

TECTRIL

AVISO DE PRIVACIDAD DEL CANAL DE INTEGRIDAD

Cómo tratamos datos personales relacionados con reportes, investigaciones y medidas de integridad

TRANSPARENCIA Y PROTECCIÓN. Tectril trata los datos del Canal de Integridad con finalidad definida, acceso restringido, confidencialidad y medidas proporcionales de seguridad. Este Aviso explica qué datos pueden tratarse, por qué son necesarios y qué derechos tienen las personas involucradas.

Documento	Versión	Vigencia
Aviso de Privacidad del Canal de Integridad	Revisión 0	18 de julio de 2026

TECTRIL SOLUÇÕES EM LOGÍSTICA E COMÉRCIO LTDA
Caieiras — São Paulo — Brasil

Control del documento

Campo	Definición
Responsable del tratamiento	Tectril Soluções em Logística e Comércio Ltda
Propietario	Administración de Tectril
Gestión	Persona formalmente designada para Integridad y Compliance, con apoyo de la función de protección de datos
Aprobación	Administración de Tectril
Revisión	Anual o cuando exista un cambio relevante en el Canal, las operaciones de tratamiento o la legislación
Documentos relacionados	Código de Ética y Conducta Comercial; Política del Canal de Integridad; Política de Seguridad de la Información; Política de Gestión de Registros

1. Quién es responsable de los datos

Tectril Soluções em Logística e Comércio Ltda es responsable del tratamiento de los datos personales del Canal de Integridad porque define las finalidades y los medios principales de recepción, evaluación, investigación, decisión, remediación y conservación de los reportes.

Proveedores de tecnología, alojamiento, seguridad, investigación, asesoría jurídica, auditoría u otros servicios podrán actuar como encargados del tratamiento o responsables independientes según la actividad y el contrato aplicable.

El contacto oficial para asuntos de privacidad y ejercicio de derechos es privacidade@tectril.com.br. Se recomienda utilizar el asunto “Privacidad — Canal de Integridad” para facilitar el encaminamiento seguro.

2. A quién se aplica este Aviso

Este Aviso se aplica a datos personales relacionados con:

- personas que presentan reportes identificados;
- personas que optan por no identificarse cuando el relato o los datos técnicos permiten identificación directa o indirecta;
- personas denunciadas, mencionadas o relacionadas con los hechos;
- testigos, colaboradores, representantes y terceros consultados;
- investigadores, responsables de clasificación y personas que deciden o ejecutan medidas;
- titulares mencionados en documentos, mensajes, imágenes, audios, videos u otros archivos.

3. Datos personales que podemos tratar

3.1. Datos de la persona informante

- nombre, cargo, empresa y relación con Tectril;
- correo electrónico, teléfono y preferencia de contacto;
- declaraciones, opiniones, documentos y evidencias presentados;
- información necesaria para evaluar protección contra represalias;

- registros de comunicación y complementaciones.

3.2. Datos de personas involucradas

- identidad, función, empresa y relación con los hechos;
- conductas atribuidas, manifestaciones y versiones presentadas;
- registros profesionales, contractuales, financieros, operativos, fiscales, aduaneros o de sistemas relacionados;
- medidas de preservación, investigación, remediación o responsabilidad;
- información de testigos y otras fuentes relevantes.

3.3. Datos sensibles y de mayor riesgo

Cuando sea pertinente, un reporte puede contener datos de salud, biometría, origen racial o étnico, religión, opinión política, afiliación sindical, vida sexual, orientación sexual u otros datos con protección reforzada.

También puede incluir sospechas de fraude, acoso, discriminación, corrupción, infracciones, procesos o sanciones, así como datos financieros, documentos de identificación y otra información de alto impacto.

Estos datos no deben incluirse por curiosidad. Solo se tratarán cuando sean necesarios, adecuados y estén relacionados con el reporte o el ejercicio de derechos.

3.4. Datos técnicos y archivos

El formulario puede generar registros de fecha y hora, identificadores de sesión, navegador, dispositivo, seguridad y, según la configuración, dirección IP.

Los archivos pueden contener metadatos, autoría, historial, geolocalización, imagen, voz u otros datos identificadores. Quien desee no identificarse debe revisar los archivos y evitar incluir información que revele su identidad.

4. Fuentes de los datos

Los datos pueden obtenerse de la persona informante; personas entrevistadas o consultadas; documentos y evidencias de personas involucradas; sistemas, registros, dispositivos, correos y archivos corporativos autorizados; clientes, proveedores, socios, transportistas, agentes y prestadores; fuentes públicas legítimas y autoridades; y asesores, auditores o investigadores autorizados.

5. Finalidades del tratamiento

Podemos tratar datos para:

- recibir, registrar y confirmar reportes;
- clasificar, analizar preliminarmente y evaluar riesgos;
- identificar conflictos y definir encaminamiento independiente;
- solicitar aclaraciones y recibir complementaciones;
- preservar documentos, sistemas y evidencias;
- investigar hechos y entrevistar personas;
- prevenir, detectar, interrumpir y remediar irregularidades;
- proteger informantes, testigos y otras personas contra represalias;
- decidir y ejecutar medidas correctivas, disciplinarias, contractuales o jurídicas;
- colaborar con auditorías, fiscalizaciones y autoridades competentes;
- ejercer derechos en procesos administrativos, arbitrales o judiciales;

- cumplir obligaciones legales, regulatorias y contractuales;
- evaluar el Programa de Integridad mediante información agregada;
- proteger la seguridad del Canal y prevenir abuso, fraude y acceso no autorizado.

6. Bases legales

El consentimiento generalmente no es la base legal principal porque su retirada podría comprometer obligaciones, investigaciones y el ejercicio de derechos.

Según el caso, el tratamiento podrá basarse en:

Categoría	Posibles bases legales
Datos personales en general	Cumplimiento de obligación legal o regulatoria; ejecución de contrato o procedimientos relacionados; ejercicio regular de derechos; interés legítimo de Tectril o de un tercero, con evaluación de necesidad y salvaguardas; protección de la vida o integridad física cuando corresponda.
Datos personales sensibles	Cumplimiento de obligación legal o regulatoria; ejercicio regular de derechos; protección de la vida o integridad física; prevención del fraude y seguridad del titular en procesos de identificación cuando corresponda; otras hipótesis autorizadas por la LGPD.
Datos de niños y adolescentes	Tratamiento excepcional, limitado a lo necesario y orientado por el interés superior, protección y seguridad del niño o adolescente.

La base aplicable se evaluará según la finalidad, naturaleza de los datos, relación y contexto.

7. Reporte identificado, confidencial y sin identificación

En un reporte identificado, Tectril conoce la identidad de la persona informante, pero restringe el acceso a quienes la necesitan para tratar el caso.

En un reporte sin identificación no se exigen nombre, correo ni teléfono. Sin embargo, el contenido, los archivos y ciertos registros técnicos pueden permitir identificación indirecta. Por ello Tectril utiliza la expresión “sin identificación” y no promete anonimato técnico absoluto.

Sin contacto o función de seguimiento, Tectril puede no conseguir solicitar aclaraciones, comunicar el cierre o responder solicitudes relacionadas con el reporte.

8. Con quién pueden compartirse los datos

El intercambio se limitará a lo necesario y podrá incluir:

- Responsable del Canal, suplente formal e investigadores autorizados;
- Administración o instancia decisoria no impedida;
- asesores jurídicos, auditores, peritos e investigadores independientes;
- proveedores de formulario, alojamiento, almacenamiento, seguridad, comunicación y soporte;
- aseguradoras, instituciones financieras o socios cuando sea estrictamente necesario y legal;
- autoridades policiales, administrativas, fiscales, aduaneras, judiciales o regulatorias competentes;
- otras personas u organizaciones cuando sea necesario para proteger derechos, seguridad o cumplimiento legal.

Una persona mencionada no recibe la identidad de la persona informante por ese solo hecho. La información se facilitará de manera compatible con el derecho de defensa, la protección de terceros, la confidencialidad y la integridad de la investigación.

9. Transferencias internacionales

Algunos proveedores de tecnología, almacenamiento, seguridad o soporte pueden tratar datos en otros países. Cuando exista transferencia internacional, Tectril procurará utilizar proveedores, contratos y mecanismos compatibles con la LGPD y limitará los datos a lo necesario.

La ubicación de servidores y subencargados deberá confirmarse antes de publicar este Aviso y mantenerse en el registro interno de operaciones.

10. Conservación

Los datos se conservarán durante el tiempo necesario para las finalidades del Canal, la remediación, el Programa de Integridad, el ejercicio de derechos y las obligaciones aplicables.

Como regla interna inicial, el expediente se conservará durante cinco años después del cierre, sujeto a revisión periódica. El plazo podrá ampliarse por investigación en curso, obligación legal o contractual, preservación, auditoría, fiscalización, proceso judicial, administrativo o arbitral, o riesgo jurídico documentado.

Finalizado el plazo y sin fundamento para conservar, los datos se eliminarán de forma segura o se anonimizarán. Las copias de seguridad seguirán el ciclo técnico aplicable.

11. Seguridad y control de acceso

Tectril aplicará medidas proporcionales al riesgo, como acceso por necesidad de conocimiento, permisos individuales, autenticación, revisión periódica de accesos, segregación de casos sensibles y personas impedidas, protección de transmisión y almacenamiento, copias de seguridad, registros de acceso cuando estén disponibles, compromisos de confidencialidad, corrección de vulnerabilidades, respuesta a incidentes y cadena de custodia.

Ningún sistema es completamente inmune. Si un incidente puede generar riesgo o daño relevante, Tectril lo evaluará y realizará las comunicaciones exigidas por la LGPD y la regulación de la ANPD.

12. Decisiones automatizadas

Tectril no pretende imponer sanciones ni determinar responsabilidad exclusivamente mediante decisiones automatizadas. Las herramientas pueden ayudar en organización, seguridad, clasificación o investigación, pero las decisiones relevantes requieren revisión humana.

13. Derechos de los titulares

Conforme a la legislación aplicable, el titular podrá solicitar:

- confirmación de la existencia del tratamiento;
- acceso a sus propios datos, respetando derechos de terceros;
- corrección de datos incompletos, inexactos o desactualizados;
- información sobre intercambios;
- anonimización, bloqueo o eliminación de datos innecesarios o tratados irregularmente;
- oposición o revisión cuando corresponda;

- información sobre consecuencias de no proporcionar determinados datos;
- petición ante la Autoridad Nacional de Protección de Datos de Brasil.

Los derechos pueden limitarse legítimamente para proteger la identidad de terceros, preservar evidencias, no comprometer una investigación, cumplir una obligación o ejercer derechos. Tectril explicará la razón aplicable cuando no pueda atender plenamente una solicitud.

Podrán solicitarse datos razonables para confirmar la identidad y evitar acceso no autorizado. Las solicitudes de representantes o relativas a personas fallecidas requieren prueba de legitimidad.

14. Responsabilidades de quien utiliza el Canal

La persona que presenta un reporte debe actuar de buena fe, informar solo lo pertinente y evitar datos excesivos, íntimos o sin relación con los hechos.

Cuando sea posible, los documentos de terceros deben limitarse a las partes necesarias. El Canal no debe utilizarse para exponer públicamente a personas, compartir contenido ilícito ni sustituir servicios de emergencia.

15. Actualizaciones

Este Aviso podrá actualizarse por cambios legales, regulatorios, técnicos u operativos. La versión vigente indicará la fecha de revisión y estará disponible junto al Canal. Los cambios relevantes podrán comunicarse por medios adicionales cuando corresponda.

16. Contacto y ejercicio de derechos

Para consultas de privacidad o ejercicio de derechos relacionados con datos del Canal, utilice:

- Contacto de privacidad: privacidade@tectril.com.br;
- Asunto recomendado: “Privacidad — Canal de Integridad”;
- Sitio oficial: www.tectril.com.br.

canaldeetica@tectril.com.br podrá utilizarse para consultas sobre el funcionamiento del Canal, pero no debe presentarse como anónimo ni sustituir el contacto específico de protección de datos después de su formalización.

17. Aprobación

Responsabilidad	Nombre/Cargo	Fecha	Firma
Elaboración			
Revisión jurídica/LGPD			
Validación del contacto de privacidad			
Aprobación			

Referencias normativas

- BRASIL. Ley n.º 13.709/2018 — Ley General de Protección de Datos Personales de Brasil — LGPD, con modificaciones posteriores.
- AUTORIDAD NACIONAL DE PROTECCIÓN DE DATOS DE BRASIL. Resolución CD/ANPD n.º 15/2024 — Reglamento de Comunicación de Incidentes de Seguridad.
- AUTORIDAD NACIONAL DE PROTECCIÓN DE DATOS DE BRASIL. Resolución CD/ANPD n.º 18/2024 — Reglamento sobre la actuación del encargado de protección de datos.
- AUTORIDAD NACIONAL DE PROTECCIÓN DE DATOS DE BRASIL. Guía sobre responsables, encargados y delegado de protección de datos.
- AUTORIDAD NACIONAL DE PROTECCIÓN DE DATOS DE BRASIL. Guía de Seguridad de la Información para Agentes de Tratamiento de Pequeño Porte.