

Self-hosting como prática profissional

Um servidor não é nada mais do que um computador. A pergunta não é se deve ter um, mas onde vivem os dados dos seus clientes, quem os sustenta e quem assume a responsabilidade quando algo falha.

Para nos entendermos: Os seus dados vivem sempre no computador de alguém: no d'um gigante ao qual confia tudo, num alugado que gere, ou no seu próprio. Quanto mais controlo quer, mais responsabilidade assume. Delegar num terceiro grande tranquiliza, mas não isenta: a informação é sua —e a dos seus clientes—, e o responsável é você.

A pergunta entre a nuvem e a cave

Convém começar por desmistificar uma palavra que assusta sem motivo: servidor. Um servidor não é uma máquina misteriosa numa sala refrigerada. É, simplesmente, o computador de outra pessoa —ou o seu— que guarda informação e a entrega a quem a pede. Durante décadas, guardámos os dados dos nossos clientes numa pasta, num arquivo, em cima da secretária do escritório, e ninguém perdia o sono por isso. A informação não metia medo por estar em papel; também não tem de meter por estar num disco.

A «nuvem» também não é etérea. É o computador de uma empresa, quase sempre longe e quase sempre de outro. Aprendi isso sem querer no dia em que, confiante de que os meus ficheiros estavam seguros no Google Drive, descobri que a pasta do meu computador não continha os meus documentos, mas sim atalhos para documentos que viviam noutra local. Se esse outro local decidisse fechar, mudar de preço ou cancelar o serviço, a minha tranquilidade iria com ele. Não possuía as minhas coisas; tinha permissão para aceder a elas.

Daí nasce a pergunta deste Caderno, mais simples de enunciar do que de responder: onde deveriam viver os dados dos seus clientes? E os seus próprios? A conversa pública coloca-a como se houvesse apenas duas respostas opostas — a nuvem das grandes plataformas ou montar tudo sozinho —, quase uma questão de campo. Mas não são dois caminhos: são três, e nenhum é um ato de fé. Lidados com calma, têm mais nuances e exigem mais do que parece.

Isto diz-lhe respeito, venda o que vender

É fácil pensar que a confidencialidade é coisa de advogados, médicos ou jornalistas, e que os restantes não têm nada a esconder. É um erro, e dos caros. Quase qualquer negócio guarda dados dos seus clientes sujeitos à lei, e muitos guardam, sem saberem, informação bastante mais sensível do que parece.

Uma loja de sofás anota o nome, a morada e o telefone de quem compra; se houver financiamento, também os seus dados económicos. Uma empresa de remodelações ou de decoração guarda fotos do interior das casas dos seus clientes e as plantas completas das suas habitações. Uma empresa de limpeza maneja as plantas dos escritórios que limpa, muitas vezes marcadas com cores e números que indicam que funcionário entra onde, a que hora e com que chave. Nada disso parece grande coisa até nos perguntarmos para quem mais teria valor: essas plantas de limpeza são, vistas com outros olhos, o mapa perfeito para quem quiser entrar para roubar.

O facto d'um negócio ser pequeno, ou de vender sofás em vez de defender pleitos, não faz com que os seus dados careçam de valor nem que a lei deixe de lhe ser aplicada. Apenas faz com que o seu dono tenda a pensar menos nisso. E pensar pouco em algo que é da sua responsabilidade é, precisamente, onde começam os problemas.

Onde vivem os seus dados?

A essa pergunta há, em essência, três respostas. E convém recordar que «os dados» não são apenas o dossiê de um cliente ou o bloco de faturas e orçamentos: são também as suas conversas com ele — por WhatsApp, por um serviço de chat profissional, por Solo2. As três respostas que se seguem não são graus de pureza nem uma escada dos bons aos maus: são três maneiras de repartir a mesma coisa, o controlo e a responsabilidade.

Delegar tudo a um fornecedor. É o mais comum, e para a maioria é a única coisa que conhece. Ponho tudo no Google Workspace ou no Microsoft 365 e confio-o inteiramente ao fornecedor. Pago a minha quota e deixo de pensar nisso. A forma mais extrema disto são os serviços onde nem sequer chega a ter os seus dados: certos programas de faturação na nuvem, por exemplo, guardam-lhe as faturas e os orçamentos — e funcionam muito bem —, mas a informação vive no sistema deles, não no seu. Enquanto paga, acede; no dia em que sai, descobre que levar consigo o seu próprio histórico é difícil ou impossível. Manter os seus dados meio reféns é, para mais de um fornecedor, justamente o que o impede de mudar para a concorrência. Em troca de comodidade entrego o controlo e — sem o dizer em voz alta — a sensação de que a responsabilidade já não é minha. Aqui cabe uma nuance que quase nunca se faz: delegar não é sinónimo de americano. Posso delegar tudo de forma igualmente cómoda a um fornecedor europeu — Infomaniak, por exemplo — e resolver de uma só vez boa parte das dúvidas sobre transferências internacionais que vimos em «Schrems II», sem auto-hospedar nada. Não são os Estados Unidos contra o resto do universo: dentro da pura delegação já há decisões que importam.

Alugar e gerir o seu próprio servidor. Tenho o mesmo que a Microsoft ou a Google me dariam, mas sou eu que o instalo. Alugo um servidor num fornecedor europeu —Hetzner, OVH, Scaleway—, instalo software livre (Nextcloud para os ficheiros, por exemplo) e administro eu o resultado. Ganho controlo real: sei o que está a correr, onde e porquê. Mas a máquina continua a estar no centro de dados de um terceiro e, acima de tudo, muda quem assume as consequências. Ao delegar, si algo falhar, tem a quem culpar. Ao geri-lo você mesmo, o mais provável é que a culpa seja sua.

Tê-lo no seu próprio computador. Esta é a opção que quase ninguém conta, e é o coração deste Caderno. Não precisa de um servidor enorme ligado vinte e quatro horas por dia dentro de um macro centro de dados para alojar as suas coisas. O computador do seu escritório já é um servidor: ele serve-o a si. Deixa-o ligado no escritório e liga-se a ele a partir do portátil em casa de um cliente, ou do telemóvel quando está em casa. Chamamos-lhe «computador do escritório», não «servidor», mas faz exatamente o mesmo que as duas opções anteriores. O controlo é máximo, tal como a proximidade: os seus dados estão onde você está. A contrapartida, dita sem adornos, é que a responsabilidade também é máxima. Se a luz faltar, não há um técnico de prevenção em Nuremberga: cabe-lhe a si ligar o disjuntor. E para que esse computador esteja acessível de fora, é necessário algo que lance a ponte entre o seu portátil e ele. No é magia, e convém sabê-lo antes de escolher este caminho.

E nem sequer é preciso reaproveitar o computador do escritório: existe um aparelho pensado justamente para isto, o NAS (fabricado pela Synology, QNAP e outros). Como quase tudo o que vimos nestes Cuadernos, por dentro não há magia: é um computador especializado, o mesmo tipo de máquina que alugaria num centro de dados, só que pensado para guardar dados e servi-los pela rede, sem monitor nem teclado pelo meio. Liga-lhe um ecrã e um teclado e tens um computador comum; instala o software adequado no teu PC e tens um NAS. A diferença é que o NAS já vem pronto a usar. Compra-lo, ligas em casa ou no escritório, e é teu. Não pagas uma mensalidade; pagas uma vez e pertence-te, como qualquer ferramenta do teu negócio. Ligas, desligas, levas para outro lugar se quiseres. E como é teu, nada impede ter dois —um em casa, outro no escritório— ou três, acrescentando um num local seguro, sincronizados entre si: a tua própria redundância, sem depender de que um terceiro a mantenha. O auto-alojamento, no fim, não é uma só coisa: é uma combinação de máquinas, de propriedade, de localizações e de software.

Aqui é inevitável nomear o que fazemos, e fazemo-lo sem disfarce: na Solo2 essa ponte é a própria aplicação que a estende. O computador do seu escritório fica acessível apenas aos seus dispositivos de confiança, e sempre sob cifragem, e os seus restantes aparelhos voltam a ligar-se a ele sozinhos. Quando um cliente fala consigo, é o seu computador — não o de um terceiro — que fala com o cliente. Não resolvemos o corte de luz; resolvemos a ponte. E não somos os únicos: para quase cada necessidade existem hoje programas — livres ou proprietários — que permitem justamente isto, ter os dados no seu equipamento e chegar a eles a partir de fora. O nosso é um exemplo; o importante é a ideia, não a marca.

A redundância não é um superpoder

Aqui surge a objeção imediata, e é razoável: si tenho tudo no computador do meu escritório, o que acontece si ele se avariar? A pergunta é boa. A resposta é que a rede de segurança que imaginamos nos grandes fornecedores é mais modesta —e mais imitável— do que parece.

Quando deixo os meus dados no centro de dados d'uma multinacional, confio que ela tenha cópias em vários locais. E provavelmente as tem: num segundo local, talvez num terceiro. Mas essa redundância não é infinita e, acima de tudo, não é minha: continua a ser um disco rígido do qual não sou o dono, gerido por alguém em quem deposito uma fé que quase nunca verifico.

Essa mesma rede posso tecê-la eu, e com uma vantagem decisiva. O meu serviço diário vive no computador do escritório. De lá guardo uma cópia encriptada no computador de uma empresa amiga —um colega de profissão, uma outra escritório de confiança— e outra cópia encriptada, se quiser, nesse mesmo fornecedor europeu de que falávamos. A diferença é tudo: o que deixo fora não é o meu serviço nem os meus dados em claro, mas uma cópia encriptada que só eu posso abrir. O fornecedor externo guarda um cofre fechado do qual não tem a chave. Não lhe confio a minha informação: confio-lhe alguns bytes que, sem mim, não significam nada.

Estava seguro até que deixou de o estar

Permita-me uma história pessoal, porque ilustra isto melhor do que qualquer argumento. Durante mais de dez anos, fui cliente fiel da CrashPlan, um serviço de cópias de segurança tecnicamente extraordinário. Fazia cópias de segurança na sua nuvem de todos os meus computadores e dos da minha família —os da empresa e os de casa, tudo—, com versões que podia recuperar com a frequência que quisesse, viajando no tempo até um ficheiro específico de há meses. Após a primeira cópia, transmitia apenas as diferenças, encriptadas e comprimidas, de forma a manter atualizada uma cópia de segurança enorme com quase nenhum esforço. Salvou-me muitas vezes, de um documento banal a um disco inteiro. O preço foi subindo com os anos e eu não me importava: pagava com satisfação.

O que eu não sabia é que CrashPlan tinha cometido um erro de cálculo: tinha prometido por contrato armazenamento ilimitado, em espaço e em tempo. E o espaço multiplicado pelo tempo —anos de história, versões a cada poucos minutos— cresce até se tornar insustentável. Um dia comunicaram-nos a todos que o serviço terminava. Fizeram-no com elegância e com um prazo generoso, quase um ano, e deram-nos meios para descarregar o que era nosso. Mas para onde vai uma pessoa com mais de dez anos de cópias com versões de todos os seus discos? Aí descobre-se que não se tem nem como descarregar tudo nem onde o pôr, e que, mesmo podendo, o novo armazém custaria uma fortuna.

Salvei quatro coisas imprescindíveis. O resto foi-se quando desligaram o interruptor. Eu estava tranquilo, a minha informação estava a salvo... até que deixou de estar. E não por uma traição: o CrashPlan portou-se de forma impecável — ao contrário do Evernote, que anos depois se portou de forma vergonhosa —; simplesmente, o meu anjo da guarda na nuvem decidiu, com todo o direito, deixar de o ser. O resultado, para mim, foi idêntico: o que julgava seguro desapareceu.

O que esta história realmente ensina tem mais a ver com a natureza humana do que com a tecnologia. Quando uma pessoa sente que algo é da sua responsabilidade, age de forma preventiva: faz cópias, protege as costas,

desconfia com bom critério. Quando acredita —erradamente— que a responsabilidade é de um terceiro grande e solvente, relaxa e deixa andar. Essa tranquilidade delegada não é prudência: é, sem maquiagem, uma forma de irresponsabilidade.

Pagar não é o mesmo que cumprir

Essa irresponsabilidade tranquila assemelha-se muito à de uns pais que matriculam o filho na escola mais cara, pagam-lhe depois um mestrado, e com isso acreditam ter cumprido o seu dever. Não cumpriram. Ser pai é preocupar-se com o que ele aprendeu hoje, com o que não entende, com os seus valores, com a sua autoconfiança. Se aos vinte e cinco anos esse filho não sabe trabalhar nem comportar-se, a culpa não é da escola que cobrou: é de quem delegou e pagou acreditando que isso bastava. Pagar a um terceiro não isenta de responsabilidade. Nunca o fez.

Com os dados passa-se o mesmo, e a história recente confirma-o. Há cinquenta ou cem anos um profissional guardava as coisas dos seus clientes em pastas, no seu gabinete ou em sua casa, e sentia-se responsável por elas. Raramente se perdia algo. Passámos para o mundo digital e, com uma facilidade espantosa, carregamos tudo para «a nuvem» — que não é mais do que o computador de uma multinacional — e deixamos de nos preocupar. E com frequência há acidentes, e há empresas que perdem tudo, e então diz-se: a culpa foi do Google, a culpa foi da Microsoft. Não. A informação é sua, ou dos seus clientes, mas o responsável é você.

Alojar os seus dados não é um capricho técnico: é recuperar essa serenidade de há décadas, a de saber onde está cada coisa e porquê. A proteção de dados, entretanto, viveu um pêndulo brusco —de não haver norma nenhuma, quando qualquer pessoa exibia os dados d'un cliente sem pensar, a uma exigência que recai com dureza desproporcionada sobre o mais pequeno, o trabalhador independente que dá o telefone d'un cliente ao estafeta. Não discuto o fim; observo o desajuste. Mas o desajuste não nos absolve: no dia em que a administração tiver meios para rastrear e sancionar em escala, o tamanho deixará de proteger ninguém, e convém não esperar por esse dia com a casa por arrumar. Ter o dado sob controlo próprio ajuda a cumprir e ajuda a prová-lo. E, acima de tudo, devolve as coisas ao seu lugar: quando a informação é sua, a responsabilidade é inteiramente sua —não há um terceiro a quem culpar, nem um terceiro cujo falha o exponha—.

A responsabilidade também protege

Seria desonesto pintar isto sem sombras. Ocupar o lugar do intermediário significa carregar com o que lhe é próprio: manter as cópias atualizadas, aplicar as atualizações e uma responsabilidade legal — a do RGPD — que, na realidade, nunca deixou de ser totalmente sua (as referências em rodapé detalham os artigos). Há trabalho, e há um dia em que algo falha a desoras. Não o escondemos.

Mas o medo que rodeia essa palavra, responsabilidade, está mal calibrado. É muito mais fácil perder os seus ficheiros num serviço da nuvem que fecha, ou as suas fotos no Google Photos, do que perder aquela pasta de documentos importantes que tem no seu próprio computador: aquela que sabe onde está e cuja falta notaria assim que desaparecesse. O que sente como seu, cuida; o que crê a salvo nas mãos de outro, descara.

Pense nos álbuns de fotos de antigamente, os de papel revelado guardados numa gaveta. Já ouviu alguma vez alguém dizer que «perdeu» o seu álbum de família? Ouve-se falar da casa que ardeu com o álbum lá dentro; perdê-lo sem mais, não. E em contrapartida, gente que tinha todas as suas fotos no Google Photos ou no Apple Fotos e ficou sem nada: essa história volta de poucos em poucos meses, porque acreditavam que estava a salvo. O Google Photos cuida das suas fotos, claro que sim; mas não as cuida como uns pais cuidam do álbum onde estão os seus filhos e os seus netos. Essa diferença não a resolve nenhum centro de dados: a responsabilidade, quando é sua, não é só um fardo; é também a melhor garantia.

Quatro perguntas antes de decidir

Se equaciona dar o passo, em qualquer das suas formas, convém responder antes a quatro perguntas com desapaixonada honestidade:

1. Que parte dos seus dados lhe doeria perder, ou não poder levar consigo? E cuidado com descartar o «rotineiro»: o histórico de faturas parece a coisa mais prosaica do mundo até mudar de programa e descobrir que essas faturas eram do fornecedor, não suas — que, quando muito, as pode imprimir em PDF, sem já poder pesquisar dentro delas. Não é só uma questão de sensibilidade: é de a quem pertence verdadeiramente aquilo que precisa de conservar.
2. Que opção é proporcional à sua capacidade técnica real? Um computador próprio bem cuidado está ao alcance de qualquer um; administrar um servidor inteiro, nem tanto. Seja honesto sobre o que sabe e o que não sabe. E lembre-se de que entre montar um servidor inteiro e delegar tudo há um terreno intermédio muito razoável: programas — livres ou proprietários — que guardam os seus dados no seu próprio equipamento e o deixam chegar a eles a partir de fora. Para muita gente é o melhor equilíbrio.
3. Que plano tem para o pior dia? Uma brecha, um disco que morre, um fornecedor que fecha, o técnico de baixa. Se o plano começa por «não deveria acontecer», não é um plano.
4. Saberá demonstrar que cumpre se amanhã for inspeccionado? Fazer bem e poder provar que o faz bem não são o mesmo. A lei pede o segundo.

Não existe resposta universal. Existe uma resposta proporcional, assumida com honestidade sobre o que se ganha e o que se herda. E, acima de toda a técnica, uma certeza simples: os seus dados vivem no computador de alguém. A única pergunta que de facto importa é de quem quer que seja esse computador.

O auto-alojamento não é nem virtude nem vício: é uma ferramenta com uma marca concreta de capacidades e responsabilidades. A pergunta nunca foi se deveria alojar o que é seu, mas sim o quê, como e com que rede de apoio. Recuperar o controlo dos dados não é voltar à cave nem desconfiar de tudo: é voltar a sentir-se responsável pelo que é nosso, como quando isso vivia numa pasta em cima da secretária. Essa responsabilidade, bem entendida, é o verdadeiro serviço que um profissional presta aos seus clientes.

Fontes e leitura adicional

- Regulamento (UE) 2016/679 — artigo 28º (subcontratante), artigo 32º (segurança do tratamento), artigo 33º (notificação de brechas), artigo 37º (designação do Encarregado de Proteção de Dados).
- Agência Espanhola de Proteção de Dados — *Guia práctico para a análise de riscos no tratamento de datos pessoais* (revisão vigente). Quadro para responsáveis pelo tratamento que assumem funções técnicas próprias.
- Comité Europeu para a Proteção de Dados — *Guidelines 1/2024 on processing of personal data based on legitimate interests*. Aplicável também ao exame de proporcionalidade em decisões de infraestrutura própria.
- Comissão Europeia — diretório público de fornecedores de serviços da informação estabelecidos em jurisdição europeia. Ponto de partida administrativo para identificar opções de hosting gerido europeu.
- Nextcloud GmbH (Alemanha) — *Nextcloud Enterprise architecture and compliance documentation*. Caso documentado de software livre con modalidades auto-alojada e gerida por fornecedor europeu; útil como referência técnica d'um projeto mantido em jurisdição europeia desde 2016.

[← AnteriorAs 24 palavras: o que é uma identidade criptográfica](#)[Seguinte → Privacidade real vs aparente: as perguntas que convém fazer-se](#)

Leituras recentes

- [Reflexão · 29 de junho de 2026 Não és anónimo](#)
- [Reflexão · 27 de maio de 2026 Lo que una firma no puede arreglar](#)
- [Análise · 26 de maio de 2026 Privacidade real vs aparente: as perguntas que convém fazer-se](#)

Leve este artigo para onde precisar.

[↓ Markdown](#) [↓ Texto simples](#) [↓ PDF](#)

O arquivo é descarregado no seu dispositivo. A partir daí, pode guardá-lo, importá-lo no Solo2 ou partilhá-lo onde quiser. Cuadernos não decide o destino por si.

Selo de lacre · SHA-256 a11954d9369f8d54cb5a425340a8794e31c91bdf939ef12a26702ec21196a620

[Funcionalidades](#) [Novidades](#) [Blog](#) [Ajuda](#) [Sobre](#) [Contacto](#)
[Transparência](#) [Verificação](#) [Privacidade](#) [Condições](#) [Cookies](#)

Cuadernos Lacre · Uma publicação da [Menzuri Gestión S.L.](#) ·
escrita por R.Eugenio · editada pela equipa do [Solo2](#).

Este site não utiliza cookies. Tudo o que o seu navegador carrega é escrito ou supervisionado por nós e hospedado em nossos servidores europeus: o contador de visitas anônimo (Umami, auto-hospedado) e o mínimo de JavaScript necessário para o seletor de idioma e a sua preferência de tema claro/escuro, que é guardada no seu próprio dispositivo. Sem recursos de terceiros, sem rastreadores, sem criação de perfis, sem compartilhamento de dados. Se quiser nos seguir: [RSS](#).