

AIVRA DIGITAL

POLÍTICA DE PRIVACIDAD Y PROTECCIÓN DE DATOS PERSONALES

AIVRA Facturación - Software como Servicio (SaaS)

Responsable	Franklin Sebastian Sanmartin Quiroz, persona natural que opera bajo el nombre comercial AIVRA Digital
Nombre comercial	AIVRA Digital
Producto	AIVRA Facturación
Sitio web	https://aivradigital.com
Plataforma	https://facturacion.aivradigital.com
Correo de privacidad	info@aivradigital.com
País	Ecuador
Última actualización	3 de octubre de 2026

Transparencia

Esta Política explica de forma clara cómo AIVRA Digital trata datos personales en AIVRA Facturación, qué finalidades persigue, qué categorías de datos intervienen, con quién pueden compartirse y cómo ejercer los derechos reconocidos por la legislación ecuatoriana.

Documento público de información sobre privacidad preparado para su publicación web. Se interpreta conforme a la legislación ecuatoriana aplicable y complementa los Términos y Condiciones de AIVRA Facturación.

Resumen de privacidad

AIVRA Digital trata datos para operar cuentas y suscripciones, prestar AIVRA Facturación, gestionar seguridad y soporte, facilitar facturación electrónica y cumplir obligaciones legales. Dependiendo del tratamiento, AIVRA puede actuar como responsable o como encargado del tratamiento.

Responsable	AIVRA es responsable respecto de sus cuentas, contratación, pagos, seguridad, soporte y cumplimiento propio.
Encargado	Cuando una empresa cliente introduce datos de sus propios clientes, ventas o documentos, AIVRA normalmente procesa esa información por cuenta de la empresa.
Proveedores relevantes	Hostinger como proveedor seleccionado para la infraestructura de producción; Google/Gmail como servicio de correo previsto; Backblaze B2 y DeepSeek como integraciones configurables que solo intervienen cuando estén habilitadas; SRI para procesos de facturación electrónica.
Derechos	Los titulares pueden ejercer los derechos reconocidos por la LOPDP mediante info@aivradigital.com , sujetos a las condiciones y excepciones legales aplicables.

1. Objeto de esta Política

La presente Política de Privacidad y Protección de Datos Personales explica cómo AIVRA Digital obtiene, utiliza, almacena, protege, comunica y, cuando corresponda, elimina datos personales relacionados con la prestación de AIVRA Facturación y con sus canales de atención.

Esta Política busca aplicar los principios de juridicidad, lealtad, transparencia, finalidad, pertinencia y minimización, proporcionalidad, confidencialidad, calidad, conservación, seguridad y responsabilidad proactiva previstos en la legislación ecuatoriana de protección de datos personales.

Conforme al derecho a la información reconocido por la Ley Orgánica de Protección de Datos Personales (LOPDP), el titular debe poder conocer, entre otros aspectos, las finalidades, bases jurídicas, tiempo de conservación, identidad y datos de contacto del responsable, destinatarios o clases de destinatarios, transferencias o comunicaciones y mecanismos para ejercer sus derechos.

Esta Política complementa los Términos y Condiciones de AIVRA Facturación y no los sustituye.

2. Alcance

Esta Política se aplica al tratamiento de datos personales realizado a través de AIVRA Digital, el sitio web aivradigital.com, la plataforma facturacion.aivradigital.com, los procesos de contratación y suscripción, soporte, facturación del servicio, gestión de usuarios y seguridad, así como a las funcionalidades de AIVRA Facturación que impliquen tratamiento de datos personales.

Puede resultar aplicable a propietarios o administradores de empresas clientes, usuarios autorizados, vendedores u operadores, personas que contacten con soporte, clientes finales, destinatarios de comprobantes y otras personas cuyos datos sean incorporados por las empresas usuarias a AIVRA Facturación.

3. Qué es AIVRA Facturación

AIVRA Facturación es una plataforma SaaS multiempresa que puede incluir, según el plan y las funcionalidades habilitadas, gestión de empresas, establecimientos, puntos de emisión, usuarios, roles y permisos, clientes, productos y servicios, inventario, ventas, POS, facturación electrónica, generación de documentos electrónicos, firma electrónica, transmisión al Servicio de Rentas Internas (SRI), consulta de comprobantes y herramientas relacionadas con la gestión empresarial.

Cada empresa utiliza sus propios datos, usuarios, configuraciones y situación tributaria. AIVRA no presume que todas las empresas usuarias pertenezcan a un mismo régimen tributario.

4. Roles en el tratamiento de datos

4.1. AIVRA como responsable del tratamiento

AIVRA Digital actúa como responsable del tratamiento cuando determina directamente las finalidades y medios esenciales del tratamiento para sus propias actividades. Esto ocurre, por ejemplo, respecto de datos necesarios para administrar cuentas de AIVRA, contratar y gestionar suscripciones, facturar el servicio SaaS, verificar pagos, atender soporte, mantener la seguridad de la plataforma, administrar accesos, registrar eventos de auditoría, prevenir abuso o fraude y cumplir obligaciones legales propias de AIVRA.

4.2. AIVRA como encargado del tratamiento

AIVRA puede actuar como encargado del tratamiento cuando una empresa cliente utiliza la plataforma para tratar datos personales correspondientes a su propia actividad y AIVRA los procesa tecnológicamente por cuenta de esa empresa. Esto puede incluir datos de clientes, destinatarios de comprobantes, compradores, proveedores, trabajadores u otras personas registradas por la empresa usuaria.

En esos casos, normalmente será la empresa cliente quien determine la finalidad y legitimidad del tratamiento, mientras que AIVRA prestará la infraestructura y las funcionalidades necesarias conforme a instrucciones documentadas y legalmente válidas.

Cuando exista un encargo de tratamiento, la relación deberá complementarse con el correspondiente Acuerdo o Contrato de Encargo de Tratamiento de Datos Personales, en los términos exigidos por la legislación ecuatoriana.

5. Categorías de datos personales tratados

Dependiendo de las funcionalidades utilizadas, AIVRA puede tratar las categorías que se indican a continuación. La tabla resume el tratamiento ordinario; determinadas operaciones pueden requerir información adicional cuando exista una obligación legal o una configuración particular del cliente.

Categoría	Datos principales	Finalidad	Base principal	Conservación
Cuenta y autenticación	Nombre, apellidos, correo, contraseña protegida mediante hash, estado, roles y datos asociados a la cuenta.	Registro, autenticación, administración de cuenta y control de acceso.	Medidas precontractuales y ejecución contractual.	Mientras sea necesario para administrar la relación con el usuario y, tras su terminación, únicamente durante el tiempo necesario para cierre, seguridad, reclamaciones u obligaciones legales.
Empresa cliente	RUC de la empresa cliente, razón social, nombre comercial, dirección, teléfono, correo y configuración tributaria.	Configuración empresarial y prestación de AIVRA Facturación.	Ejecución contractual y obligaciones legales.	Mientras resulte necesario para la relación contractual y las obligaciones legales aplicables a la información empresarial.

Categoría	Datos principales	Finalidad	Base principal	Conservación
Establecimientos y emisión	Códigos, denominaciones, direcciones y estado.	Configurar la emisión de comprobantes electrónicos.	Ejecución contractual y cumplimiento tributario.	Mientras resulte necesario para la prestación del servicio y las obligaciones tributarias asociadas.
Clientes finales	Identificación, nombres o razón social, nombre comercial, dirección, teléfono, correo y estado.	Gestión comercial y generación/entrega de comprobantes.	La base principal es determinada por la empresa cliente responsable.	Conforme a las instrucciones de la empresa responsable, la finalidad del tratamiento y las obligaciones legales aplicables; al terminar el encargo se aplicará la devolución, eliminación, anonimización o bloqueo cuando corresponda.
Ventas y transacciones	Fecha, productos o servicios, importes, impuestos, descuentos, forma de pago e información vinculada a la operación.	POS, ventas, gestión comercial y facturación.	Ejecución del servicio y bases definidas por la empresa cliente.	Durante el tiempo necesario para la finalidad comercial o tributaria correspondiente y las obligaciones legales aplicables.
Comprobantes electrónicos	Identificación de emisor y receptor, clave de acceso, XML, RIDE, importes, impuestos y demás datos exigidos.	Generar, firmar, transmitir, consultar, conservar y entregar comprobantes.	Obligación legal y ejecución del servicio.	Durante el período tributario aplicable; los contribuyentes deben conservar los comprobantes electrónicos por siete (7) años.
Firma electrónica	Archivo .p12/.pfx, contraseña cifrada y metadatos del certificado.	Firmar comprobantes autorizados por la empresa cliente.	Ejecución del servicio e instrucciones del cliente.	Mientras sea necesario para la función de firma autorizada; la revocación o sustitución activa los procesos de desactivación y eliminación aplicables, sin perjuicio del ciclo residual de respaldos.
Pago de suscripciones	Comprobante PDF/JPG/PNG, fecha declarada, referencia bancaria, estado y datos vinculados.	Verificar manualmente el pago y activar la suscripción.	Ejecución contractual y obligaciones contables o tributarias.	Durante el tiempo necesario para verificar el pago y cumplir obligaciones contables, tributarias, contractuales o de defensa de reclamaciones.
Datos técnicos y seguridad	IP, User-Agent, identificador de sesión, actividad, fecha/hora, auditoría y eventos técnicos.	Seguridad, autenticación, prevención de abuso e investigación de incidentes.	Interés legítimo cuando proceda y obligaciones de seguridad.	Durante el tiempo necesario para seguridad, auditoría, investigación de incidentes y cumplimiento, sujeto a revisión periódica de su necesidad.
Soporte	Identificación, contacto, contenido de solicitudes, tickets y actividad autorizada de soporte.	Resolver incidencias y solicitudes.	Ejecución contractual e interés legítimo cuando proceda.	Durante la atención del caso y, posteriormente, solo durante el tiempo necesario para seguimiento, seguridad, cumplimiento o defensa de reclamaciones.
Timi / IA	Texto introducido por el usuario y contexto limitado necesario para procesar la consulta.	Proporcionar funciones de asistencia mediante IA.	La base jurídica se determinará según la finalidad y configuración efectiva de la función; cuando sea exigible, se recabará el consentimiento u otra base válida conforme a la LOPDP.	Conforme a la finalidad de la consulta y a las condiciones aplicables a la integración efectivamente habilitada, bajo criterios de minimización y revisión periódica.

6. Fuentes de los datos

Los datos pueden obtenerse directamente del propio titular cuando crea o utiliza una cuenta; de la empresa cliente que lo incorpora como usuario o registra información necesaria para desarrollar su actividad; automáticamente mediante el uso técnico de la plataforma; a partir de operaciones efectuadas dentro de AIVRA; o de las respuestas generadas por sistemas del SRI.

Cuando AIVRA recibe información de una empresa cliente y actúa únicamente por cuenta de ella, la empresa cliente es responsable de contar con una base jurídica adecuada para recopilar e incorporar esos datos a la plataforma.

7. Finalidades del tratamiento

AIVRA tratará los datos únicamente para finalidades determinadas y compatibles con su recogida. Entre ellas se encuentran:

- administrar cuentas, usuarios, roles y accesos;
- prestar las funcionalidades de AIVRA Facturación;
- gestionar suscripciones, pagos y facturación del servicio SaaS;
- facilitar procesos comerciales y tributarios de las empresas clientes;
- generar, firmar, transmitir, consultar, conservar y entregar comprobantes electrónicos;
- prestar soporte y gestionar solicitudes;
- mantener registros de seguridad y auditoría, prevenir accesos no autorizados, fraude y abuso;
- realizar copias de seguridad y recuperación del servicio;
- atender solicitudes relacionadas con datos personales;
- cumplir obligaciones legales y requerimientos válidos de autoridad; y
- prestar las funcionalidades de inteligencia artificial que el usuario decida utilizar.

AIVRA no utilizará libremente los datos para finalidades incompatibles solo por encontrarse almacenados en la plataforma.

8. Bases de legitimación

La aceptación de esta Política no equivale por sí sola a otorgar consentimiento para cualquier tratamiento. Según la finalidad concreta, el tratamiento podrá sustentarse en medidas precontractuales o en la ejecución de un contrato, el cumplimiento de una obligación legal, el consentimiento cuando sea jurídicamente necesario o el interés legítimo cuando proceda y supere la ponderación exigida por la normativa aplicable.

Cuando AIVRA actúe como encargado, la empresa cliente responsable determinará la base jurídica del tratamiento principal, sin perjuicio de las obligaciones propias de AIVRA como encargado.

9. Facturación electrónica y Servicio de Rentas Internas

AIVRA Facturación puede generar, firmar electrónicamente, transmitir, consultar, almacenar y facilitar la entrega de documentos electrónicos emitidos por las empresas clientes.

Para ello puede resultar necesario comunicar al Servicio de Rentas Internas del Ecuador información incluida en los comprobantes electrónicos, como identificaciones, nombres o razones sociales, direcciones, datos económicos, impuestos y demás elementos exigidos por la normativa y especificaciones técnicas aplicables.

Esta comunicación se realiza en el contexto de las obligaciones tributarias y de las operaciones ordenadas por la empresa emisora.

La normativa tributaria ecuatoriana exige a los contribuyentes conservar los comprobantes electrónicos por siete (7) años. Cuando AIVRA los almacene por cuenta de una empresa cliente, la conservación se realizará conforme al servicio contratado, a las instrucciones del responsable y a las obligaciones legales aplicables.

10. Firma electrónica

Las empresas que utilicen funciones que requieran firma electrónica deberán disponer de un certificado válido. AIVRA puede procesar archivos de certificado .p12 o .pfx, la información necesaria para utilizarlos y determinados metadatos técnicos relacionados con su vigencia y validación.

De acuerdo con la arquitectura auditada, los certificados de firma electrónica y las credenciales necesarias para utilizarlos se protegen mediante mecanismos de cifrado y almacenamiento restringido. La información necesaria para ejecutar la firma se procesa únicamente dentro del flujo autorizado de emisión de comprobantes.

El certificado se utiliza exclusivamente para las operaciones autorizadas dentro de AIVRA Facturación. Cuando se sustituya o revoque un certificado, se aplicarán los controles de desactivación y eliminación previstos por la plataforma, sin perjuicio de la permanencia temporal de copias residuales dentro de los ciclos de respaldo.

El cliente continúa siendo responsable de disponer de un certificado válido, custodiar adecuadamente sus credenciales fuera de AIVRA y comunicar su revocación, pérdida, compromiso o sustitución.

11. Timi e inteligencia artificial

AIVRA Facturación dispone de una integración con DeepSeek para determinadas funciones de Timi. El tratamiento por este proveedor externo solo se produce cuando la integración correspondiente está habilitada y el usuario utiliza la funcionalidad.

Cuando la integración externa de Timi esté habilitada, podrá enviarse el texto necesario para interpretar la consulta y el contexto estrictamente necesario para responderla. La funcionalidad no está diseñada para transmitir contraseñas, credenciales, certificados, claves privadas ni bases completas de clientes; sin embargo, un usuario podría introducir voluntariamente datos personales en un campo de texto libre.

Los usuarios deberán evitar introducir en Timi datos sensibles, contraseñas, credenciales, certificados, secretos comerciales o datos personales de terceros que no sean necesarios para la consulta.

La utilización efectiva de un proveedor externo de inteligencia artificial puede implicar tratamiento mediante infraestructura situada fuera del Ecuador o a cargo de un encargado ubicado en el extranjero. AIVRA deberá mantener documentadas las condiciones contractuales, los subencargados y las garantías aplicables a la integración efectivamente habilitada, y actualizar esta Política cuando exista un cambio material.

Timi no está diseñado para adoptar por sí solo decisiones que produzcan efectos jurídicos o consecuencias similarmente significativas sobre una persona. Cuando una funcionalidad de inteligencia artificial trate datos personales, AIVRA aplicará la LOPDP y la normativa vigente de la SPDP sobre inteligencia artificial, bajo un enfoque basado en riesgos.

12. Proveedores tecnológicos y destinatarios

12.1. Hostinger

AIVRA ha seleccionado Hostinger para la infraestructura de alojamiento de producción. La prestación efectiva, características y ubicación física del centro de datos dependerán de la configuración contratada. Cuando Hostinger trate datos personales por cuenta de AIVRA, su intervención se gestionará conforme al régimen aplicable a encargados o subencargados.

12.2. Backblaze B2

La arquitectura de AIVRA contempla una integración configurable con Backblaze B2 para copias externas de seguridad. Este servicio solo tratará información si la integración está efectivamente

habilitada en producción. Cuando se utilice, los respaldos se protegerán antes de su almacenamiento externo y se limitarán a finalidades de continuidad y recuperación.

12.3. Google / Gmail

AIVRA prevé utilizar servicios de Google/Gmail para determinadas comunicaciones electrónicas operativas o transaccionales. Su uso efectivo dependerá de la configuración de producción. Cuando se utilice, Google podrá procesar datos necesarios para la entrega del mensaje, como dirección de correo, nombre del destinatario, contenido y archivos adjuntos cuando correspondan.

Actualmente la arquitectura auditada no incorpora un sistema propio de newsletter o marketing automatizado.

12.4. DeepSeek

DeepSeek forma parte de una integración disponible para Timi y solo interviene cuando dicha integración se encuentra habilitada y el usuario utiliza la funcionalidad. El alcance del tratamiento dependerá de la consulta, la configuración efectiva y las condiciones contractuales aplicables.

12.5. Servicio de Rentas Internas

El SRI recibe la información incluida en los comprobantes y comunicaciones tributarias cuando ello resulta necesario para los procesos de facturación electrónica.

12.6. Autoridades públicas

AIVRA podrá comunicar información a jueces, organismos de control u otras autoridades cuando exista una obligación legal, resolución judicial, requerimiento válido o base jurídica suficiente.

13. Proveedores situados fuera del Ecuador

La utilización de proveedores tecnológicos situados fuera del Ecuador no determina por sí sola la existencia de una transferencia o comunicación internacional. Conforme a la normativa vigente de la SPDP, un verdadero encargo de tratamiento mantiene esa naturaleza aunque el encargado se encuentre en el extranjero. Cuando una operación constituya jurídicamente una transferencia o comunicación a un tercero para finalidades propias, se aplicarán las reglas y garantías correspondientes.

AIVRA documentará las relaciones con encargados y subencargados y analizará cada flujo según su naturaleza jurídica. Cuando una operación constituya una transferencia o comunicación nacional o internacional, aplicará las bases de legitimación, garantías, instrumentos y deberes de información exigidos por la LOPDP, su Reglamento General y la normativa vigente de la SPDP.

14. Comunicaciones electrónicas

AIVRA puede enviar comunicaciones necesarias para administrar la relación con sus usuarios, incluyendo avisos de seguridad, recuperación de contraseñas, invitaciones, comprobantes, información contractual, soporte, suscripciones y mensajes directamente relacionados con el servicio.

Estas comunicaciones operativas no equivalen automáticamente a consentimiento para publicidad. Si posteriormente AIVRA incorpora comunicaciones comerciales, implementará los mecanismos de información, consentimiento u oposición que resulten legalmente aplicables.

15. Cookies y almacenamiento local

La plataforma utiliza tecnologías esenciales para el funcionamiento, autenticación y seguridad de las sesiones. También puede utilizar mecanismos de almacenamiento local del navegador para conservar preferencias estrictamente funcionales de la interfaz.

La auditoría técnica no identificó integraciones activas de analítica o publicidad comportamental en la versión revisada de la plataforma. Si posteriormente se incorporan herramientas de medición, publicidad o tecnologías no esenciales, AIVRA actualizará la información y aplicará los mecanismos de transparencia y elección que correspondan.

Los detalles correspondientes se desarrollarán en la Política de Cookies de AIVRA Digital. Si se incorporan cookies o herramientas no esenciales, AIVRA actualizará la información y habilitará los mecanismos requeridos antes de su utilización cuando corresponda.

16. Seguridad de los datos

AIVRA aplica medidas técnicas y organizativas razonables destinadas a proteger los datos personales frente a pérdida, alteración, destrucción, acceso no autorizado, divulgación y otros riesgos previsibles.

Las medidas incluyen controles de acceso y autorización, protección de credenciales, cifrado cuando corresponde, segregación lógica entre empresas, almacenamiento restringido de información sensible, mecanismos de respaldo, registro de eventos relevantes y procedimientos de gestión de incidentes. La descripción pública se mantiene en un nivel general para no revelar información que pueda debilitar la seguridad del servicio.

AIVRA no afirma que ningún sistema conectado a Internet sea absolutamente invulnerable ni garantiza riesgo cero. Las medidas de seguridad serán revisadas y adaptadas considerando la naturaleza, volumen, contexto y riesgos del tratamiento.

17. Aislamiento multiempresa

AIVRA Facturación está diseñada como una plataforma multiempresa. La información se vincula a la empresa correspondiente y se aplican controles de acceso, roles, permisos y mecanismos de segregación lógica para reducir el riesgo de acceso no autorizado entre organizaciones.

Cada empresa cliente es responsable de administrar adecuadamente los permisos de sus propios usuarios.

18. Acceso de soporte a información de clientes

El acceso del personal de soporte a información de una empresa cliente debe estar justificado, limitado al alcance necesario para resolver la incidencia y sujeto a controles de autorización y trazabilidad.

AIVRA procurará aplicar el principio de mínimo privilegio en las actuaciones de soporte.

En circunstancias excepcionales relacionadas con seguridad, recuperación o continuidad del servicio, podrán habilitarse accesos técnicos controlados cuando resulten necesarios y exista una base jurídica o contractual suficiente. Dichos accesos deberán mantenerse limitados, justificados y sujetos a registro.

19. Copias de seguridad

AIVRA mantiene mecanismos de respaldo destinados a la continuidad y recuperación de la información. La arquitectura permite respaldos locales y, cuando se encuentre habilitada la integración correspondiente, copias externas protegidas. Los períodos de retención de los respaldos son parámetros técnicos sujetos a configuración y no se presentan en esta Política como plazos fijos generales de conservación.

Cuando un dato sea eliminado del sistema principal, puede subsistir temporalmente dentro de copias de seguridad hasta completar su ciclo normal de rotación. Durante ese período las copias permanecerán protegidas y se utilizarán únicamente para finalidades de continuidad, recuperación o cumplimiento legal.

20. Conservación de datos

AIVRA aplica el principio de conservación: los datos personales no deberán mantenerse por un tiempo superior al necesario para las finalidades que justificaron el tratamiento, salvo que exista una obligación legal, una relación contractual válida, la necesidad de atender reclamaciones u otra base jurídica que justifique su conservación. La necesidad de conservar las distintas categorías deberá revisarse periódicamente.

Criterios de conservación

Los períodos de conservación varían según la finalidad del tratamiento, la relación contractual, las obligaciones legales, las instrucciones de la empresa responsable cuando AIVRA actúe como encargado y los ciclos técnicos de respaldo. Cuando deje de existir una base válida para conservar los datos, se aplicarán las medidas de eliminación, anonimización, bloqueo o devolución que correspondan.

- **Cuenta y perfil:** durante la relación activa y, después de su terminación, únicamente durante el tiempo necesario para gestionar el cierre, obligaciones pendientes, seguridad, reclamaciones o responsabilidades legales.
- **Datos operativos de la empresa cliente no sujetos a una conservación legal específica:** mientras dure el encargo y, al finalizar, conforme al contrato de encargo, las instrucciones válidas del responsable y las necesidades de devolución o exportación. Cuando deje de existir una base válida, procederá la eliminación, anonimización, bloqueo o devolución que corresponda.
- **Comprobantes electrónicos y documentación tributaria:** durante el período legal aplicable; los contribuyentes deben conservar sus comprobantes electrónicos por 7 años.
- **Registros de seguridad y auditoría:** durante el tiempo necesario para finalidades de seguridad, trazabilidad, investigación de incidentes, cumplimiento o defensa de reclamaciones, con revisión periódica de su necesidad.
- **Casos de soporte:** durante la tramitación y, posteriormente, únicamente durante el tiempo necesario para seguimiento, seguridad, cumplimiento o atención de reclamaciones.
- **Certificados de firma:** mientras sean necesarios para la función autorizada. Al ser revocados o sustituidos se aplicará el procedimiento de eliminación del archivo activo, sujeto al ciclo residual de backups.
- **Copias de seguridad:** durante los ciclos técnicos de rotación y recuperación configurados para la infraestructura, sin utilizarlas para nuevas finalidades incompatibles.

Cuando AIVRA actúe como encargado, la devolución, conservación o eliminación de datos al finalizar la relación se regulará además mediante el Acuerdo de Encargo de Tratamiento y las instrucciones válidas de la empresa responsable.

21. Supresión y obligaciones legales de conservación

El derecho de eliminación no significa que toda información pueda ser borrada inmediatamente en cualquier circunstancia. AIVRA podrá conservar datos cuando exista una obligación legal o contractual válida, una orden de autoridad, necesidad de formulación, ejercicio o defensa de reclamaciones, restricciones derivadas de documentación tributaria u otra excepción prevista por la legislación aplicable.

Cuando proceda la eliminación, AIVRA aplicará métodos dirigidos a suprimir, anonimizar, bloquear o hacer inaccesibles los datos de forma segura, considerando también el ciclo de copias de seguridad.

22. Exactitud de la información

Los usuarios y empresas clientes deben mantener actualizada la información que proporcionen a AIVRA. La introducción de datos incorrectos, incompletos o desactualizados puede afectar el funcionamiento de la plataforma o provocar errores en documentos electrónicos.

Cuando AIVRA actúe como encargado, la empresa cliente continuará siendo responsable de determinar la exactitud y calidad de los datos introducidos por ella, sin perjuicio de las obligaciones propias de AIVRA respecto de su procesamiento técnico.

23. Datos sensibles y categorías especiales

AIVRA Facturación no está diseñada específicamente para recopilar de manera general datos sensibles como información de salud, biométrica, genética, origen étnico, identidad de género, religión, ideología, filiación política, orientación sexual, pasado judicial u otras categorías especiales ajenas a las funciones empresariales y tributarias ordinarias del sistema.

Los usuarios no deberán introducir datos sensibles que no sean necesarios para utilizar las funciones contratadas. Si una empresa cliente decide tratar categorías especiales mediante AIVRA, deberá comprobar previamente que dispone de una base jurídica válida y que cumple las garantías reforzadas exigidas por la legislación.

24. Niñas, niños y adolescentes

AIVRA Facturación es un servicio empresarial y profesional y no se encuentra específicamente dirigido a niñas, niños o adolescentes. La auditoría no identificó funcionalidades diseñadas expresamente para crear cuentas infantiles o validar edades de menores.

Esto no impide que una empresa cliente pueda encontrarse legítimamente obligada a incluir información de una persona menor de edad en un comprobante u operación bajo su propia responsabilidad. En esos casos deberán respetarse las garantías especiales previstas por la legislación ecuatoriana.

25. Decisiones automatizadas y elaboración de perfiles

Actualmente AIVRA no utiliza datos personales para adoptar decisiones basadas única o parcialmente en tratamientos automatizados que produzcan efectos jurídicos o consecuencias similarmente significativas sobre sus usuarios.

Timi no decide si una persona puede contratar AIVRA, no determina automáticamente solvencia, no fija precios individualizados mediante perfiles personales y no adopta decisiones tributarias en nombre del contribuyente. Si AIVRA implementa posteriormente sistemas con estas características, realizará la evaluación jurídica y técnica correspondiente e informará a los titulares conforme a la LOPDP y normativa de la SPDP.

26. Derechos de los titulares

De acuerdo con la LOPDP, y sujeto a las condiciones, alcance y excepciones previstas por la ley, los titulares pueden ejercer sus derechos de información; acceso; rectificación y actualización; eliminación; oposición; portabilidad; suspensión del tratamiento; revocación del consentimiento cuando proceda; y a no ser objeto de determinadas decisiones basadas única o parcialmente en valoraciones automatizadas.

La LOPDP establece un plazo de quince (15) días para atender, en los términos de sus artículos 13 a 16, los derechos de acceso, rectificación y actualización, eliminación y oposición. Los demás derechos se atenderán conforme a los términos y condiciones previstos por la legislación y normativa aplicable.

27. Cómo ejercer los derechos

Las solicitudes relativas a protección de datos podrán enviarse a info@aivradigital.com. El interesado deberá indicar el derecho que desea ejercer y proporcionar información suficiente para identificarlo y localizar los datos relacionados con su solicitud.

AIVRA podrá solicitar información razonablemente necesaria para verificar la identidad del solicitante o, cuando actúe mediante representante, la acreditación correspondiente. AIVRA nunca requerirá como mecanismo normal de verificación que el titular envíe por correo su contraseña de AIVRA, contraseña de firma electrónica, clave privada o credenciales bancarias.

Las solicitudes serán atendidas dentro de los plazos establecidos por la legislación aplicable. Cuando proceda una negativa total o parcial, AIVRA comunicará la motivación que corresponda y los mecanismos disponibles para impugnarla o acudir a la autoridad competente.

28. Solicitudes sobre datos tratados por cuenta de una empresa cliente

Una persona puede aparecer en AIVRA Facturación porque realizó una operación con una empresa que utiliza la plataforma. En estos casos AIVRA podría actuar únicamente como encargado del tratamiento.

Si un cliente final solicita directamente a AIVRA el acceso, modificación, eliminación u otro derecho sobre información cuyo responsable sea una empresa usuaria, AIVRA podrá identificar al responsable correspondiente, remitir la solicitud o colaborar con éste para facilitar el ejercicio del derecho, de conformidad con el Acuerdo de Encargo y la legislación aplicable.

AIVRA no deberá modificar por iniciativa propia información tributaria o comercial perteneciente a una empresa responsable cuando carezca de instrucciones o base jurídica para hacerlo.

29. Revocación del consentimiento

Cuando una finalidad concreta dependa del consentimiento, el titular podrá retirarlo utilizando los canales habilitados. La retirada del consentimiento no afectará la licitud del tratamiento realizado antes de su revocación y tampoco obligará a interrumpir operaciones sustentadas válidamente en otra base jurídica, como una obligación legal.

30. Reclamos ante la autoridad

El titular puede contactar inicialmente a AIVRA mediante info@aivradigital.com para ejercer sus derechos o presentar una inquietud. Esto no limita su derecho a acudir a la Superintendencia de Protección de Datos Personales del Ecuador (SPDP) mediante los mecanismos legalmente disponibles.

31. Incidentes y vulneraciones de seguridad

AIVRA mantendrá mecanismos para detectar, analizar, documentar, contener y responder a incidentes que puedan comprometer datos personales. Cuando una vulneración de seguridad esté sujeta a notificación, AIVRA realizará las comunicaciones que correspondan dentro de las condiciones y plazos establecidos por la LOPDP y la normativa técnica vigente de la SPDP.

Cuando AIVRA actúe como encargado del tratamiento, informará al responsable afectado conforme a las obligaciones legales y contractuales aplicables.

32. Confidencialidad

Las personas que tengan acceso autorizado a datos personales deberán utilizarlos exclusivamente para las funciones correspondientes y respetar las obligaciones de confidencialidad aplicables. El

acceso técnico o administrativo a la plataforma no constituye autorización para utilizar datos de una empresa cliente con finalidades propias no relacionadas con el servicio.

33. Pagos

Actualmente AIVRA gestiona las suscripciones mediante transferencia bancaria con validación manual. Para verificar el pago, el cliente puede cargar un comprobante que puede contener información financiera o identificativa asociada a la transferencia.

Los comprobantes se almacenan en un área privada de la plataforma y su acceso se limita a las funciones necesarias para revisar el pago. La auditoría técnica no identificó una pasarela automatizada de tarjetas activa en el flujo de producción auditado.

Si posteriormente AIVRA incorpora una pasarela de pago, tokenización, cargos recurrentes u otro mecanismo electrónico, esta Política será actualizada cuando ello implique nuevos destinatarios, categorías de datos o tratamientos relevantes.

34. Cambios en proveedores o tecnología

AIVRA podrá sustituir o incorporar proveedores tecnológicos cuando resulte necesario para operar, mejorar o proteger la plataforma. Cuando el cambio produzca una modificación relevante en el tratamiento de datos personales, AIVRA actualizará esta Política y, cuando legalmente corresponda, informará previamente a los titulares o solicitará la autorización requerida.

35. Cambios en esta Política

La presente Política puede ser actualizada para reflejar modificaciones normativas, técnicas, operativas o relacionadas con nuevas funcionalidades de AIVRA Facturación. La versión vigente se encontrará disponible en el sitio web o plataforma e indicará su fecha de última actualización.

Cuando una modificación afecte sustancialmente las condiciones de un tratamiento en curso, AIVRA adoptará mecanismos razonables de información antes de aplicarla cuando corresponda.

36. Relación con otros documentos

Esta Política forma parte del conjunto documental de AIVRA Digital. Se complementa con los Términos y Condiciones de AIVRA Facturación y, cuando se publiquen o resulten aplicables, con la Política de Cookies, la Política de Cancelaciones, Devoluciones y Reembolsos y el correspondiente Acuerdo de Encargo de Tratamiento de Datos Personales.

Estos documentos deberán interpretarse de forma coherente y ninguna de sus disposiciones podrá utilizarse para reducir derechos que tengan carácter irrenunciable conforme a la legislación aplicable.

37. Contacto

Para consultas sobre privacidad, tratamiento de información o ejercicio de derechos:

AIVRA Digital	AIVRA Facturación
Responsable	Franklin Sebastian Sanmartín Quiroz
Sitio web	https://aivradigital.com
Plataforma	https://facturacion.aivradigital.com
Correo	info@aivradigital.com
País	Ecuador

Marco normativo y fuentes oficiales consideradas

Esta versión fue preparada considerando la normativa y referencias oficiales vigentes consultadas a octubre de 2026, en particular:

- Constitución de la República del Ecuador, especialmente el derecho a la protección de datos personales.
- Ley Orgánica de Protección de Datos Personales, publicada en el Quinto Suplemento del Registro Oficial No. 459 de 26 de mayo de 2021.
- Reglamento General a la Ley Orgánica de Protección de Datos Personales (Decreto Ejecutivo No. 904).
- **Normativa y criterios de la Superintendencia de Protección de Datos Personales, incluida la Norma General de Transferencias o Comunicaciones Nacionales e Internacionales (Resolución SPDP-SPD-2026-0004-R); la normativa sobre inteligencia artificial (Resolución SPDP-SPD-2026-0009-R y su reforma SPDP-SPD-2026-0037-R); la norma sobre tratamiento a gran escala (Resolución SPDP-SPD-2026-0005-R); la normativa sobre seudonimización, anonimización, bloqueo y eliminación; interés legítimo; gestión de riesgos; y la Norma Técnica de Notificaciones de Vulneraciones de Seguridad (Resolución SPDP-SPD-2026-0040-R).**
- Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos, cuando resulte aplicable.
- Normativa tributaria y resoluciones del Servicio de Rentas Internas aplicables a comprobantes electrónicos y conservación documental.
- Especificaciones técnicas vigentes del SRI para comprobantes electrónicos.