

TABLA DE CONTENIDO

1. INTRODUCCIÓN.....	2
2. PRINCIPIOS	3
4. APLICABILIDAD	4
5. NORMATIVIDAD APLICABLE	4
6. TRATAMIENTO DE DATOS PERSONALES Y SU FINALIDAD	5
7. TRATAMIENTO DE DATOS SENSIBLES	7
8. ACCESO DATOS PERSONALES SENSIBLES	8
9. COPIA DE RESPALDO DE LA INFORMACIÓN CONFIDENCIAL.....	9
10. ACUERDO DE CONFIDENCIALIDAD PARA COLABORADORES	9
11. DERECHOS DEL TITULAR DE LOS DATOS.....	10
12. RESPONSABLE DEL TRATAMIENTO	11
13. PROCEDIMIENTOS DE ASIGNACIÓN DE RESPONSABILIDADES Y AUTORIZACIONES.....	12
14. PROCEDIMIENTOS PARA EJERCER LOS DERECHOS DEL TITULAR.....	13
15. SEGURIDAD DE LA INFORMACIÓN Y DE LA TERCERIZACIÓN DEL TRATAMIENTO	13
16. VALIDACIÓN DE DATOS DE ENTRADA Y PROCESAMIENTO	13
17. PRINCIPIOS DE VERACIDAD Y CALIDAD DE LOS DATOS	14
18. INTERCAMBIO Y ALMACENAMIENTO DE DATOS	15
19. PROCEDIMIENTOS PARA LA ATENCIÓN DE CONSULTAS Y RECLAMOS	15
20. GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN.....	15
21. GESTIÓN DE RIESGOS EN EL TRATAMIENTO DE DATOS	16
22. PROCEDIMIENTOS PARA LA REVOCATORIA Y SUPRESIÓN DE DATOS	16
23. REGISTRO NACIONAL DE BASES DE DATOS (RNBD).....	17
24. VIGENCIA DE LA POLÍTICA	17
25. APROBACIÓN	18

1. INTRODUCCIÓN

TUMIPAY S.A.S., identificada con NIT 901228648-0, persona jurídica con domicilio en Colombia, regida por la normatividad colombiana, en cumplimiento de la Ley 1581 de 2012 y sus decretos reglamentarios, establece la presente Política de Tratamiento de Datos Personales, con el fin de garantizar la protección, seguridad y confidencialidad de la información personal de nuestros usuarios, colaboradores y terceros.

Esta política regula el recolección, almacenamiento, uso, circulación y supresión de datos personales en el marco de las actividades propias de la compañía, aplicando a clientes, proveedores, aliados estratégicos, empleados y demás personas que entreguen información personal a TumiPay.

La compañía reafirma su compromiso con los principios de legalidad, libertad, veracidad, transparencia, acceso y circulación restringida, seguridad y confidencialidad, establecidos en la normativa vigente.

Adicionalmente, TumiPay incorpora en sus procesos mejores prácticas internacionales en privacidad y protección de datos, tomando como referencia estándares como el Reglamento General de Protección de Datos (GDPR) de la Unión Europea, en la medida en que sean compatibles con la regulación colombiana.

Esta política se basa en la versión previa del documento y ha sido ampliada para reflejar todos los requerimientos normativos, tecnológicos y de seguridad actuales, garantizando así un tratamiento responsable y ético de la información personal.

En coherencia con lo anterior, esta Política se fundamenta en un conjunto de principios rectores que guían todas las actividades relacionadas con el tratamiento de datos personales en TumiPay. Estos principios son de obligatorio cumplimiento para todos los colaboradores, proveedores y aliados, y constituyen la base para garantizar la confianza de nuestros usuarios y el respeto por sus derechos.

2. PRINCIPIOS

El tratamiento de datos personales en TumiPay S.A.S. se rige por los siguientes principios:

1. **Legalidad:** el tratamiento de datos se realizará en estricto cumplimiento de lo dispuesto en la Ley 1581 de 2012 y demás normas aplicables.
2. **Finalidad:** la recolección y uso de datos se limita a los fines legítimos, explícitos e informados previamente al titular.
3. **Libertad:** el tratamiento solo se llevará a cabo con el consentimiento previo, expreso e informado del titular, salvo los casos autorizados por la ley.
4. **Veracidad o calidad:** la información suministrada debe ser veraz, completa, exacta, actualizada, comprobable y comprensible.
5. **Transparencia:** se garantizará al titular el acceso a su información y la posibilidad de conocer cómo está siendo utilizada.
6. **Acceso y circulación restringida:** el tratamiento de datos se hará dentro de los límites de la normatividad y con acceso únicamente por personas autorizadas.
7. **Seguridad:** se implementarán medidas técnicas, humanas y administrativas necesarias para proteger los datos personales frente a pérdida, alteración, uso indebido o acceso no autorizado.
8. **Confidencialidad:** todas las personas que intervengan en el tratamiento de datos están obligadas a garantizar la reserva de la información, incluso después de finalizada la relación con TumiPay.

3. DEFINICIONES

- **Autorización:** Consentimiento previo, expreso e informado del titular para llevar a cabo el tratamiento de sus datos personales.
- **Base de Datos:** Conjunto organizado de datos personales.
- **Dato Personal:** Cualquier información vinculada o que pueda asociarse a una persona natural determinada o determinable.
- **Dato Sensible:** Información que afecta la intimidad del titular o cuyo uso indebido puede generar discriminación.
- **Encargado del Tratamiento:** Persona o entidad que realiza el tratamiento de

los datos por cuenta del responsable.

- Responsable del Tratamiento: Persona o entidad que decide sobre la base de datos y/o el tratamiento de los datos personales.
- Titular: Persona natural cuyos datos personales son objeto de tratamiento.
- Tratamiento de Datos: Operaciones sobre datos personales, como recolección, almacenamiento, uso, circulación o supresión.
- Principio de Confidencialidad: Todas las personas que intervengan en el tratamiento de datos personales están obligadas a garantizar la reserva de la información.
- Principio de Seguridad: Obliga a adoptar medidas técnicas, humanas y administrativas para garantizar la seguridad de los registros y evitar adulteración, pérdida, consulta, uso o acceso no autorizado.

4. APLICABILIDAD

- Clientes y Usuarios: Personas naturales o jurídicas que utilizan los servicios de Tumipay.
- Proveedores: Entidades o personas que suministran bienes o servicios a Tumipay.
- Colaboradores: Personal vinculado a Tumipay bajo cualquier modalidad contractual, quienes deben cumplir con las disposiciones establecidas en esta política y firmar un acuerdo de confidencialidad.

5. NORMATIVIDAD APLICABLE

- Constitución Política de Colombia, artículos 15, 16 y 20.
- Ley 1266 de 2008 (habeas data financiero y crediticio).
- Ley 1581 de 2012 (protección de datos personales).

- Decretos Reglamentarios 1727 de 2009, 1377 de 2013 y 886 de 2014.
- Sentencias de la Corte Constitucional: C-1011 de 2008, C-748 de 2011, C-165 de 2019.
- Circulares Externas 02 de 2015 y 001 de 2016 – Superintendencia de Industria y Comercio (SIC).
- Circular Básica Jurídica de la Superintendencia Financiera de Colombia (aplicable en lo relacionado con operaciones financieras y de prevención de fraudes).
- Normatividad sectorial de prevención de lavado de activos y financiación del terrorismo (SARLAFT) aplicable a proveedores y aliados financieros.
- Normas de ciberseguridad y gestión de riesgo operativo de la Superintendencia Financiera (Circular Externa 007 de 2018 y normas posteriores).

6. TRATAMIENTO DE DATOS PERSONALES Y SU FINALIDAD

Los datos personales de clientes, usuarios, proveedores y colaboradores serán recolectados, almacenados, procesados, analizados, compartidos y utilizados dentro del marco y límites de las finalidades establecidas en esta política.

Las finalidades incluyen, pero no se limitan a:

- Prestación de servicios financieros y transaccionales ofrecidos por Tumipay.
- Verificación de identidad, validación documental y prevención de fraude.
- Cumplimiento de normativas legales y regulatorias en materia de protección de datos, prevención de lavado de activos y financiación del terrorismo (SAGRILAF), y reporte a autoridades competentes.
- Administración y monitoreo de operaciones de pago, con el fin de garantizar la seguridad, trazabilidad y legalidad de las transacciones realizadas en la plataforma.

- Evaluación y gestión de riesgos tecnológicos, operativos y de seguridad de la información.
- Contacto con clientes y usuarios para campañas informativas, educativas, comerciales y publicitarias, siempre dentro de los límites de la autorización otorgada.
- Desarrollo, innovación y mejora continua de productos y servicios mediante análisis de datos y técnicas de analítica avanzada, con mecanismos de anonimización y seudonimización cuando corresponda.
- Administración del talento humano, incluyendo procesos de selección, contratación, gestión de desempeño, capacitación y desvinculación.
- Gestión y supervisión de proveedores, incluyendo procesos de debida diligencia y validación de antecedentes.
- Transferencia y transmisión de datos personales a terceros aliados, nacionales o internacionales, cuando sea necesario para la prestación de los servicios y bajo cumplimiento de la normativa aplicable

POLÍTICA INTERNA DE MANEJO Y PROTECCIÓN DE DATOS PERSONALES DEL CONSUMIDOR

En cumplimiento de las disposiciones legales aplicables, TUMIPAY S.A.S., en su calidad de pasarela de pagos, desarrolla e implementa una política interna de manejo y protección de datos personales del consumidor, cuyo objetivo es garantizar la protección integral de la información de los usuarios, clientes, comercios y consumidores finales.

La compañía declara expresamente que está sujeta a todas las leyes de protección al consumidor, en especial a las normas de la Superintendencia de Industria y Comercio, y que su política de tratamiento de datos personales se encuentra alineada con la Ley 1581 de 2012, la Ley 1266 de 2008 y la Ley de Habeas Data, evitando el uso inadecuado o malintencionado de la información de los consumidores de los comercios asociados a la pasarela.

TUMIPAY S.A.S. dispone de una política clara, pública y transparente sobre el

manejo de los datos personales y la información sensible que recolecta, en la que se detalla cada uno de los usos y finalidades del tratamiento. Dicha política se encuentra publicada en la página web oficial de la organización y contenidos en nuestra Autorización de Tratamiento de Datos Personales.

Así mismo, la compañía garantiza un espacio visible y accesible en su página web y aplicación móvil para que los clientes, usuarios y consumidores otorguen su consentimiento expreso e informado para el tratamiento de sus datos personales. La evidencia de dicha autorización será almacenada y conservada por un período mínimo de diez (10) años, tiempo que se tendrá como prueba de la voluntad del titular, de la diligencia de la compañía en el cumplimiento de la normativa de protección de datos personales.

7. TRATAMIENTO DE DATOS SENSIBLES

TUMIPAY S.A.S. tratará datos sensibles como datos biométricos (imágenes, huellas dactilares, voz y otros que puedan capturarse en procesos de autenticación) únicamente con autorización previa, expresa (por escrito o medio verificable) e informada del titular, y en los siguientes casos específicos:

- Seguridad y autenticación reforzada de usuarios en el marco de la operación de la pasarela de pagos.
- Cumplimiento de normativas de prevención de fraudes, lavado de activos y financiación del terrorismo.
- Verificación de identidad en operaciones financieras que requieran validaciones reforzadas.
- Control de acceso y seguridad en instalaciones físicas y sistemas informáticos de la compañía.

El tratamiento de datos sensibles se realizará bajo los siguientes lineamientos:

- Será excepcional y proporcional, limitado a los fines estrictamente necesarios para el servicio.
- No se condicionará el acceso a los servicios a la entrega de datos sensibles, salvo que dichos datos sean indispensables para garantizar la seguridad de la transacción.
- Se aplicarán controles técnicos avanzados como cifrado, segmentación de

bases de datos, trazabilidad de accesos, y registros de auditoría para prevenir usos indebidos.

- En caso de transferencia o transmisión internacional de datos sensibles, Tumipay garantizará que se cumpla con la normativa colombiana y, cuando aplique, con estándares internacionales como el GDPR, asegurando que el país receptor proporcione niveles adecuados de protección de datos.

NOTA AL TITULAR:

TUMIPAY S.A.S. informa que el suministro de datos sensibles es de carácter facultativo. En todos los casos, el titular será informado de manera clara y previa sobre la finalidad de su recolección, los mecanismos de seguridad aplicables y los derechos que le asisten. La negativa a autorizar el tratamiento de datos sensibles no limitará el acceso a los servicios ofrecidos, salvo cuando dicha información resulte estrictamente necesaria para validar la identidad o garantizar la seguridad de la operación.

8. ACCESO DATOS PERSONALES SENSIBLES

El acceso a las bases de datos que contengan información personal sensible estará estrictamente restringido a personal previamente autorizado y con funciones directamente relacionadas con el tratamiento de dichos datos.

Para garantizar la seguridad y confidencialidad de esta información, se adoptan las siguientes medidas:

- Mecanismos de doble autenticación (2FA): todo acceso se realiza mediante controles de autenticación robustos, combinando credenciales personales y factores adicionales de seguridad.
- Registros de auditoría: se mantendrán logs detallados de cada acceso, consulta o modificación, incluyendo usuario, fecha, hora y operación realizada.
- Principio de mínimo privilegio: se asignan permisos únicamente al personal que requiere acceso para el cumplimiento de sus funciones.
- Protocolos de confidencialidad: todo el personal con acceso deberá firmar acuerdos específicos de confidencialidad y cumplir con la normativa vigente.

- El incumplimiento de estas medidas dará lugar a sanciones disciplinarias internas y, de ser el caso, acciones legales conforme a la ley.

9. COPIA DE RESPALDO DE LA INFORMACIÓN CONFIDENCIAL

Para evitar la pérdida de información personal, se establecerán políticas de respaldo de datos periódicos, los cuales se almacenarán en entornos seguros mediante copias de seguridad múltiples en diferentes ubicaciones, de manera que, en caso de falla, daño o indisponibilidad de un sistema, los datos puedan ser recuperados de forma íntegra y oportuna.

Las copias de seguridad serán cifradas y almacenadas en servidores con acceso restringido. Asimismo, se implementarán pruebas periódicas para garantizar la integridad y recuperación de los datos en caso de incidentes de seguridad. TUMIPAY S.A.S. implementa medidas técnicas, administrativas y organizativas para garantizar la seguridad de la información y evitar el acceso no autorizado, la pérdida o la manipulación indebida de los datos personales.

10. ACUERDO DE CONFIDENCIALIDAD PARA COLABORADORES

Todos los colaboradores, contratistas y terceros que, en el ejercicio de sus funciones, tengan acceso a información confidencial, financiera, transaccional, estratégica o tecnológica de TUMIPAY S.A.S., deberán suscribir un acuerdo de confidencialidad como condición indispensable para el inicio y continuidad de la relación laboral o contractual.

Este acuerdo implica:

- La obligación de mantener en estricta reserva cualquier información obtenida en el marco de sus funciones.
- La prohibición de divulgar, compartir, modificar o utilizar la información confidencial con fines distintos a los autorizados por la compañía.
- El compromiso de custodiar adecuadamente la información, evitando su pérdida, sustracción, alteración o uso indebido.
- La obligación de confidencialidad se mantendrá incluso después de la terminación de la relación laboral o contractual, por el periodo establecido en la

normatividad vigente o el tiempo que resulte necesario para proteger los intereses de la compañía y de sus clientes.

- El incumplimiento de este deber dará lugar a sanciones disciplinarias internas, terminación de la relación contractual y, de ser necesario, a la interposición de acciones legales de carácter civil o penal.
- Asimismo, todos los colaboradores deberán participar en capacitaciones periódicas sobre seguridad de la información, protección de datos personales y prevención de fraudes, dejando evidencia de su asistencia y cumplimiento.
- El acuerdo de confidencialidad cubrirá de manera expresa la protección de datos financieros, transaccionales y sensibles de los usuarios, así como cualquier información estratégica, tecnológica o de control interno de TUMIPAY S.A.S.

II. DERECHOS DEL TITULAR DE LOS DATOS

De acuerdo con la normativa vigente en materia de protección de datos personales, los titulares cuentan con los siguientes derechos:

- Conocer, actualizar y rectificar sus datos personales frente a TumiPay SAS en su calidad de responsable del tratamiento.
- Solicitar prueba de la autorización otorgada para el tratamiento de datos, salvo cuando no sea necesaria según lo establecido en la ley.
- Ser informado sobre el uso que se ha dado a sus datos personales.
- Presentar reclamos ante la Superintendencia de Industria y Comercio (SIC) por infracciones a lo dispuesto en la normativa de protección de datos.
- Revocar la autorización y/o solicitar la supresión de datos cuando no se respeten los principios, derechos y garantías constitucionales y legales.
- Acceder en forma gratuita a sus datos personales, al menos una vez al mes o cada vez que existan modificaciones sustanciales a la política de tratamiento.
- Obtener respuesta oportuna a consultas y reclamos dentro de los plazos legales establecidos.
- Presentar peticiones, quejas o reclamos relacionados con el tratamiento de sus datos a través de los canales de atención definidos por TumiPay SAS.

12. RESPONSABLE DEL TRATAMIENTO

TUMIPAY S.A.S., identificada con NIT 901228648-0, designa a la Coordinadora de Riesgos como responsable de la administración de la presente política de tratamiento de datos personales, garantizando la correcta implementación de las medidas de seguridad, el cumplimiento normativo y la aplicación de sanciones en caso de incumplimiento.

Asimismo, se establece un Comité de Seguridad de la Información, encargado de revisar periódicamente la política y evaluar su eficacia, así como de apoyar la gestión de riesgos asociados al tratamiento de datos personales.

En concordancia con el Manual de Peticiones, Quejas y Reclamos (PQRS), TUMIPAY S.A.S. dispone de canales oficiales para la recepción y gestión de solicitudes relacionadas con el tratamiento de datos y demás inquietudes de cumplimiento, garantizando trazabilidad, confidencialidad y atención oportuna:

- Correo electrónico: ayuda@tumipay.co
- Teléfono: (+57) 3234670890
- Centro de ayuda en línea:

<https://topup.atlassian.net/servicedesk/customer/portals>

- Página web: www.tumipay.co

La gestión de solicitudes se soporta en el aplicativo Jira Service Management (JSM), el cual permite:

- Generar un número único de radicado para cada caso.
- Clasificar solicitudes en peticiones, quejas o reclamos.
- Asignar automáticamente el caso al área responsable.
- Hacer seguimiento en tiempo real del estado de la solicitud.
- Garantizar trazabilidad, control de tiempos y cierre documentado de cada caso.

El Oficial de PQRs supervisa la adecuada atención y registro de las solicitudes en JSM, sirviendo de enlace con entes de control en coordinación con la Coordinadora de Riesgos.

Los titulares podrán ejercer sus derechos a través de estos medios, garantizando una gestión transparente, eficiente y alineada con la normatividad de protección de datos y de consumidor financiero.

Razón Social: TUMIPAY S.A.S.

Dirección: Carrera 11 # 93A – 83, Piso 4, Oficina 408, Bogotá, Colombia.

13. PROCEDIMIENTOS DE ASIGNACIÓN DE RESPONSABILIDADES Y AUTORIZACIONES

Los colaboradores que manejen datos personales deberán cumplir estrictamente con los principios de legalidad, finalidad, libertad, veracidad, transparencia, acceso restringido, seguridad y confidencialidad establecidos en esta política y en la normativa vigente.

Para garantizar un tratamiento adecuado y seguro de la información, se establecen los siguientes procedimientos:

Definición clara de roles y responsabilidades: cada área y cargo tendrá asignadas funciones específicas respecto al tratamiento de datos personales, las cuales estarán documentadas en el manual de funciones y comunicadas al colaborador.

Niveles de acceso diferenciados: el acceso a los datos personales se otorgará de acuerdo con la criticidad y sensibilidad de la información, bajo el principio de mínimo privilegio.

Acuerdos de confidencialidad: todos los colaboradores deberán firmar acuerdos de confidencialidad al inicio de su relación contractual, aplicables durante y después de su vinculación con la compañía.

Registros de acceso y trazabilidad: se mantendrán logs que documenten los accesos, modificaciones o consultas de bases de datos personales, con el fin de detectar y prevenir accesos no autorizados.

Autenticación y controles de seguridad: se implementarán mecanismos técnicos como contraseñas seguras, doble autenticación (2FA) y controles de sesión para reforzar la protección de la información.

Revisión y auditoría periódica: el Comité de Seguridad de la Información y el área de Riesgos revisarán periódicamente los accesos otorgados y las responsabilidades asignadas, ajustándolos en caso de cambios organizacionales o de funciones.

El incumplimiento de estos procedimientos dará lugar a sanciones disciplinarias internas y, de ser necesario, a acciones legales conforme a la ley.

14. PROCEDIMIENTOS PARA EJERCER LOS DERECHOS DEL TITULAR

Los titulares podrán realizar consultas y presentar reclamos a través del correo electrónico ayuda@tumipay.co o mediante el formulario disponible en www.tumipay.co. El trámite se realizará en los siguientes términos:

- Consultas: hasta 10 días hábiles.
- Reclamos: hasta 15 días hábiles, con posibilidad de prórroga en casos justificados.

15. SEGURIDAD DE LA INFORMACIÓN Y DE LA TERCERIZACIÓN DEL TRATAMIENTO

TUMIPAY S.A.S. implementa medidas técnicas, administrativas y organizativas para garantizar la seguridad de la información y evitar el acceso no autorizado, la pérdida o la manipulación indebida de los datos personales. Al momento que TUMIPAY S.A.S. delegue el tratamiento de datos personales a terceros, estos deberán garantizar medidas de seguridad adecuadas. Se incluirán cláusulas contractuales de confidencialidad y auditorías periódicas para verificar su cumplimiento.

16. VALIDACIÓN DE DATOS DE ENTRADA Y PROCESAMIENTO

TUMIPAY S.A.S. implementará procedimientos de validación de datos para garantizar su **exactitud, integridad, pertinencia y coherencia**, minimizando

riesgos asociados a errores, duplicidades o inconsistencias. Estas validaciones se aplicarán tanto en el proceso de recolección como durante el almacenamiento, procesamiento y actualización de la información.

Los controles incluirán, entre otros:

- **Tipos de datos:** verificación de que los valores registrados correspondan al tipo requerido (numéricos, alfabéticos, alfanuméricos, fechas, etc.).
- **Formatos y longitudes:** aplicación de reglas para validar estructuras predefinidas (ej. número de identificación, correos electrónicos, números de teléfono, cuentas bancarias).
- **Pertinencia y coherencia:** análisis de consistencia de la información suministrada frente a los fines declarados y frente a otras variables (ej. fechas válidas, edad coherente con la fecha de nacimiento, domicilios completos).
- **Controles de duplicidad y errores:** detección automática de registros repetidos, datos ficticios o inconsistentes, generando alertas para su corrección o exclusión.
- **Validaciones periódicas:** revisión y depuración de las bases de datos mediante procesos de actualización y auditoría de información.
- **Automatización de controles:** integración de herramientas tecnológicas (incluido el aplicativo Jira y sistemas internos) para realizar verificaciones en tiempo real y asegurar la trazabilidad de los cambios efectuados.

17. PRINCIPIOS DE VERACIDAD Y CALIDAD DE LOS DATOS

Todos los datos personales deberán ser veraces, completos, exactos, actualizados, comprobables y comprensibles. Se prohíbe el registro y divulgación de datos parciales, incompletos, fraccionados o que puedan inducir a error.

- **Legalidad:** El tratamiento de datos personales se realizará conforme a lo establecido en la ley.
- **Finalidad:** La recolección y tratamiento de datos personales tendrá un propósito legítimo e informado al titular.
- **Libertad:** El tratamiento solo se llevará a cabo con el consentimiento previo, expreso e informado del titular.
- **Veracidad o Calidad:** La información recolectada debe ser veraz, completa,

exacta, actualizada y comprobable.

- **Transparencia:** Se garantizará el derecho del titular a obtener información sobre sus datos personales en cualquier momento.
- **Acceso y Circulación Restringida:** El tratamiento estará limitado a lo estrictamente necesario, sin acceso a terceros no autorizados.
- **Seguridad:** Se implementarán medidas para evitar adulteración, pérdida, consulta, uso o acceso no autorizado.
- **Confidencialidad:** Todas las personas involucradas en el tratamiento de datos personales están obligadas a garantizar su reserva.

18. INTERCAMBIO Y ALMACENAMIENTO DE DATOS

TUMIPAY S.A.S. implementará medidas de seguridad en la transmisión y almacenamiento de datos, incluyendo cifrado, monitoreo de acceso y control de dispositivos de almacenamiento externo.

19. PROCEDIMIENTOS PARA LA ATENCIÓN DE CONSULTAS Y RECLAMOS

Se garantizarán mecanismos eficientes para que los titulares ejerzan sus derechos. Las solicitudes serán atendidas en los siguientes plazos:

3. Consultas: Hasta 10 días hábiles.
4. Reclamos: Hasta 15 días hábiles con posibilidad de prórroga.

20. GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN

Se definirá un protocolo de respuesta ante incidentes de seguridad de datos personales, el cual incluirá:

3. Identificación y contención del incidente.
4. Notificación a las partes afectadas.
5. Implementación de medidas correctivas.
6. Registro y análisis de los incidentes para prevenir futuros eventos.

En cumplimiento de la normativa expedida por la Superintendencia de Industria

y Comercio, TUMIPAY S.A.S. informará de manera inmediata a dicha autoridad cualquier incidente o violación que comprometa los códigos de seguridad, integridad o confidencialidad de los datos personales de los titulares, así como aquellos eventos que representen riesgos en la administración y manejo de la información. La comunicación incluirá una descripción del incidente, las medidas adoptadas, la magnitud del impacto y las acciones correctivas implementadas.

21. GESTIÓN DE RIESGOS EN EL TRATAMIENTO DE DATOS

TUMIPAY S.A.S. identifica y gestiona los siguientes riesgos asociados al tratamiento de datos personales:

- Acceso no autorizado.
- Fuga de información.
- Alteración indebida de datos.
- Uso inadecuado de la información.

Se implementarán controles de mitigación como autenticación reforzada, monitoreo continuo y programas de sensibilización en seguridad de la información.

22. PROCEDIMIENTOS PARA LA REVOCATORIA Y SUPRESIÓN DE DATOS

Los titulares podrán solicitar la supresión de sus datos personales de conformidad con la normatividad vigente. Se establecerán mecanismos electrónicos y físicos para la recepción y tramitación de dichas solicitudes.

Los titulares podrán solicitar la eliminación de sus datos personales cuando:

3. No sean tratados conforme a la legislación vigente.
4. Ya no sean necesarios para las finalidades establecidas.
5. Se haya cumplido el tiempo máximo de retención de datos.

23. REGISTRO NACIONAL DE BASES DE DATOS (RNBD)

TUMIPAY S.A.S. está registrada en el RNBD y cumplirá con los requisitos de actualización y reporte de información ante la Superintendencia de Industria y Comercio. Asimismo, realiza los reportes se realizan de manera semestral e incluyen:

3. Modificaciones en las finalidades del tratamiento de datos.
4. Cambios en el responsable del tratamiento de la información.
5. Inclusión o eliminación de bases de datos registradas.
6. Reporte de incidentes de seguridad que hayan afectado la confidencialidad, integridad o disponibilidad de los datos personales.

Adicionalmente, TUMIPAY S.A.S. se compromete a actualizar el RNBD anualmente y a presentar informes en caso de requerimiento por parte de la autoridad reguladora. Esta política rige a partir de la fecha de su publicación y permanecerá vigente mientras se mantenga la relación comercial o legal con el titular de los datos. Cualquier cambio sustancial será comunicado mediante la página web de Tumipay.

24. VIGENCIA DE LA POLÍTICA

Esta política rige a partir de la fecha de su publicación y permanecerá vigente mientras se mantenga la relación comercial o legal con el titular de los datos. Cualquier cambio sustancial será comunicado mediante la página web de Tumipay.

25. APROBACIÓN

FECHA	DESCRIPCION DEL CAMBIO	VERSION	PARTICIPANTES
14/07/2024	Emisión inicial	01	Marcela Santiago Rizo CEO Eder Chávez Customer Success Manager
28/02/2025	Las principales adiciones y modificaciones a la política incluyen la inclusión de Principios Rectores, ampliación de la aplicabilidad, tratamiento de datos sensibles, reportes en el RNBD, seguridad de la información y procedimientos de supresión de datos.	02	Marcela Santiago Rizo CEO Eder Chávez Gerente de Operaciones María José Mejía Sanjuán Coordinadora de Riesgos
07/10/2025	Se actualizó la política acorde a la Circular Externa No. 001 de 2025 el 18 de septiembre de 2025.		Fabián Herazo Head of Legal Ricardo Párraga Gerente de Riesgos y Cumplimiento María José Mejía Sanjuán Coordinadora de Control Interno

ELABORADO POR:	REVISADO POR:	APROBADO POR:
María José Mejía Sanjuán Coordinadora de Riesgos	Marcela Santiago Rizo CEO	Marcela Santiago Rizo CEO

	Eder Chávez Cervera Gerente de Operaciones	Eder Chávez Cervera Gerente de Operaciones
Ricardo Párraga Gerente de Riesgos y Cumplimiento	Fabián Herazo Head of Legal María José Mejía Sanjuán Coordinadora de Control Interno	Fabián Herazo Head of Legal María José Mejía Sanjuán Coordinadora de Control Interno