Análise · 25 de maio de 2026

← Anterior·Seguinte →

Self-hosting como práctica profesional

Un servidor non é máis ca un ordenador. A pregunta non é se ter un, senón onde viven os datos dos teus clientes, quen os sostén e quen carga coa responsabilidade cando algo falla.

Para entendernos: Os teus datos viven sempre no ordenador de alguén: no dun xigante ao que llo confías todo, nun alugado que xestionas ti, ou no teu propio. Canto máis control queiras, máis responsabilidade asumes. Delegar nun terceiro grande tranquiliza, pero non exime: a información é túa —e a dos teus clientes—, e o responsable es ti.

A pregunta entre a nube e o soto

Convén empezar desactivando unha palabra que asusta sen motivo: servidor. Un servidor non é unha máquina misteriosa nunha sala refrixerada. É, sinxelamente, o ordenador doutra persoa —ou o teu— que garda información e lla entrega a quen a pide. Durante décadas gardamos o dos nosos clientes nunha carpeta, nun arquivador, sobre a mesa do despacho, e a ninguén lle quitaba o sono. A información non daba medo por estar nun papel; tampouco ten por que dalo por estar nun disco.

«A nube» tampouco é etérea. É o ordenador dunha empresa, case sempre lonxe e case sempre doutro. Aprendino sen querer o día en que, confiado en que os meus ficheiros estaban a bo recado en Google Drive, descubrín que a carpeta do meu ordenador non contiña os meus documentos, senón atallos a documentos que vivían noutro sitio. Se ese outro sitio decidise pechar, cambiar de prezo ou darse de baixa, a miña tranquilidade iríase con el. Non tiña as miñas cousas: tiña permiso para acceder a elas.

De aí nace a pregunta deste Caderno, máis sinxela de enunciar que de responder: onde deberían vivir os datos dos teus clientes? E os teus propios? A conversa pública plantéaa como se só houbese dúas respostas enfrontadas —a nube das grandes plataformas o montárselo un mesmo—, case unha cuestión de bando. Pero non son dous camiños: son tres, e ningún é un acto de fe. Lidos despacio, teñen máis matices e piden máis do que parece.

Esto vai contigo, vendas o que vendas

É fácil pensar que a confidencialidade é cousa de avogados, médicos ou xornalistas, e que o resto non teñen nada que esconder. É un erro, e dos caros. Case calquera negocio garda datos dos seus clientes suxeitos á lei, e moitos gardan, sen sabelo, información bastante máis sensible do que parece.

Unha tenda de sofás anota o nome, a dirección e o teléfono de quen compra; se hai financiamento, tamén os seus datos económicos. Unha empresa de reformas ou de decoración conserva fotos do interior das casas dos seus clientes e os planos completos das súas vivendas. Unha empresa de limpeza manexa os planos das oficinas que limpa, a miúdo marcados con cores e números que indican que empregado entra onde, a que hora e con que chave. Nada diso parece gran cousa ata que un se pregunta para quen máis tería valor: eses planos de limpeza son, vistos con outros ollos, o mapa perfecto para quen queira entrar a roubar.

Que un negocio sexa pequeno, ou que venda sofás en lugar de defender preitos, non fai que os seus datos carezan de valor nin que a lei deixe de aplicarlle. Só fai que o seu dono adoite pensar menos niso. E pensar pouco en algo

que é responsabilidade túa é, precisamente, onde empezan os problemas.

Onde viven os teus datos?

A esa pregunta hai, en esencia, tres respostas. E convén lembrar que «os datos» non son só o dossier dun cliente ou o bloque de facturas e orzamentos: tamén o son as túas conversacións con el —por WhatsApp, por un servizo de chat profesional, por Solo2—. As tres respostas que seguen non son graos de pureza nin unha escaleira de bos a malos: son tres maneiras de repartir o mesmo, o control e a responsabilidade.

Delegalo todo a un provedor. É o máis común, e para a maioría é o único que coñece. Poño todo en Google Workspace ou en Microsoft 365 e confíollo enteiro ao provedor. Pago a miña cota e deixo de pensar niso. A forma máis extrema disto son os servizos onde nin sequera chegas a ter os teus datos: certos programas de facturación na nube, por exemplo, gárdanche as facturas e os orzamentos —e funcionan moi ben—, pero a información vive no seu sistema, non no teu. Mentres pagas, accedes; o día que te vas, descubres que levarte o teu propio histórico é difícil ou imposible. Ter os teus datos medio refén é, para máis dun provedor, xusto o que impide que te marches á competencia. A cambio de comodidade entrego o control e —sen dicilo en voz alta— a sensación de que a responsabilidade xa non é miña. Aquí cabe un matiz que case nunca se fai: delegar non é sinónimo de americano. Podo delegalo todo igual de comodamente nun provedor europeo —Infomaniak, por exemplo— e resolver dun plumazo boa parte das dúbidas sobre transferencias internacionais que vimos en «Schrems II», sen autohospedar nada. Non é Estados Unidos contra o resto do universo: dentro da pura delegación xa hai decisións que importan.

Alugar e xestionar o teu propio servidor. Teño o mesmo que me daría Microsoft ou Google, pero móntoo eu. Alugo un servidor nun provedor europeo —Hetzner, OVH, Scaleway—, instalo software libre (Nextcloud para os ficheiros, por exemplo) e administro eu o resultado. Gaño control de verdade: sei que corre, onde e por que. Pero a máquina segue estando no centro de datos dun terceiro e, sobre todo, cambia quen carga o morto. Deleyando, se algo falla, teño a quen culpar. Xestionándoo eu, o máis probable é que a culpa sexa miña.

Telo no teu propio ordenador. Este é o que case ninguén conta, e é o corazón deste Caderno. Non fai falta un servidor enorme acendido as vinte e catro horas dentro dun macrocentro de datos para hospedar o teu. O ordenador da túa oficina xa é un servidor: sérvete a ti. Déixalo acendido no despacho e conéctaste a el desde o portátil na casa dun cliente, ou desde o móbil cando estás na casa. Chamámolo «o ordenador da oficina», non «o servidor», pero fai exactamente o mesmo que as dúas opcións anteriores. O control é máximo e a proximidade tamén: os teus datos están onde estás ti. A contrapartida, dita sen adornos, é que a responsabilidade tamén é máxima. Se vai a luz non hai un técnico de garda en Núremberg: tócache a ti subir o diferencial. E para que ese ordenador sexa accesible desde fóra fai falta algo que tenda a ponte entre o teu portátil e el. Non é maxia, e convén sabelo antes de elixir este camiño.

E nin sequera fai falta reaproveitar o ordenador da oficina: existe un aparello pensado xustamente para isto, o NAS (fabrícanos Synology, QNAP e outros). Como case todo o que vimos nestes Cuadernos, por dentro non hai maxia: é un ordenador especializado, o mesmo tipo de máquina que alugarías nun centro de datos, só que pensado para gardar datos e servilos pola rede, sen monitor nin teclado polo medio. Conéctalle unha pantalla e un teclado e tes un ordenador corrente; instala o software axeitado no teu PC e tes un NAS. A diferenza é que o NAS xa vén listo para usar. Mércalo, enchúfalo na casa ou no despacho, e é teu. Non pagas unha cota cada mes; págalo unha vez e perténceche, como calquera ferramenta do teu negocio. Acéndelo, apágalo, lévalo a outro sitio se queres. E como é teu, nada impide ter dous —un na casa, outro na oficina— ou tres, engadindo un nun lugar seguro, sincronizados entre si: a túa propia redundancia, sen depender de que un terceiro a manteña. O auto-aloxamento, ao final, non é unha soa cousa: é unha combinación de máquinas, de propiedade, de localizacións e de software.

Aquí é inevitable nomear o que facemos, e facémolo sen disfraz: en Solo2 esa ponte téndea a propia aplicación. O ordenador da túa oficina queda accesible só para os teus dispositivos de confianza, e sempre baixo cifrado, e os teus demais aparellos reconéctanse a el sós. Cando un cliente fala contigo, é o teu ordenador —non o dun terceiro— o que fala co cliente. Non resolvemos o corte de luz; resolvemos a ponte. E non somos os únicos: para

case cada necesidade existen hoxe programas —libres ou propietarios— que permiten xusto isto, ter os datos no teu equipo e chegar a eles desde fóra. O noso é un exemplo; o importante é a idea, non a marca.

A redundancia non é un superpoder

Aquí xorde a obxección inmediata, e é razoable: se o teño todo no ordenador da miña oficina, que pasa se rompe? A pregunta é boa. A resposta é que a rede de seguridade que imaxinamos nos grandes provedores é máis modesta —e máis imitable— do que parece.

Cando deixo os meus datos no centro de datos dunha multinacional, confío en que teña copias en varios sitios. E probablemente as teña: nun segundo emprazamento, quizais nun terceiro. Pero esa redundancia non é infinita e, sobre todo, non é miña: segue sendo un disco duro do que non son o dono, xestionado por alguén en quen deposito unha fe que case nunca verifico.

Esa mesma rede pódoa tecer eu, e cunha vantaxe decisiva. O meu servizo diario vive no ordenador da oficina. De aí gardo unha copia cifrada no ordenador dunha empresa amiga —un compañeiro de profesión, outra oficina de confianza— e outra copia cifrada, se quero, nese mesmo provedor europeo do que falabamos. A diferenza é todo: o que deixo fóra non é o meu servizo nin os meus datos en claro, senón unha copia cifrada que só eu podo abrir. O provedor externo garda un cofre pechado de cuxa chave non dispón. Non lle confío a miña información: confíolle uns bytes que, sen min, non significan nada.

Estaba a salvo ata que deixou de estalo

Permíteme unha historia propia, porque ilustra esto mellor que calquera argumento. Durante máis de dez anos fun cliente devoto de CrashPlan, un servizo de copias de seguridade tecnicamente extraordinario. Respaldaba na súa nube todos os meus ordenadores e os da miña familia —os da empresa e os de casa, todo—, con versións que podía recuperar á frecuencia que quixese, viaxando cara atrás no tempo ata un ficheiro concreto de facía meses. Tras a primeira copia só transmitía as diferenzas, cifradas e comprimidas, de modo que mantiña ao día un respaldo enorme sen apenas esforzo. Salvoume moitas veces, desde un documento parvo ata un disco enteiro. O prezo foi subindo cos anos e dábame igual: pagaba feliz.

O que eu non sabía é que CrashPlan cometera un erro de cálculo: prometeran por contrato almacenamento ilimitado, en espazo e en tempo. E o espazo multiplicado polo tempo —anos de historia, versións cada poucos minutos— crece ata volverse insostible. Un día comunicáronnos a todos que o servizo terminaba. Fixérono con elegancia e cun prazo xeneroso, case un ano, e déronnos medios para descargar o noso. Pero a onde vai un con máis de dez anos de copias versionadas de todos os seus discos? Aí descobres que non tes nin como baixalo todo nin onde metelo, e que, aínda podendo, o novo almacén custaría unha fortuna.

Salvei catro cousas imprescindibles. O resto foise cando apagaron o interruptor. Eu estaba tranquilo, a miña información estaba a salvo... ata que deixou de estalo. E non por unha traizón: CrashPlan portouse de forma impecable —ao contrario que Evernote, que anos despois portouse de forma vergonzosa—; sinxelamente, o meu anxo da garda na nube decidiu, con todo o dereito, deixar de selo. O resultado, para min, foi idéntico: o que cría seguro, desapareceu.

O que de verdade ensina esta historia ten máis de natureza humana que de tecnoloxía. Cando un sente que algo é responsabilidade súa, actúa de forma preventiva: fai copias, cóbrese as costas, desconfía con bo criterio. Cando cre —equivocadamente— que a responsabilidade a sostén un terceiro grande e solvente, reláxase e deixa facer. Esa tranquilidade delegada non é prudencia: é, sen maquillaxe, unha forma de irresponsabilidade.

Pagar non é o mesmo que cumprir

Esa irresponsabilidade tranquila parécese moito á duns pais que matriculan ao seu fillo no colexio máis caro, páganlle despois un máster, e con eso cren ter cumprido. Non cumpriron. Ser pai é preocuparse de que aprendeu hoxe, do que non entende, dos seus valores, da súa seguridade en si mesmo. Se aos vinte e cinco anos ese fillo non sabe traballar nin comportarse, a culpa non é do colexio que cobrou: é de quen delegou e pagou crendo que con eso abondaba. Pagar a un terceiro non exime de responsabilidade. Nunca o fixo.

Cos datos pasa igual, e a historia recente confírmao. Hai cincuenta ou cen anos un profesional gardaba o dos seus clientes en carpetas, no seu despacho ou na súa casa, e sentíase responsable delas. Rara vez perdíase nada. Pasamos ao mundo dixital e, cunha facilidade pasmosa, subímolo todo a «a nube» —que non é máis que o ordenador dunha multinacional— e deixamos de preocuparnos. E con frecuencia hai accidentes, e hai empresas que o perden todo, e entón dise: a culpa foi de Google, la culpa foi de Microsoft. Non. A información é túa, ou a dos teus clientes, pero o responsable es ti.

Hospedar o teu non é un capricho técnico: é recuperar esa serenidade de facía décadas, a de saber onde está cada cousa e por que. A protección de datos, mentres tanto, viviu un péndulo brusco —de non haber norma ningunha, cando calquera exhibía os datos dun cliente sen pensalo, a unha esixencia que recae con dureza desproporcionada sobre o máis pequeno, o autónomo que pasa o teléfono dun cliente ao repartidor—. Non discuto o fin; observo o desajuste. Pero o desajuste non nos exime: o día en que a administración teña medios para rastrear e sancionar a escala, o tamaño deixará de protexer a ninguén, e convén non esperar a ese día coa casa sen ordenar. Ter o dato baixo control propio axuda a cumprir e axuda a demostralo. E, sobre todo, devolve as cousas ao seu sitio: cando a información é túa, a responsabilidade é enteiramente túa —non hai un terceiro a quen culpar, nin tampouco un terceiro cuxo fallo te expoña—.

A responsabilidade tamén protexe

Sería deshonesto pintar isto sen sombras. Ocupar o lugar do intermediario significa cargar co seu: manter copias ao día, aplicar actualizacións e unha responsabilidade legal —a do RGPD— que, en realidade, nunca deixou de ser do todo túa (as referencias ao pé detallan os artigos). Hai traballo, e hai un día en que algo falla a deshora. Non o escondemos.

Pero o medo que rodea a esa palabra, responsabilidade, está mal calibrado. É moito máis fácil perder os teus ficheiros nun servizo da nube que pecha, ou as túas fotos en Google Fotos, que perder esa carpeta de documentos importantes que tes no teu propio ordenador: a que sabes onde está e que notarías que falta en canto desaparecese. O que sentes teu, cóidalo; o que cres a salvo en mans de outro, descúidalo.

Pensa nos álbums de fotos de antes, os de papel revelado gardados nun caixón. Oiches algunha vez a alguén dicir que «perdeu» o seu álbum familiar? Óese o da casa que ardeu co álbum dentro; perdelo sen máis, non. E en cambio, xente que tiña todas as súas fotos en Google Fotos ou en Apple Fotos e quedou sen nada: esa historia volve cada poucos meses, porque crían que estaba a salvo. Google Fotos coida as túas fotos, claro que si; pero non as coida como uns pais coidan o álbum onde están os seus fillos e os seus netos. Esa diferenza non a arranxa ningún centro de datos: a responsabilidade, cando é túa, non es só unha carga; é tamén a mellor garantía.

Catro preguntas antes de decidir

Se te plantexas dar o paso, en calquera das súas formas, convén responder antes a catro preguntas con desapasionada honestidade:

1. Que parte dos teus datos che doería perder, ou non poder levarte? E coidado con descartar o «rutinario»: o histórico de facturas parece o máis prosaico do mundo ata que cambias de programa e descobres que esas facturas eran do provedor, non túas —que, como moito, pódelas imprimir en PDF, sen poder xa buscar dentro delas—. Non é só cuestión de sensibilidade: é de a quen pertence de verdade o que necesitas conservar.

2. Que opción é proporcional á túa capacidade técnica real? Un ordenador propio ben coidado está ao alcance de calquera; administrar un servidor enteiro, non tanto. Sé honesto sobre o que sabes e o que non. E lembra que entre montarte un servidor enteiro e delegalo todo hai un terreo intermedio moi razoable: programas —libres ou propietarios— que gardan os teus datos no teu propio equipo e déixante chegar a eles desde fóra. Para moita xente é o mellor equilibrio.
3. Que plano tes para o peor día? Unha brecha, un disco que morre, un provedor que pecha, o técnico de baixa. Se o plano empeza por «non debería pasar», non é un plano.
4. Saberías demostrar que cumpres se mañá te inspeccionan? Facelo ben e poder probar que o fas ben non son o mesmo. A lei pide o segundo.

Non hai resposta universal. Hai unha resposta proporcional, asumida con honestidade sobre o que se gaña e o que se hereda. E, por riba da técnica, unha certeza sinxela: os teus datos viven no ordenador de alguén. A única pregunta que de verdade importa é de quen queres que sexa ese ordenador.

O autohospedaxe non é nin virtude nin vicio: é unha ferramenta cunha pegada concreta de capacidades e de responsabilidades. A pregunta nunca foi se hospedar o teu, senón que, como e con que rede de apoio. Recuperar o control dos datos non é volver ao soto nin desconfiar de todo: é volver a sentirse responsable do que é noso, como cando aquello vivía nunha carpeta sobre a mesa. Esa responsabilidade, ben entendida, é o verdadeiro servizo que un profesional presta aos seus clientes.

Fontes e lectura adicional

- Regulamento (UE) 2016/679 — artigo 28 (encargado do tratamento), artigo 32 (seguridade do tratamento), artigo 33 (notificación de brechas), artigo 37 (designación do Delegado de Protección de Datos).
- Axencia Española de Protección de Datos — *Guía práctica para análise de riscos no tratamento de datos persoais* (revisión vixente). Marco para responsables do tratamento que asumen funcións técnicas propias.
- European Data Protection Board — *Guidelines 1/2024 on processing of personal data based on legitimate interests*. Aplicable tamén ao exame de proporcionalidade en decisións de infraestrutura propia.
- Comisión Europea — directorio público de provedores de servizos da información establecidos en xurisdición europea. Punto de partida administrativo para identificar opcións de hosting xestionado europeo.
- Nextcloud GmbH (Alemaña) — *Nextcloud Enterprise architecture and compliance documentation*. Caso documentado de software libre con modalidades autohospedada e xestionada por provedor europeo; útil como referencia técnica dun proxecto sostido en xurisdición europea desde 2016.

← AnteriorAs 24 palabras: que é unha identidade criptográficaSeguinte →Privacidade real vs aparente: as preguntas que convén facerse

Lecturas recentes

- Reflexión · 29 de xuño de 2026 Non es anónimo
- Reflexión · 27 de maio de 2026 O que unha firma non pode arranxar
- Análise · 26 de maio de 2026 Privacidade real vs aparente: as preguntas que convén facerse

Leva este artigo onde o necesites.

↓ Markdown ↓ Texto plano ↓ PDF

O arquivo descárgase no teu dispositivo. Desde aí podes gardalo, importalo a Solo2, o compartilo onde queiras. Cuadernos no decide o destino por ti.

Selo de lacre · SHA-256 10f721c2472907929aeb1966303c70eec2892dbf8b5ee4cb649407185c53dec4

Cuadernos Lacre · Unha publicación de Menzuri Gestión S.L. ·
escrita por R.Eugenio · editada polo equipo de Solo2.