Política de Tratamiento de Datos Personales de Wagmi S.A.S.

Versión 1.0
Fecha de publicación: 10 de septiembre de 2025
Fecha de entrada en vigencia: 10 de septiembre de 2025

¡Hola! **Wagmi S.A.S.** (en adelante, "**Minteo**") te da la bienvenida a su Política de Tratamiento de Datos Personales (la "**Política de Tratamiento de Datos**"). Minteo es responsable del tratamiento de la información personal que ha sido recolectada y almacenada en desarrollo de sus actividades de negocio. La presente Política de Tratamiento de Datos es obligatoria para Minteo de conformidad con lo dispuesto en los artículos 15 y 20 de la Constitución Política de Colombia, la Ley 1266 de 2008, la Ley 1581 de 2012, el Decreto 1377 de 2013 y demás normatividad aplicable, incluyendo sus posteriores modificaciones.

Como Titular de los Datos Personales que recopila Minteo, encontrarás en esta Política de Tratamiento de Datos información sobre:

¿Cuáles son los datos de identificación de Wagmi S.A.S.?

- **Razón social:** Wagmi S.A.S.
- **NIT:** 901.563.171-5
- **Domicilio:** Bogotá, D.C., Colombia
- **Dirección:** Cl. 99 #10-57 Bogotá, D.C., Colombia
- **Correo electrónico:** soportelegal@minteo.com
- **Teléfono de contacto:** (+57) 305 940 9049

Algunas definiciones para guiarte en la lectura de esta Política de Tratamiento de Datos

Autorización: Es el consentimiento **previo**, **expreso** e **informado** que concede cada Titular para que Minteo lleve a cabo el Tratamiento de sus Datos Personales.

Base de Datos: Es el conjunto organizado de Datos Personales que sea objeto de Tratamiento.

Datos Personales: Es cualquier información que pueda asociarse a uno o varios Titulares **determinados o determinables**.

Datos Sensibles: Son aquellos Datos Personales que afectan la intimidad del Titular o cuyo uso indebido podría generar su discriminación. Por ejemplo, se consideran Datos Sensibles el origen racial o étnico, las convicciones religiosas o filosóficas, la pertenencia a sindicatos, organizaciones sociales o de derechos humanos, la afiliación a partidos políticos (o ideas políticas de oposición), los datos relativos a la salud, a la vida sexual, y los datos biométricos (como huellas dactilares, reconocimiento facial, etc.).

Encargado: Es la persona (natural o jurídica) que realiza el Tratamiento de Datos Personales por cuenta de un Responsable. El Encargado se diferencia del Responsable en que **no puede decidir** sobre la Base de Datos ni sobre el Tratamiento de los Datos Personales. Dependiendo de la forma en la que recibamos tus Datos Personales, Minteo podría actuar como Encargado o como Responsable.

Fuente: Es la persona, entidad u organización que recibe o conoce Datos Personales de Titulares en virtud de una relación comercial o de cualquier otra índole, y que suministra estos datos a un Operador de Información (quien a su vez los entrega al Usuario).

Información Financiera, Crediticia, Comercial, de Servicios y la Proveniente de Terceros Países: Es aquella información relacionada con el nacimiento, ejecución y extinción de obligaciones dinerarias, independientemente del contrato o negocio que les dé origen. (Esta definición corresponde a la utilizada en la Ley 1266 de 2008 sobre información financiera y crediticia).

Operador: Es la persona, entidad u organización que recibe de la **Fuente** Datos Personales sobre varios Titulares, los administra y los pone en conocimiento de los Usuarios, bajo los parámetros de la Ley 1266 de 2008 y sus normas reglamentarias.

Responsable: Es la persona (natural o jurídica) que decide sobre la Base de Datos y el Tratamiento de los Datos Personales. En este caso, Minteo actúa como Responsable del Tratamiento de los datos que recopila directamente.

Titular: Eres **tú**, es decir, la persona natural cuyos Datos Personales son objeto de Tratamiento. Cualquier referencia a “Titular” en esta Política corresponde a ti u otra persona sobre la cual Minteo realiza Tratamiento de Datos Personales.

Transferencia: Ocurre cuando un Responsable del Tratamiento (por ejemplo, Minteo) envía o comunica Datos Personales a otro Responsable (tercero), dentro o fuera de Colombia, para que

ese tercero a su vez trate los datos por su propia cuenta. (Implica un cambio de responsabilidad sobre los datos, bajo cumplimiento de requisitos legales).

Transmisión: Ocurre cuando un Responsable (por ejemplo, Minteo) comunica Datos Personales a un tercero (dentro o fuera de Colombia) para que realice algún Tratamiento por encargo del Responsable y conforme a las finalidades que este le indique, sin que el tercero pueda utilizarlos para fines propios. (En este caso el tercero actúa como Encargado, siguiendo las instrucciones de Minteo).

Tratamiento: Es **cualquier operación** sobre Datos Personales, tal como su recolección, almacenamiento, uso, circulación o supresión.

Usuario: En el contexto de la Ley 1266 de 2008 (hábeas data financiero), es la persona natural o jurídica que puede acceder a la información de uno o varios Titulares, suministrada por un Operador o por una Fuente, para fines permitidos (por ejemplo, un banco que consulta información crediticia de una persona en una central de riesgos). *Nota:* Esta definición aplica principalmente para información crediticia; en el contexto general de la Ley 1581 de 2012, cuando en esta Política hablamos de "Titular" nos referimos a ti como usuario o cliente cuyos datos tratamos.

Normativa aplicable al tratamiento de tus Datos Personales

Esta Política de Tratamiento de Datos se enmarca dentro de las normas vigentes en Colombia en materia de protección de Datos Personales, entre otras, las siguientes:

- **Constitución Política de Colombia, art. 15:** Derecho fundamental a la intimidad y al hábeas data.
- **Ley 1266 de 2008:** Régimen de protección de datos personales en el ámbito de información financiera, crediticia, comercial y de servicios (habeas data financiero).
- **Ley 1273 de 2009:** Delito de violación de datos personales y otras disposiciones sobre protección de la información (introduce protecciones penales).
- **Ley 1581 de 2012:** Régimen General de Protección de Datos Personales ("Ley de Protección de Datos Personales").
- **Ley 2157 de 2021:** Modifica aspectos de la Ley 1266 de 2008 (incluyendo el llamado "borrón y cuenta nueva" en centrales de riesgo) y refuerza derechos de los Titulares.
- **Decreto Único 1074 de 2015 (Decreto 1377 de 2013 incorporado):** Reglamenta parcialmente la Ley 1581 de 2012, incluyendo disposiciones sobre avisos de privacidad, registros de bases de datos, medidas de seguridad, entre otras.

Wagmi S.A.S. declara su compromiso de dar cumplimiento a esta normativa y a los principios generales de protección de datos personales en todas sus actividades de Tratamiento. En especial, garantiza que el Tratamiento de Datos Personales se realizará respetando los principios de legalidad, finalidad, libertad, veracidad o calidad, transparencia, acceso y circulación restringida, seguridad y confidencialidad, conforme a la Ley 1581 de 2012 y normas concordantes.

¿A través de qué canales se recolectan los Datos Personales?

Minteo recolecta Datos Personales principalmente cuando te registras o utilizas sus servicios a través de sus plataformas digitales, por ejemplo: su aplicación móvil o página web. También podemos recolectar datos a través de diferentes **canales de atención al cliente**, tales como chats en línea, redes sociales oficiales, líneas telefónicas de soporte, correo electrónico y cualquier otro canal de comunicación que Minteo habilite para interactuar contigo.

Adicionalmente, podemos obtener información a través de **formularios de vinculación** o registro (ya sean virtuales o físicos) que llenes al momento de contratar con Minteo o de suscribirte a nuestros productos o servicios, así como durante la ejecución de tu relación con nosotros. Por ejemplo, al diligenciar formularios de registro KYC (Know Your Customer), formularios para eventos o promociones de Minteo, encuestas de satisfacción, entre otros.

Asimismo, es posible recolectar información cuando **tú nos contactas** por cualquiera de los medios de contacto que hayas registrado con Minteo (por ejemplo, si nos envías un correo electrónico o mensaje solicitando asistencia, o conversas con nosotros vía chat de soporte).

En algunos casos, Minteo puede recibir visitas de personas a sus instalaciones u oficinas. Si visitas nuestras instalaciones, es posible que solicitemos tus datos de identificación a la entrada, únicamente con propósitos de **control de acceso y seguridad**. Esa información de visitantes se registra para llevar control de posibles incidentes de seguridad y para identificar a las personas que ingresan físicamente a nuestras oficinas.

¿Qué tipos de Datos Personales se recolectan y de qué grupos de interés?

Minteo recolecta Datos Personales de diferentes **grupos de interés** con los que interactúa en desarrollo de su objeto social, todos los cuales son fundamentales para el éxito de nuestra operación. Estos grupos de Titulares incluyen, entre otros:

- **Clientes:** Personas que utilizan los productos o servicios de Minteo (por ejemplo, usuarios de la plataforma Minteo y sus servicios de stablecoins, monederos digitales, etc.).
- **Prospectos de Clientes:** Personas que han manifestado interés en nuestros servicios o con las cuales Minteo tiene acercamientos comerciales, pero que aún no son clientes efectivos.
- **Empleados y contratistas:** Personas vinculadas laboralmente a Minteo (empleados) y quienes prestan servicios bajo contrato independiente (contratistas).
- **Beneficiarios de empleados:** Personas naturales beneficiarias de algún empleado de Minteo, por ejemplo, familiares dependientes incluidos en planes de beneficios legales o extralegales (seguros, etc.).
- **Candidatos a empleo:** Personas que se postulan o participan en procesos de selección para trabajar o prestar servicios en Minteo.
- **Proveedores y aliados comerciales:** Personas (naturales o representantes de personas jurídicas) que proveen bienes o servicios a Minteo, o con quienes se tienen alianzas comerciales o estratégicas.

- **Accionistas:** Personas naturales accionistas de Wagmi S.A.S., si corresponde (incluyendo fundadores u otros inversionistas).
- **Visitantes:** Personas que ingresan físicamente a las instalaciones de Minteo, por ejemplo para reuniones, eventos o visitas de cualquier tipo.

Minteo puede recolectar diversos tipos de Datos Personales de los grupos de interés mencionados, entre los cuales se encuentran los siguientes:

- **Datos de identidad:** información como nombre completo, tipo y número de identificación (por ejemplo, cédula de ciudadanía, cédula de extranjería o pasaporte), fecha de nacimiento, nacionalidad, y en caso de ser necesario para ciertos trámites, copia de documentos de identidad o fotografías para verificar tu identidad.
- **Datos de contacto:** información como dirección de residencia o correspondencia, ciudad y país de domicilio, número de teléfono (móvil o fijo), dirección de correo electrónico, y otros datos similares de contacto.
- **Datos financieros:** información como números de cuenta bancaria, números de tarjetas de crédito o débito u otros instrumentos de pago que utilices en relación con nuestros servicios; información necesaria para procesar pagos o transferencias (por ejemplo, comprobantes de pago, identificadores de transacciones); historial de pagos o cumplimiento de obligaciones dinerarias; y, en caso de que aplique para nuestros servicios, información de perfil crediticio o calificación de riesgo financiero (por ejemplo, consultas o reportes en centrales de riesgo financiero, si es necesario para evaluar solvencia en ciertas operaciones).
- **Datos transaccionales en la plataforma:** información sobre las transacciones que realizas a través de la plataforma de Minteo o servicios asociados, tales como montos transaccionados, fechas y horas de las operaciones, direcciones de monederos o cuentas blockchain involucradas, identificadores de las contrapartes de la transacción (por ejemplo, identificadores de usuarios o comercios con los que interactúas), tipo de activo transado (p. ej., stablecoin, criptomoneda, moneda fíat), y cualquier otro detalle relevante de la operación.
- **Datos sobre el uso de la plataforma:** información acerca de cómo utilizas nuestros productos o servicios digitales, por ejemplo: las secciones de la aplicación o web que más usas, las funcionalidades que activas, el número de transacciones realizadas en determinado período, preferencias de configuración de usuario, entre otros. Esta información nos ayuda a entender tu comportamiento como usuario para mejorar la experiencia y detectar posibles anomalías (como transacciones inusuales que puedan indicar fraude).
- **Datos técnicos de identificación electrónica:** información que se recopila cuando interactúas con nuestras plataformas digitales, como la dirección IP desde la que te conectas, el nombre de usuario y contraseña que utilizas en nuestros servicios (almacenados de forma segura), el tipo y versión del navegador web, el sistema operativo del dispositivo, zona horaria, idioma, identificadores únicos del dispositivo (por ejemplo, ID del dispositivo móvil o identificador publicitario), la marca, modelo y

características del dispositivo, resolución de pantalla, **ubicación geográfica aproximada** (por ejemplo, ciudad o país inferido de la IP), y otros datos técnicos.

- **Datos de geolocalización precisa:** con tu autorización, podemos acceder a datos de tu ubicación geográfica exacta (coordenadas GPS) a través de la aplicación móvil u otros servicios, por ejemplo, para funcionalidades que requieran conocer tu ubicación (como prevenir fraudes o cumplir requisitos regulatorios de conocimiento del cliente). Siempre te solicitaremos permisos en tu dispositivo para ello y puedes activar o desactivar esta opción.
- **Datos de interacción con atención al cliente y mercadeo:** incluyen comunicaciones que intercambias con los equipos de servicio al cliente (por ejemplo, grabaciones de llamadas al soporte, conversaciones por chat de ayuda, correos electrónicos o mensajes que envíes con preguntas o reclamos), encuestas de satisfacción que respondas, comentarios o reseñas que dejes sobre nuestros servicios, participación en concursos o campañas promocionales, y en general cualquier información que nos suministres en interacciones de servicio o marketing.
- **Imágenes o datos de video y audio:** en ciertos casos podríamos obtener imágenes tuyas, por ejemplo, si visitas nuestras oficinas donde hay sistemas de videovigilancia (cámaras de seguridad) o si compartes voluntariamente tu imagen (foto de perfil, etc.) en alguna funcionalidad de nuestra plataforma. También podría tratarse de **datos biométricos** si los recopilamos para verificación de identidad, como tu huella dactilar, rostro o voz (siempre con el debido consentimiento, por ser datos sensibles). Igualmente, si nos llamas, es posible que las llamadas sean registradas. Estas imágenes, videos o audios serán tratados conforme a las finalidades de seguridad o verificación correspondientes.
- **Información sobre transacciones de pago y productos financieros:** si nuestros servicios implican movimientos financieros tradicionales además de blockchain, podríamos recolectar información como: banco o entidad financiera desde la que envías o recibes fondos, referencias de pagos, hora y ubicación de pagos realizados, número de cuenta asociada, confirmaciones de transferencia, y datos del titular del instrumento de pago utilizado. Por ejemplo, al recargar fondos para comprar stablecoins, obtendremos el comprobante de la transferencia y los datos asociados a esa operación.
- **Datos de actividad en línea:** podemos captar información relacionada con tu navegación e interacción en línea con nuestras plataformas, como el historial de páginas o secciones de nuestro sitio que visitaste, términos de búsqueda utilizados dentro de nuestra web, la página web o URL de referencia que te llevó a nuestro sitio, cuánto tiempo navegas en ciertas secciones, clics en botones o enlaces dentro de la plataforma, y otras métricas de interacción. También podemos recibir cierta información de seguimiento mediante cookies o tecnologías similares cuando visitas nuestros portales (ver sección de Cookies más adelante).
- **Información relacionada con la prevención de riesgos financieros y legales:** en el contexto de nuestros procesos de conocimiento del cliente (KYC) y de prevención de lavado de activos y financiación del terrorismo (LA/FT), podríamos recolectar información adicional como: respuestas a cuestionarios de debida diligencia,

documentos que demuestren el origen de fondos, información sobre tu actividad económica, referencias personales o comerciales, resultados de verificaciones en listas restrictivas nacionales e internacionales (ej.: listas OFAC, listados de personas expuestas políticamente - PEP, etc.), antecedentes judiciales o crediticios obtenidos de fuentes legítimas, entre otros datos necesarios para cumplir con obligaciones legales de monitoreo de riesgo. Igualmente, podríamos recolectar datos sobre eventuales procesos de reclamación o quejas, para gestionar adecuadamente los riesgos operativos y legales (por ejemplo, mantener un registro de incidentes de seguridad de la información o fraudes reportados).

Ten en cuenta que la lista anterior es **enunciativa mas no exhaustiva**. Según evolucione nuestra relación contigo o la naturaleza de nuevos productos/servicios de Minteo, podríamos requerir recolectar datos adicionales a los aquí mencionados. En todo caso, cualquier recolección de nuevos datos personales se realizará informándote la finalidad correspondiente y obteniendo tu Autorización cuando la ley así lo exija.

En tu calidad de Titular, **autorizas a Minteo a comprobar la veracidad** de los Datos Personales que nos entregues. Para ello, podremos utilizar fuentes legítimas, tales como consultas a entidades públicas, bases de datos públicas (por ejemplo, el Registro Nacional de Bases de Datos, centrales de riesgo con información pública, registros mercantiles), u otras fuentes de terceros legalmente facultadas para suministrar datos. Esto con el fin de mantener información precisa y actualizada, prevenir fraudes e identificar plenamente a nuestros usuarios conforme a la normativa.

Sobre las cookies que utiliza Minteo y la posibilidad de configurarlas

Minteo recoge información de los usuarios y visitantes de sus páginas web mediante el uso de **cookies** y tecnologías similares. Las cookies son archivos pequeños que se almacenan en tu navegador o dispositivo cuando visitas nuestro sitio, y nos permiten reconocerte y almacenar ciertas preferencias. Utilizamos cookies principalmente con el fin de **mejorar y optimizar tu experiencia** de usuario, ofrecer funcionalidades personalizadas (por ejemplo, recordar tu inicio de sesión o tu idioma preferido) y analizar el desempeño de nuestra plataforma.

Al navegar por el sitio web de Minteo (por ejemplo, en minteo.com y sus subdominios), entendemos que aceptas el uso de cookies, salvo que las hayas desactivado o rechazado a través de las opciones de tu navegador. En la **Política de Cookies** publicada en nuestro sitio web encontrarás información más detallada sobre qué son las cookies, qué tipos de cookies utiliza Minteo (por ejemplo, cookies de sesión, de análisis, de publicidad, propias o de terceros) y cómo puedes configurar o bloquear las cookies según tus preferencias. Ten en cuenta que si decides **rechazar algunas cookies**, es posible que ciertas funcionalidades de la plataforma no operen al 100% (por ejemplo, puede que tengamos que pedirte tus credenciales con más frecuencia al no poder “recordar” tu sesión, o que se reduzca la personalización de contenidos).

Te invitamos a consultar la Política de Cookies en nuestra página para tomar decisiones informadas sobre el uso de estas tecnologías.

¿Se recolectan Datos Sensibles?

Sí, en algunos casos Minteo **puede llegar a recolectar Datos Sensibles** tuyos, pero lo hará cumpliendo estrictamente las normas vigentes en Colombia para la protección de este tipo especial de datos. En particular, de acuerdo con la Ley 1581 de 2012 y sus decretos reglamentarios, Minteo tratará tus Datos Sensibles **solo cuando**:

- **Tengamos tu Autorización explícita como Titular.** Es decir, que nos hayas dado tu consentimiento previo, expreso e informado para tratar esos datos sensibles, excepto en los casos en que por ley **no se requiera dicha Autorización**. *Por ejemplo*, la ley permite que **no se requiera autorización** para el tratamiento de datos sensibles cuando se utilizan con fines históricos, estadísticos o científicos, siempre que se adopten las medidas de disociación correspondientes. En cualquier otro caso, de necesitar datos sensibles tuyos, te solicitaremos claramente tu consentimiento y te informaremos la finalidad.
- **El Tratamiento sea necesario para salvaguardar tu** interés vital **y estés física o jurídicamente incapacitado para dar tu autorización.** En tales eventos excepcionales (por ejemplo, emergencias médicas donde no puedas consentir), los representantes legales (como tu tutor, curador o apoderado) podrán otorgar la autorización en tu nombre. Esta excepción busca proteger tu vida o salud.
- **El Tratamiento recaiga en datos sensibles que sean necesarios para el reconocimiento, ejercicio o defensa de un derecho en un proceso judicial.** Por ejemplo, si Minteo necesita aportar o tratar datos sensibles tuyos dentro de un litigio o proceso legal para la defensa de sus derechos o los tuyos, podrá hacerlo sin autorización previa en la medida que la ley lo permita.

En todo caso, **Minteo NO realizará el Tratamiento de tus Datos Sensibles para finalidades distintas** a aquellas que te hayamos informado y para las cuales nos diste autorización, o a las previstas de manera expresa en la ley. Como Titular, tienes el **derecho de abstenerte** de autorizar el Tratamiento de tus Datos Sensibles. Por ello, la prestación de nuestros servicios **nunca está condicionada** a que nos suministres Datos Sensibles, salvo que estos sean **indispensables** para la celebración o ejecución de la relación contractual que tengas con nosotros. (En cuyo caso te explicaremos por qué son necesarios; por ejemplo, la captura de tu huella dactilar podría ser indispensable si en el futuro oficiamos como entidad obligada a tomar datos biométricos para validar identidad en transacciones financieras).

¿Cuándo se recolectan Datos Personales a través de terceros?

Minteo puede recolectar Datos Personales tuyos a través de **terceros autorizados**, en las siguientes modalidades:

1. **Directamente del Titular:** Esta es la forma principal de recolección – eres tú quien nos entrega tus datos por los distintos medios (formularios, página web, app, etc.) como describimos anteriormente.

2. **Mediante terceros autorizados a Transferir o Transmitir los Datos Personales a Minteo:** Es decir, podemos recibir datos que te conciernen desde fuentes externas que tengan tu autorización o una base legal para compartir esos datos con nosotros.
3. **A partir de fuentes de acceso público:** También podemos recopilar datos que se encuentren disponibles al público, para verificar información o enriquecer nuestros datos básicos, siempre respetando la normativa. Por ejemplo, podríamos consultar bases de datos públicas gubernamentales, registros abiertos o información que hayas hecho pública en redes sociales o internet, siempre que sea pertinente y respetando tu privacidad.

Algunas formas concretas en que Minteo recolecta Datos Personales **mediante terceros autorizados** incluyen:

- **A través de Operadores de Información crediticia o financiera:** Por ejemplo, podríamos consultar tus datos en centrales de riesgo crediticio (como Datacrédito o CIFIN) u operadores de información financiera, con tu autorización, para conocer tu historial en caso de ser necesario evaluar riesgos o cumplir obligaciones de monitoreo financiero.
- **A través de proveedores o aliados con los que tengamos contratos para operar nuestro negocio:** Por ejemplo, si usamos un servicio de verificación de identidad de un tercero, este podría recolectar y transmitirnos el resultado de la validación de tus datos; o si contamos con aliados comerciales que ofrecen servicios complementarios y tú los adquieres, ellos podrían compartirnos cierta información tuya para integrar la prestación del servicio. Siempre exigiremos que dichos terceros cuenten con tu autorización o con una base legal válida.
- **Mediante fuentes de acceso público:** Como se mencionó, esto implica extraer información de registros o publicaciones disponibles públicamente. Siempre corroboraremos que sean realmente fuentes públicas y utilizaremos la información de forma pertinente.
- **A través de otros Titulares vinculados o de entidades financieras y actores del ecosistema de pagos electrónicos:** Por ejemplo, podríamos recibir información desde una entidad financiera aliada cuando coordinamos un movimiento de fondos (si envías dinero desde tu banco a nuestra cuenta de custodia, el banco nos proveerá ciertos datos de la transacción); o de un **exchange** o plataforma externa si así lo autorizas para interoperar con Minteo; o incluso de otros usuarios, en casos como referidos (si un usuario te refiere, puede entregarnos tu correo para invitarte a usar la plataforma, siempre que ese tercero garantice tener tu permiso para compartirlo).

Por favor ten en cuenta que las formas anteriores son **enunciativas** y se dan para facilidad de referencia en esta Política. Minteo podría recolectar Datos Personales de otras formas adicionales, pero en todo caso **siempre lo hará de acuerdo con la normativa vigente en Colombia**, obteniendo las autorizaciones requeridas y respetando los principios de la protección de datos.

¿Cuáles son las finalidades del tratamiento de tus Datos Personales?

Al ser Titular de los datos y aceptar esta Política, **autorizas a Wagmi S.A.S.,** así como a sus eventuales empresas **matrices, subordinadas o afiliadas**, y a cualquier **cesionario o beneficiario** presente o futuro de sus obligaciones y derechos, para que –directamente o a través de **terceros Encargados**– puedan tener acceso a la información personal que suministras y realicen el Tratamiento de tus Datos Personales (recolección, almacenamiento, uso, circulación, supresión, etc.) de acuerdo con las finalidades establecidas en esta Política de Tratamiento de Datos.

Minteo llevará a cabo el Tratamiento de tus Datos Personales con el fin de **cumplir** las siguientes **finalidades**:

Finalidades **comunes** a **todos** los grupos de interés:

- **Registro y gestión de bases de datos:** Conocer, almacenar y procesar tus Datos Personales en las bases de datos de Minteo, de forma adecuada, ordenada y permitiendo su posterior uso para las finalidades autorizadas. Esto implica crear tu perfil o expediente como cliente, empleado, proveedor, etc., y mantener un registro actualizado de tus datos.
- **Vinculación contractual y cumplimiento legal:** Establecer, ejecutar y gestionar la relación **precontractual, contractual** o **poscontractual** que surja entre tú y Minteo, sea de naturaleza comercial, civil, laboral o de cualquier otra índole, en virtud del cumplimiento de obligaciones legales o contractuales. Por ejemplo, usar tus datos para celebrar un contrato de servicios, para ejecutar transacciones ordenadas por ti, para expedir certificaciones contractuales, o para dar cumplimiento a requisitos de ley asociados a la relación (como reportes tributarios, aportes a seguridad social en caso de empleados, etc.).
- **Validación de la información:** Validar, verificar y comprobar los Datos Personales que nos entregues en cualquier momento, o que entregue un tercero autorizado por ti. Esta validación puede incluir verificación de datos sensibles como biometría (por ejemplo, autenticar tu identidad mediante reconocimiento facial o de huella) u otras verificaciones documentales (como comparar con bases de datos gubernamentales). La finalidad es asegurar la veracidad de la información y prevenir suplantaciones o errores.
- **Prevención del fraude, lavado de activos y actividades ilícitas:** Prevenir y detectar eventuales **operaciones de lavado de activos, financiación del terrorismo**, fraude, corrupción u otras actividades ilegales. Esto incluye el derecho/deber de **“conocer al cliente”** (KYC) que tiene Minteo respecto de los Titulares con quienes entabla relaciones contractuales, a fin de evaluar el riesgo presente o futuro de dichas relaciones y servicios. Por ejemplo, Minteo podría monitorear transacciones inusuales y, de ser necesario, reportar ciertas operaciones a las autoridades competentes (UIAF) conforme a la ley.
- **Consulta en listas restrictivas y cumplimiento de SARLAFT:** Consultar en listas vinculantes y restrictivas nacionales o internacionales (como las listas de personas bloqueadas por OFAC, listados de la ONU, entre otras) y obtener toda la información necesaria para el cumplimiento de las obligaciones derivadas del **SARLAFT** (Sistema de

Administración de Riesgos de LA/FT) y **SAGRILAFT** (Sistema de Autocontrol y Gestión del Riesgo Integral LA/FT y de la Financiación de la Proliferación de Armas de Destrucción Masiva) que apliquen a Minteo. En resumen, adoptar debida diligencia ampliada cuando corresponda, para no vincular a la plataforma personas reportadas por actividades ilícitas.

- **Consulta de bases de datos públicas:** Consultar y tratar Datos Personales que se encuentren en bases de datos de naturaleza pública (por ejemplo, registros públicos, datos abiertos del gobierno, información en medios de comunicación) cuando sea pertinente para las finalidades aquí señaladas, respetando siempre la finalidad para la cual esos datos son públicos.
- **Comunicación y transferencia a aliados y terceros autorizados:** Transferir o Transmitir tus Datos Personales –dentro o fuera de Colombia– a **terceros** con los cuales Minteo tenga una relación comercial, a sus aliados estratégicos, o a sus **empresas vinculadas** (por ejemplo, una empresa matriz o subsidiaria, o entidades pertenecientes al mismo grupo empresarial), siempre en el marco del respeto de las finalidades informadas al Titular y aplicando medidas de diligencia para cuidar la información. Cualquier Transferencia o Transmisión se realizará de acuerdo con la normatividad vigente en Colombia, lo que implica que el tercero receptor estará sujeto a obligaciones de protección de datos equivalentes. (Por ejemplo, podríamos transmitir datos a un proveedor de servicios en la nube que almacena la base de datos, o a un aliado que provee un servicio complementario que has solicitado, asegurándonos de que ese tercero proteja tus datos).
- **Atender peticiones, quejas o reclamos:** Responder y gestionar las peticiones, consultas, reclamos o quejas que presentes a través de los canales habilitados por Minteo. Esto incluye usar tus datos de contacto para darte respuesta en los términos de ley, hacer seguimiento interno a tu requerimiento y eventualmente mejorar nuestros procesos con base en tu retroalimentación.
- **Consultas a operadores de información financiera/crediticia:** Consultar tus Datos Personales y tu "Información Financiera, Crediticia, Comercial, de Servicios y la Proveniente de Terceros Países" en **centrales de riesgo crediticio** u otros Operadores de información, con el fin de determinar la viabilidad de entablar o mantener una relación contractual contigo y gestionar riesgos financieros y crediticios asociados. Esto puede incluir, por ejemplo, verificar tu comportamiento de pago o nivel de endeudamiento si Minteo llegase a ofrecerte una línea de crédito o facilidad de pago. También puede relacionarse con actividades de prevención de LA/FT, recaudación de cartera e identificación de posible fraude. *(Esta finalidad se aplica principalmente si Minteo desarrolla productos financieros como créditos, lo cual podría no ser el caso actualmente; de no aplicar, estos datos no serán consultados.)*
- **Reportes a centrales de riesgo u operadores de información:** Reportar ante **Centrales de Riesgo** u otros operadores de información financiera o crediticia el **cumplimiento o incumplimiento** de tus obligaciones con Minteo, incluyendo tu historial de pagos, eventuales **solicitudes de crédito** que realices, obligaciones de contenido patrimonial a tu cargo, así como cualquier otra información relacionada con la administración del

riesgo financiero y crediticio. Esta finalidad se llevará a cabo **solo si** Minteo en algún momento te otorga créditos, financiamientos u obligaciones dinerarias cuyo reporte sea procedente; en tal caso se te informará debidamente. También cubre la posibilidad de reportar conductas fraudulentas comprobadas para alertar al sistema financiero, conforme a la ley.

- **Solicitar autorizaciones de cobro ante entidades autorizadas:** Solicitar, en caso de ser necesario, la autorización de cobro ante las entidades definidas y autorizadas para ello. Por ejemplo, si has dado una instrucción de cargo automático a tu tarjeta o cuenta bancaria para fondear tu cuenta en Minteo, podríamos enviar tu identificación a la red financiera para solicitar dichos cobros recurrentes, con tu previo consentimiento.
- **Control de acceso físico y seguridad en instalaciones:** Controlar el acceso a las instalaciones físicas de Minteo (oficinas, centros de experiencia, etc.), con el fin de mantener la seguridad de nuestros colaboradores, visitantes, bienes y activos de la compañía. Esto incluye registrar quién ingresa (como mencionamos en la sección de recolección de datos de visitantes) y llevar un registro que pueda usarse en caso de incidentes de seguridad (por ejemplo, una emergencia o investigación interna por pérdida de equipos).
- **Videovigilancia y seguridad física:** Implementar políticas de seguridad física que pueden involucrar sistemas de **videovigilancia** en nuestras instalaciones. Si tenemos cámaras de seguridad, su uso se rige por las directrices de la Superintendencia de Industria y Comercio (SIC) plasmadas en la "Guía para la Protección de Datos Personales en Sistemas de Videovigilancia". Solo se usarán las grabaciones para propósitos de seguridad, protección de personas y bienes, y eventualmente como prueba ante actos que atenten contra la seguridad.
- **Gestiones de facturación y contabilidad:** Realizar todos los trámites relacionados con la facturación, cobro y pago de nuestros productos y/o servicios, tanto hacia clientes como con proveedores. Esto incluye emitir facturas electrónicas o documentos equivalentes, llevar contabilidad de las operaciones, gestionar cobranzas de facturas vencidas, y conservar los soportes contables que contengan tus datos conforme a la ley tributaria y comercial.

Finalidades del Tratamiento de Datos Personales de **clientes, prospectos de clientes y compradores:**

- **Seguimiento al contrato y soporte al cliente:** Contactarte para hacer seguimiento a la ejecución del contrato que tienes con Minteo e informarte sobre el desarrollo del mismo. Esto abarca comunicaciones operativas, por ejemplo, para notificarte del estado de una transacción, confirmación de la apertura de tu cuenta, cambios en políticas que afecten el servicio, anuncios de mantenimiento de la plataforma, entre otros asuntos directamente relacionados con el servicio contratado.
- **Prevención de fraudes en el ecosistema de pagos:** Transferir o Transmitir a los diferentes actores del sistema de pagos (tradicional o cripto) información relacionada con **posibles fraudes o suplantaciones de identidad**, con el fin de prevenir dichas conductas ilícitas. Por ejemplo, si Minteo detecta o tiene evidencia de que cierta

transacción está vinculada a un fraude, podrá alertar a otras entidades financieras o plataformas involucradas en la red de pagos para bloquear fondos o tomar medidas, conforme a los protocolos establecidos en la industria y la ley. Esto siempre se hará protegiendo, en lo posible, tu identidad frente a terceros no autorizados y únicamente con entidades facultadas para manejar dicha información.

- **Actividades de mercadeo y promociones:** Contactarte –directamente Minteo o a través de terceros aliados– con fines de **mercadeo**, para proporcionarte información sobre **productos, servicios, regalos, ofertas y promociones** tanto propios de Minteo como de sus aliados comerciales. Este contacto promocional puede realizarse a través de diversos medios, por ejemplo: notificaciones push en la aplicación, correos electrónicos de marketing, llamadas telefónicas, mensajes de texto SMS, mensajes por aplicaciones de mensajería instantánea (como WhatsApp o Telegram), anuncios en redes sociales, o cualquier otro canal de comunicación que hayas autorizado. Siempre tendrás la posibilidad de optar por no recibir este tipo de comunicaciones ("opt-out") a través de los mecanismos que proveamos en cada mensaje.
- **Personalización de experiencia y publicidad dirigida:** Contactarte (o mostrarte contenido) de forma **personalizada** para proporcionarte anuncios, contenidos e información adaptados a tus intereses y perfil; así como para **monitorizar y analizar la efectividad** de nuestras actividades de marketing. Esto puede implicar el **perfilamiento** de tus hábitos de uso y preferencias, utilizando información recopilada en múltiples sitios, dispositivos o plataformas asociadas (p. ej., si interactúas con nuestras redes sociales y también con nuestra app). Por ejemplo, podríamos mostrarte en nuestra app una promoción especial en base a tu uso frecuente de cierto servicio, o podríamos contratar la difusión de publicidad en sitios web de terceros dirigida a segmentos de usuarios similares a ti. Todas estas actividades se realizan con herramientas que pueden usar cookies, pixel tags u otros medios, pero siempre podrás ajustar tus preferencias de privacidad en dichos servicios de terceros (por ejemplo, a través de la configuración de anuncios de Google o Facebook) para limitar la publicidad basada en intereses.
- **Gestión de cobranza:** Contactarte (directamente o a través de gestores de cobranza externos) para realizar la **gestión de cobro** de obligaciones pendientes que tengas con Minteo, ya sea por cuotas de crédito vencidas (en caso de que existan productos de crédito), tarifas o comisiones no pagadas, saldos en mora u otras obligaciones financieras. Este contacto de cobranza podrá efectuarse mediante llamadas telefónicas, notificaciones push, correos electrónicos, mensajes de texto, mensajes por aplicaciones de mensajería instantánea u otros medios que hayas autorizado. Asimismo, se te podrán enviar recordatorios de pago y notificaciones sobre el estado de tu deuda. Siempre buscaremos manejar esta información de manera confidencial y respetuosa.
- **Prospección comercial:** Analizar tu información para identificar posibles **necesidades, preferencias o gustos** y así desarrollar o ofrecer productos y servicios que se ajusten a ellos. Esto implica que Minteo puede realizar estudios de mercado, segmentación de clientes, análisis estadísticos y de comportamiento, con base en la información de tus transacciones y uso de nuestros servicios, con miras a mejorar la oferta comercial y proponer nuevas soluciones que sean relevantes para ti.

- **Comunicación legal y transaccional:** Enviarte información de carácter legal o transaccional relacionada con los productos o servicios que uses. Por ejemplo, notificaciones de cambios en los términos y condiciones o en esta Política de Datos, avisos sobre actualización de tarifas, comunicaciones sobre la disponibilidad de nuevos features de seguridad, o mensajes transaccionales como alertas de transferencia, comprobantes digitales de tus movimientos, entre otros. Estos mensajes pueden ser enviados vía email, notificación en la aplicación, SMS u otros canales pertinentes, y a diferencia de los mensajes de mercadeo, estos **no puedes dejarlos de recibir** mientras seas cliente activo, ya que son necesarios para la correcta prestación del servicio y para informarte tus derechos u obligaciones.
- **Analítica de datos para mejoras y modelos de negocio:** Analizar tus Datos Personales, datos transaccionales y datos de comportamiento en la aplicación, página web o interacciones por correo, con el fin de **definir perfiles de usuario** y extraer conocimiento que sirva para múltiples propósitos empresariales, tales como estructurar modelos de crédito (en caso de ofrecerse financiamiento), habilitar alianzas comerciales (por ejemplo, identificando segmentos para programas de beneficios con terceros), mejorar nuestros productos y servicios existentes, establecer preferencias generales de los usuarios, y realizar **investigaciones estadísticas, de riesgo, de mercado, comerciales y financieras**. Estas actividades analíticas buscan en conjunto entender mejor a nuestra clientela para innovar y fortalecer la propuesta de valor de Minteo. En la medida de lo posible, para estos fines utilizamos datos **anonimizados o agregados** que no te identifiquen personalmente, a menos que el análisis individualizado sea estrictamente necesario.
- **Procesar pagos electrónicos en la plataforma:** Ejecutar y facilitar los pagos electrónicos que realices a través de la plataforma de Minteo, lo cual incluye: procesar órdenes de transferencia o intercambio de activos digitales o fiat, comunicarnos con las redes o entidades encargadas de liquidar dichas operaciones (como pasarelas de pago, redes blockchain, bancos corresponsales), mantener el debido soporte y registro de todas las transacciones para fines contables y de atención al cliente, y resolver cualquier solicitud o reclamo en relación con esos pagos electrónicos (por ejemplo, investigar un pago no reconocido o reversar una transacción duplicada). Para cumplir esta finalidad, Minteo puede designar **Encargados** que provean infraestructura tecnológica o servicios operativos (por ejemplo, un procesador de pagos, un custodio de activos digitales, servicios de “nodo” en blockchain, etc.), en cuyo caso dichos encargados tratarán tus datos únicamente para los fines aquí descritos.
- **Prestación eficiente de servicios financieros asociados:** Brindar una adecuada prestación y administración de los servicios financieros que pudieran estar asociados a tu relación con Minteo, incluyendo la gestión de **cobros**, pagos, depósitos, retiros, conversiones de moneda y, de ofrecerse en el futuro, **créditos** u otros productos financieros que solicites. Esto comprende todo el ciclo operacional necesario para ejecutar tus instrucciones y mantener tus fondos seguros: desde registrar un depósito en tu cuenta en pesos, convertirlo a un stablecoin, facilitar pagos a terceros, hasta procesar tus retiros de vuelta a dinero fiat; así como administrar cualquier cartera de créditos

(otorgar, hacer seguimiento, cobrar, etc.). Siempre conforme a lo pactado en los contratos de servicio y siguiendo las normas aplicables del sector financiero, de valores o las que correspondan a la naturaleza de las operaciones.

- **Atención de solicitudes de servicios:** Estudiar y dar trámite a las **solicitudes de servicios** o productos que realices en cualquier momento. Por ejemplo, si pides aumentar tus límites transaccionales, solicitar la emisión de un nuevo producto, cambiar de plan de servicio, etc., Minteo usará tus datos para evaluar la solicitud (incluyendo posiblemente tu historial con nosotros u otra información relevante) y luego procederá a ejecutar lo solicitado y a prestarte el nuevo servicio derivado de esa solicitud. Esta finalidad incluye asegurar el cumplimiento de la normativa y la jurisprudencia aplicable para cada nuevo servicio que se te brinde (por ejemplo, si pides un producto regulado, cumplir con sus requisitos).
- **Ofrecimiento de servicios de terceros o complementarios:** Ofrecerte, ya sea en conjunto con terceros, separadamente o a nombre de terceros, **servicios financieros, comerciales, de seguridad social y/o conexos** a los servicios de Minteo. Esto significa que podríamos presentarte o recomendarte servicios adicionales que consideramos pueden aportar valor para ti, aunque no sean desarrollados directamente por Minteo, sino por aliados o terceros. Por ejemplo, podríamos facilitarte la afiliación a un servicio de billetera asegurada por un aliado, o presentarte productos de seguro, o beneficios de seguridad social simplificada, entre otros, siempre informándote quién ofrece el servicio y bajo qué condiciones. En tales casos, si aceptas, Minteo podría actuar como intermediario para tu vinculación con ese tercero (transfiriéndole tus datos básicos con tu autorización) o integrando funcionalidades de ese tercero en nuestra plataforma.

(Nota: Las finalidades anteriores aplican a los usuarios en su rol de clientes o potenciales clientes de Minteo. Siempre que te contactemos con fines comerciales, respetaremos tus decisiones frente a recibir o no dichas comunicaciones, y nos abstendremos de enviarte publicidad no solicitada si has manifestado no desearla.)

Finalidades del Tratamiento de Datos Personales de **empleados, contratistas y beneficiarios de empleados:**

- **Administración del talento humano:** Llevar a cabo todos los procesos necesarios para la **contratación** y vinculación de nuestros empleados y contratistas, así como la gestión integral de la **relación laboral** o de prestación de servicios. Esto incluye el Tratamiento de datos desde la firma del contrato (o nombramiento) hasta su terminación, cumpliendo con obligaciones legales laborales y de seguridad social.
- **Cumplimiento de obligaciones laborales y derechos del empleado:** Desarrollar los **deberes y derechos** que emanan de la relación laboral o contractual. Por ejemplo, usar los datos del empleado para afiliarlo a EPS, ARL, Caja de Compensación; reportar novedades a la seguridad social; gestionar licencias, ausentismos o vacaciones; procesar el pago de nómina y prestaciones sociales; efectuar retenciones de ley; evaluar el desempeño; aplicar medidas disciplinarias si fuere el caso; y en general todo lo relacionado con la administración del personal.

- **Comunicación interna y seguimiento:** Hacer **seguimiento a la gestión** del empleado o contratista, para lo cual Minteo puede recolectar información sobre el cumplimiento de sus responsabilidades (indicadores de trabajo, reportes de proyectos, etc.) y generar comunicaciones o informes internos. Asimismo, enviar al empleado o contratista información relevante para la adecuada ejecución de sus labores (por ejemplo, comunicaciones corporativas, anuncios de cambios en políticas internas, invitaciones a capacitaciones, etc.).
- **Salud y seguridad en el trabajo:** Gestionar la información necesaria en materia de seguridad y salud en el trabajo, incluyendo datos de accidentes laborales o incidentes, historias clínicas ocupacionales (si las administra Minteo directamente o a través de proveedores de salud ocupacional), restricciones médicas, etc., con el fin de garantizar un ambiente de trabajo seguro y cumplir con la normativa de riesgos laborales. Este tratamiento de datos sensibles (salud) se hace con estricta confidencialidad y solo para dichos fines preventivos o de atención en caso de emergencias.
- **Beneficios y bienestar:** Administrar los **beneficios** ofrecidos a los empleados y, en su caso, a los beneficiarios de estos (como cónyuge e hijos). Por ejemplo, si Minteo otorga un seguro colectivo o un plan de medicina prepagada, tratará los datos necesarios de los beneficiarios para afiliarlos; igualmente, gestionar programas de bienestar, fondos de empleados, actividades de capacitación, educación o recreación, para lo cual se podrán usar datos como fechas de cumpleaños, número de hijos (para días especiales), intereses formativos, etc. Siempre buscando el bienestar del empleado y su familia dentro del marco laboral.
- **Relación con beneficiarios:** En caso de beneficiarios de empleados (p. ej., para pago de cesantías por fallecimiento, beneficiarios de seguro de vida colectivo, etc.), tratar sus datos únicamente para realizar las gestiones necesarias derivadas de la relación que tenían con el empleado. Por ejemplo, contactar al cónyuge supérstite o padres de un empleado para tramitar un pago pendiente.
- **Control de acceso y recursos corporativos:** Gestionar el acceso de los colaboradores a las instalaciones y a los sistemas de información de Minteo. Esto puede implicar el registro y seguimiento de accesos con tarjeta o biometría, la asignación de credenciales de usuario para sistemas internos, monitoreo del uso de recursos tecnológicos corporativos conforme a las políticas de la empresa, etc., siempre dentro del marco de la relación laboral y con respeto a la dignidad del empleado. Cualquier monitoreo de correo corporativo u otros medios se realizará conforme a la ley y a las políticas explícitas informadas al empleado.
- **Terminación de la relación y post-contractual:** Una vez terminado el vínculo laboral o contractual, conservar la información del ex-colaborador conforme a los plazos legales (ej.: archivo de historia laboral mínimo 30 años según la ley colombiana) y utilizarla para finalidades legales post-contractuales, como emisión de certificados de trabajo, responder solicitudes de referencias laborales (si el empleado lo autoriza), atender requerimientos de autoridades (ej.: aportes, investigaciones) o gestiones de seguridad social post-empleo.

Finalidades del Tratamiento de Datos Personales de candidatos a empleados o contratistas:

- **Procesos de selección:** Llevar a cabo los procesos de **reclutamiento, evaluación y selección** de personal para eventuales vinculaciones laborales o contractuales con Minteo. Esto implica usar los datos que nos proporcionas en tu **hoja de vida (currículum)**, formularios de aplicación, entrevistas, pruebas psicotécnicas o técnicas, verificación de referencias personales y laborales, validación de títulos académicos, resultados de pruebas, entre otros, con el fin de determinar tu idoneidad para el cargo o proyecto al cual te postulaste.
- **Contactar al candidato:** Comunicarnos contigo durante el proceso de selección para informar avances, solicitar documentación adicional, agendar entrevistas o pruebas, o finalmente extenderte (o no) una oferta de vinculación. Utilizaremos tus datos de contacto para estos fines dentro de un período razonable relacionado con el proceso de selección.
- **Cumplir requisitos pre-contractuales:** En caso de que avances en el proceso, recolectar datos adicionales necesarios antes de la contratación, como antecedentes disciplinarios (Certificado Procuraduría), antecedentes judiciales (Certificado Policía o antecedentes penales), resultados de exámenes médicos de ingreso (datos de salud ocupacional, sensibles, tratados con estricta reserva), entre otros que la ley permita y sean pertinentes para formalizar la contratación.
- **Reserva de candidatos para futuras oportunidades:** Salvo que nos indiques lo contrario, Minteo podría conservar tu información como candidato (hoja de vida, resultados de pruebas, etc.) en nuestro **banco de talentos** incluso si en esta ocasión no fuiste seleccionado, con el propósito de tenerte en cuenta en futuros procesos de selección que se ajusten a tu perfil. Si prefieres que eliminemos tus datos tras culminar el proceso actual, puedes ejercer tu derecho de supresión y los eliminaremos, conservando únicamente los datos mínimos necesarios para no volver a contactarte si así lo señalas.

Finalidades del Tratamiento de Datos Personales de proveedores y aliados:

- **Selección y evaluación de proveedores:** Llevar a cabo el proceso de **búsqueda, evaluación, selección y contratación** de proveedores de bienes y servicios que Minteo requiera para su operación, así como de aliados comerciales. Esto incluye tratar los datos de contacto e identificación del proveedor (o su representante legal y personas de contacto), su información legal y financiera (certificados de existencia, estados financieros si se solicitan, referencias comerciales), con el fin de verificar su **idoneidad personal** y la **experiencia técnica o profesional** requerida para la labor que prestará. También podemos realizar validaciones en listas restrictivas o antecedentes de los proveedores claves, en cumplimiento de políticas LA/FT similares a las aplicadas a clientes, para asegurar la debida diligencia en la cadena de suministro.
- **Gestión del contrato con el proveedor/aliado:** Administrar la relación contractual con nuestros proveedores y aliados comerciales. Esto implica usar la información de contacto para las comunicaciones ordinarias (órdenes de compra, envío de instrucciones, coordinación de entregas o prestación de servicios), procesar y pagar las facturas presentadas por el proveedor, llevar registros de cumplimiento, gestionar

renovaciones o terminaciones de contrato, y en general, cumplir con las obligaciones contractuales adquiridas.

- **Cumplimiento de obligaciones legales con proveedores:** Dar cumplimiento a disposiciones legales relativas a nuestros proveedores, por ejemplo, reportes tributarios (retenciones en la fuente practicadas a un contratista independiente, que implican tratar su NIT/Cédula y valores pagados), reportes a entes de control si aplica (p. ej., informes a la DIAN sobre pagos a terceros), cumplimiento de la normativa de pagos de seguridad social para contratistas, entre otros.
- **Comunicación y coordinación:** Mantener una comunicación eficiente con el proveedor o aliado para asegurar la calidad en la prestación del servicio o entrega del bien. Podremos usar los datos (teléfono, email) de sus representantes o personas designadas para notificar requisiciones, solicitar soporte técnico, coordinar proyectos conjuntos de alianza, intercambiar publicidad conjunta, o cualquier interacción propia del relacionamiento comercial.
- **Registro como tercero en sistemas contables:** Incluir los datos básicos del proveedor (razón social, NIT, dirección, cuenta bancaria, representante) en nuestros sistemas contables y de pagos, así como en nuestras bases de datos de terceros, para efectos administrativos y financieros. Esto conlleva conservar sus datos por el tiempo requerido legalmente (p. ej., soportes de pago mínimo 5 años por normatividad tributaria).

(Adicionalmente, aunque no esté separado como categoría, Minteo también podría tratar datos de accionistas de la compañía, con finalidades como: llevar el registro de accionistas conforme a la ley, realizar convocatorias a asambleas, pagar dividendos o utilidades, y atender consultas o solicitudes de los propios accionistas. Estos tratamientos se realizan en el marco de lo dispuesto en el Código de Comercio y normas societarias. Dado que son pocas personas y usualmente no se difunde a terceros esa información, se considera incluida dentro de las finalidades generales y legales.)

Importante: Minteo garantiza que todas las finalidades descritas se realizan respetando los principios de necesidad y proporcionalidad. Es decir, **solo trataremos tus Datos Personales en la medida en que sean adecuados, pertinentes y limitados a lo necesario** en relación con las finalidades mencionadas. Si en el futuro necesitáramos tratar tus datos para una finalidad distinta a las aquí listadas, te informaremos de ello y, cuando la ley lo exija, solicitaremos nuevamente tu autorización.

Transferencia y Transmisión de Datos Personales

De acuerdo con las finalidades expuestas en la sección anterior, Minteo, en calidad de Responsable del Tratamiento, **puede Transferir o Transmitir tus Datos Personales** a terceros, tanto a nivel nacional como internacional. Esto siempre se hará **en la medida necesaria** para cumplir las finalidades descritas y **respetando la normatividad vigente en Colombia**, en especial las disposiciones de la Ley 1581 de 2012 sobre transferencias internacionales de datos.

Minteo se compromete a adoptar lineamientos y medidas de diligencia apropiadas para garantizar la seguridad y confidencialidad de tus datos durante una Transferencia o Transmisión. Antes de compartir datos personales con cualquier tercero, nos aseguramos de que:

- Exista una **causal legal** que permita la entrega de los datos (por ejemplo, tu autorización, un contrato con cláusulas de protección de datos, un deber legal, etc.).
- El tercero receptor (sea un aliado, proveedor o filial) esté **obligado contractualmente** a proteger tus Datos Personales con estándares iguales o superiores a los que aplicamos internamente. Esto suele formalizarse mediante acuerdos de confidencialidad o acuerdos de Tratamiento de Datos (DTAs) con cláusulas de protección de datos.
- Si es una **Transmisión** (el tercero actúa como Encargado), únicamente trate los datos conforme nuestras instrucciones y para los fines autorizados, y no los use para propósitos propios no autorizados.
- Si es una **Transferencia internacional** (entrega a un Responsable en otro país), verificamos que el país de destino tenga niveles adecuados de protección de datos según los estándares de la SIC, o de lo contrario implementamos las **cláusulas contractuales** o instrumentos jurídicos que exige la ley para proteger la información (por ejemplo, cláusulas tipo de la SIC, o solicitamos autorización explícita del Titular para dicha transferencia cuando es particular).

Algunos ejemplos de situaciones en las que Minteo podría Transferir o Transmitir tus datos incluyen: envío de datos a un **servicio en la nube** cuya infraestructura puede estar en otro país (para almacenamiento y backup de información), compartición de datos con una empresa matriz o inversor de Minteo para reportes corporativos (respetando confidencialidad), envío de información a un proveedor tecnológico en el exterior para soporte de la plataforma, entre otros. En cada caso, Minteo procurará que el tercero receptor entienda y acepte sus obligaciones en materia de protección de datos.

En cualquier momento, **tus derechos como Titular prevalecen**. Minteo se abstendrá de transferir datos a terceros que no brinden garantías suficientes de respeto a tus derechos, y en caso de que debamos compartir información por exigencia de autoridades extranjeras (p. ej., por una orden judicial internacional válida), lo haremos a través de los cauces legales correspondientes, informándote cuando la ley nos lo permita.

¿Cómo se tratan los Datos Personales en la tecnología blockchain u otras tecnologías utilizadas por Minteo?

El modelo de negocio de Minteo implica el uso de tecnología blockchain (cadena de bloques) para ofrecer sus servicios de activos digitales (como stablecoins y tokenización). Entendemos que la incorporación de blockchain presenta retos particulares para la privacidad de los datos personales, por lo cual a continuación te explicamos las consideraciones relevantes:

La tecnología blockchain es esencialmente un registro digital distribuido, transparente y descentralizado que se mantiene en una red de computadoras a nivel mundial. Una característica fundamental de muchas blockchains públicas (como las que usamos para stablecoins) es su inmutabilidad: los datos o transacciones que se registran en un bloque, una

vez validados, no pueden ser modificados ni eliminados del historial de la cadena. Esto significa que, si cierta información queda grabada en la blockchain, nadie –ni siquiera Minteo ni una autoridad central– puede posteriormente alterarla o borrarla. Esta inmutabilidad aporta seguridad y confianza a las transacciones, pero dificulta el ejercicio de derechos como la rectificación o supresión de datos personales en caso de haberse incluido directamente en la cadena.

¿Qué datos se registran en la blockchain? Por diseño, Minteo procura **minimizar la inclusión de datos personales directamente en la blockchain**. Las transacciones en la red normalmente contienen identificadores **seudónimos**, como direcciones de cartera (wallet addresses) alfanuméricas, montos y referencias técnicas, pero no datos personales explícitos como nombres o identificaciones civiles. Por ejemplo, si realizas una transferencia de COPM (nuestro stablecoin) a otra persona, la transacción visible en la blockchain mostrará que la dirección X envió Y tokens a la dirección Z en determinada fecha y hora, pero la relación de esas direcciones con tu identidad real no es visible en la cadena. **Minteo maneja esa asociación de forma interna y confidencial.**

Siempre que sea **posible técnicamente**, mantendremos cualquier **dato personal sensible off-chain** (fuera de la cadena). Es decir, tus datos identificables (nombre, documento, etc.) residen en nuestras bases de datos seguras y no se escriben en la blockchain pública. En la blockchain puede quedar tu dirección digital y tu historial de transacciones, pero **no tu nombre**. De esta forma, si ejercieras tus derechos de rectificación o supresión, Minteo puede **actuar sobre los datos que están bajo su control** (por ejemplo, corregir o eliminar tu información en nuestros sistemas internos) sin que ello afecte la integridad de la blockchain. Asimismo, si llegases a solicitar la **eliminación de tus datos personales**, Minteo podría disociar o eliminar la información identificatoria en nuestras bases de datos internas, a la vez que **no hay datos personales tuyos en la cadena** que pudieran comprometer ese derecho.

Debes tener en cuenta que al usar servicios basados en blockchain, ciertas operaciones tuyas (por ejemplo, las transacciones con criptoactivos) quedan registradas en un libro mayor **público** y **transparente**. Aunque, como explicamos, esas transacciones son **seudónimas** (identificadas por códigos y no por nombres), existe la posibilidad de que, mediante análisis avanzados de la cadena o correlacionando información, **alguien podría llegar a inferir la identidad real** detrás de una dirección blockchain. Por ejemplo, si públicamente anuncias que cierto monedero es tuyo, cualquiera podría ver el historial de ese monedero. O si un analista ve que una dirección pertenece a Minteo y la vincula a un registro de retiro asociado a ti, podría deducir algo sobre tus actividades. Por eso, **Minteo te recomienda precaución** con la información que haces pública sobre tus direcciones o transacciones cripto.

En cuanto a la **transferencia internacional** de datos, es importante señalar que las redes blockchain son globales por naturaleza. Cuando realizas una operación en blockchain, esta es procesada por nodos (computadores) alrededor del mundo que validan la transacción. En la práctica, esto implica una transferencia transfronteriza automática de la información de la transacción a todos esos nodos de la red. **Dichos nodos no necesariamente están sujetos a la legislación colombiana**, pero la información que manejan típicamente no incluye datos

personales directos, sino los datos transaccionales seudónimos. Aun así, Minteo considera este factor y por ello concentra el Tratamiento de datos personales identificables en entornos controlados.

En resumen, Minteo adopta las siguientes medidas en cuanto a datos personales y blockchain:

- **Minimización de datos en cadena:** Solo los datos estrictamente necesarios para la lógica transaccional (direcciones, hashes, montos) se llevan a la blockchain. No se incluyen nombres, ni documentos, ni otros datos personales directos en las transacciones on-chain.
- **Segregación on-chain / off-chain:** Los datos personales se gestionan off-chain en servidores seguros. En la blockchain permanece la capa transaccional seudónima. Vinculamos ambas capas internamente de forma segura para brindarte el servicio (ejemplo: sabemos qué dirección te pertenece, pero esa asociación vive en nuestros sistemas, no en la cadena pública).
- **Protección de la asociación identidad-dirección:** Tratamos la lista que relaciona tu identidad con tus direcciones blockchain como información confidencial de alto nivel. Solo personal autorizado y por motivos justificados puede acceder a ella, y está sujeta a estrictos controles de seguridad.
- **Cumplimiento normativo:** Evaluamos continuamente cómo cumplir con los derechos ARCO (Acceso, Rectificación, Cancelación -supresión-, Oposición) en un entorno blockchain. Por ahora, si quisieras cancelar tu cuenta y datos, eliminaríamos o anonimizaremos tus datos en nuestros sistemas. Las transacciones históricas en la cadena no pueden borrarse, pero al estar seudonimizadas y ya no estar vinculadas a ti en nuestras bases (tras la supresión), **no serían atribuibles a tu persona** de forma inmediata.
- **Tecnologías complementarias:** Exploramos el uso de soluciones como **blockchains privadas**, **cifrado avanzado**, o métodos de **almacenamiento fuera de cadena** para datos personales, de modo que podamos aprovechar los beneficios de blockchain (transparencia, seguridad) sin comprometer la privacidad. Por ejemplo, podríamos usar smart contracts que registren solo referencias cifradas a datos personales almacenados fuera de la cadena, de modo que la cadena solo contenga datos incomprensibles para terceros.

Ten la confianza de que Minteo está comprometida con la protección de tus datos personales **incluso en entornos descentralizados**. La innovación tecnológica va de la mano con la responsabilidad en el manejo de la información. Continuamente actualizaremos nuestras prácticas a medida que evolucione la industria blockchain y la normativa de protección de datos, buscando ese balance óptimo entre los beneficios de la descentralización y tu derecho fundamental a la privacidad.

Si tienes preguntas específicas sobre cómo tus datos se manejan en relación con la blockchain, puedes contactarnos a través de los canales de atención de datos personales, y con gusto atenderemos tus inquietudes con la mayor transparencia posible.

¿Cuáles son tus derechos como Titular de Datos Personales?

Como Titular de datos personales, la ley colombiana (especialmente la Ley 1581 de 2012 y decretos reglamentarios) te reconoce una serie de **derechos** frente a tus datos. En Minteo, queremos recordarte que cuentas con los siguientes derechos en relación con tus Datos Personales, los cuales respetamos y garantizamos en el marco de esta Política:

- **Derecho de acceso y conocimiento:** Puedes **conocer** en cualquier momento qué Datos Personales tuyos están siendo tratados por Minteo, así como el origen de esos datos (cuando procedieron de una fuente diferente a ti) y las comunicaciones que se hayan realizado con ellos. Este derecho te permite acceder de forma gratuita a la información personal que tenemos sobre ti en nuestras Bases de Datos.
- **Derecho de actualización y rectificación:** Tienes derecho a **actualizar** tus datos (por ejemplo, si cambias de número telefónico, dirección, estado civil, etc.) y a **rectificar** aquellos datos que estén parcial, inexacta, incompleta o desactualizadamente registrados, o que puedan inducir a error. Igualmente, puedes rectificar datos cuyo Tratamiento esté expresamente prohibido o no haya sido autorizado. En resumen, puedes solicitar que corrijamos información incorrecta o que completemos datos que falten, para asegurar la veracidad de tus datos personales.
- **Derecho a solicitar prueba de la Autorización:** Salvo en los casos en que la ley no lo requiera, tienes derecho a solicitarnos prueba de la Autorización que nos otorgaste para tratar tus Datos Personales. Minteo llevará un registro adecuado de las autorizaciones recibidas (por medios electrónicos, formularios físicos, etc.), de modo que ante una consulta podamos indicarte cuándo y cómo nos diste tu consentimiento. Ten en cuenta que hay situaciones en que no se requiere autorización (por ejemplo, datos de naturaleza pública, o casos de urgencia vital), en cuyo caso te informaremos la fuente legal de la excepción.
- **Derecho a ser informado sobre el uso:** Puedes **solicitar en cualquier momento** que Minteo te informe acerca del **uso** que le ha dado a tus Datos Personales. Es decir, podemos explicarte con qué finalidad específica los hemos usado, si se han compartido con terceros (y quiénes), cuánto tiempo los conservaremos, etc. Esto te da transparencia sobre el ciclo de vida de tus datos en nuestra organización.
- **Derecho a presentar quejas ante la SIC:** Si consideras que Minteo ha vulnerado tus derechos o ha infringido las normas de protección de datos aplicables en Colombia, tienes derecho a presentar una **queja** o reclamo ante la **Superintendencia de Industria y Comercio (SIC)**, que es la autoridad de protección de datos en Colombia. La SIC, a través de su Delegatura de Protección de Datos, puede adelantar investigaciones y resolver sobre eventuales incumplimientos. Te invitamos, no obstante, a primero agotar nuestros canales internos de consulta o reclamo (que se describen más adelante), y si tras ello no obtienes respuesta o solución, acudir a la SIC.
- **Derecho a solicitar la revocatoria de la Autorización y/o supresión de datos:** Puedes en cualquier momento **revocar** la autorización que nos hayas otorgado para tratar tus datos, o solicitar la **supresión (borrado)** de tus Datos Personales de nuestras bases, cuando consideres que Minteo no está respetando los principios, derechos y garantías

constitucionales y legales aplicables. Por ejemplo, si ya no deseas que tratemos más un dato tuyo en particular, puedes pedirnos que lo eliminemos (lo que también se conoce como ejercer el **derecho al olvido** en algunos casos). Este derecho tiene ciertas limitaciones: no siempre podremos eliminar tus datos si existe un deber legal o contractual de conservarlos. Por ejemplo, la ley nos exige conservar registros contables por cierto tiempo, o mantener datos de transacciones financieras. En tales casos te informaremos la razón por la cual no es viable eliminar inmediatamente, pero cesaremos los tratamientos que no sean obligatorios. Revocar la autorización podría implicar la terminación de los servicios que dependan de esos datos; te informaremos las consecuencias de la revocatoria para que tomes una decisión informada.

- **Derecho a la portabilidad de datos:** (Este derecho no está explícitamente nombrado en la ley colombiana actual, pero se deriva del principio de libertad y disposición sobre los datos). Consiste en que, en los casos aplicables, puedas solicitar que tus datos que nos has proporcionado sean entregados a ti o transmitidos a otro proveedor de servicios en un formato estructurado y común, cuando ello sea técnicamente posible. Por ejemplo, si en un futuro deseas migrar a otro servicio y quisieras llevarte ciertos datos personales aportados, haríamos lo posible por facilitarte esa portabilidad.
- **Derecho a exigir el cumplimiento del Habeas Data:** En general, puedes exigir el cumplimiento pleno de tu **derecho fundamental al habeas data**, que abarca todos los anteriores. Esto significa que puedes esperar de Minteo un tratamiento respetuoso, seguro y conforme a ley de tus datos, y puedes reclamar si notas cualquier falla en ello. Tienes derecho a **acceder en forma gratuita** a tus Datos Personales objeto de Tratamiento al menos una vez al mes, y cada vez que existan modificaciones sustanciales a esta Política que motiven nuevas consultas. Minteo no te cobrará por ejercer tus derechos, solo eventualmente podría cobrar costos de envío o reproducción de copias si los hubiere, conforme lo permite la ley, pero hasta ahora manejamos todo por medios electrónicos de forma gratuita.

Estos derechos los puedes ejercer en cualquier momento. Para ello, Minteo ha dispuesto mecanismos y procedimientos que describimos a continuación.

¿Cómo puedes presentar una solicitud o reclamo en relación con tus Datos Personales?

En Minteo contamos con canales de atención para que, como Titular de datos, puedas **ejercer tus derechos** de consulta, actualización, rectificación, supresión, revocatoria y demás, así como para que eleves cualquier **reclamo** relacionado con el Tratamiento de tus Datos Personales. Puedes escribir tu correo a soportelegal@minteo.com

Área encargada de la recepción de consultas y reclamos

Hemos designado al equipo de **Servicio al Cliente** (Customer Experience) de Minteo como el área responsable de atender las consultas y reclamos de los Titulares en materia de datos personales. Este equipo trabaja en coordinación con nuestro Delegado de Protección de Datos (si existe formalmente) o con el responsable interno de cumplimiento en privacidad, para dar trámite oportuno a tus solicitudes.

En concreto, puedes dirigir tus peticiones relacionadas con datos personales a la **Gerencia de Atención al Usuario** o al **Oficial de Protección de Datos** de Minteo, a través de los canales que mencionamos abajo. Ellos se encargarán de recibir, procesar y responder a tu comunicación en los plazos de ley, y de guiarte en caso de requerir información adicional.

Procedimiento para la presentación y solución de consultas y reclamos

Canales de contacto disponibles: Para ejercer tus derechos como Titular o presentar cualquier consulta/reclamo referente a tus Datos Personales, puedes comunicarte con Minteo a través de los siguientes medios:

- **Correo electrónico:** Puedes enviarnos tu solicitud al correo destinado para protección de datos: **soportelegal@minteo.com** *(Nota: Este correo es atendido por el equipo encargado de datos personales. A través de él puedes tanto realizar consultas sobre tus datos como presentar quejas formales.)*
- **Formulario web:** En nuestro sitio web oficial, dentro de la sección de Política de Privacidad o Contacto, encontrarás un formulario específico para ejercer derechos ARCO. Allí podrás diligenciar tus datos y la solicitud puntual; este formulario nos llegará a la misma área encargada. *(Si aún no está disponible el formulario, el correo electrónico es la vía principal).*
- **Dirección física:** Si lo prefieres, puedes enviar una comunicación escrita a nuestra dirección Calle 70 #4-36, Bogotá, dirigida a "Wagmi S.A.S. – Atención Protección de Datos". Recuerda incluir tus datos de contacto en la carta para poder responderte.
- **Otros canales electrónicos:** Minteo podría habilitar canales adicionales, como un chat en la aplicación o página web, o una línea de atención telefónica, para atender temas de privacidad. De existir, se informarán en la web. Por ejemplo, si ya eres usuario registrado, quizás mediante la app puedas ir a Configuración > Privacidad > Solicitar mis datos, etc. En ausencia de estos, los canales principales son los mencionados arriba.

Procedimiento para consultas***: Si deseas simplemente** ***consultar** la información personal que Minteo tiene sobre ti (por ejemplo, qué datos están registrados, en qué bases de datos, finalidades, o solicitar copia de tu Autorización), puedes presentar una **solicitud de consulta** a través de cualquiera de los canales indicados.

- La consulta debe contener al menos tu identificación (nombre completo y tipo/número de documento), la descripción clara de la consulta (por ejemplo: "Solicito me informen los datos personales míos que están en sus bases de datos y el uso que les han dado"), y un medio de contacto para enviarte la respuesta (correo electrónico, dirección física). No está de más que adjuntes copia de un documento de identificación para validar tu identidad, pero si la consulta llega del email registrado en tu cuenta, asumiremos que eres tú.
- Una vez recibida tu consulta, Minteo te responderá en un **término máximo de 10 días hábiles** contados a partir de la fecha de recepción. En la respuesta te proporcionaremos la información solicitada o copia de los datos personales que tengamos tuyos, según aplique.

- Si por alguna razón no nos es posible atender tu consulta dentro de esos 10 días, te informaremos antes de su vencimiento las razones de la demora y te indicaremos la fecha en que daremos respuesta, la cual en ningún caso superará los **5 días hábiles siguientes** al primer plazo. Es decir, en el peor de los casos recibirás respuesta a tu consulta a más tardar en **15 días hábiles** desde que la recibimos, conforme lo establece la ley.

Procedimiento para reclamos***: Si consideras que hay un problema con el Tratamiento de tus datos —por ejemplo, si encuentras que está desactualizado, quieres rectificar o suprimir algún dato, o piensas que hemos incumplido nuestras obligaciones de protección— puedes presentar un* *reclamo** formal. El proceso es el siguiente:

- El reclamo debe presentarse mediante comunicación dirigida a Minteo, preferiblemente por escrito (vía correo electrónico o carta física). Debe contener tu identificación (nombre completo y documento) o la de tu representante (si actúas a través de apoderado, adjuntar poder); una descripción de los **hechos** que dan lugar al reclamo y lo que solicitas (p. ej., “actualizar mi dirección”, “eliminar mi correo de sus bases de marketing” o “no estoy de acuerdo con X uso, solicito se corrija”); la dirección de notificación (física o correo electrónico) y, si aplica, **documentos de soporte** que quieras hacer valer (por ejemplo, copia de un dato correcto para probar que el nuestro está errado).
- Si el reclamo resulta **incompleto** o le falta información esencial, te contactaremos dentro de los **5 días hábiles** siguientes a su recepción para que aportes lo que haga falta. Por ejemplo, si no adjuntaste la copia del poder siendo un apoderado, o no especificaste claramente el dato a rectificar. Si tras 2 meses desde la fecha del requerimiento no nos has enviado la información pendiente, entenderemos que **desististe** del reclamo.
- En caso de que Minteo no sea competente para resolver tu reclamo (por ejemplo, porque el asunto es de otra empresa, o los datos no están en nuestras bases), te lo comunicaremos en un plazo máximo de **2 días hábiles** y, si es posible, redirigiremos tu reclamo al responsable correcto. Por ejemplo, si nos reclamas por un dato que en realidad maneja una entidad financiera aliada, le remitiremos el reclamo a dicha entidad y te informaremos.
- Una vez recibamos un reclamo **completo**, incluiremos en nuestra base de datos una leyenda que diga “reclamo en trámite” junto con el motivo del reclamo, en un término no mayor a **2 días hábiles** desde que lo recibimos completo. Esto para dejar constancia de que tus datos están en revisión de acuerdo al reclamo presentado, lo cual permanecerá hasta que este sea resulto.
- Minteo resolverá tu reclamo en un plazo máximo de **15 días hábiles** contados a partir del día en que recibimos el reclamo con toda la información necesaria. Si por alguna circunstancia excepcional no podemos responder en ese término, te informaremos antes de su vencimiento las razones de la demora y la fecha en que daremos respuesta, la cual no podrá exceder de **8 días hábiles** adicionales a los 15 iniciales. En resumen, **no excederá 23 días hábiles** desde que se recibió el reclamo completo.

- Conforme al artículo 16 del Decreto 1377 de 2013 (y el artículo 7 de la Ley 2157 de 2021, aplicable a datos financieros), si transcurre el término máximo legal sin que Minteo te hubiere respondido el fondo del reclamo, se considerará que **hemos resuelto a tu favor** o lo que se llama "silencio positivo". Por supuesto, nuestra intención es responderte siempre de forma expresa y en plazo.

Por último, ten en cuenta que **cualquier consulta o reclamo** puede ser ejercido **por ti como Titular**, por tus **causahabientes** (herederos) en caso de fallecimiento, por tu **representante legal** (en caso de menores de edad sus padres, en caso de incapaces su tutor, etc.), o por tu **apoderado** mediante poder otorgado conforme a la ley. En todos los casos, quien interponga la consulta o reclamo deberá **acreditar su identidad** y, si actúa en representación de alguien, la calidad en que lo hace. Minteo establecerá mecanismos de autenticación de identidad para protegerte, de modo que podamos verificar que quien solicita tus datos o su modificación realmente eres tú o alguien autorizado. Esta verificación podría incluir preguntas de seguridad, envío de código al correo/teléfono registrado, entre otros medios.

¿Cuáles son las medidas de seguridad?

Wagmi S.A.S. es consciente de la importancia de proteger tus datos personales contra riesgos de pérdida, uso no autorizado, acceso indebido, alteración o destrucción. Por ello, hemos implementado un **Sistema de Gestión de Seguridad de la Información** que incluye medidas técnicas, humanas y administrativas necesarias para garantizar la **integridad, disponibilidad y confidencialidad** de la información personal que recopilamos y procesamos en nuestras Bases de Datos.

Algunos de los **controles de seguridad** que implementamos en Minteo son los siguientes:

- Contamos con mecanismos de **control de acceso** robustos: definimos perfiles de usuarios internos de manera que solo el personal autorizado y que lo necesita para sus funciones puede acceder a tus datos, y aún así únicamente a aquellos datos relevantes para su rol. Cada empleado tiene credenciales individuales, utilizamos autenticación multifactor (MFA) donde es posible, y registramos los accesos a sistemas que contienen datos personales.
- **Conexiones seguras y cifrado:** Todos nuestros sistemas que manejan información personal operan bajo conexiones cifradas (ej.: HTTPS/TLS) para la transmisión de datos, evitando la interceptación por terceros. Asimismo, los datos sensibles y datos financieros se almacenan cifrados en nuestras bases de datos, o al menos se cifran campos críticos (por ejemplo, contraseñas se guardan usando algoritmos de hash seguros, información financiera con cifrado de grado bancario). En general, procuramos que los datos estén cifrados tanto **en tránsito** como **en reposo** en nuestros sistemas.
- **Protección contra software malicioso:** Todos nuestros equipos, servidores y entornos en la nube cuentan con herramientas de **protección contra malware** (antivirus, anti-malware) actualizadas. Realizamos escaneos periódicos para detectar y eliminar posibles virus, spyware, ransomware u otras amenazas.

- **Manejo de vulnerabilidades:** Realizamos periódicamente **escaneos de vulnerabilidades** y pruebas de penetración sobre nuestros sistemas y aplicaciones. Si llegamos a encontrar alguna vulnerabilidad o falla de seguridad, la atendemos de forma oportuna priorizando las críticas. Adicionalmente, mantenemos nuestros sistemas actualizados (parches de seguridad al día) para reducir riesgos conocidos.
- **Gestión de identidades y accesos:** Tenemos un proceso formal de **gestión de identidades**: las altas, modificaciones y bajas de usuarios internos del sistema siguen un procedimiento aprobado. Cuando un empleado deja la compañía o cambia de rol, sus accesos se revocan o ajustan inmediatamente. También implementamos controles de **contraseña robusta** (complejidad mínima, caducidad periódica cuando corresponde) y fomentamos el uso de **MFA** en todos nuestros sistemas críticos.
- **Monitoreo y respuesta a incidentes:** Contamos con capacidades de monitoreo de seguridad casi en tiempo real. Tenemos habilitado un sistema de alertas (tipo SOC – Security Operations Center) que opera 24/7 gestionando las alertas que puedan surgir en nuestra infraestructura. Esto nos permite detectar actividades inusuales o potenciales incidentes (por ejemplo, múltiples intentos fallidos de login, accesos fuera de horario, alta transferencia de datos) y responder rápidamente para contener amenazas.
- **Concientización y capacitación:** Reconocemos que el factor humano es crítico en seguridad. Por eso, **entrenamos y concientizamos constantemente a nuestros colaboradores** (y a veces, también a aliados estratégicos) en temas de seguridad de la información, ciberseguridad y protección de Datos Personales. Realizamos charlas, cursos en línea, simulacros de phishing, etc., para asegurarnos de que todos entiendan la importancia de proteger la información y sepan cómo manejar los datos personales correctamente.

Además de lo anterior, exigimos contractualmente a todos nuestros **aliados y proveedores** que manejen Datos Personales de parte nuestra, que cuenten con **medidas de seguridad adecuadas y suficientes** para proteger esos datos. Antes de vincular un proveedor que vaya a tener acceso a datos personales, evaluamos sus prácticas de seguridad y de ser necesario auditamos su cumplimiento.

Minteo también mantiene **documentados sus procesos de seguridad**. Tenemos políticas internas, manuales y procedimientos sobre clasificación de la información, gestión de incidentes, copia de respaldo (backups), continuidad del negocio, etc. Existen funciones y responsables asignados expresamente para velar por el cumplimiento eficaz de todos estos controles. Esto nos permite tener una gestión proactiva y mejorar continuamente en materia de seguridad de la información.

Nota: Si bien ninguna medida de seguridad es 100% infalible, en Minteo hacemos nuestro máximo esfuerzo por proteger tus datos. En caso de presentarse **brechas de seguridad** que comprometan significativamente tus Datos Personales (por ejemplo, un acceso no autorizado masivo debido a un ciberataque), te notificaremos oportunamente conforme lo exige la ley e implementaremos inmediatamente los planes de contingencia para minimizar cualquier impacto. Tu confianza es fundamental para nosotros, y por eso la seguridad es una prioridad transversal a todas nuestras operaciones.

Cambios a la Política de Tratamiento de Datos

Minteo podrá modificar o actualizar esta Política de Tratamiento de Datos en cualquier momento, cuando sea necesario para adaptarla a nuevos requisitos legales, a cambios en nuestros servicios o a políticas internas. Si efectuamos **cambios sustanciales** (por ejemplo, nuevas finalidades de tratamiento, modificación en los datos recolectados, cambios en los responsables, etc.), informaremos dichas modificaciones de manera oportuna a los Titulares.

Pondremos la versión actualizada de la Política a disposición del público en nuestra página web oficial (por ejemplo, en el apartado legal o de privacidad en **minteo.com**). Además, cuando los cambios puedan afectarte materialmente, podremos utilizar otros medios para notificarte, tales como un correo electrónico a la dirección que nos hayas proporcionado, avisos destacados en nuestra aplicación móvil, o notificaciones emergentes cuando inicies sesión.

En esa comunicación indicaremos **la fecha a partir de la cual rigen los cambios**. Ten la seguridad de que ningún cambio en la Política reducirá tus derechos legales como Titular sin tu consentimiento expreso. Si la ley requiere tu Autorización para cambios en ciertas finalidades, te la solicitaremos antes de implementarlos.

Te invitamos a revisar periódicamente nuestra Política de Tratamiento de Datos publicada en el sitio web, para que siempre estés enterado de cómo protegemos tu información. La continuidad en el uso de nuestros servicios después de la entrada en vigencia de una actualización se interpretará como aceptación de la Política modificada, en lo que respecta a aspectos que no requieran consentimiento expreso.

Vigencia de la Política de Tratamiento de Datos

La presente Política de Tratamiento de Datos Personales está vigente desde su fecha de publicación (10 de septiembre de 2025) y se mantendrá vigente hasta que una nueva versión la reemplace. Cualquier cambio se realizará conforme al procedimiento descrito en la sección anterior.

En cuanto al período de **vigencia de las Bases de Datos** de Minteo que contienen Datos Personales, te informamos que manejamos tus datos por el tiempo que sea necesario para cumplir las finalidades para las cuales fueron recolectados. Por ejemplo, los datos de clientes se conservarán mientras tengas una relación activa con nosotros y, tras la terminación, durante el tiempo requerido para cumplir obligaciones legales (p. ej., obligaciones contables, fiscales, de archivo) o para el ejercicio de acciones legales derivadas de la relación. Los datos que hayan cumplido su finalidad y no deban ser conservados por disposición legal, serán eliminados o anonimizados de nuestras bases.

Esta Política seguirá aplicando inclusive a los datos recolectados durante su vigencia, aun si posteriormente deja de regir (por ser reemplazada), en lo que respecta al periodo durante el cual estuvieron vigentes dichas disposiciones. En otras palabras, los compromisos asumidos bajo esta versión de la Política cobijan el tratamiento efectuado bajo su vigencia.

Última actualización: 10 de septiembre de 2025.

Si tienes alguna duda sobre la interpretación o alcance de esta Política, no dudes en contactarnos a través de los canales proporcionados. En Wagmi S.A.S. estamos comprometidos con la protección de tus datos personales y con brindarte la información clara y transparente sobre su Tratamiento.