Descripción:** Ataque de software malicioso que cifra archivos exigiendo rescate.
- **Activos Críticos:** Software Comercial y Administrativo.
- **Estrategia de Tratamiento:** MITIGAR.
- **Controles (Acciones Concretas):**

    1. **Backups Inmutables:** Realización de copias fuera de línea para evitar cifrado simultáneo.
    2. **Restricción de Red:** Bloqueo de puertos remotos innecesarios.
    3. **Hacking Ético:** Pruebas de penetración para cerrar brechas técnicas.

- **Fecha Límite:** marzo 2026 (Hacking Ético) / Mensual (Backups).
- **Responsable:** Líder TI

RIESGO N.º 2: VIOLACIÓN DE DATOS PERSONALES (HABEAS DATA)

- **Descripción:** Fuga o acceso no autorizado a datos de suscriptores o empleados.
- **Activos Críticos:** Bases de datos de usuarios y nómina.
- **Estrategia de Tratamiento:** MITIGAR (Jurídicamente).
- **Controles (Acciones Concretas):**

    1. **Cifrado:** Encriptación de bases de datos sensibles.
    2. **Legal:** Actualización del Registro Nacional de Bases de Datos (RNBD) y revisión de cláusulas con terceros.
    3. **Auditoría a Terceros:** Revisión de seguridad a proveedores de software.

- **Fecha Límite:** abril 2026 (RNBD) / Julio 2026 (Auditoría Proveedores).

- **Responsable:** Jurídica / TI.

RIESGO N.º 3: INGENIERÍA SOCIAL Y PHISHING

- **Descripción:** Robo de credenciales mediante engaño, permitiendo acceso ilegítimo a la red.
- **Activos Críticos:** Correo electrónico, Accesos VPN.
- **Estrategia de Tratamiento:** MITIGAR (Preventivo).
- **Controles (Acciones Concretas):**

    1. **Autenticación Robusta:** Implementación de Doble Factor de Autenticación (MFA).
    2. **Cultura de Seguridad:** Campaña "ERAT Segura" con talleres de simulación de Phishing.

- **Fecha Límite:** junio 2026 (MFA) / Mayo-Agosto (Campaña).
- **Responsable:** Talento Humano / TI.

RIESGO N.º 4: INDISPONIBILIDAD DE SERVICIOS MISIONALES

- **Descripción:** Interrupción de la facturación o recaudo por fallas técnicas o eléctricas.
- **Activos Críticos:** Servidores de Sede Principal.
- **Estrategia de Tratamiento:** RECUPERAR.
- **Controles (Acciones Concretas):**

    1. **Infraestructura:** Adquisición de planta eléctrica en sede principal.
    2. **Redundancia:** Servidor de contingencia activo.
    3. **Continuidad:** Simulacro de recuperación de desastres.

- **Fecha Límite:** septiembre 2026 (Simulacro).
- **Responsable:** Líder de TI.

5. CRONOGRAMA DE IMPLEMENTACIÓN DE CONTROLES

La ejecución de los tratamientos seguirá el ciclo PHVA detallado en el plan de acción:

- **Marzo:** Ejecución de Hacking Ético en infraestructura crítica.
- **Abril:** Actualización RNBD ante la SIC.
- **Mayo:** Inicio campaña de cultura "ERAT Segura".
- **Junio:** Implementación total de MFA (Doble Factor).
- **Julio:** Auditoría de seguridad a proveedores.
- **Septiembre:** Simulacro de continuidad del negocio.

6. MONITOREO E INDICADORES

La eficacia del tratamiento de riesgos se medirá trimestralmente utilizando los siguientes indicadores:

Indicador	Fórmula	Meta 2026
Efectividad de Backups	(N° Backups Exitosos / N° Programados) * 100	100%
Gestión de Incidentes	(Incidentes Resueltos / Incidentes Reportados) * 100	100%
Disponibilidad Servicios	(Horas operativas reales / Horas planificadas) * 100	> 99.5%

7. GESTIÓN DE RIESGO RESIDUAL (INCIDENTES)

Si a pesar de los tratamientos el riesgo se materializa, se activa el **Protocolo de Gestión de Incidentes**:

1. **Reporte:** Inmediato a *sistemas@aguasdeltequendama.com*.
2. **Contención:** Aislamiento de equipos y bloqueo de usuarios.
3. **Recuperación:** Restauración desde backups validados.

8. GLOSARIO DE TÉRMINOS

Para la correcta interpretación del plan:

- **Activo de Información:** Información o sistema de valor para la ERAT.
- **Amenaza:** Causa potencial de un incidente no deseado.
- **MFA:** Autenticación de múltiples factores.
- **Ransomware:** Software malicioso que secuestra datos.
- **SGSI:** Sistema de Gestión de Seguridad de la Información.

BIBLIOGRAFIA

-Plan de tratamiento de riesgos 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