Política de Protección de la Información, los Datos y los Sistemas TIC — 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, reconoce que la información, los datos y los sistemas de tecnologías de la información y las comunicaciones constituyen activos estratégicos esenciales para el desarrollo de sus actividades empresariales.

En consecuencia, la sociedad adopta la presente política en cumplimiento de la Ley 1273 de 2009 y de las demás disposiciones legales relacionadas con la protección de la información, la seguridad digital, la prevención de delitos informáticos y la protección de los derechos de usuarios, clientes, proveedores y terceros que interactúan con la Plataforma.

SANEZ TECH GROUP S.A.S. declara su compromiso de implementar medidas técnicas, administrativas, jurídicas y organizacionales destinadas a preservar la confidencialidad, integridad, disponibilidad, autenticidad y trazabilidad de la información administrada a través de DINUU.

La presente política tiene por objeto establecer los principios, mecanismos, controles y procedimientos dirigidos a prevenir, detectar, gestionar y mitigar riesgos asociados a la afectación de la información, los datos, los sistemas informáticos y las infraestructuras tecnológicas utilizadas por DINUU, garantizando el cumplimiento de la Ley 1273 de 2009.

2. Alcance

La presente política aplica a:

1. Usuarios de la Plataforma DINUU.
2. Empleados y directivos.
3. Contratistas.
4. Proveedores tecnológicos.
5. Administradores de sistemas.
6. Desarrolladores de software.
7. Consultores externos.
8. Encargados del tratamiento de datos.
9. Cualquier persona que acceda, utilice o interactúe con los sistemas de información de la sociedad.

3. Marco normativo

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

1. Constitución Política de Colombia.
2. Ley 1273 de 2009 (delitos informáticos).
3. Ley 1581 de 2012 (protección de datos personales).
4. Decreto 1074 de 2015.
5. Ley 527 de 1999 (comercio electrónico y mensajes de datos).
6. Ley 1266 de 2008 (habeas data financiero).
7. Título V de la Circular Única de la Superintendencia de Industria y Comercio y Circulares Externas expedidas por la SIC.
8. Demás normas nacionales e internacionales relacionadas con seguridad de la información y protección de datos.

4. Principios rectores

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

1. **Confidencialidad:** la información solo podrá ser conocida por personas debidamente autorizadas.
2. **Integridad:** los datos deberán permanecer completos, exactos y libres de modificaciones no autorizadas.
3. **Disponibilidad:** los sistemas y servicios deberán encontrarse disponibles para los usuarios autorizados cuando sea requerido.
4. **Autenticidad:** la identidad de usuarios, sistemas y transacciones deberá poder verificarse mediante mecanismos adecuados.
5. **Trazabilidad:** las actividades realizadas dentro de la Plataforma deberán ser susceptibles de seguimiento, monitoreo y auditoría.
6. **Seguridad proactiva:** la sociedad implementará controles preventivos orientados a reducir riesgos antes de que se materialicen incidentes.

5. Protección del bien jurídico de la información y los datos

SANEZ TECH GROUP S.A.S. reconoce que la información y los datos constituyen bienes jurídicos protegidos por la legislación colombiana y, por tanto, implementa mecanismos destinados a evitar cualquier conducta que pueda afectar:

1. La confidencialidad de la información.
2. La integridad de los datos.
3. La disponibilidad de los sistemas.
4. La seguridad de las redes.
5. La protección de bases de datos.

6. La privacidad de los usuarios.
7. La continuidad operativa de la Plataforma.

6. Prohibición de conductas relacionadas con delitos informáticos

SANEZ TECH GROUP S.A.S. prohíbe expresamente cualquier conducta que pueda constituir alguno de los delitos contemplados en la Ley 1273 de 2009, incluyendo, entre otros:

1. **Acceso abusivo a sistemas informáticos:** intentar ingresar, permanecer o acceder sin autorización a sistemas, redes, aplicaciones o bases de datos.
2. **Obstaculización ilegítima de sistemas:** interferir, bloquear, degradar o afectar el funcionamiento normal de sistemas informáticos o redes de comunicaciones.
3. **Interceptación de datos informáticos:** capturar, monitorear o acceder a información transmitida por medios electrónicos sin autorización.
4. **Daño informático:** alterar, destruir, deteriorar o inutilizar información, programas, aplicaciones o sistemas.
5. **Uso de software malicioso:** introducir virus, malware, ransomware, spyware u otros programas destinados a afectar sistemas o información.
6. **Violación de datos personales:** obtener, recopilar, utilizar, divulgar o comercializar datos personales sin autorización legal o contractual.
7. **Suplantación de sitios web:** crear o utilizar mecanismos destinados a engañar usuarios para obtener información confidencial.
8. **Fraude informático:** manipular sistemas o procesos digitales para obtener beneficios indebidos o causar perjuicios económicos.
9. **Transferencia no consentida de activos:** realizar movimientos, modificaciones o apropiaciones de activos digitales o económicos mediante medios informáticos sin autorización.

7. Controles de seguridad

SANEZ TECH GROUP S.A.S. implementa medidas orientadas a proteger la información y los sistemas, incluyendo:

1. Gestión segura de accesos.
2. Autenticación segura de usuarios y, para accesos administrativos, mecanismos de autenticación reforzada.
3. Cifrado de información.
4. Monitoreo de eventos.
5. Registros de auditoría.
6. Gestión de vulnerabilidades.
7. Copias de seguridad.
8. Recuperación ante desastres.

9. Protección perimetral.
10. Seguridad de aplicaciones.
11. Segmentación de redes.
12. Evaluaciones periódicas de seguridad.

8. Gestión de incidentes de seguridad

SANEZ TECH GROUP S.A.S. contará con procedimientos para:

1. **Identificación:** detectar incidentes o eventos sospechosos.
2. **Contención:** reducir el impacto del incidente.
3. **Investigación:** determinar causas, alcance y responsables.
4. **Recuperación:** restablecer los servicios afectados.
5. **Mejoramiento:** implementar acciones correctivas y preventivas.

9. Preservación de evidencia digital

Cuando se detecten incidentes que puedan constituir delitos informáticos, SANEZ TECH GROUP S.A.S. adoptará medidas para:

1. Preservar la evidencia digital.
2. Mantener registros de auditoría.
3. Documentar los hechos.
4. Garantizar la cadena de custodia cuando resulte aplicable.
5. Facilitar la actuación de las autoridades competentes.

10. Deber de reporte

Todo empleado, contratista, proveedor o usuario que tenga conocimiento de una posible vulneración deberá informar inmediatamente cualquier evento relacionado con:

1. Accesos no autorizados.
2. Intentos de intrusión.
3. Fugas de información.
4. Malware.
5. Fraude electrónico.
6. Vulnerabilidades críticas.
7. Posibles delitos informáticos.

11. Capacitación y concientización

SANEZ TECH GROUP S.A.S. desarrollará programas periódicos de formación en:

1. Seguridad de la información.
2. Protección de datos personales.
3. Prevención de delitos informáticos.
4. Ciberseguridad.
5. Gestión de incidentes.
6. Uso seguro de herramientas digitales.

12. Cooperación con las autoridades

SANEZ TECH GROUP S.A.S. colaborará con las autoridades administrativas, judiciales y de policía en investigaciones relacionadas con delitos informáticos, protección de datos y seguridad digital, de conformidad con la legislación vigente.

13. Responsabilidades

SANEZ TECH GROUP S.A.S. y todos los usuarios, empleados, contratistas y terceros deberán:

1. Cumplir esta política.
2. Proteger las credenciales de acceso.
3. Utilizar adecuadamente los recursos tecnológicos.
4. Reportar incidentes.
5. Respetar la confidencialidad de la información.

14. Consecuencias del incumplimiento

El incumplimiento de la presente política podrá dar lugar a:

1. Suspensión o cancelación de accesos.
2. Medidas disciplinarias internas.
3. Terminación de contratos.
4. Acciones civiles por daños y perjuicios.
5. Denuncias ante autoridades competentes.
6. Responsabilidades penales previstas en la Ley 1273 de 2009.

15. Auditoría y control

SANEZ TECH GROUP S.A.S. realizará auditorías periódicas para evaluar:

1. Riesgos tecnológicos.

2. Cumplimiento normativo.
3. Eficacia de controles.
4. Vulnerabilidades.
5. Incidentes registrados.

Los resultados servirán para fortalecer continuamente el sistema de gestión de seguridad de la información.

16. Declaración corporativa de cumplimiento

SANEZ TECH GROUP S.A.S., como propietaria y administradora de la Plataforma DINUU, declara expresamente que adopta, implementa y se compromete a cumplir integralmente las disposiciones de la Ley 1273 de 2009, mediante la aplicación de medidas jurídicas, técnicas, administrativas y organizacionales destinadas a proteger la información, los datos, las redes, las bases de datos y los sistemas de tecnologías de la información y las comunicaciones, promoviendo una cultura corporativa de seguridad digital, prevención de delitos informáticos y protección efectiva de los activos de información bajo su responsabilidad.

17. 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 sus 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.