2026

POLÍTICA DE TRATAMIENTO DE DATOS PERSONALES

CONTROL DEL DOCUMENTO

Versión	Título	Fecha de vigencia
2.0	Política de Tratamiento de Datos Personales	Indefinida — revisión anual obligatoria

Campo	Detalle
Preparado por:	Katerine Restrepo
Fecha preparado:	Febrero 2026
Revisado por:	Carlos Arismendy
Fecha revisado:	Febrero 2026
Aprobado por:	Comité Ejecutivo Kronux Solutions S.A.S.
Fecha aprobado:	Marzo 2026
Vigencia:	Indefinida — revisión anual obligatoria

Historia de Revisión

Versión	Fecha	Responsable	Cambios
0.1	29-08-2017	Katerine Restrepo	Creación de política
1.0	29-08-2017	Comité Ejecutivo	Primera versión aprobada
2.0	Marzo 2026	Katerine Restrepo	Actualización normativa y regulatoria

1. OBJETIVO

Definir y exponer la política de tratamiento de datos personales de Kronux Solutions S.A.S. en cumplimiento con la legislación colombiana aplicable, garantizando los derechos de los titulares a través de un tratamiento lícito, seguro y transparente, conforme a los principios establecidos en los artículos 4° y 5° de la Ley Estatutaria 1581 de 2012.

2. ALCANCE

La presente política aplica a todas las bases de datos y archivos que contengan datos personales objeto de tratamiento por parte de Kronux Solutions S.A.S., incluyendo aquellos gestionados en formato físico, digital o en la nube, sin importar el medio de almacenamiento o procesamiento.

3. IDENTIFICACIÓN DEL RESPONSABLE DEL TRATAMIENTO

Campo	Dato
Razón Social:	Kronux Solutions S.A.S.
NIT:	900.464.926-0
Dirección:	Carrera 80 AA #36-39, Medellín, Antioquia, Colombia
Teléfono:	+57 (604) 444-6705
Correo electrónico:	soc@kronux.com.co / info@kronux.com.co
Responsable de protección de datos:	Área de Seguridad de la Información

Nota: En el desarrollo de sus servicios de ciberseguridad (SOC, análisis forense, gestión de vulnerabilidades), Kronux podrá actuar como Encargado del Tratamiento de datos de terceros, sujeto a las obligaciones del artículo 18 de la Ley 1581 de 2012.

4. TRATAMIENTO Y FINALIDADES

Kronux Solutions S.A.S. gestiona datos de las siguientes categorías de titulares:

- **Empleados:** Comunicaciones laborales, vinculación/desvinculación, cambios contractuales, beneficios laborales, contacto familiar en emergencias, obligaciones legales (SENA, UGPP, ARL, EPS, Pensiones), control de acceso.
- **Contratistas:** Solicitud de cotizaciones, soporte, realización de pedidos, comunicación en proyectos, gestión de contratos.
- **Clientes:** Comunicaciones de proyectos de ciberseguridad, visitas de soporte, reportes de seguridad, facturación y gestión comercial.
- **Aliados y Proveedores:** Comunicación para desarrollo de alianzas, proyectos conjuntos y gestión de acuerdos.

Nota sobre datos sensibles: En su actividad de ciberseguridad, Kronux puede acceder incidentalmente a datos sensibles (p. ej., datos biométricos en registros de seguridad). En tal caso, el tratamiento se realizará conforme a los artículos 5° y 6° de la Ley 1581 de 2012, con medidas reforzadas de seguridad.

5. PRINCIPIOS QUE RIGEN EL TRATAMIENTO

De conformidad con el artículo 4° de la Ley 1581 de 2012:

- **Legalidad:** Todo tratamiento se realizará conforme a la ley vigente.
- **Finalidad:** Finalidades legítimas, determinadas, explícitas e informadas al titular.
- **Libertad:** Solo con consentimiento previo, expreso e informado, salvo mandato legal.
- **Veracidad y calidad:** Información veraz, completa, exacta, actualizada y comprensible.
- **Transparencia:** El titular podrá conocer el tratamiento de sus datos en cualquier momento.
- **Acceso y circulación restringida:** Datos disponibles solo para personas autorizadas.
- **Seguridad:** Medidas técnicas, humanas y administrativas contra pérdida o acceso no autorizado.
- **Confidencialidad:** Reserva de la información incluso tras finalizar la relación con la empresa.

6. DERECHOS DE LOS TITULARES

De conformidad con el artículo 8° de la Ley 1581 de 2012, el titular tiene derecho a:

- Conocer, actualizar y rectificar sus datos personales.
- Solicitar prueba de la autorización otorgada para el tratamiento de sus datos.
- Ser informado sobre el uso dado a sus datos personales.
- Presentar quejas ante la Superintendencia de Industria y Comercio (SIC).
- Revocar la autorización y/o solicitar la supresión de sus datos.
- Acceder gratuitamente a sus datos personales objeto de tratamiento.

7. DEBERES DE KRONUX COMO RESPONSABLE DEL TRATAMIENTO

En cumplimiento del artículo 17 de la Ley 1581 de 2012, Kronux adoptará los siguientes deberes:

- Garantizar al titular el pleno ejercicio de sus derechos en todo momento.
- Conservar la información bajo condiciones de seguridad que impidan adulteración, pérdida o acceso no autorizado.
- Rectificar la información cuando sea incorrecta.
- Tramitar consultas y reclamos en los términos señalados por la ley.
- Informar a la SIC cuando se presenten violaciones de seguridad con riesgo para los titulares.
- Cumplir las instrucciones y requerimientos que imparta la SIC.
- Registrar y mantener actualizado en el RNBD el inventario de bases de datos personales (Decreto 090 de 2018).

8. RESPONSABLE DE ATENCIÓN Y PROCEDIMIENTO PARA EJERCER DERECHOS

Área Responsable: Seguridad de la Información / Oficial de Protección de Datos

Canales de atención:

- Correo: soc@kronux.com.co / info@kronux.com.co
- Teléfono: +57 (604) 444-6705

- Dirección: Carrera 80 AA #36-39, Medellín, Antioquia

Tiempos de respuesta — Arts. 14 y 15, Ley 1581/2012:

Tipo de solicitud	Plazo máximo	Prórroga permitida
Consultas	10 días hábiles	5 días hábiles adicionales, informando al titular
Reclamos (corrección, supresión, revocatoria)	15 días hábiles	8 días hábiles adicionales, informando al titular
Reclamo incompleto	5 días hábiles para requerir corrección al titular	Si no subsana en 2 meses, se entiende desistido

En caso de no obtener respuesta satisfactoria, el titular podrá acudir a la Superintendencia de Industria y Comercio (SIC), Autoridad Nacional de Protección de Datos. www.sic.gov.co (Art. 21, Ley 1581/2012).

9. AUTORIZACIÓN PARA EL TRATAMIENTO DE DATOS PERSONALES

Kronux Solutions S.A.S., en cumplimiento de los artículos 9° y 10° de la Ley 1581 de 2012, solicita consentimiento previo, expreso e informado para el tratamiento de datos. Dicha autorización podrá obtenerse por escrito, de forma oral o mediante conductas inequívocas.

No se requiere autorización cuando el tratamiento sea ordenado por autoridad pública, se trate de datos públicos, o medien razones de urgencia médica o sanitaria (Art. 10°, Ley 1581/2012).

10. TRANSFERENCIA Y TRANSMISIÓN INTERNACIONAL DE DATOS

Kronux podrá realizar transmisiones de datos a Encargados del Tratamiento (proveedores cloud, plataformas SIEM/SOAR) cuando sea necesario para la prestación de servicios. En tal caso:

- Se suscribirán contratos de transmisión de datos (Data Processing Agreements) que obliguen al Encargado a aplicar las mismas garantías de la Ley 1581 de 2012.
- En transferencias internacionales a países sin niveles adecuados de protección, se obtendrá autorización del titular o se aplicarán las excepciones del artículo 26 de la Ley 1581 de 2012.
- Las revelaciones a autoridades competentes se realizarán exclusivamente bajo requerimiento legal formal.

11. SEGURIDAD EN EL TRATAMIENTO DE LOS DATOS PERSONALES

Kronux Solutions S.A.S. garantiza la confidencialidad, integridad y disponibilidad de los datos personales mediante:

- Controles de acceso basados en roles y principio de mínimo privilegio.
- Cifrado de datos en tránsito y en reposo.
- Monitoreo continuo de eventos de seguridad.
- Planes de respuesta a incidentes de seguridad de la información.
- Capacitación periódica del personal en protección de datos personales.
- Revisiones periódicas de vulnerabilidades y pruebas de penetración.

Períodos de retención: Los datos se conservarán únicamente el tiempo necesario para cumplir su finalidad o el exigido por ley. Vencido dicho período, serán suprimidos de forma segura o anonimizados. Los períodos

específicos por tipo de titular están definidos en el Inventario de Bases de Datos de Kronux.

12. NOTIFICACIÓN DE INCIDENTES DE SEGURIDAD

En cumplimiento del artículo 17, literal f) de la Ley 1581 de 2012, ante incidentes que comprometan datos personales, Kronux seguirá el siguiente procedimiento:

- **1. Identificación y contención:** En un plazo no mayor a 72 horas desde la detección del incidente.
- **2. Notificación interna:** Al Área de Seguridad de la Información y a la Dirección.
- **3. Evaluación de riesgos:** Para determinar el alcance e impacto sobre los titulares afectados.
- **4. Notificación a titulares:** Cuando el incidente genere riesgo alto para sus derechos y libertades.
- **5. Reporte a la SIC:** Conforme a los lineamientos vigentes de dicha autoridad.
- **6. Registro del incidente:** En el historial de incidentes para trazabilidad y auditoría interna.

13. TRATAMIENTO DE DATOS EN SISTEMAS DE INTELIGENCIA ARTIFICIAL

En cumplimiento de la Circular Externa SIC No. 002 del 21 de agosto de 2024 — "Lineamientos sobre el Tratamiento de Datos Personales en Sistemas de IA" —, Kronux Solutions S.A.S. establece:

13.1. Declaración de no uso de datos personales en sistemas de IA:

Kronux Solutions S.A.S. **no utiliza datos personales, datos privados ni secretos comerciales de sus clientes** como insumo en sus sistemas o herramientas de Inteligencia Artificial. Los sistemas de IA empleados en la operación de Kronux se alimentan exclusivamente de **información técnica de carácter público**, que incluye, entre otros:

- Indicadores de Compromiso (IoC) de fuentes abiertas (*OSINT*).
- Registros de vulnerabilidades públicas (CVE, NVD, bases de datos de amenazas).
- Inteligencia de amenazas (*Threat Intelligence*) proveniente de fuentes públicas y compartidas por la comunidad de ciberseguridad.
- Información técnica de campañas de ataque o malware publicada por organizaciones reconocidas (MITRE ATT&CK, CISA, entre otros).

En consecuencia, el tratamiento de datos en los sistemas de IA de Kronux **no está sujeto al ámbito de aplicación de la Ley Estatutaria 1581 de 2012**, dado que dicha ley aplica exclusivamente sobre datos de personas naturales determinadas o determinables, conforme a su artículo 3°.

13.2. Rol de los sistemas de IA — Apoyo y referencia:

Los sistemas de IA implementados por Kronux Solutions S.A.S. actúan únicamente como **herramientas de apoyo y referencia técnica** para tareas como análisis de amenazas, correlación de eventos de seguridad y automatización operativa. Estos sistemas **no toman**

decisiones automatizadas que afecten de manera directa, personalizada o significativa a ninguna persona natural. La toma de decisiones con efectos sobre personas o clientes recae siempre en **analistas humanos calificados**.

13.3. Principio de precaución y compromiso de no expansión:

Kronux Solutions S.A.S. se compromete a **no ampliar el alcance** de sus sistemas de IA al procesamiento de datos personales sin haber adoptado previamente las medidas técnicas y jurídicas exigidas por la Circular SIC No. 002 de 2024 y la Ley 1581 de 2012. En caso de que en el futuro se evalúe el uso de datos personales en sistemas de IA, se deberá:

- Realizar una **Evaluación de Impacto en Privacidad (PIA)** conforme a la ISO 29134.
- Actualizar la presente política e informar a los titulares afectados.
- Obtener las autorizaciones correspondientes o implementar procesos de anonimización irreversible previamente validados.

13.4. Minimización de datos:

Solo se utilizarán en sistemas de IA los datos estrictamente necesarios para la finalidad perseguida.

13.5. Confidencialidad de información técnica de clientes:

Sin perjuicio de lo anterior, Kronux garantiza que la **información técnica privada de sus clientes** (configuraciones, arquitecturas, logs internos, datos de incidentes gestionados, entre otros) **tampoco es utilizada como insumo en sistemas de IA**, y se mantiene bajo estrictas obligaciones de confidencialidad en los términos de los contratos de prestación de servicios y los acuerdos de no divulgación (NDA) suscritos con cada cliente.

14. LEGISLACIÓN APLICABLE

- **Artículo 15, Constitución Política de Colombia:** Derecho fundamental al Habeas Data.
- **Ley 1266 de 2008:** Habeas Data financiero y comercial.
- **Ley 1273 de 2009:** Delitos informáticos (relevante para empresa de ciberseguridad).
- **Ley Estatutaria 1581 de 2012:** Protección de datos personales.
- **Decreto 1074 de 2015, Capítulo 25:** Compilación y derogatoria del Decreto 1377 de 2013.
- **Decreto 090 de 2018:** Registro Nacional de Bases de Datos (RNBD).
- **Circular Externa SIC No. 002 de 2024:** Lineamientos para el tratamiento de datos en sistemas de IA.
- **Demás normas:** Las que complementen, modifiquen o sustituyan las anteriores.

15. AVISO DE PRIVACIDAD

"Kronux Solutions S.A.S., en cumplimiento de la Ley Estatutaria 1581 de 2012 y el Decreto 1074 de 2015, le informa que los datos personales suministrados por usted serán gestionados de acuerdo con la presente Política de Tratamiento de Datos Personales, con todas las medidas de seguridad requeridas y exclusivamente para las finalidades aquí descritas. Para ejercer sus derechos como titular, podrá

contactarnos a través de los canales indicados en la sección 8. La política completa está disponible en [sitio web de Kronux]."

16. FORMATO DE AUTORIZACIÓN AL TRATAMIENTO DE DATOS

"En cumplimiento de la Ley Estatutaria 1581 de 2012 y el Decreto 1074 de 2015, y habiendo sido informado(a) sobre la Política de Tratamiento de Datos Personales de Kronux Solutions S.A.S., sus finalidades, los derechos que me asisten como titular y los canales para ejercerlos, autorizo de forma libre, previa, expresa, voluntaria e informada a Kronux Solutions S.A.S. para recolectar, almacenar, usar, circular y en general tratar mis datos personales de acuerdo con las finalidades descritas en su política de tratamiento de datos personales."

17. VIGENCIA

La presente Política rige a partir de [FECHA DE APROBACIÓN] y tendrá vigencia indefinida. Será revisada anualmente o ante cambios normativos significativos. Cualquier modificación sustancial será comunicada a los titulares con al menos treinta (30) días calendario de antelación.

La versión anterior (v1.0 de agosto de 2017) queda sin efecto a partir de la fecha de vigencia de la presente política.

18. DEFINICIONES

- **Anonimización:** Proceso irreversible mediante el cual los datos personales son modificados de tal forma que no es posible identificar al titular, directa ni indirectamente.
- **Autorización:** Consentimiento previo, expreso e informado del Titular para el Tratamiento de sus Datos Personales.
- **Aviso de Privacidad:** Comunicación del Responsable al Titular para informarle sobre las Políticas de Tratamiento y las finalidades del mismo.
- **Base de Datos:**Conjunto organizado de Datos Personales que sea objeto de Tratamiento.
- **Clientes:**Persona natural o jurídica con la cual la empresa tiene una relación comercial.
- **Aliados:**Persona natural o jurídica con la cual la empresa tiene un proyecto o alianza.
- **Proveedor:**Persona natural o jurídica a la cual la empresa contrata por un producto o servicio.
- **Dato Personal:**Cualquier información vinculada o que pueda asociarse a una o varias personas naturales determinadas o determinables.
- **Dato Sensible:**Información que afecta la intimidad del Titular o cuyo uso puede generar discriminación: origen racial, orientación política, convicciones religiosas, datos de salud, vida sexual, datos biométricos, entre otros.
- **Dato Anonimizado:** Dato que ha perdido definitivamente su calidad de dato personal y no está sujeto a la Ley 1581 de 2012.
- **Dato Pseudonimizado:** Dato que no puede atribuirse a un titular sin información adicional separada. Sigue siendo dato personal sujeto a la ley.
- **Encargado del Tratamiento:** Persona natural o jurídica que realiza el Tratamiento de Datos por cuenta del Responsable.

- **Evaluación de Impacto en Privacidad — PIA:** Proceso para evaluar los efectos de un tratamiento de datos sobre la privacidad, especialmente en contextos de IA o tratamientos a gran escala (ISO 29134).
- **Incidente de Seguridad:** Evento que compromete la confidencialidad, integridad o disponibilidad de los datos personales.
- **Reclamo:** Solicitud del Titular para corregir, actualizar o suprimir sus datos, o para revocar la autorización.
- **Responsable del Tratamiento:** Persona natural o jurídica que decide sobre la Base de Datos y/o el Tratamiento de los datos.
- **RNBD:** Registro Nacional de Bases de Datos. Mecanismo de la SIC para garantizar la transparencia en el manejo de datos personales (Decreto 090 de 2018).
- **SIC:** Superintendencia de Industria y Comercio, Autoridad Nacional de Protección de Datos Personales en Colombia (Art. 21, Ley 1581/2012).
- **Sistema de IA:** Sistema basado en máquinas que realiza predicciones, recomendaciones o decisiones usando datos como insumo (Circular SIC 002/2024).
- **Titular:** Persona natural cuyos Datos Personales sean objeto de Tratamiento.
- **Transferencia:** Envío de datos personales a un receptor Responsable, dentro o fuera del país.
- **Transmisión:** Comunicación de datos al Encargado para que realice el tratamiento por cuenta del Responsable.
- **Tratamiento:** Cualquier operación sobre Datos Personales: recolección, almacenamiento, uso, circulación o supresión.