SISTEMA INTEGRADO DE GESTIÓN

RENTAN EICE

PROCESO

GESTIÓN DE TECNOLOGÍAS DE LA INFORMACIÓN

PROCEDIMIENTO

SEGURIDAD Y CONTROL DE LA INFORMACIÓN

POLÍTICA DE USO DE RECURSOS TECNOLOGICOS

Diciembre 2025

Tabla de contenido

1. DECLARACIÓN DE COMPROMISO

La Empresa **RENTING DE ANTIOQUIA, RENTAN - EICE**, reconoce que los recursos tecnológicos y de información son herramientas fundamentales para el cumplimiento de nuestra misión. La Alta Dirección se compromete a facilitar estos recursos a sus colaboradores, esperando a cambio un uso responsable, ético, legal y productivo de los mismos.

Nos comprometemos a monitorear y proteger estos activos para evitar su uso indebido, garantizando así la eficiencia operativa, la seguridad de la información y la reputación de la entidad.

2. POLÍTICA

RENTING DE ANTIOQUIA, RENTAN - EICE, reconocemos que la infraestructura tecnológica es el motor que habilita nuestra capacidad de servicio y gestión pública; por ello, asume el compromiso ineludible de proveer herramientas digitales eficientes y seguras, estableciendo mediante la presente política un marco de actuación que exige un uso ético, responsable y estrictamente profesional de dichos activos. Nos comprometemos a salvaguardar la integridad, disponibilidad y confidencialidad de la información institucional, promoviendo una cultura de autocontrol donde cada colaborador comprenda que el cuidado de los recursos tecnológicos (hardware, software y conectividad) es fundamental para minimizar riesgos, evitar sanciones legales y garantizar la sostenibilidad operativa de la entidad.

3. OBJETIVO PRINCIPAL

Establecer las directrices y normas de comportamiento para el uso adecuado de los recursos informáticos y de comunicaciones de RENTAN (hardware, software, internet, correo electrónico y redes), con el fin de protegerlos contra daños, accesos no autorizados y fugas de información.

4. ALCANCE

Esta política aplica a todos los empleados, contratistas, proveedores y terceros que utilicen los equipos, redes o sistemas de información de propiedad de RENTAN, o que se conecten a ellos, independientemente de su ubicación (presencial o trabajo en casa).

Inicia con la asignación de los equipos a empleados, contratistas proveedores y terceros de RENTAN, con uso específico para el desarrollo de las labores inherentes a la misión de la entidad y va hasta la terminación del vínculo de cada persona.

5. PRINCIPIOS Y VALORES

El uso de los recursos tecnológicos en RENTAN se rige por:

- **Uso Profesional:** Los recursos se suministran para fines laborales. El uso personal debe ser ocasional, moderado y no interferir con las funciones.
- **Legalidad:** No se tolerará el uso de recursos para actividades ilegales, descarga de software pirata o violación de derechos de autor.
- Uso responsable de IA: El uso de herramientas de inteligencia artificial (IA) debe ser transparente y ético. se debe evitar compartir datos confidenciales, secretos industriales o datos sensibles de la entidad en plataformas públicas de IA (como chatgpt, gemini, etc.) para prevenir fugas de información.
- **Privacidad Limitada:** RENTAN se reserva el derecho de monitorear y auditar el uso de sus activos tecnológicos por razones de seguridad y control.
- **Cuidado y Custodia:** Todo usuario es responsable de la integridad física y lógica del equipo asignado a su cargo.
- **Seguridad:** Ningún usuario debe inhabilitar o eludir los controles de seguridad instalados (antivirus, firewalls, bloqueos).

6. MARCO LEGAL Y NORMATIVO

El uso de los recursos tecnológicos en RENTAN se fundamenta en la siguiente normativa, la cual exige a los "sujetos obligados" adoptar estas medidas:

- **Decreto 767 de 2022:** Lineamientos generales de la Política de Gobierno Digital.
- **Ley 1273 de 2009:** Por medio de la cual se modifica el Código Penal (Delitos Informáticos).
- **Ley 23 de 1982:** Sobre derechos de autor (Software y Propiedad Intelectual).
- **Directrices MinTIC:** Sobre seguridad y privacidad de la información.

7. RESPONSABILIDADES Y ROLES

- **Proceso Gestión de TI :** Responsable de administrar los activos, configurar los controles de acceso, monitorear el uso de la red y reportar incidentes de mal uso a los lideres de proceso, buscando se subsane la situación reportada.
- **Proceso Gestión del Talento Humano / Gestión Jurídica:** Apoyar la aplicación de

sanciones disciplinarias en caso de violaciones a esta política.

- **Líderes de Procesos:** Velar por que su equipo de trabajo haga un uso productivo de las herramientas asignadas.
- **Usuarios Finales (Empleados/Contratistas):** responsables directos de cumplir estas normas, cuidar sus claves de acceso y reportar cualquier pérdida o anomalía en sus equipos.

8. REQUISITOS Y CUMPLIMIENTO

Para mayor claridad, se definen las expectativas de comportamiento (Deberes) y las acciones no permitidas (Prohibiciones), incluyendo los lineamientos específicos sobre **Hardware, Seguridad y Dispositivos Externos**:

1. Expectativas (Deberes del Usuario)

- **Gestión de Cuentas:** Mantener la confidencialidad de sus contraseñas. Está prohibido compartir credenciales de acceso. Cada funcionario es responsable de las acciones realizadas bajo su identidad digital.
- **Hardware (Cuidado de Activos):** El usuario es responsable de la custodia y buen trato del hardware asignado (computador, pantalla, periféricos). Se debe evitar el consumo de alimentos o bebidas directamente sobre los equipos y reportar inmediatamente cualquier daño físico o fallo de funcionamiento.
- **Seguridad:** Es deber de todo usuario mantener activos los controles de seguridad instalados por TI (Antivirus, Agentes de monitoreo). El usuario debe bloquear la sesión de su equipo (Win+L) siempre que se ausente de su puesto de trabajo para prevenir accesos no autorizados.
- **Cuidado Físico y Movilidad:** Los usuarios con equipos portátiles deben extremar medidas de seguridad física fuera de las instalaciones, evitando dejarlos en vehículos o lugares expuestos al robo.

2. Prohibiciones Expresas

- **Dispositivos Externos:** Se prohíbe la conexión de dispositivos de almacenamiento masivo (Memorias USB, Discos Duros Externos) personales o de origen desconocido a la red corporativa sin previa autorización o escaneo de seguridad por parte de TI, para mitigar el riesgo de infección por malware o exfiltración de datos.
- **Modificación de Hardware:** Está terminantemente prohibido abrir, desarmar, cambiar componentes internos o intentar reparar por cuenta propia el hardware suministrado por la entidad.

- **Navegación y Contenidos:** Se prohíbe el acceso a sitios de contenido pornográfico, apuestas, juegos de azar, piratería o cualquier otro que atente contra la moral, las leyes y la reputación de RENTAN.
- **Correo Electrónico:** No se debe usar el correo institucional para cadenas masivas, spam, acoso, proselitismo político o suscripciones a sitios personales no laborales.
- **Software Ilegal:** Está estrictamente prohibida la descarga e instalación de software pirata, cracks, keygens o programas no autorizados por TI.

El incumplimiento de estas normas será considerado falta disciplinaria, según el Reglamento Interno de Trabajo y/o las normas contractuales vigentes.

9. COMUNICACIÓN Y REVISIÓN

Esta política será socializada a todo funcionario al momento de su ingreso (inducción) estará disponible permanentemente en la carpeta del Sistema de Gestión Integrado (SGI) y en el sitio web de la entidad.

Se revisará anualmente para adaptarse a nuevas tecnologías o modalidades de trabajo (como el trabajo remoto).

10. CONTROL DE CAMBIOS

N°. de Versión	Fecha de Versión	Autor	Revisado por	Aprobado por	Descripción del cambio
01	30/12/2025	Dirección de TI	Direccionamiento Estratégico	Comité Institucional de Gestión y Desempeño	Creación del documento