POLÍTICA DE USO ACEPTABLE (AUP)

1. OBJETIVO

La presente Política de Uso Aceptable establece las reglas aplicables al acceso y utilización de AQHora, con el fin de proteger la seguridad, estabilidad, disponibilidad e integridad del servicio, así como los derechos de EL CLIENTE, sus usuarios, otros clientes y terceros.

Esta Política forma parte del Contrato SaaS, los Términos y Condiciones y los demás documentos aplicables a AQHora.

2. ALCANCE

Esta Política aplica a EL CLIENTE, sus administradores, supervisores, empleados, usuarios autorizados, socios comerciales autorizados, consultores, integradores, distribuidores y terceros a quienes se otorgue acceso a AQHora bajo responsabilidad de EL CLIENTE.

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

3. PRINCIPIOS GENERALES DE USO

- utilizar AQHora de buena fe y conforme a la legislación aplicable;
- respetar los derechos de terceros;
- utilizar únicamente las funciones, módulos y recursos habilitados;
- no comprometer la seguridad, estabilidad o disponibilidad del servicio;
- mantener un uso proporcional al plan contratado y a la finalidad del servicio;
- proteger credenciales, sesiones, dispositivos y accesos bajo su administración.

4. USOS AUTORIZADOS

AQHora podrá utilizarse para las funcionalidades incluidas en el plan contratado o expresamente habilitadas, entre ellas:

- control de asistencia y marcaciones;
- gestión de horarios, turnos, jornadas, vacaciones, permisos y horas extraordinarias;
- acciones de personal y procesos de gestión laboral;
- gestión documental vinculada con las funcionalidades habilitadas;

MATRIZ
Grecia N32-85 y Av. Mariana de Jesús
(593-2) 2 504675 - 2557512 - 2557514
Whatsapp: +593 98 332 1518
ventas@casapazmino.com.ec
Quito - Ecuador

- reportes;
- aplicación móvil y geolocalización cuando se encuentren habilitadas;
- integraciones y API cuando hayan sido contratadas, autorizadas e implementadas;
- módulos o servicios adicionales expresamente contratados.

5. ACTIVIDADES PROHIBIDAS

- **Acceso no autorizado**
  - acceder o intentar acceder a información de otros clientes, cuentas de terceros, bases de datos, servidores, API restringidas o infraestructura no autorizada;
  - eludir controles de autenticación, autorización o segregación lógica;
  - utilizar credenciales, tokens o sesiones que no le hayan sido asignados.
- **Ingeniería inversa y copia no autorizada**
  - descompilar, desensamblar o realizar ingeniería inversa;
  - intentar obtener el código fuente;
  - copiar algoritmos, documentación confidencial, interfaces o componentes protegidos;
  - reproducir sustancialmente elementos protegidos mediante copia no autorizada.
- **Manipulación de registros y configuraciones**
  - modificar configuraciones técnicas, de seguridad, integración o infraestructura fuera de los permisos habilitados;
  - alterar, eliminar u ocultar registros de auditoría o evidencias;
  - crear, modificar o eliminar marcaciones mediante mecanismos no autorizados o con intención de falsear la asistencia;
  - manipular tokens, sesiones, localStorage, sessionStorage o comunicaciones para alterar el comportamiento del sistema.
- **Ataques y pruebas no autorizadas**
  - realizar escaneos, pruebas de penetración o explotación de vulnerabilidades sin autorización previa y escrita;
  - ejecutar ataques de denegación de servicio, automatizaciones maliciosas o consultas destinadas a degradar el servicio;
  - utilizar bots, scripts o herramientas que afecten la estabilidad o seguridad de AQHora.

- **Malware y contenido peligroso**
  - cargar o distribuir virus, ransomware, spyware, troyanos, scripts maliciosos o código destinado a afectar la plataforma;
  - cargar archivos ejecutables, formatos no permitidos o contenido técnicamente peligroso.
- **Uso fraudulento o ilícito**
  - suplantar usuarios o marcar por cuenta de otra persona;
  - simular o falsificar la ubicación, incluida la utilización de GPS spoofing;
  - alterar deliberadamente la fecha u hora del dispositivo para falsear registros;
  - registrar información falsa, ocultar información relevante o utilizar AQHora para actividades ilícitas.
- **Uso abusivo de recursos**
  - consumir recursos de forma desproporcionada o mediante automatizaciones no autorizadas;
  - utilizar AQHora para minería de criptomonedas;
  - usar la gestión documental como almacenamiento general, repositorio de copias externas o para archivos ajenos a los procesos habilitados;
  - realizar cargas masivas no autorizadas o exceder límites técnicos, de tamaño o formato establecidos.

6. API E INTEGRACIONES

Esta sección aplica únicamente cuando EL CLIENTE haya contratado y tenga habilitado el acceso a una API o integración oficial de AQHora.

- utilizar exclusivamente credenciales autorizadas;
- proteger las llaves y no publicarlas ni incorporarlas en repositorios accesibles;
- respetar límites de frecuencia, métodos documentados y alcance autorizado;
- no consultar datos de organizaciones distintas de la autorizada;
- revocar o renovar credenciales comprometidas;
- validar y proteger los datos recibidos;
- informar incidentes o consumos anómalos relacionados con la integración.

EL PROVEEDOR podrá limitar temporalmente el acceso cuando el consumo afecte o pueda afectar la seguridad, estabilidad o disponibilidad del servicio.

7. CREDENCIALES, SESIONES Y DISPOSITIVOS

- mantener la confidencialidad de credenciales y no compartir cuentas personales;
- utilizar contraseñas seguras conforme a los controles implementados;
- cerrar sesión en equipos compartidos;
- desactivar oportunamente usuarios desvinculados;
- reportar pérdida, robo o compromiso de dispositivos o credenciales;
- no extraer, modificar o reutilizar tokens y sesiones fuera de los mecanismos autorizados;
- proteger los dispositivos biométricos, móviles, servidores y redes bajo administración de EL CLIENTE.

Cuando la aplicación móvil solicite la autenticación configurada en el dispositivo, dicha validación será ejecutada localmente por el sistema operativo. AQHora no recibe ni almacena rostros, huellas, PIN, patrones, contraseñas ni plantillas biométricas.

8. DATOS PERSONALES Y CONTENIDO DEL CLIENTE

EL CLIENTE será responsable de garantizar que los datos y contenidos incorporados a AQHora:

- cuenten con una base jurídica válida;
- sean adecuados, pertinentes y limitados a la finalidad informada;
- se mantengan actualizados cuando corresponda;
- no infrinjan derechos de terceros;
- no contengan información ilícita, maliciosa o ajena a las funciones habilitadas;
- no incluyan datos biométricos de enrolamiento, huellas, rostros o plantillas biométricas, salvo acuerdo previo y escrito con EL PROVEEDOR;
- sean accesibles únicamente para usuarios autorizados.

EL PROVEEDOR podrá bloquear, aislar o limitar archivos maliciosos, formatos no permitidos o contenido que represente un riesgo técnico. Cuando sea razonablemente posible, informará a EL CLIENTE antes de eliminar contenido.

9. GEOLOCALIZACIÓN Y MARCACIONES

- utilizar la geolocalización únicamente para las finalidades configuradas e informadas;
- no simular, falsificar o manipular la ubicación;
- no realizar marcaciones por cuenta de terceros;
- considerar posibles limitaciones técnicas de precisión antes de adoptar decisiones laborales;
- utilizar únicamente los mecanismos autorizados para corregir o justificar marcaciones.

MATRIZ
Grecia N32-85 y Av. Mariana de Jesús
(593-2) 2 504675 - 2557512 - 2557514
Whatsapp: +593 98 332 1518
ventas@casapazmino.com.ec
Quito - Ecuador

AQHora obtiene la ubicación únicamente al realizar una acción que requiere validación geográfica y no realiza seguimiento continuo del dispositivo.

10. REPORTE RESPONSABLE DE VULNERABILIDADES

La identificación de una posible vulnerabilidad deberá comunicarse de manera confidencial a EL PROVEEDOR. No podrá explotarse, divulgarse públicamente ni utilizarse para acceder a información ajena.

Toda prueba autorizada deberá contar con un alcance escrito que determine fechas, sistemas, responsables, direcciones de origen, técnicas permitidas y procedimiento de notificación.

11. MONITOREO DEL SERVICIO

EL PROVEEDOR podrá monitorear información técnica, registros y eventos necesarios para la operación, seguridad, soporte, cumplimiento, disponibilidad, auditoría y prevención de abusos.

El acceso al contenido de EL CLIENTE se realizará únicamente cuando resulte necesario, esté autorizado contractualmente, responda a una solicitud de soporte, exista un incidente de seguridad o una obligación legal.

12. MEDIDAS CORRECTIVAS

Cuando EL PROVEEDOR detecte un incumplimiento, podrá adoptar medidas proporcionales considerando la gravedad, intencionalidad, reincidencia, riesgo, impacto y posibilidad de corrección.

- advertencia o requerimiento de corrección;
- cambio obligatorio de credenciales;
- bloqueo preventivo de un usuario o sesión;
- limitación temporal de funcionalidades o integraciones;
- suspensión temporal del servicio;
- terminación contractual en casos graves, intencionales, reiterados o no subsanados;
- notificación a autoridades cuando corresponda.

En incumplimientos corregibles, EL PROVEEDOR procurará informar y conceder un plazo razonable para subsanar. Podrá actuar de inmediato cuando exista un ataque activo, malware, acceso no autorizado, uso ilícito, riesgo grave para otros clientes, datos personales o la continuidad del servicio, o requerimiento de autoridad competente.

13. RESPONSABILIDADES DE EL CLIENTE

- administrar usuarios, perfiles y permisos;
- desactivar usuarios desvinculados;

- proteger credenciales, tokens, dispositivos, redes y sistemas bajo su administración;
- gestionar los equipos biométricos y el servidor o computador del módulo de descarga;
- informar a sus usuarios sobre esta Política;
- supervisar a integradores, consultores y terceros autorizados;
- cumplir la normativa laboral y de protección de datos;
- notificar oportunamente incidentes o sospechas de uso indebido.

EL CLIENTE será responsable de las acciones efectuadas mediante sus cuentas y credenciales cuando sean atribuibles a su administración, usuarios autorizados, negligencia o incumplimiento de sus obligaciones de seguridad.

14. RESPONSABILIDADES DE EL PROVEEDOR

- mantener medidas técnicas y organizativas razonables y proporcionales al riesgo sobre la infraestructura bajo su administración;
- investigar incidentes relacionados con AQHora;
- aplicar actualizaciones y correcciones de seguridad conforme a su criticidad;
- proteger la confidencialidad de la información conforme a sus obligaciones;
- revisar y ajustar razonablemente controles y funcionalidades de acuerdo con riesgos, incidentes y evolución tecnológica.

15. INCUMPLIMIENTO

El incumplimiento de esta Política podrá constituir incumplimiento del Contrato SaaS y dar lugar a las medidas previstas en dicho contrato, sin perjuicio de las acciones legales que correspondan.

16. ACTUALIZACIONES

AQHora podrá actualizar esta Política por cambios legales, regulatorios, tecnológicos, funcionales o de seguridad.

Cuando una actualización introduzca restricciones sustanciales o modifique materialmente las obligaciones de EL CLIENTE, se informará por los canales habituales y se solicitará una nueva aceptación cuando corresponda.

17. ACEPTACIÓN

EL CLIENTE aceptará esta Política mediante los mecanismos electrónicos o contractuales establecidos por AQHora y será responsable de comunicar a sus usuarios las reglas aplicables.

MATRIZ
Grecia N32-85 y Av. Mariana de Jesús
(593-2) 2 504675 - 2557512 - 2557514
Whatsapp: +593 98 332 1518
ventas@casapazmino.com.ec
Quito - Ecuador

Como evidencia de aceptación, AQHora podrá registrar:

- fecha y hora;
- usuario administrador;
- versión de la política aceptada.

18. DOCUMENTOS RELACIONADOS

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);
5. Política de Seguridad de la Información;
6. Política de Almacenamiento Local y Tecnologías de Autenticación;
7. Política de Geolocalización;
8. Política sobre Dispositivos Biométricos y Autenticación Local;
9. Política de Retención y Eliminación de Datos;
10. Acuerdo de Nivel de Servicio (SLA).

ANEXO A – CUADRO DE CONDUCTAS

Conducta	Estado	Medida posible
Corregir marcaciones mediante funciones autorizadas	Permitida	La acción deberá quedar registrada en auditoría cuando corresponda.
Ejecutar pruebas de seguridad autorizadas	Permitida con autorización	Sujeta al alcance y condiciones aprobadas por escrito.
Cargar software malicioso	No permitida	Bloqueo inmediato, aislamiento, investigación y posible notificación.
Usar la API oficial	Permitida cuando esté contratada	Sujeta a límites, credenciales y documentación oficial.
Usar autenticación local del dispositivo	Permitida	Validación local sin transmisión de datos biométricos a AQHora.
Cargar documentos relacionados con los módulos habilitados	Permitida	Sujeta a límites de formato, tamaño, finalidad y almacenamiento.

MATRIZ
Grecia N32-85 y Av. Mariana de Jesús
(593-2) 2 504675 - 2557512 - 2557514
Whatsapp: +593 98 332 1518
ventas@casapazmino.com.ec
Quito - Ecuador