

Política de Copias y Conservación de Datos

Entiende las copias, la restauración y la conservación.

Lo esencial para consultar

- Copia diaria y siete puntos de restauración.
- Infraestructura separada del entorno principal.
- Copia, archivo y conservación legal son distintos.

Resumen orientativo. Prevalecen las cláusulas completas siguientes.

1. Cobertura de las copias incluidas

Esta política cubre copias del alojamiento que incluya el recurso. Comprende archivos y bases del entorno contratado; los buzones nativos se incluyen si forman parte de él. El alcance debe identificarse antes de contratar, sin presumir cobertura de plataformas externas.

Workspace, correo de terceros, equipos propios y almacenamiento externo tienen condiciones específicas. Las exclusiones por tipo, tamaño o cantidad deben informarse en la oferta, no al restaurar. Caché regenerable y temporales pueden excluirse si no perjudican la recuperación de datos necesarios.

2. Frecuencia, puntos y rotación

La rutina es diaria y conserva siete puntos en rotación: una copia completada sustituye al punto más antiguo. No significa siete versiones por archivo ni recuperar cualquier hora intermedia. Se deben considerar las horas de copias completadas.

La referencia diaria es una ventana de hasta 24 horas en operación normal, no pérdida cero. Los fallos y copias incompletas se investigan y corrigen sin presentarlos como saludables sin validar. Objetivos específicos de pérdida admisible (RPO) o tiempo de recuperación (RTO) requieren contratación expresa.

3. Separación y protección de copias

Los puntos incluidos se mantienen en infraestructura separada del alojamiento principal, no en una carpeta del mismo disco. El acceso debe limitarse a personas y sistemas autorizados, con credenciales protegidas y trazabilidad administrativa.

La separación reduce exposición a fallos principales sin eliminar todos los riesgos o sustituir una copia independiente del cliente. No se presume redundancia geográfica, inmutabilidad, conservación permanente o certificación sin descripción expresa.

4. Solicitar y autorizar restauración

Usa soporte autenticado indicando servicio, datos, punto, motivo y cambios posteriores. Se confirma el alcance antes de sobrescribir: archivos, bases y mensajes pueden tener tiempos diferentes. El solicitante debe estar autorizado.

Restaurar puede sustituir cambios posteriores. Cuando sea viable, guarda el estado actual y prueba por separado. No se impone una tasa oculta para el alcance incluido; trabajos extraordinarios requieren presupuesto aceptado. El plazo depende de volumen y complejidad, sin prometer recuperación instantánea.

5. Integridad y colaboración del cliente

Mantén copias propias fuera del alojamiento y de las credenciales principales, especialmente antes de cambios. Prueba archivos y bases: existir una copia no demuestra integridad. El cifrado del cliente depende de sus claves, que no deben enviarse por formularios públicos.

Una copia puede conservar corrupción o malware previo. Restaurar no audita ni limpia toda la aplicación. Se evalúan causas y obligaciones; recomendar copias propias no excluye la responsabilidad de Zovvi por su rutina contratada.

6. Suspensión, cierre y eliminación

Suspender acceso no equivale a eliminar. Durante la conservación por impago se comunican cobertura y restricciones. Antes del cierre, pide exportación y confirma qué se eliminará. No dependas de un punto que ya salió de la rotación.

Tras eliminar producción, copias residuales pueden permanecer aisladas hasta completar siete días de rotación, sin nuevo uso y con restricciones legales. No garantizan reactivación. Pagar después no reconstruye datos. Una obligación válida puede exigir conservación separada y restringida.

7. Conservación legal no es archivo de la web

Documentos fiscales, contrato, seguridad y accesos con obligación legal tienen finalidades y plazos propios según Privacidad y ley. Guardarlos no significa conservar archivos, bases o mensajes por el mismo plazo.

El backup no es archivo histórico permanente o recuperación forense. Los derechos sobre datos y

pedidos de autoridad requieren legitimidad y minimización. Los cambios de cobertura, frecuencia o conservación se comunican sin reducir retroactivamente el servicio.

