SISTEMA INTEGRADO DE GESTIÓN
RENTING DE ANTIOQUIA,
RENTAN-EICE

PROCESO
GESTIÓN DE TECNOLOGÍAS DE LA INFORMACIÓN

PROCEDIMIENTO SEGURIDAD Y CONTROL DE LA INFORMACIÓN

POLÍTICA DE GESTIÓN DE RIESGOS DE SEGURIDAD DIGITAL

FEBRERO 2026

TABLA DE CONTENIDO

1. DECLARACIÓN DE COMPROMISO

La Empresa RENTING DE ANTIOQUIA, RENTAN - EICE, a través de su Alta Dirección, se compromete a adoptar un enfoque preventivo y sistemático frente a las amenazas del entorno digital. Reconocemos que la gestión de riesgos no es solo un requisito normativo, sino una herramienta estratégica fundamental para asegurar la continuidad del negocio y la protección de los activos de información.

Nos comprometemos a identificar, analizar, evaluar y tratar los riesgos de seguridad digital de manera periódica, asignando los recursos necesarios para mantenerlos en niveles aceptables y promoviendo una cultura organizacional donde la gestión del riesgo sea responsabilidad de todos.

Es obligatorio para entidades públicas en Colombia, ya que normativas como la política de gobierno digital y resoluciones del Mintic exigen medidas para proteger la información, mitigar riesgos y garantizar la confianza en los servicios digitales, siendo su incumplimiento sujeto a sanciones.

2. POLÍTICA

RENTING DE ANTIOQUIA, RENTAN - EICE establece como directriz institucional la gestión de los riesgos de seguridad digital, integrando esta práctica en todos sus procesos estratégicos, misionales y de apoyo. La entidad adoptará metodologías estandarizadas para anticiparse a las amenazas cibernéticas, asegurando que cada decisión tecnológica y operativa considere los riesgos asociados a la confidencialidad, integridad y disponibilidad de la información.

Esta política formaliza la obligación de tratar los riesgos que superen los niveles de aceptación definidos, implementando controles efectivos que protejan la infraestructura crítica, los datos personales y la reputación institucional frente a un entorno digital cambiante.

3. OBJETIVO PRINCIPAL

Establecer la metodología y el marco de gobernanza para la identificación, análisis, evaluación, tratamiento y monitoreo continuo de los riesgos de seguridad digital que puedan afectar la confidencialidad, integridad y disponibilidad de los activos de información de rentan, en alineación con los objetivos estratégicos de la entidad y el cumplimiento normativo.

4. ALCANCE

Esta política aplica a todos los activos de información, sistemas, infraestructura tecnológica y procesos de la entidad. Cubre tanto los riesgos internos como los externos (ciberataques, fugas de información, fallos tecnológicos) y es aplicable a todos los empleados, contratistas y terceros conectados a la red de RENTAN.

Nota Conceptual: Esta política se entiende como un componente operativo y disciplinar dentro del Modelo de Seguridad y Privacidad de la Información (MSPI). Mientras el MSPI es el marco general estratégico, la Política de Gestión de Riesgos es la disciplina operativa enfocada en la mitigación de peligros específicos.

5. MARCO NORMATIVO

La gestión de riesgos de seguridad digital en RENTAN debe cumplir con los siguientes marcos normativos y estándares:

- Norma ISO/IEC 27001: Requisitos para el Sistema de Gestión de Seguridad de la Información.
- Norma ISO/IEC 27005: Directrices para la Gestión de Riesgos de Seguridad de la Información.
- Modelo MIPG: Guía de Administración del Riesgo del Departamento Administrativo de la Función Pública (DAFP).
- Ley 1581 de 2012: En lo referente a riesgos sobre datos personales.

6. PRINCIPIOS Y VALORES

La gestión de riesgos en RENTAN se guía por los siguientes principios fundamentales:

- Prevención (Enfoque Proactivo): Priorizamos la identificación temprana de amenazas y vulnerabilidades antes de que se materialicen en incidentes.
- Cultura de Riesgo: Fomentamos el reporte transparente de eventos y vulnerabilidades sin temor a represalias.
- Mejora Continua: Evaluamos constantemente la efectividad de nuestros controles para adaptarnos a nuevas amenazas del entorno.
- Responsabilidad Compartida: Cada líder de proceso es dueño de los riesgos de su área y responsable de gestionar sus controles, con el apoyo técnico de TI.
- Toma de Decisiones Basada en Riesgo: Las inversiones en seguridad se priorizan según el nivel de riesgo identificado (Alto, Medio, Bajo).

7. RESPONSABILIDADES Y ROLES

- Comité Institucional de Gestión y Desempeño: Responsable de aprobar esta política, definir el "Apetito de Riesgo" de la entidad y revisar los riesgos críticos (Nivel Extremo/Alto).
- Dirección de TI (Líder del Proceso): Responsable de liderar la metodología, facilitar los talleres de riesgos, consolidar la Matriz de Riesgos y monitorear la efectividad de los planes de tratamiento.
- Líderes de Proceso: Responsables de identificar los activos críticos de su área, participar en la valoración de los riesgos y ejecutar los controles asignados.
- Direccionamiento Estratégico: Responsable de alinear la gestión de riesgos digitales con la gestión de riesgos institucionales y el mapa estratégico.
- Oficina de Control Interno: Responsable de auditar el cumplimiento de esta política y verificar la efectividad de la gestión de riesgos de manera independiente.

8. REQUISITOS Y CUMPLIMIENTO

El incumplimiento de los controles de riesgo críticos definidos en esta política y sus instrumentos asociados podrá acarrear las sanciones disciplinarias o contractuales correspondientes, conforme al Reglamento Interno de Trabajo y el Código Sustantivo del Trabajo.

9. PROCEDIMIENTOS Y DIRECTRICES

Para la operatividad de esta política, se aplicarán los siguientes instrumentos detallados:

- Metodología de Gestión de Riesgos: Se utilizará la metodología institucional aprobada para identificar, analizar y evaluar riesgos.
- Matriz de Riesgos de Seguridad Digital: Documento vivo donde se registran y valoran todos los riesgos identificados.
- Plan de Tratamiento de Riesgos de Seguridad (PTRSPI): Plan de acción para mitigar los riesgos que superen el nivel aceptable.
- Niveles de Aceptación: Se tratarán obligatoriamente todos los riesgos clasificados como "Extremos" o "Altos" según el mapa de calor institucional.

10. COMUNICACIÓN Y REVISIÓN

Esta política será comunicada a todas las partes interesadas pertinentes y estará disponible de manera digital.

La política se revisará anualmente o cuando existan cambios significativos en la infraestructura tecnológica o el entorno de amenazas, para garantizar su relevancia y eficacia.

11. CONTROL DE CAMBIOS

N°. de Versión	Fecha de Versión	Autor	Revisado por	Aprobado por	Descripción del cambio
1	25/02/2026	Directora de TI	Dirección de Planeación Institucional	Comité Institucional de Gestión y Desempeño	Creación del documento