

POLÍTICA DE TRATAMIENTO DE DATOS PERSONALES

TECJUR OUTSOURCING PROFESIONAL SAS

NIT: 900.485.111-5

TECJUR OUTSOURCING PROFESIONAL SAS (en adelante, TECJUR SAS) es una sociedad constituida y domiciliada en la República de Colombia, cuyo objeto social consiste en la prestación de servicios de gestión, asesoría y representación legal, contable, administrativa, financiera y ambiental, dirigidos a empresas, personas naturales y comerciantes, mediante la implementación de soluciones apoyadas en herramientas tecnológicas y plataformas digitales.

En el desarrollo de sus actividades, TECJUR SAS se encuentra comprometida con la protección de los datos personales y con el respeto del derecho fundamental al habeas data y a la privacidad de sus clientes, empleados, proveedores y demás partes interesadas. En tal sentido, la presente Política de Tratamiento de Datos Personales establece los principios, lineamientos y procedimientos aplicables al tratamiento de datos personales, en cumplimiento de lo dispuesto en la Ley 1581 de 2012, el Decreto 1377 de 2013, las normas concordantes del ordenamiento jurídico colombiano y las directrices emitidas por la Superintendencia de Industria y Comercio. El objetivo de esta política es garantizar que los datos personales que sean objeto de tratamiento en el marco de las actividades de TECJUR SAS sean gestionados de manera lícita, ética, segura y transparente, asegurando el respeto y la protección de los derechos de los titulares, en especial los derechos de conocer, actualizar, rectificar, suprimir la información y revocar la autorización otorgada, conforme a la normativa vigente.

La presente política se estructura dentro de un marco normativo integral, mediante el cual TECJUR SAS se compromete a cumplir las disposiciones legales aplicables en Colombia y, como referencia de buenas prácticas, los estándares técnicos internacionales relacionados con la seguridad de la información y la protección de datos personales, con el fin de garantizar la confidencialidad, integridad y disponibilidad de la información. En este sentido, la Ley 1581 de 2012 establece el régimen general de protección de datos personales en Colombia y consagra los principios que rigen el tratamiento de datos personales, entre ellos:

1. Finalidad: Los datos personales deben ser recolectados para una finalidad específica, clara y legítima, la cual debe ser informada al titular.
2. Libertad: El tratamiento de datos personales solo puede realizarse con el consentimiento previo, expreso e informado del titular, salvo las excepciones legales.
3. Transparencia: Los titulares tienen derecho a obtener información clara y accesible sobre el tratamiento de sus datos personales.
4. Seguridad: El responsable y el encargado del tratamiento deben implementar medidas técnicas, humanas y administrativas que protejan los datos personales contra accesos no autorizados o tratamientos indebidos.

Así mismo, el Decreto 1377 de 2013, expedido para reglamentar parcialmente la Ley 1581 de 2012, desarrolla las obligaciones de los responsables y encargados del tratamiento, entre ellas:

- Informar a los titulares sobre la existencia de esta política y los mecanismos para el ejercicio de sus derechos.
- Obtener autorización previa, expresa e informada para el tratamiento de datos personales.
- Garantizar la veracidad, actualización y exactitud de la información.
- Implementar medidas de seguridad y confidencialidad acordes con la naturaleza de los datos tratados.

De manera complementaria, TECJUR SAS adopta como referencia las disposiciones de la Ley 1266 de 2008 (Ley de Habeas Data), especialmente en lo relacionado con las buenas prácticas para el tratamiento de información de carácter financiero, crediticio, comercial y de servicios, cuando resulte aplicable a los servicios prestados, observando principios como

la finalidad exclusiva, el derecho de supresión y la responsabilidad en la custodia de la información.

Igualmente, la presente política se apoya en las directrices contenidas en las Circulares Externas 052 de 2007 de la Superintendencia Financiera de Colombia y 002 de 2015 de la Superintendencia de Industria y Comercio, en cuanto desarrollan lineamientos sobre la protección de la información, el registro de bases de datos y la implementación de políticas de tratamiento de datos personales. Como parte de su compromiso con la seguridad de la información, TECJUR SAS adopta estándares internacionales reconocidos como referencia de buenas prácticas, entre ellos:

- a. NTC-ISO/IEC 27001:2013 – Sistemas de Gestión de Seguridad de la Información, orientada a garantizar la confidencialidad, integridad y disponibilidad de la información, mediante la gestión de riesgos, controles de acceso y procedimientos de respuesta a incidentes.
- b. NTC-ISO/IEC 27701:2019 – Gestión de la Privacidad de la Información, como extensión de la ISO 27001, que establece lineamientos para la protección de datos personales y la atención de los derechos de los titulares.
- c. Marco de Ciberseguridad del NIST, el cual proporciona directrices para la identificación, protección, detección, respuesta y recuperación frente a riesgos de ciberseguridad, contribuyendo a la continuidad operativa y a la protección de la información tratada en entornos digitales.

Este marco normativo y técnico fortalece las prácticas de TECJUR SAS en materia de protección de datos personales y seguridad de la información, asegurando un tratamiento responsable y conforme a la legislación colombiana vigente.

1. DEFINICIONES CLAVE

Con el fin de asegurar la claridad, uniformidad y correcta interpretación de la presente Política de Tratamiento de Datos Personales, a continuación se establecen las principales definiciones aplicables al tratamiento de datos personales realizado por TECJUR OUTSOURCING PROFESIONAL SAS (TECJUR SAS). Estas definiciones se encuentran alineadas con la legislación colombiana vigente, en especial la Ley 1581 de 2012 y el Decreto 1377 de 2013, así como con estándares internacionales de protección de datos, y deberán ser aplicadas de manera uniforme en todas las actividades de tratamiento desarrolladas por la sociedad.

- **1.1 Dato Personal.** Se entiende por Dato Personal cualquier información vinculada o que pueda asociarse, directa o indirectamente, a una persona natural determinada o determinable. Esta información puede referirse tanto a datos básicos de identificación como a información más específica que permita individualizar al titular.

Ejemplos de datos personales incluyen, entre otros: nombre completo, número de identificación, dirección física o electrónica, número de teléfono, información financiera, laboral o académica.

Tipos de Datos Personales:

- Datos de Identificación: Nombre, cédula de ciudadanía, pasaporte, fecha de nacimiento u otros datos que permitan identificar directamente al titular.
- Datos de Contacto: Dirección de residencia, correo electrónico, teléfono fijo o móvil.
- Datos Socioeconómicos y Laborales: Estado civil, nivel de ingresos, actividad económica, información laboral o referencias profesionales.

TECJUR SAS garantiza que el tratamiento de los datos personales se realizará respetando los principios de legalidad, finalidad, libertad, transparencia, seguridad y confidencialidad, conforme a la normativa aplicable.

- **1.2 Dato Sensible.** El Dato Sensible es aquel que afecta la intimidad del titular o cuyo tratamiento indebido puede generar discriminación. De conformidad con la Ley 1581 de 2012, los datos sensibles gozan de una protección reforzada y su suministro es facultativo.

El tratamiento de datos sensibles requiere autorización previa, expresa e informada del titular, salvo las excepciones previstas en la ley. Se consideran datos sensibles, entre otros:

- **Datos de Salud:** Información relacionada con el estado de salud, historial clínico, diagnósticos o tratamientos médicos.
- **Creencias Religiosas o Filosóficas.**
- **Opiniones Políticas.**
- **Pertenencia a Sindicatos, Asociaciones o Grupos Sociales.**
- **Origen Racial o Étnico.**
- **Datos Biométricos:** Huellas dactilares, reconocimiento facial, patrones de voz u otros datos destinados a identificar de manera inequívoca a una persona.

Tratamiento de Datos Sensibles: TECJUR SAS adopta medidas de seguridad reforzadas para el tratamiento de datos sensibles y garantiza el respeto de los derechos de los titulares a conocer, actualizar, rectificar y solicitar la supresión de dichos datos, salvo que exista un deber legal o contractual que impida su eliminación.

- **1.3 Responsable del Tratamiento** El Responsable del Tratamiento es la persona natural o jurídica, pública o privada, que decide sobre la recolección, uso y finalidad del tratamiento de los datos personales. En el marco de esta política, TECJUR SAS actúa como Responsable del Tratamiento de los datos personales tratados en desarrollo de sus actividades comerciales, administrativas y laborales.

En tal calidad, TECJUR SAS tiene las siguientes responsabilidades:

- a. **Definir las finalidades del tratamiento:** Determinar los fines lícitos, específicos y explícitos para los cuales se recolectan y tratan los datos personales.
- b. **Diseñar y actualizar políticas de tratamiento:** Elaborar, implementar y divulgar la presente Política de Tratamiento de Datos Personales.
- c. **Supervisar el tratamiento:** Verificar que el tratamiento de los datos personales se realice conforme a la normativa vigente y a las instrucciones impartidas a los encargados del tratamiento.

TECJUR SAS garantiza a los titulares el ejercicio efectivo de sus derechos de acceso, actualización, rectificación, supresión y revocatoria de la autorización, en los términos establecidos por la ley.

- **1.4 Encargado del Tratamiento** El Encargado del Tratamiento es la persona natural o jurídica, pública o privada, que realiza el tratamiento de datos personales por cuenta del Responsable del Tratamiento. En el contexto de TECJUR SAS, los encargados del tratamiento son, principalmente, proveedores de servicios tecnológicos y plataformas digitales que requieren acceso a datos personales para la ejecución de los servicios contratados.

Los encargados del tratamiento deberán cumplir, como mínimo, con las siguientes obligaciones:

- a. Tratar los datos personales conforme a esta política y a las instrucciones impartidas por TECJUR SAS.
- b. Implementar medidas técnicas, administrativas y organizativas adecuadas para garantizar la seguridad de la información.
- c. Mantener la confidencialidad de los datos personales y abstenerse de divulgarlos sin autorización.

TECJUR SAS suscribe con los encargados contratos y acuerdos de confidencialidad y de tratamiento de datos personales, en los que se establecen claramente las obligaciones, responsabilidades y niveles de seguridad exigidos.

- **1.5 Titular** El Titular es la persona natural a quien corresponden los datos personales objeto de tratamiento. En el ámbito de TECJUR SAS, los titulares pueden ser, entre otros, clientes, empleados, proveedores y usuarios de los servicios.

De conformidad con la Ley 1581 de 2012 y el Decreto 1377 de 2013, los titulares tienen los siguientes derechos:

- **Derecho de Acceso:** Conocer los datos personales que estén siendo tratados y la finalidad del tratamiento.
- **Derecho de Rectificación:** Solicitar la corrección o actualización de datos inexactos o incompletos.
- **Derecho de Supresión:** Solicitar la eliminación de los datos cuando haya cesado la finalidad o se retire la autorización, salvo obligación legal.
- **Derecho de Oposición:** Oponerse al tratamiento en los casos permitidos por la ley.
- **Derecho de Portabilidad:** Solicitar la entrega de sus datos en un formato estructurado, cuando sea legal y técnicamente procedente.

TECJUR SAS dispone de mecanismos claros, sencillos y accesibles para el ejercicio de estos derechos, a través de canales como el correo electrónico institucional, líneas de atención y su sitio web.

2. PRINCIPIOS DEL TRATAMIENTO DE DATOS PERSONALES

El tratamiento de datos personales realizado por **TECJUR OUTSOURCING PROFESIONAL SAS (TECJUR SAS)** se rige por los principios consagrados en la **Ley 1581 de 2012**, el **Decreto 1377 de 2013** y las demás disposiciones que regulan la protección de datos personales en Colombia. Estos principios constituyen el marco ético y legal que garantiza el tratamiento adecuado de la información y la protección efectiva de los derechos de los titulares. TECJUR SAS adopta y aplica de manera estricta los principios de **legalidad, finalidad, libertad, veracidad o calidad de los datos, transparencia, confidencialidad, seguridad, acceso y circulación restringida, y temporalidad**, los cuales se desarrollan a continuación:

2.1 Principio de Legalidad. El tratamiento de datos personales es una actividad reglada que solo puede realizarse conforme a lo dispuesto en la ley. De acuerdo con el artículo 4 de la Ley 1581 de 2012, todo tratamiento debe sujetarse a las disposiciones que regulan la materia. En aplicación de este principio, TECJUR SAS:

- a. Realiza el tratamiento de datos personales únicamente cuando exista una base jurídica válida.
- b. Se abstiene de adelantar actividades de tratamiento que no se encuentren expresamente permitidas por el ordenamiento jurídico.
- c. Garantiza el cumplimiento de la Ley 1581 de 2012, el Decreto 1377 de 2013 y las directrices impartidas por la Superintendencia de Industria y Comercio.

2.2 Principio de Finalidad

Los datos personales serán recolectados y tratados exclusivamente para fines **específicos, explícitos y legítimos**, los cuales serán informados previamente al titular, conforme al artículo 4 de la Ley 1581 de 2012. TECJUR SAS desarrolla este principio de la siguiente manera:

- a. **Información clara al titular:** Antes de la recolección de los datos, se informa de manera clara y suficiente la finalidad del tratamiento.

b. **Limitación del tratamiento:** Los datos personales no serán utilizados para finalidades distintas a las autorizadas por el titular, salvo disposición legal en contrario.

c. **Supresión de datos:** Una vez cumplida la finalidad, los datos serán eliminados, salvo que exista una obligación legal o contractual que exija su conservación.

2.3 Principio de Libertad. El tratamiento de datos personales solo puede realizarse con el consentimiento **libre, previo, expreso e informado** del titular, conforme al artículo 9 de la Ley 1581 de 2012. Para garantizar este principio, TECJUR SAS:

a. Obtiene autorizaciones claras e informadas, indicando la finalidad del tratamiento y los derechos del titular.

b. Permite al titular revocar su autorización en cualquier momento, siempre que no exista un deber legal o contractual que lo impida.

2.4 Principio de Veracidad o Calidad de los Datos

Los datos personales objeto de tratamiento deberán ser **veraces, completos, exactos, actualizados, comprobables y comprensibles**.

TECJUR SAS adopta medidas para garantizar la calidad de la información, tales como:

a. Actualización periódica de los datos.

b. Corrección o rectificación de información inexacta o incompleta.

c. Recolección limitada a los datos estrictamente necesarios para cumplir con la finalidad del tratamiento.

2.5 Principio de Transparencia Este principio garantiza el derecho del titular a obtener información clara, suficiente y accesible sobre el tratamiento de sus datos personales, en cualquier momento. En cumplimiento de este principio, TECJUR SAS:

a. Dispone de canales para consultas, solicitudes y reclamos.

b. Informa de manera clara sobre las finalidades del tratamiento, los encargados y las medidas de protección implementadas.

2.6 Principio de Confidencialidad. Todas las personas que intervengan en el tratamiento de datos personales están obligadas a guardar reserva sobre la información, incluso después de finalizada su relación con la actividad, conforme al artículo 18 de la Ley 1581 de 2012.

Para garantizar este principio, TECJUR SAS:

a. Restringe el acceso a los datos personales únicamente al personal autorizado.

b. Exige la suscripción de acuerdos de confidencialidad.

c. Garantiza la protección de la información una vez finalizada la relación laboral o contractual.

2.7 Principio de Seguridad. El principio de seguridad impone la obligación de adoptar medidas técnicas, humanas y administrativas necesarias para proteger los datos personales contra accesos no autorizados, pérdida, alteración o uso indebido. TECJUR SAS aplica, entre otras, las siguientes medidas:

a. Medidas técnicas, como controles de acceso, autenticación y cifrado.

b. Medidas organizativas, incluyendo capacitación permanente del personal.

c. Evaluaciones periódicas de riesgos y vulnerabilidades.

2.8 Principio de Acceso y Circulación Restringida. Los datos personales solo podrán ser tratados por personas autorizadas y no estarán disponibles en acceso público o irrestricto.

TECJUR SAS garantiza este principio mediante:

a. Autorizaciones previas de acceso.

b. Controles de permisos y autenticación.

c. Prohibición de divulgación sin autorización expresa del titular.

2.9 Principio de Temporalidad de la Información. Los datos personales serán conservados únicamente durante el tiempo necesario para cumplir la finalidad del tratamiento, conforme al Decreto 1377 de 2013.

a. **Conservación limitada:** Solo por el tiempo requerido legal o contractualmente.

b. **Eliminación o anonimización:** Una vez finalizada la finalidad del tratamiento.

La aplicación de estos principios permite a TECJUR SAS garantizar el cumplimiento del régimen de protección de datos personales en Colombia y establecer un marco ético y legal para el tratamiento responsable de la información personal.

3. DERECHOS DE LOS TITULARES

De conformidad con la **Constitución Política de Colombia**, la **Ley 1581 de 2012**, el **Decreto 1377 de 2013** y las demás normas concordantes en materia de protección de datos personales, los titulares de la información tienen derecho a **conocer, acceder, actualizar, rectificar, suprimir sus datos personales y revocar la autorización otorgada** para su tratamiento. No obstante, **TECJUR OUTSOURCING PROFESIONAL SAS (TECJUR SAS)** actúa exclusivamente como **intermediario** en la prestación de sus servicios y **no es responsable del almacenamiento, custodia ni tratamiento directo de los datos personales**, los cuales son gestionados de manera exclusiva por **proveedores externos de plataformas digitales**, con quienes TECJUR SAS mantiene relaciones contractuales y comerciales.

En consecuencia, el ejercicio de los derechos de los titulares deberá realizarse **directamente ante los terceros encargados del tratamiento**, conforme a sus políticas de privacidad y a la normativa vigente.

PROVEEDORES ENCARGADO DEL ALMACENAMIENTO DIRECTO DE LA INFORMACIÓN PERSONAL

PROVEEDOR	POLÍTICA DE PRIVACIDAD
Google	https://policies.google.com/privacy?hl=es
Colombia Informática	https://www.colombiainformatica.com/politicadeprivacidad.pdf
WIX	https://es.wix.com/about/privacy https://support.wix.com/es/article/reglamentos-de-protección-de-datos-y-usuarios-de-wix
Jotform	https://www.jotform.com/privacy/
MercadoPago	https://www.mercadopago.com.co/ayuda/terminos-condiciones_299
Telegram	https://telegram.org/privacy
WhatsApp Business	https://business.whatsapp.com/policy?lang=es_LA
Facebook	https://www.facebook.com/help/155833707900388
X (Twitter)	https://x.com/es/privacy https://x.com/es/tos
LinkedIn	https://es.linkedin.com/legal/privacy-policy
Instagram	https://privacycenter.instagram.com/policy https://help.instagram.com/515230437301944

3.1 EXONERACIÓN DE RESPONSABILIDAD. TECJUR SAS se exime de cualquier responsabilidad relacionada con el ejercicio, trámite, respuesta o cumplimiento de los derechos de los titulares de datos personales, en la medida en que el tratamiento, almacenamiento y custodia de dicha información es realizado de forma exclusiva por los proveedores externos anteriormente relacionados. No obstante, TECJUR SAS cumple con su deber de información y transparencia, orientando a los titulares sobre sus derechos y facilitando los datos de contacto de los encargados del tratamiento.

3.2 DERECHOS DE LOS TITULARES Y PROCEDIMIENTOS

3.2.1 Derecho de Acceso. El derecho de acceso permite al titular conocer, en cualquier momento, qué datos personales están siendo tratados, almacenados o utilizados, así como la finalidad del tratamiento, conforme al artículo 15 de la Constitución Política y al artículo 8 de la Ley 1581 de 2012.

Procedimiento:

- a. El titular deberá contactar directamente al proveedor encargado del almacenamiento.
- b. El proveedor deberá suministrar información clara, completa y actualizada sobre los datos tratados.

3.2.2 Derecho de Rectificación. El titular tiene derecho a solicitar la corrección, actualización o complementación de los datos personales que resulten inexactos, incompletos o desactualizados.

Procedimiento:

- a. El titular deberá presentar la solicitud directamente ante el proveedor encargado.
- b. El proveedor realizará la actualización conforme a la normativa aplicable y a sus políticas internas.

3.2.3 Derecho de Supresión. El titular podrá solicitar la eliminación de sus datos personales cuando haya cesado la finalidad del tratamiento, se haya revocado la autorización o el tratamiento no se ajuste a la ley, salvo que exista un deber legal de conservación.

Procedimiento:

- a. La solicitud deberá presentarse directamente ante el proveedor encargado del almacenamiento.
- b. El proveedor evaluará la solicitud y procederá conforme a la ley.
- c. TECJUR SAS no asume responsabilidad alguna frente a la supresión de los datos.

3.2.3 Derecho de Revocación del Consentimiento. El titular podrá revocar, en cualquier momento, la autorización otorgada para el tratamiento de sus datos personales, conforme al artículo 9 de la Ley 1581 de 2012.

Procedimiento:

- a. El titular deberá contactar directamente al proveedor encargado.
- b. El proveedor deberá cesar el tratamiento, salvo que exista obligación legal o contractual que lo impida.

3.3 ACLARACIÓN FINAL

TECJUR SAS informa que todas las solicitudes relacionadas con el ejercicio de los derechos de los titulares deberán ser tramitadas directamente con los proveedores encargados del tratamiento, quienes son los responsables legales de la administración, custodia y protección de los datos personales.

4. FINALIDADES DEL TRATAMIENTO DE DATOS

La finalidad del tratamiento de datos personales corresponde al **propósito específico, claro, legítimo y previamente informado** para el cual se recolecta, almacena, usa, circula o transmite información personal, de conformidad con lo dispuesto en la **Ley 1581 de 2012**, el **Decreto 1377 de 2013** y demás normas concordantes vigentes en la República de Colombia.

La normativa colombiana en materia de protección de datos personales establece que todo tratamiento debe encontrarse **debidamente justificado** y limitado de manera estricta al cumplimiento de las finalidades legítimas para las cuales el titular otorgó su autorización. En este contexto, **TECJUR OUTSOURCING PROFESIONAL SAS (TECJUR SAS)** actúa **únicamente como intermediario y facilitador de servicios**, mientras que la **recolección, almacenamiento, custodia y tratamiento efectivo de los datos personales** es realizada por **proveedores externos de plataformas digitales**. En consecuencia, **TECJUR SAS no asume responsabilidad directa** sobre la gestión, seguridad, conservación o eliminación de los datos personales tratados en dichas plataformas, sin perjuicio de su deber de informar y garantizar la transparencia frente a los titulares.

4.1 CONTEXTO LEGAL Y TÉCNICO DE LAS FINALIDADES DEL TRATAMIENTO DE DATOS EN COLOMBIA

De conformidad con el **artículo 4 de la Ley 1581 de 2012**, el tratamiento de datos personales en Colombia debe fundamentarse en los principios de **legalidad, finalidad, libertad, transparencia, acceso y circulación restringida, seguridad y confidencialidad**. En particular, el **principio de finalidad** exige que los datos personales sean recolectados y tratados **exclusivamente para objetivos específicos, explícitos y legítimos**, los cuales deben ser informados de manera clara y suficiente al titular antes de la obtención de su consentimiento.

Así mismo, el **Decreto 1377 de 2013** desarrolla el alcance práctico del principio de finalidad, imponiendo a las organizaciones el deber de informar detalladamente a los titulares sobre el uso que se dará a sus datos personales. En este sentido, el titular debe conocer, como mínimo:

- Quién realiza la recolección y el tratamiento de los datos (en este caso, los **proveedores de plataformas digitales contratados por TECJUR SAS**).
- Con qué propósito específico se recopilan, procesan y utilizan los datos personales.
- Durante cuánto tiempo serán tratados y almacenados los datos personales.

En cumplimiento de estas disposiciones, TECJUR SAS informa a los titulares sobre las finalidades generales del tratamiento, aclarando expresamente que la **recolección, almacenamiento y tratamiento directo de los datos personales en plataformas digitales de terceros es responsabilidad exclusiva de dichos proveedores**.

4.2 FINALIDADES ESPECÍFICAS DEL TRATAMIENTO DE DATOS EN TECJUR SAS

Dado el rol de **intermediario** que desempeña TECJUR SAS, las finalidades del tratamiento de datos personales en las plataformas digitales utilizadas se limitan a los **fines comerciales, administrativos y operativos** estrictamente necesarios para la prestación de los servicios ofrecidos. Los datos personales se recolectan principalmente para facilitar la comunicación, contratación, ejecución y seguimiento de los servicios, sin que TECJUR SAS almacene o administre directamente dicha información.

A. Gestión Comercial y Operativa de los Servicios Los datos personales recolectados en plataformas digitales externas podrán ser utilizados para:

- Facilitar el contacto con clientes, proveedores y partes interesadas para el desarrollo de actividades comerciales, administrativas y contractuales.
- Realizar el seguimiento de contratos, solicitudes de servicios y gestiones efectuadas a través de formularios digitales y plataformas externas.

Nota: TECJUR SAS informa de manera expresa que el proveedor de la plataforma utilizada es el **responsable de la gestión, custodia y seguridad de los datos**, limitándose TECJUR SAS a coordinar y supervisar la prestación del servicio, sin almacenar directamente la información recolectada.

B. Comunicación y Promoción de Servicios. Las plataformas digitales de terceros podrán recolectar información personal con el fin de enviar comunicaciones, información institucional, novedades y promociones relacionadas con los servicios ofrecidos por TECJUR SAS, bajo las siguientes condiciones:

- ✓ Las comunicaciones se realizarán únicamente con la **autorización previa, expresa e informada del titular**.
- ✓ El titular podrá solicitar, en cualquier momento, la suspensión de dichas comunicaciones, dirigiéndose directamente al proveedor encargado de la plataforma.

Exoneración de Responsabilidad: La gestión, control y seguridad de los datos utilizados para fines promocionales es responsabilidad exclusiva de los proveedores de las plataformas digitales. TECJUR SAS no retiene, almacena ni administra directamente esta información.

C. Atención al Cliente y Soporte Para la adecuada atención de solicitudes, consultas, quejas o requerimientos, las plataformas de terceros podrán recopilar y tratar datos personales tales como nombres, datos de contacto y detalles de la solicitud presentada. Los proveedores externos recopilan esta información mediante formularios de contacto, sistemas de mensajería o plataformas de chat integradas en sitios web o redes sociales. La **custodia, seguridad y tratamiento** de dichos datos es responsabilidad directa de los proveedores.

D. Cumplimiento de Obligaciones Legales y Contractuales En determinados casos, la información recolectada a través de plataformas de terceros podrá ser utilizada para el cumplimiento de obligaciones legales o contractuales, tales como requerimientos de autoridades competentes o disposiciones de carácter fiscal, contable o administrativo. En estos eventos:

- ❖ El tratamiento de los datos se realizará bajo la **responsabilidad directa del proveedor externo**.
- ❖ TECJUR SAS garantiza la transparencia informando al titular sobre el proveedor que almacena y gestiona sus datos.

4.3 RESPONSABILIDAD DE LOS PROVEEDORES EXTERNOS EN EL TRATAMIENTO DE DATOS

Dado que TECJUR SAS no almacena, conserva ni procesa directamente los datos personales, la responsabilidad del tratamiento recae **íntegramente en los proveedores externos**, quienes actúan como **encargados del tratamiento** y están obligados a:

- Custodiar y proteger los datos personales mediante medidas de seguridad técnicas, físicas y administrativas.
- Atender y responder las solicitudes de los titulares en ejercicio de sus derechos
- Cumplir con la normativa colombiana de protección de datos personales conforme a las finalidades autorizadas.

4.4 EXONERACIÓN DE RESPONSABILIDAD DE TECJUR SAS

TECJUR SAS **no se hace responsable** de la gestión, custodia, protección o tratamiento directo de los datos personales recolectados en plataformas de terceros, limitándose a coordinar la prestación de servicios y a garantizar la transparencia mediante la divulgación de las políticas de privacidad y términos de uso de cada proveedor.

4.5 FINALIDADES EXCLUSIVAS DE LOS PROVEEDORES DE PLATAFORMAS DIGITALES

Cada proveedor de plataforma digital contratado por TECJUR SAS debe definir y publicar sus propias finalidades de tratamiento de datos personales, las cuales comprenden, entre otras, la gestión técnica, administración de la información y seguridad de sus sistemas. En consecuencia:

- ❖ Los proveedores deberán informar claramente al titular sobre el uso de sus datos y los mecanismos para ejercer sus derechos.
- ❖ Cualquier finalidad adicional deberá ser autorizada expresamente por el titular, sin intervención de TECJUR SAS.

4.6 CANAL DE CONTACTO PARA INFORMACIÓN SOBRE FINALIDADES DEL TRATAMIENTO

En cumplimiento de su deber de información, TECJUR SAS pone a disposición de los titulares el siguiente canal de contacto para orientar sobre los proveedores encargados y sus políticas de tratamiento:  tecjur@tecjursas.com TECJUR SAS brindará asistencia informativa para identificar al proveedor correspondiente, **eximiéndose de cualquier responsabilidad frente al tratamiento directo de los datos personales.**

5. RECOLECCIÓN Y ALMACENAMIENTO DE DATOS

La recolección y el almacenamiento de datos personales constituyen **etapas esenciales y críticas** dentro del proceso de tratamiento de datos, las cuales deben ejecutarse en **estricto cumplimiento del marco normativo vigente en Colombia**, así como de las normas técnicas nacionales e internacionales en materia de seguridad de la información y protección de datos personales.

En este contexto, **TECJUR OUTSOURCING PROFESIONAL SAS (TECJUR SAS)** actúa exclusivamente como **intermediario** en la recolección de datos personales, la cual se realiza a través de **plataformas digitales administradas por proveedores externos**. En consecuencia, **TECJUR SAS NO ES RESPONSABLE DIRECTO DEL ALMACENAMIENTO, CUSTODIA NI GESTIÓN DE LOS DATOS PERSONALES**, siendo dichas funciones asumidas íntegramente por los proveedores de servicios tecnológicos, quienes ostentan la calidad de **encargados del tratamiento** y son responsables de la protección de la información recolectada en sus sistemas.

La presente política de recolección y almacenamiento de datos se fundamenta en el cumplimiento de la **Ley 1581 de 2012**, el **Decreto 1377 de 2013**, la **Ley 1266 de 2008**, así como en las demás disposiciones legales, reglamentarias y técnicas que promueven un tratamiento **seguro, responsable, transparente y conforme a los derechos de los titulares de los datos personales**.

5.1 FUNDAMENTO NORMATIVO PARA LA RECOLECCIÓN Y ALMACENAMIENTO DE DATOS EN COLOMBIA

La Ley 1581 de 2012 (Ley de Protección de Datos Personales) establece que todo tratamiento de datos personales debe respetar los principios de finalidad, libertad, veracidad o calidad, transparencia, acceso y circulación restringida, seguridad y confidencialidad. Bajo el principio de finalidad, los datos personales deben ser recolectados únicamente para fines específicos, explícitos y legítimos, los cuales deben ser informados previamente al titular. El principio de libertad exige que la recolección se realice con el consentimiento previo, expreso e informado del titular, mientras que el principio de seguridad impone la obligación de adoptar medidas para proteger los datos frente a accesos no autorizados, pérdida, alteración o uso indebido.

El Decreto Reglamentario 1377 de 2013 desarrolla aspectos esenciales de la Ley 1581 de 2012, estableciendo los procedimientos para la obtención del consentimiento, los mecanismos de información al titular y las medidas mínimas de seguridad exigibles durante el almacenamiento de datos personales. Dicho decreto exige, además, que los responsables y encargados del tratamiento implementen sistemas de control, protección y gestión de riesgos que garanticen la integridad, confidencialidad y disponibilidad de la información.

Adicionalmente, TECJUR SAS adopta principios y prácticas de protección de la información y de los derechos de los titulares conforme a la Ley 1266 de 2008, la cual garantiza la calidad de los datos personales, exigiendo que estos sean veraces, completos, exactos y actualizados, requisitos que TECJUR SAS impone contractualmente a sus proveedores encargados del almacenamiento de los datos.

Así mismo, se observan las disposiciones contenidas en:

- Circular Externa 052 de 2007 de la Superintendencia Financiera de Colombia, que establece lineamientos sobre la protección de la información en el sector financiero. Aunque TECJUR SAS no administra directamente datos financieros, adopta estas directrices como buenas prácticas para exigir altos estándares de confidencialidad y seguridad a sus proveedores.
- Circular Externa 002 de 2015 de la Superintendencia de Industria y Comercio (SIC), la cual establece criterios para la implementación de políticas de tratamiento de datos personales y la obligación de garantizar a los titulares información clara y accesible sobre la gestión de sus datos.

5.2 NORMAS INTERNACIONALES DE SEGURIDAD Y PROTECCIÓN DE DATOS

TECJUR SAS exige a sus proveedores de plataformas digitales la adopción y/o implementación de normas técnicas internacionales reconocidas en materia de seguridad de la información y protección de datos personales, entre ellas:

- ✓ NTC-ISO/IEC 27001:2013 – Sistemas de Gestión de Seguridad de la Información, orientada a garantizar la confidencialidad, integridad y disponibilidad de la información.
- ✓ NTC-ISO/IEC 27002:2013 – Código de Prácticas para la Gestión de Seguridad de la Información, que establece controles específicos para prevenir accesos no autorizados y gestionar incidentes de seguridad.
- ✓ NTC-ISO/IEC 27701:2019 – Extensión para la Gestión de Información de Privacidad, que define requisitos adicionales para el tratamiento seguro y ético de datos personales.
- ✓ NTC-ISO/IEC 29100:2011 – Marco de Privacidad, que establece principios y definiciones para la protección de la privacidad.
- ✓ NTC-ISO/IEC 22301:2012 – Sistema de Gestión de Continuidad del Negocio, orientado a asegurar la resiliencia operativa y la protección de datos ante incidentes.
- ✓ Marco de Ciberseguridad del NIST, que proporciona directrices para identificar, proteger, detectar, responder y recuperar frente a incidentes de seguridad de la información.

5.3 PROCEDIMIENTOS PARA LA RECOLECCIÓN DE DATOS

La recolección de datos personales en el contexto de TECJUR SAS se realiza exclusivamente a través de plataformas digitales de terceros, las cuales cumplen con el marco normativo colombiano e internacional de protección de datos. Los datos recolectados pueden incluir información de contacto, identificadores únicos y datos necesarios para la prestación de servicios y comunicaciones de interés. En todo caso, la recolección se efectúa únicamente con el consentimiento previo, expreso e informado del titular, y los datos son utilizados de manera exclusiva para las finalidades definidas en la presente política.

En aplicación del principio de responsabilidad en la recolección, TECJUR SAS informa de manera expresa a los titulares que la recolección se realiza en plataformas de terceros, quienes son los únicos responsables del tratamiento directo, almacenamiento y gestión de los datos, incluyendo el cumplimiento normativo y la implementación de mecanismos de seguridad y gestión de riesgos.

5.4 RESPONSABILIDAD DEL ALMACENAMIENTO DE DATOS

TECJUR SAS aclara que no almacena ni custodia datos personales en sus propios sistemas, siendo dicha actividad desarrollada por proveedores externos de plataformas digitales, quienes son responsables de:

- ❖ Custodiar los datos conforme a los estándares de seguridad de la información exigidos.
- ❖ Implementar políticas de acceso restringido para prevenir accesos no autorizados.
- ❖ Cumplir con la normativa colombiana de protección de datos y con normas técnicas internacionales aplicables.

Exoneración de Responsabilidad: TECJUR SAS se exime de cualquier responsabilidad relacionada con la gestión directa, protección o administración de los datos personales recolectados, recayendo el control de acceso, cifrado, integridad y disponibilidad exclusivamente en los proveedores externos.

5.5 MEDIDAS DE SEGURIDAD EN LA RECOLECCIÓN Y ALMACENAMIENTO

Los proveedores de plataformas contratados por TECJUR SAS deben adoptar medidas de seguridad avanzadas, entre ellas:

- A. Seguridad Técnica y Física Implementación de autenticación multifactor, monitoreo de accesos, controles físicos y auditorías de seguridad.
- B. Gestión de Riesgos Evaluaciones periódicas de riesgos y vulnerabilidades, con estrategias de mitigación documentadas.
- C. Auditorías y Revisiones Periódicas Auditorías regulares de cumplimiento normativo y técnico, con disponibilidad para inspección por autoridades competentes.
- D. Capacitación y Conciencia. Capacitación continua del personal con acceso a datos personales, garantizando la correcta aplicación de las políticas de seguridad.

5.6 PROCEDIMIENTOS PARA LA RETENCIÓN Y ELIMINACIÓN DE DATOS

Los proveedores de TECJUR SAS deben aplicar políticas de retención de datos acordes con la finalidad del tratamiento y con la normativa vigente. Una vez cumplida la finalidad, los datos deberán ser eliminados de forma segura, evitando cualquier posibilidad de recuperación no autorizada.

5.7 DERECHOS DE LOS TITULARES EN EL CONTEXTO DE RECOLECCIÓN Y ALMACENAMIENTO

Los titulares de datos personales podrán ejercer sus derechos de acceso, rectificación, supresión y revocatoria del consentimiento directamente ante los proveedores de plataformas digitales, quienes son responsables de atender dichas solicitudes conforme a la legislación aplicable.

6. MEDIDAS DE SEGURIDAD

La protección de los datos personales recolectados y tratados mediante plataformas digitales gestionadas por proveedores externos constituye un aspecto **esencial y transversal** para garantizar la **seguridad, privacidad, confidencialidad, integridad y disponibilidad** de la información. En tal sentido, **TECJUR OUTSOURCING PROFESIONAL SAS (TECJUR SAS)** promueve, exige y supervisa el cumplimiento de medidas estrictas de seguridad, tanto **técnicas** como **organizativas, administrativas y físicas**, dirigidas a los proveedores de servicios digitales que captan, almacenan, administran y gestionan información personal asociada a los titulares. Estas medidas se implementan en armonía con el marco normativo colombiano vigente, particularmente con la **Ley 1581 de 2012**, el **Decreto 1377 de 2013**, la **Ley 1266 de 2008**, y las directrices administrativas complementarias contenidas en las **Circulares Externas 052 de 2007** (Superintendencia Financiera de Colombia) y **002 de 2015** (Superintendencia de Industria y Comercio – SIC), en cuanto establecen lineamientos sobre seguridad, custodia, control y buenas prácticas aplicables al tratamiento de información.

Así mismo, como referencia de buenas prácticas y estándares internacionalmente reconocidos, TECJUR SAS se alinea con normas técnicas como la **NTC-ISO/IEC 27001:2013**, la **NTC-ISO/IEC 27002:2013**, la **NTC-ISO/IEC 27701:2019**, la **NTC-ISO/IEC 29100:2011**, la **NTC-ISO/IEC 22301:2012**, y con el **Marco de Ciberseguridad del NIST**, con el fin de asegurar que los proveedores adopten controles robustos, verificables y trazables en la gestión de seguridad de la información.

En todo caso, se precisa que, aunque TECJUR SAS puede tener acceso funcional a ciertos datos para la adecuada prestación de los servicios, el **almacenamiento, administración y control directo de los datos personales es responsabilidad exclusiva de los proveedores**

externos, quienes actúan como **encargados del tratamiento** y, por tanto, deben garantizar la protección de la información conforme a sus propias políticas y a las obligaciones contractuales y legales aplicables.

6.1 CUMPLIMIENTO NORMATIVO EN SEGURIDAD DE LA INFORMACIÓN

La implementación de medidas de seguridad en la gestión de datos personales debe observar tanto las disposiciones legales nacionales como los estándares técnicos internacionales aplicables. En este sentido, TECJUR SAS exige que los proveedores se adhieran de manera estricta a los siguientes marcos normativos y criterios de cumplimiento:

a) Ley 1581 de 2012. La Ley 1581 de 2012 consagra el **principio de seguridad** como una de las bases del tratamiento adecuado de datos personales, estableciendo que los responsables y encargados deberán adoptar medidas necesarias para evitar la adulteración, pérdida, consulta, uso o acceso no autorizado o fraudulento. En concordancia con el deber previsto en el **artículo 17**, los proveedores deberán implementar medidas efectivas para proteger los datos contra accesos indebidos, alteración o pérdida.

b) Decreto 1377 de 2013 El Decreto 1377 de 2013 desarrolla la obligación de establecer procedimientos para el manejo seguro de la información, e impone a responsables y encargados implementar medidas **técnicas, administrativas y físicas** adecuadas para proteger los datos personales. Así mismo, exige garantizar mecanismos documentados de control que permitan evidenciar cumplimiento, trazabilidad y respuesta ante incidentes.

c) Ley 1266 de 2008 (Habeas Data – Sector Financiero) Aunque esta norma se refiere especialmente al tratamiento de datos de naturaleza financiera, crediticia, comercial y de servicios, TECJUR SAS adopta sus lineamientos como referencia de buenas prácticas, particularmente en materia de custodia reforzada, integridad y control de información. Por ello, exige a sus proveedores la adopción de estándares elevados de seguridad, incluso en escenarios donde se trate información relacionada con pagos electrónicos, operaciones comerciales o datos de contacto asociados a transacciones.

d) Circulares Externas 052 de 2007 y 002 de 2015 Las Circulares Externas 052 de 2007 y 002 de 2015 establecen lineamientos complementarios sobre protección y manejo seguro de la información, supervisión, control del tratamiento de datos, medidas de administración del riesgo, y requisitos para garantizar un control estricto sobre el acceso, la disponibilidad, la integridad y el uso autorizado de la información, especialmente en entornos digitales y plataformas tecnológicas.

6.2 ESTÁNDARES INTERNACIONALES DE SEGURIDAD Y PRIVACIDAD EXIGIDOS

Para TECJUR SAS, la aplicación de estándares internacionales de seguridad y privacidad constituye un elemento clave para garantizar un nivel adecuado de protección de los datos personales tratados por sus proveedores. En consecuencia, se exige la adopción de los siguientes estándares:

- ✓ **NTC-ISO/IEC 27001:2013 – Sistemas de Gestión de Seguridad de la Información (SGSI):** Establece los requisitos para implementar un SGSI basado en gestión de riesgos y controles de seguridad para proteger la confidencialidad, integridad y disponibilidad.
- ✓ **NTC-ISO/IEC 27002:2013 – Código de Prácticas:** Define controles específicos sobre acceso, redes, seguridad física, desarrollo de sistemas, mantenimiento, continuidad y gestión operativa de seguridad.
- ✓ **NTC-ISO/IEC 27701:2019 – Gestión de Privacidad de la Información:** Extiende ISO 27001 con controles orientados al tratamiento de datos personales, atención de derechos del titular, minimización, protección y gobernanza.
- ✓ **NTC-ISO/IEC 29100:2011 – Marco de Privacidad:** Define principios de privacidad y buenas prácticas para el tratamiento responsable de datos personales.
- ✓ **NTC-ISO/IEC 22301:2012 – Continuidad del Negocio:** Obliga a la existencia de planes de continuidad y recuperación para mantener la disponibilidad y protección de datos ante eventos críticos.

- ✓ **Marco de Ciberseguridad del NIST:** Establece una estructura funcional para la gestión del riesgo mediante los pilares: identificar, proteger, detectar, responder y recuperar.

6.3 MEDIDAS TÉCNICAS DE SEGURIDAD EXIGIDAS A LOS PROVEEDORES

Con el fin de proteger los datos personales, TECJUR SAS exige a sus proveedores implementar medidas técnicas mínimas, reforzadas y verificables, incluyendo:

1. **Cifrado de Datos:** Implementación de cifrado en tránsito y en reposo, con algoritmos y protocolos robustos, con el fin de impedir accesos no autorizados.
2. **Control de Acceso:** Controles basados en roles, autenticación multifactor y principio de mínimo privilegio, restringiendo el acceso únicamente al personal autorizado.
3. **Monitoreo de Seguridad:** Sistemas de detección de intrusiones, monitoreo continuo, alertas y trazabilidad que permitan detectar actividades sospechosas en tiempo real.
4. **Respaldo y Recuperación:** Procedimientos periódicos de respaldo, redundancia, recuperación y pruebas de restauración para asegurar continuidad y disponibilidad de la información.

6.4 MEDIDAS ORGANIZATIVAS Y FÍSICAS DE SEGURIDAD

Además de las medidas técnicas, TECJUR SAS requiere que los proveedores adopten controles organizacionales y físicos para garantizar la protección integral, entre ellos:

1. **Restricción de Acceso Físico:** Limitación de acceso a centros de datos o infraestructuras tecnológicas mediante controles físicos, registros y protocolos de seguridad.
2. **Capacitación y Conciencia:** Programas formativos permanentes en seguridad de la información, privacidad, gestión de incidentes y prevención del riesgo humano.
3. **Gestión de Incidentes:** Procedimientos documentados de detección, escalamiento, respuesta, mitigación y notificación de incidentes de seguridad, incluyendo brechas de información cuando sea aplicable.
4. **Auditorías y Revisiones:** Auditorías internas y externas periódicas para evaluar efectividad de controles, cumplimiento normativo y mejora continua.

6.5 GESTIÓN DE RIESGOS Y EVALUACIÓN CONTINUA

TECJUR SAS exige que los proveedores realicen evaluaciones periódicas de riesgos para identificar, reducir y mitigar vulnerabilidades, incluyendo:

- ✓ **Análisis de Riesgos:** Identificación de amenazas, vulnerabilidades e impactos sobre la seguridad de los datos personales, con planes de acción y controles preventivos.
- ✓ **Pruebas de Penetración:** Evaluaciones técnicas de seguridad y pruebas de resiliencia sobre sistemas críticos, con corrección de hallazgos y planes de mejora.

6.6 ACCESO Y LIMITACIONES DE RESPONSABILIDAD DE TECJUR SAS

Si bien TECJUR SAS puede acceder a la información en función de la prestación de servicios y el desarrollo de sus finalidades operativas, dicho acceso se limita estrictamente al uso autorizado por el titular, conforme a la finalidad informada y a los términos contractuales aplicables. En todo caso, la **administración, custodia, almacenamiento y seguridad** de los datos personales tratados en las plataformas digitales corresponde de manera directa a los proveedores externos, quienes deben aplicar todas las medidas necesarias y exigibles.

Exoneración de responsabilidad: TECJUR SAS se exime de cualquier responsabilidad relacionada con la seguridad, custodia o almacenamiento directo de los datos personales, en la medida en que estas funciones son ejecutadas y gestionadas exclusivamente por proveedores externos, quienes asumen las obligaciones de seguridad técnicas, organizativas, administrativas y físicas, así como la atención y respuesta ante incidentes que comprometan la integridad, confidencialidad o disponibilidad de la información.

7. TRANSFERENCIA Y TRANSMISIÓN DE DATOS A TERCEROS

La **transferencia y transmisión de datos personales a terceros** constituye un elemento esencial dentro del ciclo de tratamiento de datos personales, en tanto garantiza que dicho tratamiento se realice de manera **segura, controlada, transparente y conforme a los principios de confidencialidad, privacidad, legalidad y responsabilidad demostrada**. En el ordenamiento jurídico colombiano, la **Ley 1581 de 2012**, el **Decreto 1377 de 2013**, la **Ley 1266 de 2008** y demás disposiciones reglamentarias vigentes regulan las condiciones bajo las cuales los datos personales pueden ser transferidos o transmitidos a terceros, imponiendo la obligación de informar de manera previa al titular y de obtener su consentimiento cuando así lo exija la ley.

En este contexto, **TECJUR OUTSOURCING PROFESIONAL SAS (TECJUR SAS)** actúa como **intermediario funcional** en la gestión de datos personales, teniendo acceso limitado a la información estrictamente necesaria para la prestación de sus servicios profesionales. No obstante, la **responsabilidad directa sobre el almacenamiento, custodia, administración y tratamiento técnico de los datos personales recae en proveedores externos**, quienes operan como **encargados del tratamiento** y son los responsables de ejecutar las transferencias o transmisiones de datos requeridas para el cumplimiento de los servicios contratados, así como de garantizar el cumplimiento integral de la normativa de protección de datos personales aplicable.

7.1 MARCO NORMATIVO DE LA TRANSFERENCIA Y TRANSMISIÓN DE DATOS EN COLOMBIA

La transferencia y transmisión de datos personales en Colombia se rige por el régimen general de protección de datos personales, el cual establece que todo tratamiento, y en particular la transmisión o transferencia de información a terceros, debe respetar los **principios de finalidad, libertad, seguridad, confidencialidad, acceso restringido y transparencia**.

Conforme a la **Ley 1581 de 2012**, el tratamiento de datos personales solo puede realizarse cuando exista una base legal válida, principalmente el **consentimiento previo, expreso e informado del titular**, o cuando la transferencia sea necesaria para la ejecución de una relación contractual, el cumplimiento de una obligación legal o alguna de las excepciones previstas por la ley. El **Decreto 1377 de 2013** reglamenta de manera específica la **transferencia nacional e internacional de datos personales**, estableciendo que, en los casos en que los datos sean transferidos o transmitidos a terceros ubicados fuera del territorio colombiano, el país receptor deberá contar con **niveles adecuados de protección de datos equivalentes o superiores** a los exigidos por la legislación colombiana, o en su defecto, deberán adoptarse garantías contractuales, técnicas y organizativas que aseguren la protección efectiva de los datos.

En cumplimiento de estas disposiciones, **TECJUR SAS informa a los titulares sobre la existencia de transferencias o transmisiones internacionales** y exige a sus proveedores la verificación y cumplimiento de los estándares de seguridad y protección exigidos por la normativa vigente.

7.2 APLICACIÓN DE LA LEY DE HABEAS DATA Y DIRECTRICES ADMINISTRATIVAS

La **Ley 1266 de 2008 (Ley de Habeas Data)**, aunque orientada principalmente al sector financiero, refuerza los principios de **calidad, seguridad, veracidad e integridad de los datos** cuando estos son objeto de transferencia o transmisión a terceros. TECJUR SAS adopta estos principios como referencia obligatoria de buenas prácticas, exigiendo a sus proveedores que las transferencias de datos se realicen garantizando la exactitud, actualización y protección de la información.

De igual manera, la **Circular Externa 052 de 2007** de la Superintendencia Financiera de Colombia establece directrices sobre la **transferencia segura de información sensible**, promoviendo estándares de seguridad y confidencialidad que TECJUR SAS incorpora en

sus relaciones contractuales con proveedores. Así mismo, la **Circular Externa 002 de 2015** de la Superintendencia de Industria y Comercio (SIC) exige que responsables y encargados del tratamiento implementen políticas claras de privacidad y seguridad que incluyan procedimientos específicos para la transferencia y transmisión de datos personales.

7.3 ESTÁNDARES INTERNACIONALES APLICABLES A LA TRANSFERENCIA DE DATOS

Con el fin de garantizar una infraestructura tecnológica robusta y segura, TECJUR SAS exige que sus proveedores adopten estándares internacionales de seguridad y privacidad de la información aplicables a la transferencia y transmisión de datos personales, entre ellos:

- **Sistemas de Gestión de Seguridad de la Información (ISO/IEC 27001):** Orientados a establecer controles que protejan la información durante su transmisión o transferencia.
- **Código de Prácticas para la Gestión de Seguridad de la Información (ISO/IEC 27002):** Marco de referencia para implementar medidas técnicas y organizativas que prevengan accesos no autorizados durante la transferencia de datos.
- **ISO/IEC 27701 – Gestión de Información de Privacidad:** Extensión de la ISO 27001 que introduce controles específicos para la protección de datos personales durante procesos de transmisión y transferencia.
- **Marco de Privacidad (ISO/IEC 29100):** Define principios y prácticas de privacidad aplicables a la circulación de información personal.
- **Sistema de Gestión de Continuidad del Negocio (ISO/IEC 22301):** Exige planes de continuidad que aseguren la protección de los datos frente a interrupciones o incidentes que afecten su transmisión.
- **Marco de Ciberseguridad del NIST:** Proporciona directrices para identificar, proteger, detectar, responder y recuperar la información durante procesos de transmisión y transferencia.

7.4 TIPOS DE TRANSFERENCIA Y TRANSMISIÓN DE DATOS

a) Transferencia Internacional de Datos

La transferencia de datos personales a terceros ubicados fuera de Colombia requiere la verificación previa de que el país receptor cuente con un nivel adecuado de protección de datos o que el proveedor haya implementado garantías suficientes que aseguren la confidencialidad, integridad y disponibilidad de la información. TECJUR SAS exige a sus proveedores el cumplimiento estricto de estas condiciones en toda transferencia internacional.

b) Transmisión de Datos a Proveedores y Aliados Estratégicos

Para la adecuada prestación de sus servicios, TECJUR SAS puede autorizar la transmisión de datos personales a proveedores o aliados estratégicos que actúan en su nombre. Dichas transmisiones se encuentran sujetas a **acuerdos contractuales de confidencialidad, cláusulas de protección de datos y obligaciones de seguridad**, garantizando el tratamiento responsable de la información.

7.5 OBLIGACIONES DE LOS PROVEEDORES EN LA TRANSFERENCIA Y TRANSMISIÓN

Dado que TECJUR SAS no es responsable directo del almacenamiento o procesamiento técnico de los datos personales, se exige a los proveedores que implementen medidas estrictas en cada etapa de la transferencia o transmisión, incluyendo:

- a) Cumplir integralmente la normativa colombiana de protección de datos y las obligaciones contractuales pactadas con TECJUR SAS.
- b) Implementar controles técnicos y organizativos como cifrado, autenticación robusta y monitoreo de accesos durante la transmisión.
- c) Garantizar que toda transferencia o transmisión cuente con el consentimiento expreso del titular y se limite a las finalidades autorizadas.

7.6 EXONERACIÓN DE RESPONSABILIDAD DE TECJUR SAS

Si bien TECJUR SAS puede acceder a la información necesaria para la prestación de servicios, la **transferencia y transmisión de datos personales es gestionada exclusivamente por proveedores externos**, quienes actúan como encargados del tratamiento. En consecuencia, **TECJUR SAS se exime de cualquier responsabilidad**

relacionada con la administración, custodia, seguridad y cumplimiento normativo en la transmisión o transferencia de datos personales, en la medida en que dichas funciones son ejecutadas y supervisadas por los proveedores.

7.7 MEDIDAS DE SEGURIDAD EN LA TRANSFERENCIA Y TRANSMISIÓN DE DATOS

Con el fin de asegurar la confidencialidad, integridad y disponibilidad de los datos durante su circulación, TECJUR SAS exige a sus proveedores implementar, como mínimo, las siguientes medidas:

Primero. Cifrado de la información en tránsito mediante protocolos seguros.

Segundo. Autenticación robusta y control de acceso para restringir el uso de la información a personal autorizado.

Tercero. Monitoreo continuo, registros de actividad y auditorías periódicas para prevenir accesos indebidos o incidentes de seguridad.

7.8 PROCEDIMIENTO PARA LA TRANSFERENCIA DE DATOS PERSONALES

- ✓ **Notificación al Titular:** TECJUR SAS informa a los titulares que los proveedores encargados del tratamiento pueden transferir o transmitir datos personales a terceros para fines específicos relacionados con la prestación de servicios, siempre que se garantice el cumplimiento normativo y un nivel adecuado de seguridad.
- ✓ **Contratos de Transferencia y Transmisión:** Los contratos celebrados entre TECJUR SAS y sus proveedores incluyen cláusulas específicas de confidencialidad, seguridad y protección de datos, que obligan a la implementación de medidas técnicas, administrativas y organizativas durante todo el proceso de transferencia de información.

8. RECOLECCIÓN DE DATOS MEDIANTE PLATAFORMAS DE TERCEROS

La recolección de datos personales mediante plataformas de terceros permite a **TECJUR OUTSOURCING PROFESIONAL SAS (TECJUR SAS)** gestionar información de clientes, proveedores, aliados, usuarios y demás partes interesadas de manera eficiente, manteniendo un enfoque de **transparencia, confidencialidad, seguridad de la información y cumplimiento normativo**. TECJUR SAS se adhiere estrictamente al marco regulatorio colombiano, en especial a la **Ley 1581 de 2012**, el **Decreto 1377 de 2013**, la **Ley 1266 de 2008**, así como a las directrices emitidas por la **Superintendencia de Industria y Comercio (SIC)** y, en lo pertinente como buenas prácticas, las circulares aplicables en materia de seguridad de la información.

Es fundamental precisar que **TECJUR SAS actúa como intermediario y facilitador** en la recolección de datos personales cuando la captura se efectúa mediante plataformas digitales administradas por terceros. En consecuencia, el **almacenamiento, gestión, custodia, administración técnica y operación de dichas plataformas** constituye una responsabilidad directa de los **proveedores tecnológicos**, quienes operan como **encargados del tratamiento**, y por tanto deben implementar las medidas de seguridad exigidas por la normativa aplicable, garantizando la adecuada protección de la información y la atención de los derechos de los titulares conforme al marco legal vigente. En Colombia, la recolección de datos personales se encuentra regulada principalmente por la **Ley 1581 de 2012**, la cual exige el **consentimiento previo, expreso e informado** del titular, y por el **Decreto 1377 de 2013**, que desarrolla condiciones de transparencia, deber de información y reglas operativas para el tratamiento de datos, especialmente cuando intervienen plataformas o encargados externos. Adicionalmente, la **Ley 1266 de 2008** refuerza lineamientos aplicables a la protección de datos en materia financiera y crediticia cuando ello resulte pertinente, y las **Circulares Externas 052 de 2007 y 002 de 2015** establecen parámetros de seguridad y responsabilidad en el manejo de información, fortaleciendo los estándares exigibles en entornos digitales.

Como referencia complementaria de buenas prácticas, TECJUR SAS exige a sus proveedores el alineamiento con estándares internacionales tales como **NTC-ISO/IEC**

27001 (seguridad de la información), **NTC-ISO/IEC 27701** (gestión de privacidad) y **NTC-ISO/IEC 29100** (marco de privacidad), así como con el **Marco de Ciberseguridad del NIST**, en la medida en que proveen directrices para prevenir riesgos, fortalecer controles, y gestionar incidentes de seguridad relacionados con la información personal.

8.1 PROCEDIMIENTOS PARA LA RECOLECCIÓN DE DATOS MEDIANTE PLATAFORMAS DE TERCEROS

La recolección de datos personales mediante plataformas digitales permite a TECJUR SAS prestar servicios profesionales de forma oportuna, asegurando que la información se recopile únicamente con el **consentimiento expreso e informado** del titular y en estricta relación con finalidades legítimas previamente informadas. Las plataformas de terceros que captan, registran y procesan datos vinculados a la prestación de servicios para TECJUR SAS deben operar conforme a procedimientos que promuevan **transparencia, minimización de datos y seguridad** en cada etapa del tratamiento, incluyendo como mínimo:

- **Obtención del consentimiento del titular:** Antes de recolectar cualquier dato personal, el proveedor de la plataforma debe informar al titular, de manera clara y accesible, la finalidad específica del tratamiento, el tipo de datos solicitados, el uso previsto, la forma en que serán almacenados y los canales habilitados para el ejercicio de derechos. El consentimiento deberá quedar registrado conforme a la trazabilidad exigida por la normativa.
- **Notificación del proveedor responsable:** TECJUR SAS informa a los titulares que la recolección se realiza por medio de plataformas administradas por terceros, quienes actúan como encargados del tratamiento y responden por la custodia y seguridad de la información.
- **Limitación y proporcionalidad en la recolección:** Solo se solicitarán datos pertinentes, necesarios y adecuados para la finalidad informada, evitando la recolección excesiva o no relacionada con la prestación del servicio.
- **Trazabilidad y soporte de recolección:** Los proveedores deberán mantener registros que permitan identificar cuándo, cómo y bajo qué autorización fueron recolectados los datos, de forma que se garantice la auditoría y el cumplimiento ante eventuales requerimientos del titular o de autoridad competente.

8.2 RESPONSABILIDAD DE LOS PROVEEDORES EN LA RECOLECCIÓN DE DATOS

Dado que los datos son captados y almacenados por los proveedores de plataformas digitales, TECJUR SAS exige a dichos terceros el cumplimiento estricto de la normativa vigente y de altos estándares técnicos y organizativos en cada fase del proceso, incluyendo:

- **Implementación de medidas de seguridad:** Los proveedores deberán aplicar medidas técnicas, administrativas y organizativas para prevenir pérdida, destrucción, alteración o acceso no autorizado a los datos. Lo anterior incluye, entre otros, cifrado, controles de acceso, autenticación multifactor, segmentación de permisos, monitoreo de eventos y registros de auditoría.
- **Auditorías y revisiones periódicas:** TECJUR SAS podrá exigir que los proveedores acrediten la ejecución de auditorías periódicas de seguridad y cumplimiento, garantizando que sus plataformas se mantengan alineadas con estándares legales y técnicos aplicables.
- **Capacitación y conciencia del personal:** El proveedor deberá garantizar que su personal esté capacitado en protección de datos, seguridad de la información y manejo seguro de incidentes, promoviendo una cultura de cumplimiento y confidencialidad.
- **Gestión de incidentes de seguridad:** El proveedor deberá contar con protocolos documentados para detección, respuesta, mitigación y notificación de incidentes de seguridad que comprometan datos personales, incluyendo la comunicación oportuna a TECJUR SAS cuando corresponda.

8.3 EXONERACIÓN Y LIMITACIÓN DE RESPONSABILIDAD DE TECJUR SAS

Aunque TECJUR SAS puede acceder a datos recolectados mediante plataformas digitales de terceros en la medida necesaria para la prestación de servicios, **no es el responsable directo del almacenamiento, gestión ni custodia técnica** de dicha información. La responsabilidad del tratamiento operativo, conservación, disponibilidad, seguridad y control de la información recae en los proveedores externos de las plataformas digitales, quienes actúan como encargados del tratamiento y se encuentran sujetos al cumplimiento de la legislación colombiana y de estándares internacionales de seguridad y privacidad. En consecuencia, TECJUR SAS se exime de responsabilidad por la administración directa de datos, limitándose a exigir, verificar y supervisar contractualmente que los proveedores implementen medidas adecuadas de seguridad y protección.

8.4 DERECHOS DEL TITULAR SOBRE DATOS RECOLECTADOS EN PLATAFORMAS DE TERCEROS

Los titulares de datos personales conservan el derecho a **conocer, actualizar, rectificar, suprimir información y revocar la autorización**, en los términos previstos por la Ley 1581 de 2012 y el Decreto 1377 de 2013. Cuando los datos hayan sido recolectados y almacenados en plataformas de terceros, el titular deberá dirigir su solicitud directamente al proveedor responsable del almacenamiento y gestión, sin perjuicio de que TECJUR SAS pueda orientar al titular sobre la identificación del proveedor correspondiente.

TECJUR SAS, en cumplimiento del deber de información y transparencia, facilitará al titular los datos de contacto del proveedor cuando sea necesario y brindará soporte de orientación para ubicar el canal adecuado de atención, **sin asumir la obligación de resolver directamente la solicitud**, toda vez que la respuesta, ejecución y trámite material del derecho corresponde al encargado de la plataforma donde reposan los datos.

9. RESPONSABILIDADES DEL ENCARGADO DEL TRATAMIENTO

En el marco de la presente Política, se entiende por **Encargado del Tratamiento** la persona natural o jurídica, pública o privada, que, **en virtud de un contrato o vínculo jurídico con el Responsable**, realiza por cuenta de este la **recolección, almacenamiento, administración, custodia, uso, circulación, transmisión, supresión y, en general, cualquier actividad de tratamiento de datos personales**. En el contexto operativo de **TECJUR OUTSOURCING PROFESIONAL SAS (TECJUR SAS)**, los **Encargados del Tratamiento** corresponden a los **proveedores externos** que administran y operan las **plataformas digitales** utilizadas para captar, alojar, procesar y conservar datos personales de los titulares (clientes, empleados, proveedores, usuarios y/o terceros relacionados). En consecuencia, dichos proveedores, en su condición de encargados, deberán cumplir **de manera estricta** con las obligaciones legales, técnicas y de seguridad establecidas en la normativa colombiana aplicable y en los estándares internacionales referenciados en esta Política.

Se deja expresa constancia de que **TECJUR SAS NO actúa como Encargado del Tratamiento**, por cuanto **no ejecuta la custodia técnica, el almacenamiento directo ni la administración de las bases de datos** donde reposan los datos recolectados a través de plataformas de terceros. TECJUR SAS actúa como **intermediario y facilitador** de la prestación del servicio, exigiendo contractualmente estándares de seguridad y cumplimiento, sin asumir la operación técnica del tratamiento.

9.1 MARCO NORMATIVO APLICABLE A LOS ENCARGADOS DEL TRATAMIENTO

Las obligaciones del Encargado del Tratamiento se soportan, entre otras disposiciones, en:

1. **Ley 1581 de 2012 (Régimen General de Protección de Datos Personales):** Establece los principios del tratamiento y fija obligaciones para responsables y encargados, especialmente en materia de **seguridad, confidencialidad, acceso restringido y deber de garantizar los derechos del titular**. En particular, el

- Encargado debe implementar medidas adecuadas para evitar adulteración, pérdida, consulta, uso o acceso no autorizado o fraudulento.
2. **Decreto 1377 de 2013 (Reglamentario parcial de la Ley 1581 de 2012):** Desarrolla deberes operativos del Encargado, exigiendo que el tratamiento se realice **conforme a las instrucciones del Responsable**, manteniendo condiciones de seguridad apropiadas, garantizando la **confidencialidad** y asegurando mecanismos que faciliten el ejercicio de los derechos del titular, cuando resulte procedente según la arquitectura de la plataforma.
 3. **Ley 1266 de 2008 (Habeas Data – cuando aplique):** Refuerza criterios de **calidad, veracidad, exactitud y actualización** en el manejo de información, especialmente cuando exista tratamiento de información financiera, comercial o crediticia, lo cual, en los casos en que corresponda, obliga al Encargado a adoptar controles reforzados para evitar afectaciones al titular por información inexacta o desactualizada.
 4. **Directrices y lineamientos aplicables de la Superintendencia de Industria y Comercio (SIC) y demás autoridades competentes:** En cuanto orientan el cumplimiento del régimen de protección de datos, especialmente sobre políticas, seguridad, registro de bases de datos cuando haya lugar, y atención de consultas y reclamos.

En todo caso, el **cumplimiento normativo y operativo** derivado de las anteriores disposiciones recae **directamente en los Encargados del Tratamiento**, en cuanto son quienes **almacenan, procesan y custodian** la información en sus plataformas.

9.2 ESTÁNDARES TÉCNICOS Y BUENAS PRÁCTICAS EXIGIBLES A LOS ENCARGADOS

Para fortalecer la protección de los datos personales, TECJUR SAS exige a sus proveedores, en calidad de encargados, la adopción o alineación con estándares técnicos reconocidos, tales como:

- **Sistemas de Gestión de Seguridad de la Información (SGSI)**, como referencia técnica para administrar riesgos, controles, accesos, continuidad y gestión de incidentes.
- **Código de buenas prácticas en seguridad de la información**, orientado a controles de acceso, segregación de funciones, cifrado, registros de auditoría, control de cambios y manejo de vulnerabilidades.
- **Gestión de privacidad y protección de datos personales**, mediante controles específicos orientados a limitar el uso no autorizado, asegurar la minimización y garantizar la atención de derechos.
- **Marco de privacidad**, para transparencia en el uso y administración de información personal.
- **Seguridad y resiliencia / continuidad del negocio**, de manera que las plataformas aseguren disponibilidad, recuperación y protección ante incidentes.
- **Marco de Ciberseguridad del NIST**, como guía para identificación, protección, detección, respuesta y recuperación ante amenazas.

Estas referencias constituyen **estándares de buenas prácticas** que fortalecen el cumplimiento normativo y soportan la diligencia debida exigible a los Encargados del Tratamiento.

9.3 PRINCIPALES RESPONSABILIDADES DEL ENCARGADO DEL TRATAMIENTO

Como Encargado del Tratamiento, cada proveedor de plataformas digitales deberá garantizar que los datos personales sean gestionados conforme a la normativa vigente, observando como mínimo las siguientes obligaciones:

- a) **Cumplimiento de instrucciones del responsable.** El Encargado deberá tratar los datos personales **únicamente conforme a las instrucciones documentadas** de TECJUR SAS (en lo aplicable), y de acuerdo con el objeto contractual. Cualquier desviación, uso distinto o tratamiento no autorizado se considerará incumplimiento contractual y legal.
- b) **Implementación de medidas técnicas, administrativas y organizativas** El Encargado deberá adoptar medidas adecuadas para prevenir **acceso no autorizado, pérdida, alteración, destrucción, divulgación indebida o tratamiento fraudulento**, incluyendo

cifrado, autenticación, control por roles, registros de actividad, control de sesiones y medidas de endurecimiento de sistemas.

c) Confidencialidad y control de acceso El Encargado deberá asegurar que el acceso a datos personales se limite a personal estrictamente autorizado y capacitado, bajo compromisos de confidencialidad vigentes, evitando divulgaciones o transferencias no permitidas.

d) Integridad, veracidad y calidad de la información El Encargado deberá mantener mecanismos razonables para garantizar que la información sea **precisa, actualizada, completa y comprensible**, y deberá habilitar mecanismos para corrección o actualización cuando el titular ejerza sus derechos ante el proveedor.

e) Gestión de incidentes de seguridad El Encargado deberá contar con protocolos formales de **detección, respuesta, contención, remediación y documentación** de incidentes que comprometan datos personales, incluyendo la notificación a TECJUR SAS cuando ello sea necesario para la trazabilidad contractual y la adopción de medidas de coordinación.

f) Auditorías, evidencias y revisión periódica El Encargado deberá ejecutar auditorías internas o externas de seguridad y cumplimiento, conservar evidencias de controles, bitácoras y registros, y entregar soportes cuando TECJUR SAS lo requiera contractualmente para verificar el cumplimiento de obligaciones.

g) Capacitación y sensibilización El Encargado deberá implementar programas de capacitación continua a su personal sobre protección de datos, seguridad de la información, gestión de riesgos y manejo seguro de incidentes, promoviendo cultura de cumplimiento.

h) Subencargados y terceros Cuando el Encargado utilice subencargados o terceros para operar servicios, deberá garantizar que dichos subencargados asuman obligaciones equivalentes de seguridad, confidencialidad y cumplimiento normativo, manteniendo la trazabilidad del tratamiento y evitando transferencias no autorizadas.

9.4 EXONERACIÓN Y LIMITACIÓN DE RESPONSABILIDAD DE TECJUR SAS

Aunque TECJUR SAS puede acceder a información personal en la medida necesaria para la prestación de sus servicios, se deja establecido que:

1. **TECJUR SAS NO es el Encargado del Tratamiento**, por cuanto no realiza la custodia técnica, el almacenamiento directo ni la administración de las plataformas donde reposan los datos personales.
2. La **custodia, seguridad, administración, operación técnica y responsabilidad directa del tratamiento** recaen en los **Encargados del Tratamiento (proveedores externos)**, quienes son los únicos responsables de implementar y mantener controles de seguridad, gestionar la base de datos y atender materialmente las solicitudes de los titulares en sus plataformas.
3. En consecuencia, TECJUR SAS se **exime de responsabilidad** por el manejo operativo, administración, almacenamiento, conservación, seguridad técnica y control directo de los datos recolectados en plataformas de terceros, limitándose a:
 - Informar al titular sobre el uso de plataformas de terceros,
 - Exigir contractualmente estándares adecuados de seguridad y protección, y
 - Facilitar la identificación del proveedor responsable cuando sea requerido, sin asumir la obligación de custodiar o administrar la base de datos.

9.5 ARTICULACIÓN CON LOS DERECHOS DE LOS TITULARES Y CANALES DE ATENCIÓN

En coherencia con lo dispuesto en el capítulo de **Derechos de los Titulares**, se precisa que el ejercicio de los derechos de **acceso, actualización, rectificación, supresión de datos y revocatoria de la autorización**, respecto de la información personal recolectada y almacenada en **plataformas digitales de terceros**, deberá realizarse **directamente ante el Encargado del Tratamiento**, esto es, el proveedor de la plataforma en la cual reposan materialmente los datos personales.

Lo anterior obedece a que dichos proveedores son quienes **administran, custodian, procesan y controlan técnicamente las bases de datos**, y por tanto son los únicos habilitados para ejecutar de manera efectiva las solicitudes de los titulares, en los términos previstos en la **Ley 1581 de 2012** y el **Decreto 1377 de 2013**.

En consecuencia:

a) TECJUR OUTSOURCING PROFESIONAL SAS NO es responsable de atender materialmente las solicitudes de los titulares, ni de ejecutar la actualización, supresión o

modificación de los datos personales, por cuanto no ostenta la calidad de Encargado del Tratamiento ni administra las bases de datos.

b) **TECJUR SAS actúa únicamente como intermediario informativo y orientador**, facilitando al titular la identificación del proveedor responsable y, cuando resulte necesario, suministrando los canales de contacto disponibles para el ejercicio de sus derechos.

c) La intervención de TECJUR SAS **no implica asunción de responsabilidad**, ni traslada al Responsable obligaciones propias del Encargado del Tratamiento, manteniéndose la responsabilidad plena y exclusiva en cabeza del proveedor que almacena y gestiona los datos.

d) Cualquier respuesta de fondo, actuación técnica, modificación de datos, supresión o conservación de la información será realizada **exclusivamente por el Encargado del Tratamiento**, conforme a sus políticas internas, términos de uso y obligaciones legales.

*La orientación, remisión o apoyo informativo brindado por TECJUR SAS al titular **no constituye aceptación de responsabilidad**, ni genera obligación de custodia, administración, almacenamiento o tratamiento directo de los datos personales. TECJUR SAS se limita a cumplir su deber de información y transparencia, sin asumir funciones operativas propias del Encargado del Tratamiento.*

10. POLÍTICA DE COOKIES

La presente **Política de Cookies** de **TECJUR OUTSOURCING PROFESIONAL SAS** (en adelante, **TECJUR SAS**) regula el uso de cookies y tecnologías similares en las plataformas digitales a través de las cuales se prestan o apoyan los servicios de la compañía, en estricto cumplimiento de la **Constitución Política de Colombia (artículo 15)**, la **Ley 1581 de 2012**, el **Decreto 1377 de 2013**, la **Ley 1266 de 2008**, así como las directrices emitidas por la **Superintendencia de Industria y Comercio (SIC)** y, como buenas prácticas técnicas, las normas internacionales de seguridad de la información tales como la **NTC-ISO/IEC 27001:2013** y el **Marco de Ciberseguridad del NIST**.

Las cookies son **pequeños archivos de texto** que se almacenan en el dispositivo del usuario (computador, tableta, teléfono móvil u otro) cuando este accede a un sitio web o plataforma digital. Estas permiten recopilar información relacionada con la navegación, preferencias, configuración del dispositivo y comportamiento de uso, con el fin de mejorar la experiencia del usuario y optimizar el funcionamiento de los servicios digitales. Se aclara de manera expresa que, **si bien TECJUR SAS puede acceder de forma limitada a ciertos datos derivados del uso de cookies para fines informativos o de mejora del servicio**, la **instalación, gestión, almacenamiento, custodia, control y seguridad de las cookies** corresponde **exclusivamente a los proveedores de las plataformas digitales** utilizadas, quienes actúan como **Encargados del Tratamiento** y son responsables de cumplir la normativa aplicable en materia de protección de datos personales.

10.1 FINALIDADES DEL USO DE COOKIES

Las cookies utilizadas en las plataformas digitales asociadas a TECJUR SAS tienen como finalidad principal **optimizar la experiencia de navegación**, mejorar la funcionalidad de los sitios y permitir la prestación eficiente de los servicios. Los usuarios pueden, en todo momento, **configurar su navegador para aceptar, restringir o deshabilitar el uso de cookies**, de acuerdo con sus preferencias.

Las finalidades legítimas del uso de cookies pueden incluir, entre otras:

- **Mejorar la experiencia del usuario:** Permiten recordar preferencias, configuraciones de idioma, sesiones activas y otros parámetros que facilitan una navegación más eficiente y personalizada.
- **Análisis y estadísticas:** Permiten recolectar información de carácter técnico y, en muchos casos, anonimizada, relacionada con el uso de la plataforma, tales como número de visitas, tiempo de permanencia, interacción con contenidos y comportamiento general de navegación, con el fin de mejorar el desempeño y calidad de los servicios.
- **Publicidad y remarketing:** En determinados casos, los proveedores de las plataformas pueden utilizar cookies para mostrar contenidos o anuncios relevantes

conforme al comportamiento de navegación del usuario. Esta finalidad se encuentra sujeta a las políticas de privacidad del proveedor correspondiente y al consentimiento previo del usuario.

TECJUR SAS informa que **todas estas finalidades son gestionadas, controladas y ejecutadas directamente por los proveedores de las plataformas digitales**, quienes son responsables del tratamiento de la información recolectada mediante cookies y de la implementación de las medidas de seguridad correspondientes.

10.2 DERECHOS DEL USUARIO FRENTE AL USO DE COOKIES

De conformidad con la legislación colombiana y los estándares internacionales de protección de datos y privacidad, los usuarios cuentan con los siguientes derechos en relación con el uso de cookies:

- **Derecho al consentimiento informado:** Los usuarios deben ser informados de manera clara, previa y suficiente sobre el uso de cookies antes de su instalación, incluyendo su finalidad, duración y opciones de configuración disponibles.
- **Derecho a revocar el consentimiento:** El usuario puede revocar en cualquier momento su consentimiento para el uso de cookies, mediante la configuración de su navegador o a través de los mecanismos habilitados por el proveedor de la plataforma digital.
- **Derecho a la transparencia y acceso a la información:** Los proveedores deben garantizar que los usuarios puedan acceder a información detallada sobre las cookies utilizadas, su naturaleza, duración, finalidad y terceros que puedan tener acceso a la información.
- **Derecho a la configuración personalizada:** El usuario puede seleccionar qué tipos de cookies acepta o rechaza, en los casos en que la plataforma ofrezca mecanismos de gestión granular del consentimiento.

El ejercicio de estos derechos se realiza **directamente ante el proveedor de la plataforma digital**, quien es el encargado del tratamiento de los datos recolectados mediante cookies.

10.3 RESPONSABILIDADES DEL ENCARGADO DEL TRATAMIENTO EN LA GESTIÓN DE COOKIES

Los **Encargados del Tratamiento**, esto es, los proveedores de plataformas digitales utilizadas por TECJUR SAS, son los responsables directos de la correcta gestión del uso de cookies. En tal virtud, deberán cumplir, como mínimo, con las siguientes obligaciones:

- **Implementación de políticas de privacidad y cookies:** Desarrollar, mantener y publicar políticas claras, accesibles y actualizadas que expliquen el uso de cookies, sus finalidades, duración y los derechos de los usuarios.
- **Obtención y gestión del consentimiento:** Garantizar que la instalación de cookies se realice con el consentimiento previo, libre e informado del usuario, cuando la normativa así lo exija.
- **Medidas de seguridad:** Aplicar medidas técnicas y organizativas adecuadas para proteger la información recolectada mediante cookies, incluyendo controles de acceso, cifrado cuando aplique y mecanismos de protección frente a accesos no autorizados.
- **Auditorías y revisiones periódicas:** Realizar evaluaciones y auditorías periódicas de sus prácticas de uso de cookies, con el fin de asegurar el cumplimiento de la normativa vigente y de los estándares técnicos aplicables.
- **Gestión de terceros:** Garantizar que cualquier tercero que participe en el uso de cookies cumpla con obligaciones equivalentes de protección de datos y privacidad.

10.4 EXONERACIÓN DE RESPONSABILIDAD DE TECJUR SAS

Aunque TECJUR SAS puede tener acceso limitado a información derivada del uso de cookies para fines informativos o de mejora del servicio, **no es responsable de la administración, custodia, almacenamiento ni tratamiento técnico de los datos recolectados mediante cookies**, funciones que recaen de manera exclusiva en los proveedores de las plataformas digitales.

En consecuencia, **TECJUR SAS se exime de cualquier responsabilidad relacionada con la instalación, gestión, seguridad, conservación o eliminación de cookies**, así como del tratamiento de los datos personales recolectados a través de estas tecnologías, limitándose a informar a los usuarios sobre su uso y a exigir contractualmente que los proveedores

cumplan con la normativa de protección de datos y las buenas prácticas de seguridad de la información.

11. MEDIDAS ADICIONALES TÉCNICAS DE SEGURIDAD

La presente política establece las **Medidas Técnicas, Administrativas y Organizativas de Seguridad Avanzada** que **TECJUR OUTSOURCING PROFESIONAL SAS (TECJUR SAS)** adopta y exige para la protección de los datos personales recolectados y tratados a través de plataformas digitales de terceros, en estricta alineación con el **marco normativo colombiano** y con **estándares técnicos internacionales reconocidos** en materia de seguridad de la información y privacidad.

Estas medidas se desarrollan en cumplimiento de las obligaciones previstas en la **Constitución Política de Colombia (artículo 15)**, la **Ley 1581 de 2012**, el **Decreto 1377 de 2013**, la **Ley 1266 de 2008 (Habeas Data)**, la **Circular Externa 052 de 2007** de la Superintendencia Financiera de Colombia y la **Circular Externa 002 de 2015** de la Superintendencia de Industria y Comercio (SIC). Así mismo, este marco se complementa con normas internacionales tales como la **NTC-ISO/IEC 27001:2013**, **NTC-ISO/IEC 27002:2013**, **NTC-ISO/IEC 27701:2019**, **NTC-ISO/IEC 29100:2011**, **NTC-ISO/IEC 22301:2012** y el **Marco de Ciberseguridad del NIST**, las cuales permiten consolidar un **sistema integral de seguridad, privacidad y continuidad operativa**.

Se precisa que estas medidas se implementan bajo el principio de **responsabilidad demostrada**, sin perjuicio de que la **custodia técnica, almacenamiento y administración directa de los datos personales** recaiga en los **proveedores de plataformas digitales**, quienes actúan como **Encargados del Tratamiento**.

11.1 PRINCIPIOS RECTORES DE LAS MEDIDAS DE SEGURIDAD

Para garantizar el cumplimiento normativo y la protección integral de los datos personales, **TECJUR SAS** adopta los siguientes principios rectores, los cuales orientan la exigencia y supervisión de medidas de seguridad frente a los proveedores tecnológicos:

a) Confidencialidad y Privacidad Los datos personales tratados mediante cookies, formularios, sistemas de mensajería y demás herramientas digitales deberán ser gestionados bajo estrictos protocolos de confidencialidad. El acceso a la información se restringe al personal autorizado y su uso se limita exclusivamente a las finalidades previamente informadas y consentidas por los titulares, conforme a la Ley 1581 de 2012.

b) Seguridad Técnica y Física **TECJUR SAS** exige la implementación de medidas de seguridad técnicas y físicas apropiadas, entre ellas:

- **Cifrado de datos en tránsito y en reposo**, garantizando que la información solo sea accesible por personal autorizado.
- **Controles de acceso estrictos**, basados en roles, privilegios mínimos y autenticación robusta.
- **Firewalls, sistemas de detección y prevención de intrusos (IDS/IPS)**, orientados a la identificación y bloqueo de amenazas en tiempo real.
- **Gestión segura de credenciales**, incluyendo políticas de contraseñas fuertes y autenticación multifactor.
- **Protección de infraestructura física**, aplicable a centros de datos y entornos tecnológicos del proveedor.

c) Gestión Integral de Riesgos **TECJUR SAS** promueve un enfoque preventivo de **gestión de riesgos**, orientado a la identificación, análisis y mitigación de vulnerabilidades que puedan afectar la seguridad de los datos personales. Este enfoque se fundamenta en la **ISO/IEC 27001**, incorporando evaluaciones periódicas, controles correctivos y planes de mejora continua.

d) Transparencia y Consentimiento En cumplimiento de la Ley 1581 de 2012 y el Decreto 1377 de 2013, se garantiza que los titulares sean informados de manera clara, suficiente y previa sobre la recolección y uso de datos personales mediante herramientas digitales, incluyendo cookies, y sobre su derecho a **aceptar, rechazar o revocar el consentimiento** en cualquier momento.

e) Capacitación y Conciencia Organizacional TECJUR SAS implementa programas permanentes de capacitación y sensibilización dirigidos a su personal, orientados a fortalecer el conocimiento en protección de datos, seguridad de la información, gestión de riesgos y cumplimiento normativo, fomentando una **cultura organizacional de privacidad y responsabilidad**.

f) Auditorías y Revisiones Periódicas Se promueve la realización de auditorías periódicas de seguridad y privacidad, tanto internas como externas, con el fin de verificar el cumplimiento normativo, identificar oportunidades de mejora y mantener un nivel adecuado de protección de los datos personales.

11.2 MARCO NORMATIVO Y CUMPLIMIENTO LEGAL

La protección de los datos personales se soporta en el cumplimiento articulado de las siguientes disposiciones:

- **Ley 1581 de 2012 y Decreto 1377 de 2013:** Establecen los principios, derechos y deberes aplicables al tratamiento de datos personales, exigiendo consentimiento informado, medidas de seguridad y deber de información.
- **Ley 1266 de 2008 (Habeas Data):** Refuerza los derechos de acceso, rectificación y actualización de la información, especialmente en contextos financieros o comerciales cuando resulte aplicable.
- **Circulares Externas 052 de 2007 y 002 de 2015:** Imponen obligaciones relacionadas con seguridad de la información, control interno, gestión de riesgos y transparencia en el tratamiento de datos en entornos digitales.
- **Normas Internacionales de Seguridad**
- **NTC-ISO/IEC 27001 y 27002:** Definen controles y buenas prácticas para la gestión de la seguridad de la información.
- **NTC-ISO/IEC 27701 y 29100:** Refuerzan la gestión de privacidad y la protección de datos personales.
- **NTC-ISO/IEC 22301:** Garantiza continuidad del negocio y resiliencia operativa.
- **Marco de Ciberseguridad del NIST:** Orienta la identificación, protección, detección, respuesta y recuperación ante incidentes de seguridad.

11.3 RESPONSABILIDAD DE LOS PROVEEDORES Y LIMITACIÓN DE RESPONSABILIDAD DE TECJUR SAS

Si bien TECJUR SAS puede acceder de forma limitada a información derivada del uso de cookies u otras herramientas digitales para fines operativos o de mejora del servicio, **no actúa como Encargado del Tratamiento ni como custodio técnico de los datos personales**. En consecuencia, la **administración, almacenamiento, custodia, seguridad y control directo de la información** recae exclusivamente en los **proveedores de plataformas digitales**, quienes están obligados a:

- Desarrollar y mantener **políticas de privacidad claras, accesibles y actualizadas**, incluyendo el uso de cookies y tecnologías similares.
- Implementar **medidas técnicas, administrativas y organizativas adecuadas** para proteger los datos personales.
- Ejecutar **auditorías periódicas** y mantener evidencia de cumplimiento normativo y técnico.
- Actualizar continuamente sus prácticas de seguridad conforme a la evolución de riesgos tecnológicos y regulatorios.

Exoneración de responsabilidad: TECJUR SAS se exime de cualquier responsabilidad relacionada con la custodia, almacenamiento, administración técnica, seguridad o eliminación de los datos personales recolectados a través de plataformas de terceros, limitándose a cumplir su deber de información, exigir contractualmente estándares adecuados de seguridad y orientar al titular cuando sea necesario.

12. PROTOCOLOS DE AUDITORÍA Y CONTROL

TECJUR OUTSOURCING PROFESIONAL SAS (TECJUR SAS) establece un marco estructurado y robusto de **protocolos de auditoría, control y verificación continua** orientado a garantizar que los procesos de tratamiento y seguridad de los datos personales

recolectados mediante **plataformas digitales de terceros** se desarrollen conforme al marco normativo colombiano y a los estándares técnicos nacionales e internacionales aplicables. La implementación de auditorías, controles internos y revisiones periódicas permite asegurar la **confidencialidad, integridad, disponibilidad, trazabilidad y transparencia** en el tratamiento de los datos personales. No obstante, se deja expresa constancia de que, **si bien TECJUR SAS puede acceder a la información para el cumplimiento de sus obligaciones contractuales y de prestación de servicios, la responsabilidad directa de ejecutar auditorías técnicas, controles de seguridad, monitoreos continuos y revisiones operativas recae exclusivamente en los proveedores de plataformas digitales**, quienes actúan como **Encargados del Tratamiento** y administran de manera directa las bases de datos.

12.1 FUNDAMENTO NORMATIVO DE LOS PROTOCOLOS DE AUDITORÍA

La adopción de protocolos de auditoría y control se encuentra sustentada, entre otras disposiciones, en:

- a) **Ley 1581 de 2012.** Establece la obligación de implementar medidas de seguridad que garanticen la confidencialidad e integridad de los datos personales. En este sentido, los procesos de auditoría deben verificar de manera periódica que el tratamiento de datos se ajuste a los principios de **legalidad, finalidad, seguridad, transparencia y confidencialidad**, así como a la finalidad informada al titular.
- b) **Decreto 1377 de 2013** Dispone que los responsables y encargados del tratamiento deben implementar **controles internos y auditorías periódicas** que permitan evaluar la eficacia de las medidas de seguridad adoptadas y garantizar el **cumplimiento continuo** de la normativa. Tales procedimientos deben documentarse y mantenerse disponibles para verificación y control.
- c) **Ley 1266 de 2008 (Habeas Data – cuando aplique)** Si bien esta ley se orienta principalmente al sector financiero, refuerza la importancia de la **veracidad, exactitud, actualización y calidad de la información**, estableciendo criterios que justifican la realización de auditorías destinadas a prevenir errores, inconsistencias o afectaciones a los titulares derivadas del tratamiento de datos personales.
- d) **Circulares Externas 052 de 2007 y 002 de 2015** Las Circulares de la Superintendencia Financiera de Colombia y de la Superintendencia de Industria y Comercio (SIC) exigen la implementación de **auditorías periódicas, controles internos y sistemas de gestión del riesgo**, especialmente cuando el tratamiento involucra información sensible, financiera o de alto impacto, reforzando la necesidad de control continuo en entornos digitales.

12.2 ESTÁNDARES INTERNACIONALES APLICABLES A LOS PROCESOS DE AUDITORÍA

Con el fin de garantizar un nivel avanzado de seguridad y protección de los datos personales, TECJUR SAS exige a sus proveedores el cumplimiento de auditorías alineadas con normas y marcos internacionales, entre ellos:

- **NTC-ISO/IEC 27001:2013:** Exige auditorías internas periódicas como parte del Sistema de Gestión de Seguridad de la Información (SGSI), permitiendo evaluar la planificación, implementación y mejora continua de los controles de seguridad.
- **NTC-ISO/IEC 27002:2013:** Establece buenas prácticas que incluyen la revisión periódica de controles de acceso, registros de actividad, protección de la información y evaluación de riesgos.
- **NTC-ISO/IEC 27701:2019:** Introduce auditorías específicas de privacidad, orientadas a verificar el cumplimiento de los derechos de los titulares y la correcta gestión de datos personales.
- **NTC-ISO/IEC 29100:2011 (Marco de Privacidad):** Guía la evaluación de prácticas de privacidad, promoviendo transparencia, responsabilidad y protección efectiva de la información.
- **Marco de Ciberseguridad del NIST:** Establece directrices para auditorías de seguridad, evaluación de riesgos, controles internos y capacidad de respuesta ante incidentes, bajo los pilares de identificar, proteger, detectar, responder y recuperar.

12.3 PLANIFICACIÓN Y EJECUCIÓN DE AUDITORÍAS DE SEGURIDAD

Los proveedores de TECJUR SAS, en su calidad de **Encargados del Tratamiento**, son responsables de planificar, ejecutar y documentar auditorías de seguridad periódicas, las cuales deberán incluir, como mínimo:

- **Evaluación de vulnerabilidades y amenazas:** Identificación y análisis de riesgos técnicos, operativos y humanos asociados al tratamiento de datos personales, incluyendo revisión de infraestructura, accesos, permisos y configuraciones.
- **Pruebas de penetración:** Ejecución de pruebas controladas que simulen intentos de intrusión o ataques cibernéticos, con el fin de evaluar la robustez de los controles de seguridad y corregir debilidades detectadas.
- **Revisión de cumplimiento normativo:** Verificación del cumplimiento de la legislación colombiana de protección de datos y de los estándares internacionales adoptados, dejando evidencia documentada que podrá ser puesta a disposición de TECJUR SAS cuando contractualmente se requiera.

12.4 CONTROLES INTERNOS Y SEGUIMIENTO DE INCIDENTES

La implementación de controles internos y mecanismos de seguimiento es esencial para preservar la integridad de los datos personales y garantizar una respuesta eficaz ante incidentes de seguridad. En este sentido, los proveedores deberán implementar:

- **Monitoreo continuo de seguridad:** Sistemas de supervisión en tiempo real que permitan detectar accesos no autorizados, comportamientos anómalos o eventos de riesgo.
- **Registro de accesos y actividades:** Bitácoras detalladas de accesos, modificaciones y operaciones realizadas sobre los datos, incluyendo identificación del usuario, fecha, hora y motivo del acceso.
- **Plan de respuesta a incidentes:** Protocolos documentados para la detección, contención, mitigación y notificación de incidentes de seguridad, incluyendo la comunicación oportuna a TECJUR SAS y, cuando aplique, a autoridades competentes y titulares afectados.

12.5 CAPACITACIÓN CONTINUA Y SENSIBILIZACIÓN DEL PERSONAL

La formación del personal que interviene en el tratamiento de datos personales constituye un elemento esencial del sistema de control. Por ello, los Encargados del Tratamiento deberán garantizar:

- **Programas de capacitación continua:** En seguridad de la información, protección de datos personales, gestión de riesgos y cumplimiento normativo.
- **Sensibilización en privacidad:** Conciencia permanente sobre la importancia de la confidencialidad y los riesgos asociados al manejo inadecuado de la información.
- **Evaluaciones periódicas:** Medición del nivel de conocimiento del personal respecto de los protocolos de auditoría, control y respuesta a incidentes, fortaleciendo una cultura de responsabilidad y cumplimiento.

12.6 RESPONSABILIDAD DEL ENCARGADO DEL TRATAMIENTO Y EXONERACIÓN DE TECJUR SAS

Responsabilidad del Encargado del Tratamiento Los proveedores de plataformas digitales, en su calidad de Encargados del Tratamiento, son responsables de implementar, ejecutar y mantener los protocolos de auditoría y control, así como de adoptar las medidas correctivas necesarias para garantizar la seguridad y protección de los datos personales. Esta responsabilidad incluye la revisión continua de sus sistemas, la identificación de vulnerabilidades y la ejecución de acciones de mejora.

Exoneración de Responsabilidad de TECJUR SAS Aunque TECJUR SAS pueda acceder a datos personales en el marco de la prestación de sus servicios, la **responsabilidad de realizar auditorías, controles internos, monitoreo de seguridad y custodia técnica de la información corresponde exclusivamente a los proveedores externos**. En consecuencia, **TECJUR SAS se exime de cualquier responsabilidad relacionada con la administración, almacenamiento, control técnico y ejecución directa de auditorías sobre los datos personales**, manteniéndose su rol limitado a la exigencia contractual de estándares adecuados y al deber de información y transparencia frente a los titulares.

13. MODIFICACIÓN Y VIGENCIA DE LA POLÍTICA

La presente **Política de Tratamiento de Datos Personales** entró en vigencia y actualizada desde **el 1 de enero de 2026**, fecha hasta la cual incorpora las modificaciones, ajustes y actualizaciones realizadas por **TECJUR OUTSOURCING PROFESIONAL SAS** en atención a cambios normativos, técnicos, operativos o a lineamientos emitidos por autoridades competentes.

TECJUR SAS se reserva el derecho de **modificar, actualizar o ajustar** esta política en cualquier momento, cuando resulte necesario para garantizar el cumplimiento de la normativa aplicable o la adopción de mejores prácticas en materia de protección de datos personales.

Cualquier modificación sustancial será **informada oportunamente a los titulares** mediante su publicación en el sitio web institucional de TECJUR SAS y, cuando la ley lo exija, a través de los mecanismos adicionales de notificación previstos en la legislación vigente.

