

Política de Uso Aceptable

Qué puede y qué no puede pasar por nuestra infraestructura.

Lo esencial para consultar

- Uso lícito y respeto a personas y datos.
- Sin fraude, intrusión, malware o spam.
- Contención proporcional y posibilidad de revisión.

Resumen orientativo. Prevalecen las cláusulas completas siguientes.

1. Personas y usos comprendidos

La AUP abarca al cliente, representantes y usuarios de sitios, aplicaciones, correo, integraciones, bots y herramientas bajo su administración. Debe informar reglas y actuar ante abuso conocido sin presumir responsabilidad automática por todo tercero.

Usar un recurso no autoriza acceder a cuentas, datos, redes o equipos ajenos. Se aplican pedido y licencias. Criticar, reclamar o ejercer derechos no constituye abuso por sí solo.

2. Actividades ilícitas e infracción de derechos

Se prohíben fraude, phishing, robo de credenciales, suplantación engañosa, explotación infantil, trata, imágenes íntimas sin consentimiento, incitación criminal a violencia y discriminación ilícita. También comercio ilegal y distribución sin autorización o fundamento exigido.

Se analizan ley, evidencia, contexto y función de Zovvi. Discrepar de una opinión no la hace ilícita. Los avisos identifican recursos y hechos; no toda denuncia implica retirada automática.

3. Seguridad e integridad de red

Se prohíben malware, ransomware, botnets, explotación no autorizada, captura indebida de tráfico, fuerza bruta, distribución de credenciales y denegación de servicio. No alojes archivos para atacar a Zovvi o terceros.

Investigar responsablemente no es autorización general: pruebas de riesgo, escaneo o explotación requieren alcance escrito más allá del uso normal propio. Las consultas públicas no invasivas tienen límites. Ante datos ajenos, detén la exploración y reporta evidencia mínima.

4. Mensajes, datos y privacidad

No envíes spam, ocultes remitente, uses listas compradas o abusivas, ignores bajas o explotes cuentas comprometidas. Los mensajes requieren finalidad lícita y reglas de correo; SPF o cuota disponible no autoriza abuso.

Los datos y materiales ajenos requieren legitimidad. No se publican credenciales, filtraciones o datos ilícitos. Las finalidades de datos de visitantes no se transfieren automáticamente al alojamiento; las funciones dependen de actividad y ley.

5. Recursos, automatización y entorno compartido

Usa CPU, memoria, I/O, procesos, almacenamiento y envíos dentro del plan. No eludas aislamiento, cuotas o autenticación con múltiples cuentas o automatización. Alojar una web no equivale a repositorio irrestricto, minería o procesamiento no incluido.

Bots y tareas necesitan control de consumo. Los picos legítimos exigen diagnóstico, no presunción de infracción. Los límites se informan antes; uso justo no crea límites ocultos posteriores.

6. Gestión de incidentes y medidas

Se evalúan evidencia e impacto. Puede orientarse corrección, limitar envío o proceso, aislar recursos o suspender si es necesario. La medida es proporcional y limita el componente cuando protege al resto. Riesgo urgente u orden válida pueden exigir actuar antes de avisar.

Se registran motivo, alcance y regularización sin exponer denunciantes o protecciones. Gravedad o reiteración pueden justificar terminación conforme a ley. Contener no autoriza explotar o divulgar datos.

7. Informe, impugnación y derechos

Usa Denunciar abuso para recursos sospechosos y Reportar error para fallos de plataforma. Indica URL, hechos, fechas y evidencia mínima sin archivos ilícitos, contraseñas o bases ajenas. La propiedad intelectual sigue su política. No uses el canal para intimidar retirada de contenido lícito.

El cliente puede pedir revisión y aportar contexto. Preservar o entregar datos a autoridades requiere fundamento y legitimidad. La AUP no elimina derechos o permite retenciones abusivas.