

Seguridad de Acceso y Autenticación

Responsabilidades para proteger cuentas y autorizar operaciones.

Lo esencial para consultar

- Usa cuentas individuales y doble factor.
- Nunca envíes contraseñas en formularios públicos.
- Recuperar acceso requiere verificación proporcional.

Resumen orientativo. Prevalecen las cláusulas completas siguientes.

1. Responsabilidades y alcance

Cubre cuenta, paneles, accesos administrativos, integraciones y autorizados. Zovvi protege componentes que administra; el cliente protege dispositivos, aplicaciones y permisos propios. Se evalúan causa y obligaciones sin atribuir automáticamente todo al titular.

2. Contraseñas, factores y dispositivos

Usa contraseña larga y única, gestor fiable y doble factor disponible. Guarda recuperación separada. No se exige cambio periódico arbitrario como sustituto de seguridad; cambia ante compromiso o indicación fundada.

Acciones sensibles pueden requerir segundo factor o confirmación informada. Actualiza y bloquea equipos. Soporte no pide contraseña o código en contacto no solicitado.

3. Equipo, delegación y privilegios

Prefiere accesos individuales, privilegios mínimos y revocación al terminar vínculos. Identifica quién puede administrar, comprar o borrar. No compartas credencial principal con agencias; usa delegación o autorización limitada disponible.

Cambios sensibles requieren verificar poderes. Conocer dominio o estar copiado no acredita titularidad. Las disputas requieren evidencia y protección de las partes.

4. Claves, integraciones y acceso técnico

Tokens y claves requieren alcance mínimo, protección y rotación si se exponen. No los publiques en código, URL, capturas o tickets abiertos. Para soporte o migración usa acceso temporal por canal seguro y revócalo después.

El acceso técnico será necesario, limitado y confidencial. Diagnosticar no autoriza otros usos de datos. Sobrescribir o afectar disponibilidad requiere alcance y autorización adecuados.

5. Recuperación e incidentes

Avisa a soporte si pierdes acceso, detectas sesión sospechosa o fraude. Indica servicio, hora y hechos sin secretos. Recuperar requiere comprobar titularidad proporcionalmente y proteger documentos; un recibo aislado no transfiere control.

Ante riesgo concreto pueden cerrarse sesiones, revocarse tokens o aislar componentes, informando motivo y pasos cuando viable. No se impide impugnar o ejercer derechos. Aplica privacidad.

6. Aplicaciones y revisión

Actualiza CMS, plugins y dependencias, elimina accesos sin uso y conserva copias independientes. SSL protege transporte, no garantiza ausencia de vulnerabilidades o legitimidad de mensajes. Exigencias adicionales serán proporcionales, explicadas y compatibles. Puedes pedir revisión ante verificaciones excesivas.

