

Política de Backup e Retenção de Dados

Saiba o que precisa de cópia, como restaurar e o que a retenção significa.

O essencial para consulta

- Cópia diária e sete pontos de restauração.
- Infraestrutura separada do ambiente principal.
- Backup, arquivo e retenção legal são coisas diferentes.

Resumo de consulta. As cláusulas completas abaixo prevalecem.

1. Cobertura do backup incluído

Esta política cobre a rotina de backup da hospedagem de sites com esse recurso incluído no pedido. Abrange arquivos do site e bancos de dados do ambiente contratado; caixas de e-mail nativas da hospedagem entram quando fazem parte desse ambiente. O escopo deve estar identificado antes da contratação. Não presumimos cobertura de dados mantidos apenas em plataformas externas.

Workspace, e-mail de terceiros, equipamentos do cliente, armazenamento externo e produtos com backup próprio dependem de suas condições específicas. Qualquer exclusão por tipo, tamanho ou quantidade de arquivos deve constar na oferta, não surgir somente na hora de restaurar. Cache regenerável e arquivos temporários podem ficar fora da cópia quando essa exclusão não comprometer os dados necessários à recuperação.

2. Frequência, pontos e rotação

A rotina é diária e conserva sete pontos de restauração, em rotação: uma nova cópia concluída substitui o ponto mais antigo. Sete pontos não significam sete versões por arquivo nem garantia de recuperar qualquer horário intermediário. Os horários dos pontos efetivamente concluídos devem ser considerados na escolha da restauração.

A periodicidade diária tem como referência uma janela de até 24 horas entre cópias em operação normal, sem equivaler a perda zero de dados. Falha de execução, cópia incompleta ou inconsistência deve ser investigada e corrigida, sem apresentar o ponto como saudável sem validação. Um objetivo específico de perda admissível de dados (RPO) ou prazo de recuperação (RTO) exige contratação expressa.

3. Separação e proteção das cópias

Os pontos incluídos ficam em infraestrutura separada do ambiente principal de hospedagem. Separação não deve ser confundida com manter uma pasta de backup no mesmo disco do site. O acesso às cópias deve se limitar a pessoas e sistemas autorizados, com credenciais protegidas e rastreabilidade das ações administrativas.

A separação reduz exposição a falhas do ambiente principal, mas não elimina todos os riscos ou substitui uma cópia independente do cliente. Não se presume redundância geográfica, imutabilidade, retenção permanente ou certificação específica sem que isso esteja expressamente descrito no produto.

4. Solicitar e autorizar restauração

Use o atendimento autenticado e informe serviço, dados afetados, ponto desejado, motivo e se houve alterações depois desse ponto. A Zovvi deve confirmar o escopo antes de sobrescrever conteúdo: arquivos, banco e mensagens podem ter horários diferentes e precisam de avaliação conjunta. Quem solicita deve ter autorização sobre os dados e a conta.

Restaurar pode substituir alterações posteriores. Quando viável, preserve uma cópia do estado atual e teste em ambiente separado antes do corte. Restauração do escopo incluído pode ser solicitada sem uma taxa oculta; serviços extraordinários fora do produto dependem de orçamento e aceite prévios. O prazo é informado conforme volume e complexidade, sem prometer recuperação instantânea.

5. Integridade e colaboração do cliente

Mantenha cópias próprias fora da hospedagem e das credenciais de acesso principais, especialmente antes de atualizações, importações ou exclusões. Teste a abertura de arquivos e a restauração dos bancos; ter um arquivo de backup não prova que ele está íntegro. Dados criptografados pelo cliente dependem de suas chaves, que não devem ser enviadas por formulário público.

Uma cópia pode preservar um erro, arquivo corrompido ou malware já existente. Recuperar um ponto não equivale a auditar ou limpar toda a aplicação. As responsabilidades são apuradas pela causa e obrigações de cada parte; recomendar cópias próprias não exclui a responsabilidade da Zovvi pela rotina que contratou fornecer.

6. Suspensão, encerramento e eliminação

Suspender o acesso não é o mesmo que excluir conteúdo. Enquanto os dados forem conservados no ciclo de inadimplência, a cobertura e eventuais restrições técnicas devem ser tratadas com o

cliente. Antes do encerramento, solicite exportação e confirme o que será eliminado. Não conte com uma cópia que já saiu da rotação.

Após a exclusão do ambiente principal, pontos residuais podem permanecer isolados até completar sua rotação de sete dias, sem uso para nova prestação e sujeitos a restrições legais de preservação. A existência residual não garante reativação. Pedido de pagamento depois da eliminação não reconstrói dados. Ordens válidas ou obrigações específicas podem exigir conservação separada e acesso restrito.

7. Retenção legal não é arquivo do site

Documentos fiscais, prova da contratação, registros de segurança e registros de acesso sujeitos a guarda legal têm finalidades e prazos próprios, conforme a Política de Privacidade e a legislação aplicável. Guardar esses registros não significa manter por igual prazo os arquivos, o banco ou as mensagens do cliente.

A rotina de backup não é serviço de arquivo histórico permanente, descoberta jurídica ou recuperação forense. Pedidos de dados pessoais e preservação por autoridade seguem verificação de legitimidade, minimização e canal adequado. Alterações relevantes de cobertura, frequência ou retenção devem ser informadas sem reduzir retroativamente o serviço contratado.

