

	CASA PAZMIÑO IMPORT & EXPORT SISTEMA AQHORA	01/07/2026	01/07/2026
		Versión 1.1	Página 1 de 8

POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

1. OBJETIVO

La presente Política de Seguridad de la Información establece los principios, responsabilidades y medidas técnicas y organizativas orientadas a proteger la confidencialidad, integridad, disponibilidad, autenticidad, trazabilidad y resiliencia de la información tratada mediante la plataforma AQHora.

Esta Política define el marco general de seguridad aplicable a los sistemas, aplicaciones, bases de datos, servicios y procesos administrados por Casa Luis Pazmiño Import & Export S.A. durante la prestación de AQHora bajo modalidad Software como Servicio (SaaS).

2. ALCANCE

La presente Política aplica, según corresponda, a:

- plataforma web AQHora;
- aplicaciones móviles de AQHora;
- API e integraciones, únicamente cuando se encuentren expresamente contratadas, habilitadas o implementadas;
- infraestructura cloud y servicios tecnológicos administrados por EL PROVEEDOR;
- bases de datos y sistemas de almacenamiento;
- archivos y documentos almacenados mediante las funcionalidades de gestión documental habilitadas;
- sistemas de respaldo y recuperación;
- personal, contratistas y proveedores tecnológicos que intervengan en la prestación del servicio;
- información proporcionada o gestionada por los clientes mediante AQHora.

Esta Política aplica a los sistemas e infraestructura administrados por EL PROVEEDOR. Los dispositivos móviles, equipos biométricos, redes locales, estaciones de trabajo, servidores y demás infraestructura administrada por EL CLIENTE estarán sujetos a sus propios controles de seguridad, sin perjuicio de las obligaciones de integración o soporte que correspondan a AQHora.

	CASA PAZMIÑO IMPORT & EXPORT SISTEMA AQHORA	01/07/2026	01/07/2026
		Versión 1.1	Página 2 de 8

3. PRINCIPIOS DE SEGURIDAD

AQHora adopta los siguientes principios como base de su gestión de seguridad de la información:

- **Confidencialidad**

La información será accesible únicamente por personas debidamente autorizadas y conforme a las funciones, perfiles y necesidades de acceso asignadas.

- **Integridad**

Se aplicarán controles orientados a prevenir modificaciones no autorizadas, detectar alteraciones relevantes y mantener la consistencia de la información.

- **Disponibilidad**

Los servicios serán operados con medidas orientadas a mantener su disponibilidad y recuperación conforme a la arquitectura implementada y al Acuerdo de Nivel de Servicio (SLA).

- **Autenticidad**

AQHora utilizará mecanismos de autenticación orientados a verificar que el acceso sea realizado mediante las credenciales o mecanismos de seguridad asociados al usuario autorizado.

- **Trazabilidad**

AQHora mantendrá registros de auditoría sobre las operaciones, accesos y cambios definidos como relevantes según la funcionalidad, el nivel de riesgo y las capacidades técnicas de la plataforma.

- **Mínimo privilegio**

Los accesos se concederán únicamente en la medida necesaria para el cumplimiento de las funciones asignadas.

- **Responsabilidad compartida**

La seguridad del servicio depende de controles implementados tanto por EL PROVEEDOR como por EL CLIENTE y sus usuarios, de acuerdo con los componentes que cada parte administra.

4. GESTIÓN DE ACCESOS

AQHora aplicará controles de acceso basados en los principios de mínimo privilegio, necesidad de conocer y separación de funciones cuando resulte aplicable.

- Cada usuario dispondrá de credenciales individuales, salvo excepciones técnicas debidamente justificadas.
- Las credenciales deberán mantenerse confidenciales y no podrán compartirse.
- AQHora aplicará los controles de longitud, complejidad, bloqueo, recuperación o vigencia de credenciales que se encuentren implementados y documentados para cada tipo de usuario.

	CASA PAZMIÑO IMPORT & EXPORT SISTEMA AQHORA	01/07/2026	01/07/2026
		Versión 1.1	Página 3 de 8

- Los accesos administrativos del personal de EL PROVEEDOR estarán restringidos y serán revisados de acuerdo con su criticidad.
- EL CLIENTE será responsable de revisar, actualizar y revocar los usuarios, perfiles y permisos asignados dentro de su organización.
- Los accesos deberán ser revocados o modificados cuando cambien las funciones del usuario o finalice su relación con la organización.
- Podrán implementarse mecanismos de autenticación multifactor cuando se encuentren disponibles y habilitados.

5. AUTENTICACIÓN LOCAL EN DISPOSITIVOS MÓVILES

Cuando un usuario realice una marcación desde la aplicación móvil, AQHora podrá solicitar la validación del mecanismo de autenticación configurado en el dispositivo.

Esta validación será ejecutada localmente por el sistema operativo mediante reconocimiento facial, huella dactilar, código PIN, patrón, contraseña u otro mecanismo disponible.

AQHora no recopila, consulta, transmite ni almacena: huellas, rostros, plantillas biométricas, códigos PIN, contraseñas, patrones de desbloqueo ni datos de enrolamiento del dispositivo. La plataforma recibe únicamente el resultado técnico de la validación.

Si el dispositivo no tiene configurado un mecanismo de autenticación compatible, la marcación podrá efectuarse sin esta validación adicional, de acuerdo con la configuración disponible.

6. SEGURIDAD DE LAS COMUNICACIONES

Las comunicaciones entre los usuarios, aplicaciones, servicios de AQHora e integraciones administradas por EL PROVEEDOR utilizarán protocolos y mecanismos de transmisión seguros cuando sean técnicamente aplicables. La seguridad, disponibilidad y configuración de las redes, conexiones a Internet y equipos de comunicación administrados por EL CLIENTE serán responsabilidad de este último.

7. SEGURIDAD DE LOS DATOS

EL PROVEEDOR implementará medidas técnicas y organizativas razonables y proporcionales al riesgo para proteger la información que se encuentre bajo su administración, incluyendo, según corresponda:

- segregación lógica de los datos entre organizaciones;
- controles de acceso a bases de datos y servicios;
- registros de auditoría;
- monitoreo de actividades y eventos relevantes;

	CASA PAZMIÑO IMPORT & EXPORT SISTEMA AQHORA	01/07/2026	01/07/2026
		Versión 1.1	Página 4 de 8

- protección frente a modificaciones no autorizadas;
- restricción de acceso al personal autorizado;
- medidas de continuidad, respaldo y recuperación.

La incorporación de controles adicionales, como cifrado en reposo u otras medidas específicas, dependerá de la arquitectura, servicios y capacidades técnicas efectivamente implementadas.

8. COPIAS DE SEGURIDAD Y RECUPERACIÓN

AQHora realizará copias de seguridad conforme a la arquitectura del servicio, el SLA y la Política de Backups y Recuperación vigente, cuando dicho documento se encuentre aprobado.

Las copias de seguridad estarán sujetas a condiciones de frecuencia, retención, verificación, restauración y eliminación definidas por EL PROVEEDOR.

Los respaldos constituyen una medida de continuidad y recuperación, pero no garantizan que cualquier dato pueda restaurarse en todos los escenarios ni sustituyen las exportaciones, verificaciones o controles que correspondan a EL CLIENTE.

9. SEGURIDAD DEL DESARROLLO Y GESTIÓN DE CAMBIOS

Durante el ciclo de vida de AQHora se aplicarán controles de gestión de versiones, control de cambios, pruebas funcionales y revisión antes del despliegue.

Según la naturaleza y el riesgo del cambio, podrán efectuarse revisiones de código, pruebas de seguridad y validaciones adicionales.

Se procurará mantener una separación razonable entre los ambientes, accesos y datos utilizados para desarrollo, pruebas y producción. Los datos reales de clientes no deberán utilizarse en ambientes de desarrollo o pruebas salvo necesidad justificada, autorización y aplicación de medidas adecuadas de protección.

10. GESTIÓN DE VULNERABILIDADES

EL PROVEEDOR mantendrá un proceso proporcional al riesgo para recibir, identificar, evaluar, priorizar y corregir vulnerabilidades que afecten a los componentes bajo su administración.

La prioridad y los plazos de atención dependerán de la severidad, posibilidad de explotación, nivel de exposición, impacto, disponibilidad de una corrección, complejidad técnica y riesgo operativo, sin perjuicio de las obligaciones legales o contractuales aplicables.

	CASA PAZMIÑO IMPORT & EXPORT SISTEMA AQHORA	01/07/2026	01/07/2026
		Versión 1.1	Página 5 de 8

11. REGISTROS Y AUDITORÍA

La plataforma podrá mantener registros relacionados con:

- autenticaciones;
- accesos administrativos;
- cambios relevantes;
- configuración del sistema;
- eventos de seguridad;
- aceptación de documentos legales;
- operaciones definidas como relevantes para soporte, trazabilidad o cumplimiento.

Los registros se conservarán conforme a la Política de Retención y Eliminación de Datos y su acceso estará restringido al personal autorizado.

12. GESTIÓN DE INCIDENTES DE SEGURIDAD

AQHora mantendrá procedimientos para identificar, registrar, analizar, contener, corregir y documentar incidentes de seguridad que puedan afectar la plataforma o la información tratada.

Cuando EL PROVEEDOR tenga conocimiento de un incidente o vulneración de seguridad que afecte de manera significativa los datos tratados por cuenta de EL CLIENTE, lo notificará sin demora injustificada y dentro de los plazos aplicables, proporcionando la información disponible y colaborando razonablemente con la gestión del incidente.

No todo error funcional, indisponibilidad o evento técnico constituye una vulneración de datos personales. La clasificación dependerá de la naturaleza, alcance e impacto del evento.

13. CONTINUIDAD DEL SERVICIO

EL PROVEEDOR mantendrá medidas y procedimientos razonables de continuidad y recuperación orientados a restablecer los servicios frente a eventos que afecten su operación, de acuerdo con la criticidad del evento, la arquitectura disponible y los compromisos establecidos en el SLA.

La continuidad de AQHora no comprende fallas originadas exclusivamente en la conexión a Internet, redes locales, dispositivos biométricos, equipos móviles, estaciones de trabajo o servidores administrados por EL CLIENTE.

	CASA PAZMIÑO IMPORT & EXPORT SISTEMA AQHORA	01/07/2026	01/07/2026
		Versión 1.1	Página 6 de 8

14.SEGURIDAD DE PROVEEDORES Y TERCEROS

EL PROVEEDOR evaluará, de manera proporcional al riesgo, las condiciones de seguridad y protección de datos de los terceros que intervengan en la prestación del servicio.

Cuando corresponda, se establecerán obligaciones contractuales de confidencialidad, seguridad, tratamiento de datos, continuidad y notificación de incidentes.

15.SEGURIDAD DEL PERSONAL

El personal y los contratistas que accedan a información o sistemas de AQHora estarán sujetos, según corresponda, a obligaciones de confidencialidad, controles de acceso, capacitación y deberes de reporte de incidentes.

Los accesos serán otorgados de acuerdo con las funciones asignadas y deberán revocarse o modificarse cuando finalice o cambie la relación laboral o contractual.

16.DISPOSITIVOS BIOMÉTRICOS ADMINISTRADOS POR EL CLIENTE

Los equipos biométricos utilizados por EL CLIENTE operan dentro de su propia infraestructura. Los datos de enrolamiento, plantillas de huellas, patrones faciales y demás información biométrica almacenada directamente en dichos equipos no forman parte de la información administrada por AQHora.

Cuando se encuentre habilitado el módulo de descarga, este transmitirá únicamente las marcaciones y datos operativos asociados necesarios para el control de asistencia.

La adquisición, instalación, configuración, mantenimiento, seguridad, enrolamiento y administración de dichos dispositivos será responsabilidad de EL CLIENTE.

17.RESPONSABILIDADES DE EL CLIENTE

EL CLIENTE deberá:

- administrar adecuadamente sus usuarios, perfiles y permisos;
- revocar oportunamente los accesos de personas que ya no deban utilizar la plataforma;
- proteger las credenciales y evitar que sean compartidas;
- mantener actualizados y protegidos los dispositivos, navegadores, sistemas operativos y redes bajo su administración;
- gestionar adecuadamente los permisos de la aplicación móvil;
- administrar y proteger sus equipos biométricos, datos de enrolamiento y la infraestructura donde opere el módulo de descarga;
- notificar oportunamente sospechas de acceso no autorizado, pérdida de credenciales o incidentes;

	CASA PAZMIÑO IMPORT & EXPORT SISTEMA AQHORA	01/07/2026	01/07/2026
		Versión 1.1	Página 7 de 8

- utilizar AQHora conforme al Contrato SaaS y a las políticas vigentes;
- mantener respaldos propios de la información exportada cuando corresponda;
- no intentar vulnerar, eludir o alterar los controles de seguridad de la plataforma.

18. RESPONSABILIDADES DE EL PROVEEDOR

Casa Luis Pazmiño Import & Export S.A. se compromete a:

- implementar medidas técnicas y organizativas razonables y proporcionales al riesgo para proteger la infraestructura bajo su administración;
- restringir los accesos de su personal autorizado;
- mantener obligaciones de confidencialidad y capacitación aplicables;
- revisar los controles de acuerdo con su criticidad, los riesgos identificados, los cambios tecnológicos y los resultados de incidentes o evaluaciones internas;
- mantener procesos de mejora continua razonables y acordes con las capacidades de la organización;
- colaborar con EL CLIENTE en los asuntos de seguridad dentro del alcance técnico y contractual del servicio.

19. CUMPLIMIENTO Y BUENAS PRÁCTICAS

AQHora podrá considerar estándares y buenas prácticas reconocidas, como ISO/IEC 27001, ISO/IEC 27002, NIST Cybersecurity Framework o CIS Controls, en función de la naturaleza del servicio, los riesgos identificados y las capacidades de la organización.

La referencia a dichos marcos no implica certificación ni conformidad integral, salvo declaración expresa y verificable de EL PROVEEDOR.

20. REVISIÓN DE LA POLÍTICA

La presente Política será revisada al menos una vez al año y cuando existan cambios relevantes en la legislación, infraestructura, riesgos, servicios, proveedores o arquitectura de AQHora.

Las revisiones deberán quedar documentadas mediante fecha, versión y aprobación correspondiente.

21. DOCUMENTOS RELACIONADOS

La presente Política deberá interpretarse conjuntamente con:

1. Contrato de Licencia de Uso de Software como Servicio (SaaS);
2. Términos y Condiciones;
3. Política de Privacidad;
4. Acuerdo de Tratamiento de Datos Personales (DPA);

	CASA PAZMIÑO IMPORT & EXPORT SISTEMA AQHORA	01/07/2026	01/07/2026
		Versión 1.1	Página 8 de 8

5. Acuerdo de Nivel de Servicio (SLA);
6. Política de Uso Aceptable;
7. Política de Retención y Eliminación de Datos;
8. Política de Geolocalización;
9. Política de Almacenamiento Local;
10. Política de Backups y Recuperación, cuando se encuentre aprobada;

22. ACEPTACIÓN

EL CLIENTE aceptará la presente Política mediante los mecanismos electrónicos o contractuales establecidos por AQHora.

Como evidencia de aceptación, AQHora podrá registrar la fecha y hora, el usuario administrador, el cliente u organización asociada y la versión aceptada.

EL CLIENTE será responsable de comunicar a sus usuarios las obligaciones de seguridad que les resulten aplicables.

