

**SISTEMA INTEGRADO DE GESTIÓN
RENTAN EICE**

**PROCESO
GESTIÓN DE TECNOLOGÍA DE LA
INFORMACIÓN**

**PROCEDIMIENTO
ESTRUCTURACIÓN Y SEGUIMIENTO A
PLANES**

**PLAN DE SEGURIDAD Y PRIVACIDAD
DE LA INFORMACIÓN**

**Período
2026**

Enero de 2026

TABLA DE CONTENIDO

1. INTRODUCCIÓN	3
2. DECLARACIÓN DE COMPROMISO	3
3. OBJETIVO GENERAL	3
3.1 OBJETIVOS ESPECÍFICOS	3
4. ALCANCE	4
5. MARCO LEGAL Y NORMATIVO	4
5.1 Normas Superiores y Leyes	4
5.2 Decretos y Reglamentos	4
5.3 POLÍTICAS INTERNAS:	5
6. PLAN ESTRATÉGICO INSTITUCIONAL PEI	5
6.1 ESTRATEGIA DE IMPLEMENTACIÓN (CICLO PHVA)	6
6.2 MATRIZ DE RIESGOS DE SEGURIDAD DE LA INFORMACIÓN	6
7. CRONOGRAMA PLAN DE ACCION PARA 2026	7
8. INDICADORES DEL PLAN DE ACCION	8
9. RECURSOS Y PRESUPUESTO	8
10. SEGUIMIENTO Y EVALUACIÓN	9
11. CONTROL DE CAMBIOS	10

1. INTRODUCCIÓN

La seguridad digital y la privacidad de la información no son opciones, son mandatos legales y estratégicos para cualquier entidad del Estado. El presente Plan de Seguridad y Privacidad de la Información (PSPI) es el instrumento táctico mediante el cual RENTAN operacionaliza su Modelo de Seguridad y Privacidad de la Información (MSPI), en cumplimiento de la Política de Gobierno Digital.

Este documento define la hoja de ruta, los proyectos, los recursos y los controles específicos que la entidad implementará durante la vigencia 2026 para proteger sus activos de información, garantizar la continuidad del servicio y asegurar el derecho fundamental de Habeas Data de sus grupos de valor.

2. DECLARACIÓN DE COMPROMISO

RENTING DE ANTIOQUIA, RENTAN - EICE, reconoce la información como un activo estratégico fundamental para el cumplimiento de su misión. A través de este Plan de Seguridad y Privacidad de la Información (PSPI), la Alta Dirección se compromete a operacionalizar el Modelo de Seguridad y Privacidad de la Información (MSPI) del MinTIC, garantizando la Confidencialidad, Integridad y Disponibilidad de los datos.

Este plan actúa como el brazo táctico del Plan Estratégico de TI (PETI 2026), ejecutando los controles necesarios para proteger a la entidad frente a ciberamenazas, asegurar el derecho de Habeas Data de los ciudadanos y dar continuidad a la operación bajo el modelo de "Orquestador de Servicios".

3. OBJETIVO GENERAL

Implementar, mantener y mejorar el Sistema de Gestión de Seguridad de la Información (SGSI) y Sistema de Gestión de Privacidad de la Información (SGPI) de RENTAN para la vigencia 2026, ejecutando los controles definidos en la matriz de riesgos de seguridad de la información y asegurando el cierre de las brechas de seguridad identificadas, en estricta alineación con los objetivos estratégicos del PEI aprobado y el cumplimiento de la normatividad vigente.

3.1 OBJETIVOS ESPECÍFICOS

- Formalizar la adopción del marco de políticas de seguridad y garantizar su cumplimiento operativo a través de la ejecución y monitoreo mensual de la Matriz de Seguimiento.

- Mitigar los riesgos de seguridad digital priorizados en el mapa institucional, con especial énfasis en la protección de datos personales (Habeas Data) y la resiliencia de la infraestructura crítica.
- Ejecutar el plan de capacitación y sensibilización transversal para fortalecer las competencias digitales de los funcionarios y reducir los riesgos asociados al factor humano (Ingeniería social/Phishing).
- Garantizar la seguridad tecnológica en la prestación de servicios mediante la gestión efectiva de los Acuerdos de Nivel de Servicio (ANS) de seguridad en el contrato marco con TIGO-UNE.

4. ALCANCE

Este plan aplica a todos los procesos del mapa institucional de RENTAN. Cubre la totalidad de los activos de información (físicos y digitales), la infraestructura tecnológica y vincula a todos los servidores públicos, contratistas y proveedores.

Inicia con el diagnóstico de seguridad y finaliza con el seguimiento a los controles de los riesgos de la Matriz de Riesgos de Seguridad de la Información evitando su materialización.

5. MARCO LEGAL Y NORMATIVO

El presente plan se fundamenta en un marco jurídico exhaustivo, ordenado cronológicamente, que obliga a RENTAN a gestionar la seguridad y privacidad de la información bajo estándares estrictos:

5.1 Normas Superiores y Leyes

- Constitución Política de Colombia (1991): Artículos 15 (Derecho a la intimidad y Habeas Data) y 209 (Principios de la función administrativa).
- Ley 23 de 1982: Sobre derechos de autor.
- Ley 594 de 2000: Ley General de Archivos.
- Ley 1273 de 2009: Delitos Informáticos.
- Ley 1581 de 2012: Ley General de Protección de Datos Personales.
- Ley 1712 de 2014: Ley de Transparencia.

5.2 Decretos y Reglamentos

- Decreto 1377 de 2013: Reglamentario de Protección de Datos.

- Decreto 1078 de 2015: Decreto Único Reglamentario del Sector TIC (DUR-TIC).
- Decreto 767 de 2022: Lineamientos generales de la Política de Gobierno Digital.

5.3 POLÍTICAS INTERNAS:

- Política de Seguridad y Privacidad de la Información: base rectora de este plan que incluye los principios de seguridad por diseño y continuidad del negocio.
- Política de Gobierno Digital.
- Política de Uso de Recursos Tecnológicos.

6. PLAN ESTRATÉGICO INSTITUCIONAL PEI

A continuación, se presenta la consolidación que vincula los Programas del PEI con los Proyectos del PETI:

LÍNEA 4 DEL PEI TRANSFORMACIÓN DIGITAL	NOMBRE DEL INDICADOR	RESULTADO CLAVE
Programa 4.1 Estrategia integral para la seguridad y privacidad de la información.	Política Seguridad y Privacidad de la Información documentada, aprobada e implementada.	Capacitar al 100% del personal sobre la Política Seguridad y Privacidad de la Información
Programa 4.2 Modernización e innovación tecnológica para la eficiencia.	Numero de soluciones de automatización implementada (PETI).	Capacitar al personal en el uso de los nuevos sistemas de automatización cada trimestre después de haberse implementados las automatizaciones.
Programa 4.4 Cultura para la transformación digital.	Capacitaciones dadas al personal en temas de tecnología e Innovación.	Desarrollar un programa de capacitación en competencias digitales y tecnologías emergentes en un plazo de 4 semestres. Implementar el programa de capacitación, alcanzando al menos el 50% del personal capacitado en los primeros 4 semestres del periodo de gobierno.

6.1 ESTRATEGIA DE IMPLEMENTACIÓN (CICLO PHVA)

La ejecución del PSPI sigue el ciclo de mejora continua:

PLANEAR

- Hacer un plan de trabajo para la implementación del plan de seguridad y privacidad de la información.
- Articular el plan de trabajo con el PEI.

HACER

- Diligenciamiento de la Matriz de Riesgos de Seguridad de la Información, con la periodicidad establecida.
- Socialización de la política de uso de recursos tecnológicos, con énfasis en el uso responsable de la seguridad de la información, blindándose con contraseñas fuertemente tipadas.

VERIFICAR

- Realización de una auditoría al proceso de Gestión de Tecnología de la Información.
- Seguimiento a los indicadores del proceso de Gestión de Tecnología de la Información.
- Verificar el diligenciamiento oportuno Matriz de Riesgos de Seguridad de la Información.

ACTUAR

- Plan de Mejoramiento: Acciones correctivas derivadas de los hallazgos.

6.2 MATRIZ DE RIESGOS DE SEGURIDAD DE LA INFORMACIÓN

Este plan lleva integrada la matriz de riesgos de seguridad de la información, por medio de la cual se gestiona la seguridad de la información tal como se solicita en el PEI. Esta matriz consolida los riesgos priorizados y el estado de avance de sus controles, sirviendo como instrumento principal de monitoreo del proceso de Gestión de Tecnología de la Información.

A continuación, se relaciona los controles establecidos en la matriz:

Controles:**1. Capacitación y concienciación:**

- Programa de capacitación integral.
- Identificación y reporte de incidentes de seguridad.
- Realización de simulacros.

2. Procedimiento Estándar de operación (P.E.O)

- Transferencia de información.
- Gestión de medios removibles.
- Acceso a redes.

3. Herramientas y tecnología

- Sistemas de detección de intrusiones.
- Software de seguridad.
- Sistemas de respaldo.

4. Reportes y seguimiento:

- Canales de reporte.
- Análisis de incidentes.
- Indicadores claves de desempeño.
- Evaluación y mejora continua.
- Auditorías internas.
- Revisión de los controles.

7. CRONOGRAMA PLAN DE ACCION PARA 2026

La estrategia se materializa a través de proyectos, algunos de los cuales dan continuidad a las actividades iniciadas en 2025 y otros son nuevos retos para 2026:

PROGRAMA	INDICADOR	VIGENCIA 2026				RESPONSABLE
		T1	T2	T3	T4	
Programa 4.1 Estrategia integral para la seguridad y privacidad de la información.	Capacitar al 100% del personal Política Seguridad y Privacidad de la Información		X			Gestión de Tecnología de la Información
Programa 4.2 Modernización e innovación tecnológica para la eficiencia.	Capacitar al personal en el uso de los nuevos sistemas de automatización cada trimestre después de haberse implementados las automatizaciones.			X		Gestión de Tecnología de la Información
Programa 4.4 Cultura para la transformación digital.	Desarrollar un programa de capacitación en competencias digitales y tecnologías emergentes en un plazo de 4 semestres. Implementar el programa de capacitación, alcanzando al menos el 50% del personal capacitado en los primeros 4 semestres del periodo de gobierno.			X	X	Gestión de Tecnología de la Información

8. INDICADORES DEL PLAN DE ACCION

INDICADOR	FÓRMULA	META 2026	FRECUENCIA
Cobertura de Capacitación	$(\text{Personal Capacitado} / \text{Total del personal}) * 100$	100%	Trimestral

9. RECURSOS Y PRESUPUESTO

La ejecución de este plan cuenta con viabilidad financiera garantizada a través de los recursos asignados en el PETI para la vigencia 2026, específicamente:

RUBRO	CONCEPTO	ASIGNACIÓN	DESTINACIÓN ESPECÍFICA PARA EL PSPÍ
21201010050203010101	Paquetes de software VA	\$430.393.809	Soluciones digitales con su implementación en todas las fases de los proyectos de tecnología para el fortalecimiento y avance de la transformación digital de Rentan Antioquia.
21202020080901	Servicios de Internet y Conexión VA	\$293.518.976	

RUBRO	CONCEPTO	ASIGNACIÓN	DESTINACIÓN ESPECÍFICA PARA EL PSPI
TOTAL		\$723.912.785	
21202020080901	Servicios de Internet y Conexión VA	\$120.376.439	Implementación del proceso de transición del protocolo IPv4 hacia el protocolo IPv6 para Renting de Antioquia RENTAN EICE de conformidad con los lineamientos establecidos por la Resolución 2710 del Ministerio de Tecnologías de la Información y las Comunicaciones modificada por la Resolución 01126 del mismo Ministerio.
2120101003030201	Maquinaria de informática y sus partes, piezas y accesorios VA	\$289.280.987	Adquisición de equipos tecnológicos para el correcto funcionamiento de las labores que desempeñan las diferentes dependencias de la empresa de Renting de Antioquia RENTAN, EICE.
TOTAL, PRESUPUESTO VIGENCIA 2026		\$1.133.570.211	

Nota: Este presupuesto puede variar de acuerdo con la necesidad y dinámica de la entidad.

10. SEGUIMIENTO Y EVALUACIÓN

El seguimiento al Plan de Seguridad y Privacidad de la Información se realizará de la siguiente manera:

- Trimestral: Revisión de la Matriz de Riesgos de Seguridad de la Información.
- Trimestral: Medición de indicadores del Plan de Seguridad y Privacidad de la Información

11. CONTROL DE CAMBIOS

No. de Versión	Fecha de Versión	Autor	Revisado por	Aprobado por	Descripción del cambio
1	30/01/2025	Dirección de TI y Seguridad de la Información.	Dirección de Planeación Institucional	Comité Institucional de Gestión y Desempeño	Creación del documento
2	28/01/2026	Dirección de TI y Seguridad de la Información.	Dirección de Planeación Institucional	Comité Institucional de Gestión y Desempeño	Actualización del Plan en cumplimiento al Decreto 612 de 2018