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 SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

Diciembre 2025

TABLA DE CONTENIDO

1. DECLARACIÓN DE COMPROMISO

Renting de Antioquia EICE Rentan, se compromete a liderar, implementar, mantener y mejorar continuamente el Sistema de Gestión de Seguridad y Privacidad de la Información.

Nuestro compromiso es proteger la información de la entidad, contra amenazas internas o externas, gestionando los riesgos para asegurar su Confidencialidad, Integridad y Disponibilidad.

Para este fin, la Dirección de TI y Seguridad de la Información definirá los roles, responsabilidades y controles necesarios, promoviendo una cultura de seguridad y privacidad en todos los niveles de la organización, asegurando el cumplimiento de los objetivos estratégicos, los requisitos legales (Ley 1581 de 2012) y los estándares contractuales aplicables.

Es obligatorio tener la política, para dar cumplimiento a la Ley 1581 de 2012, adicional es un componente fundamental de la norma ISO 27001, el Modelo de Seguridad y privacidad de la información (MSPI) del Gobierno Nacional, incluyendo el compromiso claro de confidencialidad, integridad y disponibilidad de la información y una necesidad para protegerse contra riesgos cibernéticos y cumplir con las expectativas de los usuarios, con consecuencias legales y administrativas por su incumplimiento.

2. POLÍTICA

RENTING DE ANTIOQUIA, RENTAN - EICE, entendemos la información como un activo estratégico vital para el cumplimiento de nuestra misión y la generación de valor público; por ello, asume el compromiso inquebrantable de liderar y proveer los recursos necesarios para la política de Seguridad y Privacidad de la Información. A través de esta política, establecemos un marco de actuación obligatorio que garantiza la confidencialidad, integridad y disponibilidad de nuestros datos, gestionando de manera preventiva los riesgos digitales y asegurando el estricto cumplimiento de la normativa legal vigente, con el fin de proteger la confianza de nuestros grupos de interés y la continuidad de nuestras operaciones.

3. OBJETIVO PRINCIPAL

Establecer el marco de referencia y los principios rectores para proteger los activos de información de RENTAN, preservando su Confidencialidad, Integridad y Disponibilidad (CID), mediante la implementación y operación de un Sistema de Gestión de Seguridad y Privacidad de la Información (SGSI/SGPI).

4. ALCANCE

Esta Política aplica a todos los funcionarios, contratistas, proveedores y terceros que tengan acceso, procesen, almacenen o administren información propiedad de RENTAN o bajo su custodia.

El alcance cubre la información digital y los activos de información que la soportan (hardware, software, redes, infraestructura) en todas las sedes y procesos de la entidad.

5. MARCO NORMATIVO

Esta política se desarrolla en cumplimiento y concordancia con el siguiente marco normativo (entre otros):

- Constitución Política de Colombia (Art. 15, 20).
- Ley Estatutaria 1581 de 2012 (Protección de Datos Personales).
- Ley 1273 de 2009 (Delitos Informáticos - Protección de la información y de los datos).
- Ley 1712 de 2014 (Transparencia y Acceso a la Información Pública).
- Decreto 1078 de 2015 (Decreto Único del Sector TIC).
- Modelo de Seguridad y Privacidad de la Información (MSPI) y Política de Gobierno Digital (MinTIC).
- Política de Gobierno Digital (Decreto 1008 de 2018**):** Lineamientos para entidades públicas
- Estándares Internacionales**:** Referencia a ISO 27001 (Sistema de Gestión de Seguridad de la Información - SGSI)

6. PRINCIPIOS Y VALORES

RENTAN adopta los siguientes principios como pilares de su gestión de seguridad y privacidad:

Confidencialidad: La información solo debe ser accesible por personal autorizado por cada líder de proceso.

Integridad: La información debe ser exacta, completa y protegida contra modificaciones no autorizadas.

Disponibilidad: La información y los sistemas que la procesan deben estar disponibles para los usuarios autorizados cuando así lo requieran.

Responsabilidad Compartida: La seguridad y la privacidad son una responsabilidad de todos los colaboradores de RENTAN, NO solo de la Dirección de TI y Seguridad de la Información.

Gestión Basada en Riesgos: Las decisiones y controles de seguridad se basarán en una valoración de los riesgos para los activos de información.

Privilegio Mínimo: Los usuarios solo tendrán el nivel de acceso estrictamente necesario para cumplir sus funciones.

Seguridad por Defecto y en Profundidad: La seguridad debe estar integrada en todos los procesos, sistemas y capas de la arquitectura tecnológica desde su diseño.

Mejora Continua: El SGSI/SGPI será revisado y mejorado permanentemente para adaptarse a nuevos riesgos y desafíos.

7. RESPONSABILIDADES Y ROLES

Alta Dirección: asignar recursos y recibir informes de desempeño del SGSI/SGPI.

Comité Institucional de Gestión y Desempeño: Liderar, aprobar la política Actuar como órgano supervisor. Revisar y aprobar la metodología de riesgos y los planes de tratamiento del riesgo.

Dirección de TI y Seguridad de la Información: Lidera la implementación, operación y mantenimiento del SGSI, gestionar incidentes y coordinar la implementación de controles.

Lideres de Areas: Son los responsables de la información generada en sus procesos, además deben clasificar sus activos y definir los criterios de acceso, mismos que serán reportados a la dirección de TI, vía correo electrónico.

Todos los funcionarios y Contratistas: Conocer y cumplir esta política y todos los procedimientos de seguridad y privacidad de la información y reportar oportunamente cualquier incidente o debilidad de seguridad detectada.

8. REQUISITOS Y CUMPLIMIENTO

Gestión de Riesgos y Mejora Continua

RENTAN implementará una metodología de gestión de riesgos de seguridad y privacidad, alineada con la gestión de riesgos institucional. El ciclo de vida de los riesgos

(Identificación, Análisis, Evaluación y Tratamiento) será la base fundamental para la selección e implementación de los controles de seguridad.

El SGSI/SGPI se someterá a un ciclo de mejora continua bajo el modelo PHVA (Planear, Hacer, Verificar, Actuar). Esto se realizará mediante auditorías internas y revisiones por la Dirección de TI y Seguridad de la Información. Para asegurar el cumplimiento y la evolución del sistema, se aplicarán acciones correctivas frente a hallazgos y se gestionarán oportunidades de mejora, entendiendo que la gestión preventiva estará cubierta por intrínsecamente por el Plan de Tratamientos de Riesgos de Seguridad y Privacidad de la Información.

9. PROCEDIMIENTOS Y DIRECTRICES

Esta Política General establece el marco que se desarrolla y ejecuta a través de los siguientes documentos, los cuales son de obligatorio cumplimiento:

1. **Políticas Específicas:**

   i. POLÍTICA DE SEGURIDAD DIGITAL: Se mantiene como la política específica que rige el uso de activos digitales y la ciberseguridad.

   ii. POLÍTICA DE TRATAMIENTO DE DATOS PERSONALES: Se mantiene como la política específica que da cumplimiento legal al dominio de privacidad y habeas data, la cual esta a cargo de la Secretaria General, quién deberá garantizar la gestión de datos personales (habeas data).

2. **Plan de Implementación**

   PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN (PSPI): Se mantiene como el documento táctico que define las acciones, proyectos y cronogramas para implementar los controles (el "Cómo" y el "Cuándo"). Este plan se fundamenta y ejecuta utilizando las metodologías y herramientas descritas en el Numeral 3 (Metodologías y Herramientas de Seguridad y Privacidad) presentado a continuación.

3. **Metodologías y Herramientas de Seguridad y Privacidad**

   Para garantizar la efectividad del sistema, RENTAN dispone de los siguientes componentes transversales:

   - **Identificación y Clasificación de Activos:** Herramienta fundamental para saber qué proteger. Se cuenta con inventarios actualizados donde cada activo (información, software, hardware) está clasificado por su criticidad (Confidencial,

Interno, Público), permitiendo asignar controles de seguridad proporcionales a su valor.

- **Gestión de Riesgos de Seguridad Digital:** Metodología proactiva para identificar, evaluar y tratar amenazas (como phishing, malware, fugas de información). Se instrumentaliza a través de la Política de Seguridad Digital y su respectiva matriz de riesgos, la cual determina los controles a implementar.

- **Seguridad por Diseño:** Directriz metodológica que asegura que los controles de seguridad y privacidad se integren desde la fase de concepción y diseño de cualquier proyecto, adquisición de software o desarrollo, garantizando sistemas seguros. Incluyendo la seguridad perimetral la cual amplia el cierre seguro de la actividad.

- **Continuidad del Negocio (BCP):** Conjunto de herramientas y planes de contingencia (incluyendo políticas de copias de seguridad/Backups y recuperación ante desastres) diseñados para recuperar la operación crítica de la entidad en el menor tiempo posible tras un incidente grave.

- **Uso de Recursos Tecnológicos:** Es la actividad que regula el comportamiento de los usuarios frente a las herramientas corporativas (Correo, Internet, Equipos, mantenimiento de equipos tecnológicos), constituyendo un control administrativo clave para prevenir fugas de información y uso indebido. Adicional a lo anterior, también incluye la adquisición de recursos tecnológicos.

- **Gestión de Incidentes:** Actividad estandarizada para la detección, reporte, contención y erradicación de eventos de seguridad, garantizando una respuesta oportuna y la minimización del impacto operativo y legal ante ciberataques. También se incluye el control de accesos y contraseñas.

4. Plan de Implementación:

PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN: Se mantiene como el documento táctico que define las acciones, proyectos y cronogramas para implementar los controles (el "Cómo" y el "Cuándo"). Pero como… metodología, herramienta, que va a tener en cuenta, si se responde con el siguiente numeral 3, colocar acá que ya se relacionará y ampliar cada componente del 3, una explicación amplia y como se dan las herramientas para la seguridad y privacidad

10. COMUNICACIÓN Y REVISIÓN

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

11. CONTROL DE CAMBIOS

No. de Versión	Fecha de Versión	Autor	Revisado por	Aprobado por	Descripción del cambio
1	30/12/2025	Directora de TI	Directora de Planeación Institucional	Comité Institucional de Gestión y Desempeño	Creación del documento