# Política de Habeas Data, Seguridad de la Información y Gestión de Incidentes — Plataforma Dinuu

**SANEZ TECH GROUP S.A.S. NIT 902.058.180-1**

**Versión 1.0**
**Fecha de Entrada en Vigencia:** junio 5 de 2026

---

## 1. Objeto

SANEZ TECH GROUP S.A.S., en calidad de propietaria y administradora de la Plataforma tecnológica DINUU, manifiesta su compromiso permanente con la protección de los datos personales, la seguridad de la información, la privacidad digital y la gestión responsable de los riesgos asociados al tratamiento de información.

La presente política establece el marco corporativo para la protección de los datos personales, la gestión de riesgos de privacidad, la seguridad de la información, la prevención de incidentes de seguridad y el cumplimiento normativo aplicable a DINUU y a todas las operaciones realizadas por SANEZ TECH GROUP S.A.S.

## 2. Alcance

La presente política aplica a todos los intervinientes en la operatividad, funcionamiento, administración y acceso a la Plataforma DINUU, a saber:

1. Usuarios registrados en la Plataforma DINUU (Partners y Clientes).
2. Aliados comerciales.
3. Empleados y contratistas.
4. Desarrolladores y administradores de sistemas.
5. Proveedores tecnológicos y encargados del tratamiento.
6. Terceros con acceso autorizado a la Plataforma.
7. Cualquier persona natural o jurídica que interactúe con los sistemas de información de DINUU.

## 3. Marco normativo

SANEZ TECH GROUP S.A.S. adopta, implementa y mantiene los lineamientos establecidos en:

1. Constitución Política de Colombia.
2. Ley 1581 de 2012 (protección de datos personales).
3. Ley 1266 de 2008 (habeas data financiero).
4. Ley 1273 de 2009 (delitos informáticos).
5. Decreto 1074 de 2015.

6. Título V de la Circular Única de la Superintendencia de Industria y Comercio.
7. Circulares Externas 001, 002 y 003 de 2024 de la Superintendencia de Industria y Comercio.
8. Guías, instructivos y demás disposiciones emitidas por la Superintendencia de Industria y Comercio.
9. Estándares internacionales aplicables en materia de privacidad, seguridad de la información y gestión de riesgos.

## 4. Principios rectores

SANEZ TECH GROUP S.A.S. desarrollará sus actividades bajo los siguientes principios:

1. **Legalidad:** el tratamiento de datos se realizará conforme a la ley.
2. **Libertad:** el tratamiento requerirá autorización previa, expresa e informada del titular cuando sea procedente.
3. **Transparencia:** los titulares podrán conocer el uso dado a su información.
4. **Finalidad:** los datos serán tratados únicamente para fines legítimos previamente informados.
5. **Seguridad:** se implementarán medidas técnicas, humanas, administrativas y organizacionales apropiadas para proteger la información.
6. **Confidencialidad:** toda persona que intervenga en el tratamiento de datos deberá garantizar reserva permanente sobre la información.
7. **Responsabilidad Demostrada (Accountability):** la sociedad implementará mecanismos verificables que evidencien el cumplimiento efectivo de las obligaciones legales en materia de protección de datos personales.

## 5. Modelo de gobernanza de datos y privacidad

SANEZ TECH GROUP S.A.S. adoptará un sistema integral de gestión de privacidad que incluirá:

1. Inventario de bases de datos.
2. Inventario de activos de información.
3. Identificación de flujos de información.
4. Clasificación de información.
5. Gestión documental.
6. Mecanismos de control de acceso.
7. Gestión de terceros.
8. Monitoreo continuo.
9. Auditorías periódicas.
10. Evaluaciones de impacto en privacidad cuando corresponda.
11. Programas permanentes de capacitación.

## 6. Sistema de gestión de riesgos, privacidad y seguridad

SANEZ TECH GROUP S.A.S. implementará un proceso continuo de gestión de riesgos que contemple:

1. **Identificación:** detección de amenazas internas y externas que puedan afectar los datos personales.
2. **Análisis:** evaluación del impacto y probabilidad de ocurrencia de riesgos.
3. **Valoración:** clasificación de riesgos conforme a criterios de criticidad.
4. **Tratamiento:** definición e implementación de controles preventivos, correctivos y mitigadores.
5. **Monitoreo:** seguimiento continuo de la eficacia de los controles implementados.

## 7. Medidas de seguridad de la información

SANEZ TECH GROUP S.A.S. tiene implementados mecanismos de prevención orientados a proteger los activos digitales, sistemas de información, bases de datos, aplicaciones, plataformas tecnológicas, infraestructura informática y servicios digitales de la Plataforma DINUU. Entre las medidas de seguridad implementadas se encuentran:

1. Cifrado de información.
2. Protocolos HTTPS/TLS.
3. Autenticación segura de usuarios y, para accesos administrativos, mecanismos de autenticación reforzada.
4. Sistemas de respaldo y recuperación.
5. Monitoreo continuo de eventos de seguridad.
6. Gestión de vulnerabilidades.
7. Control de accesos basado en roles.
8. Registros de auditoría.
9. Mecanismos de detección de actividad anómala e intentos de intrusión.
10. Evaluaciones periódicas de seguridad.
11. Gestión segura de bases de datos.
12. Capacitación permanente en ciberseguridad.

## 8. Gestión de incidentes de seguridad

SANEZ TECH GROUP S.A.S. contará con un procedimiento formal para la gestión de incidentes de seguridad que permita:

1. **Detectar:** identificar oportunamente eventos anómalos o vulneraciones.
2. **Contener:** limitar la propagación y el impacto del incidente.
3. **Analizar:** determinar causas, alcance y riesgos asociados.

4. **Corregir:** aplicar acciones correctivas y mitigadoras.
5. **Recuperar:** restablecer los servicios afectados.
6. **Documentar:** conservar evidencia suficiente para fines de auditoría e investigación.

## 9. Reporte de incidentes ante la SIC

Cuando un incidente de seguridad involucre datos personales y genere riesgos para los titulares, SANEZ TECH GROUP S.A.S. realizará el reporte correspondiente a la Superintendencia de Industria y Comercio a través de los mecanismos que dicha autoridad disponga para el efecto, incluyendo la siguiente información:

1. Fecha del incidente.
2. Tipo de incidente.
3. Datos comprometidos.
4. Impacto generado.
5. Medidas adoptadas.
6. Acciones preventivas futuras.

El reporte de incidentes a través del Registro Nacional de Bases de Datos (RNBD) se efectuará en el evento en que SANEZ TECH GROUP S.A.S. se encuentre obligada a inscribir sus bases de datos en dicho registro, conforme a los umbrales de activos y demás criterios establecidos por la normativa vigente. La obligación de reportar incidentes de seguridad subsiste con independencia de la obligación de registro en el RNBD.

## 10. Derechos de los titulares

Los titulares (Partners/Clientes) podrán ejercer los siguientes derechos ante la Plataforma:

1. Conocer sus datos personales.
2. Actualizar información.
3. Rectificar información.
4. Solicitar prueba de la autorización.
5. Revocar autorizaciones.
6. Solicitar supresión de datos cuando proceda.
7. Presentar consultas.
8. Presentar reclamos.
9. Acceder gratuitamente a sus datos personales.

El procedimiento y los canales para el ejercicio de estos derechos se encuentran detallados en la Política de Tratamiento y Protección de Datos Personales de la Plataforma DINUU.

## 11. Gestión de terceros encargados

SANEZ TECH GROUP S.A.S. informará a todo tercero que trate datos personales por cuenta de la empresa que deberá:

1. Cumplir la legislación colombiana de protección de datos.
2. Implementar medidas de seguridad equivalentes o superiores a las exigidas por la compañía.
3. Suscribir acuerdos de confidencialidad y los respectivos contratos de transmisión.
4. Permitir auditorías cuando sea requerido.
5. Reportar incidentes de seguridad de forma inmediata.

El detalle de los encargados del tratamiento que apoyan la operación de la Plataforma DINUU se encuentra en el Anexo I de la Política de Tratamiento y Protección de Datos Personales.

## 12. Capacitación, cultura organizacional y auditoría

SANEZ TECH GROUP S.A.S. desarrollará programas permanentes de formación dirigidos a la protección de datos personales, habeas data, seguridad digital, gestión de incidentes, ciberseguridad, responsabilidad demostrada y prevención de delitos informáticos. La capacitación será periódica y documentada.

Asimismo, SANEZ TECH GROUP S.A.S. realizará revisiones periódicas para verificar:

1. Cumplimiento normativo.
2. Eficacia de controles.
3. Gestión de riesgos.
4. Respuesta a incidentes.
5. Protección efectiva de los datos personales.

Los resultados servirán como base para la mejora continua del sistema de gestión de privacidad y seguridad.

## 13. Responsabilidad demostrada (Accountability)

SANEZ TECH GROUP S.A.S. mantendrá evidencia suficiente para demostrar ante cualquier autoridad competente:

1. La adopción de políticas y procedimientos.
2. La implementación de medidas de seguridad.
3. La gestión de riesgos.
4. Los programas de capacitación.
5. La gestión de incidentes.
6. El cumplimiento de las obligaciones legales en materia de protección de datos personales.

## 14. Declaración final de cumplimiento

SANEZ TECH GROUP S.A.S., como propietaria y administradora de la Plataforma DINUU, declara que adopta, implementa y se compromete a cumplir integralmente los principios, obligaciones, procedimientos y estándares establecidos en la legislación colombiana de protección de datos personales, en el Título V de la Circular Única de la Superintendencia de Industria y Comercio y en las Circulares Externas 001, 002 y 003 de 2024, promoviendo una cultura corporativa de privacidad, seguridad de la información, transparencia, responsabilidad demostrada y protección efectiva de los derechos de los titulares de los datos personales.

## 15. Vigencia y actualización

La presente política entra en vigencia a partir del 5 de junio de 2026 y permanecerá vigente mientras SANEZ TECH GROUP S.A.S. realice actividades a través de la Plataforma DINUU.

SANEZ TECH GROUP S.A.S. se reserva el derecho de modificar esta política en cualquier momento, informando oportunamente a los titulares a través de los canales oficiales de comunicación de la Plataforma DINUU.