Análisis · 25 de mayo de 2026

← Anterior·Siguiente →

Self-hosting como práctica profesional

Un servidor no es más que un ordenador. La pregunta no es si tener uno, sino dónde viven los datos de tus clientes, quién los sostiene y quién carga con la responsabilidad cuando algo falla.

Para entendernos: Tus datos viven siempre en el ordenador de alguien: en el de un gigante al que se lo confías todo, en uno alquilado que gestionas tú, o en el tuyo propio. Cuanto más control quieres, más responsabilidad asumes. Delegar en un tercero grande tranquiliza, pero no exime: la información es tuya —y la de tus clientes—, y el responsable eres tú.

La pregunta entre la nube y el sótano

Conviene empezar desactivando una palabra que asusta sin motivo: servidor. Un servidor no es una máquina misteriosa en una sala refrigerada. Es, sencillamente, el ordenador de otra persona —o el tuyo— que guarda información y se la entrega a quien la pide. Durante décadas guardamos lo de nuestros clientes en una carpeta, en un archivador, sobre la mesa del despacho, y a nadie le quitaba el sueño. La información no daba miedo por estar en un papel; tampoco tiene por qué darlo por estar en un disco.

«La nube» tampoco es etérea. Es el ordenador de una empresa, casi siempre lejos y casi siempre de otro. Lo aprendí sin querer el día en que, confiado en que mis archivos estaban a buen recaudo en Google Drive, descubrí que la carpeta de mi ordenador no contenía mis documentos, sino atajos a documentos que vivían en otro sitio. Si ese otro sitio decidía cerrar, cambiar de precio o darse de baja, mi tranquilidad se iría con él. No tenía mis cosas: tenía permiso para acceder a ellas.

De ahí nace la pregunta de este Cuaderno, más sencilla de enunciar que de responder: ¿dónde deberían vivir los datos de tus clientes? ¿Y los tuyos propios? La conversación pública la plantea como si solo hubiera dos respuestas enfrentadas —la nube de las grandes plataformas o montárselo uno mismo—, casi una cuestión de bando. Pero no son dos caminos: son tres, y ninguno es un acto de fe. Leídos despacio, tienen más matices y piden más de lo que parece.

Esto va contigo, vendas lo que vendas

Es fácil pensar que la confidencialidad es cosa de abogados, médicos o periodistas, y que el resto no tiene nada que esconder. Es un error, y de los caros. Casi cualquier negocio guarda datos de sus clientes sujetos a la ley, y muchos guardan, sin saberlo, información bastante más sensible de lo que parece.

Una tienda de sofás anota el nombre, la dirección y el teléfono de quien compra; si hay financiación, también sus datos económicos. Una empresa de reformas o de decoración conserva fotos del interior de las casas de sus clientes y los planos completos de sus viviendas. Una empresa de limpieza maneja los planos de las oficinas que limpia, a menudo marcados con colores y números que indican qué empleado entra dónde, a qué hora y con qué llave. Nada de eso parece gran cosa hasta que uno se pregunta para quién más tendría valor: esos planos de limpieza son, vistos con otros ojos, el mapa perfecto para quien quiera entrar a robar.

Que un negocio sea pequeño, o que venda sofás en lugar de defender pleitos, no hace que sus datos carezcan de valor ni que la ley deje de aplicarle. Solo hace que su dueño suela pensar menos en ello. Y pensar poco en algo que es responsabilidad tuya es, precisamente, donde empiezan los problemas.

¿Dónde viven tus datos?

A esa pregunta hay, en esencia, tres respuestas. Y conviene recordar que «los datos» no son solo el dossier de un cliente o el bloque de facturas y presupuestos: también lo son tus conversaciones con él —por WhatsApp, por un servicio de chat profesional, por Solo2—. Las tres respuestas que siguen no son grados de pureza ni una escalera de buenos a malos: son tres maneras de repartir lo mismo, el control y la responsabilidad.

Delegarlo todo a un proveedor. Es lo más común, y para la mayoría es lo único que conoce. Pongo todo en Google Workspace o en Microsoft 365 y se lo confío entero al proveedor. Pago mi cuota y dejo de pensar en ello. La forma más extrema de esto son los servicios donde ni siquiera llegas a tener tus datos: ciertos programas de facturación en la nube, por ejemplo, te guardan las facturas y los presupuestos —y funcionan muy bien—, pero la información vive en su sistema, no en el tuyo. Mientras pagas, accedes; el día que te vas, descubres que llevarte tu propio histórico es difícil o imposible. Tener tus datos medio rehén es, para más de un proveedor, justo lo que impide que te marches a la competencia. A cambio de comodidad entrego el control y —sin decirlo en voz alta— la sensación de que la responsabilidad ya no es mía. Aquí cabe un matiz que casi nunca se hace: delegar no es sinónimo de americano. Puedo delegarlo todo igual de cómodamente en un proveedor europeo —Infomaniak, por ejemplo— y resolver de un plumazo buena parte de las dudas sobre transferencias internacionales que vimos en «Schrems II», sin autohospedar nada. No es Estados Unidos contra el resto del universo: dentro de la pura delegación ya hay decisiones que importan.

Alquilar y gestionar tu propio servidor. Tengo lo mismo que me daría Microsoft o Google, pero me lo monto yo. Alquilo un servidor en un proveedor europeo —Hetzner, OVH, Scaleway—, instalo software libre (Nextcloud para los archivos, por ejemplo) y administro yo el resultado. Gano control de verdad: sé qué corre, dónde y por qué. Pero la máquina sigue estando en el centro de datos de un tercero y, sobre todo, cambia quién carga el muerto. Delegando, si algo falla, tengo a quién culpar. Gestionándolo yo, lo más probable es que la culpa sea mía.

Tenerlo en tu propio ordenador. Este es el que casi nadie cuenta, y es el corazón de este Cuaderno. No hace falta un servidor enorme encendido las veinticuatro horas dentro de un macrocentro de datos para hospedar lo tuyo. El ordenador de tu oficina ya es un servidor: te sirve a ti. Lo dejas encendido en el despacho y te conectas a él desde el portátil en casa de un cliente, o desde el móvil cuando estás en casa. Lo llamamos «el ordenador de la oficina», no «el servidor», pero hace exactamente lo mismo que las dos opciones anteriores. El control es máximo y la cercanía también: tus datos están donde estás tú. La contrapartida, dicha sin adornos, es que la responsabilidad también es máxima. Si se va la luz no hay un técnico de guardia en Núremberg: te toca a ti subir el diferencial. Y para que ese ordenador sea accesible desde fuera hace falta algo que tienda el puente entre tu portátil y él. No es magia, y conviene saberlo antes de elegir este camino.

Y no hace falta siquiera reaprovechar el ordenador de la oficina: existe un aparato pensado justo para esto, el NAS (los fabrican Synology, QNAP y otros). Como casi todo lo que hemos visto en estos Cuadernos, por dentro no hay magia: es un ordenador especializado, el mismo tipo de máquina que alquilarías en un centro de datos, solo que pensado para guardar datos y servirlos por la red, sin monitor ni teclado de por medio. Enchúfale una pantalla y un teclado y tienes un ordenador corriente; instala el software adecuado en tu PC y tienes un NAS. La diferencia es que el NAS ya viene listo. Lo compras, lo enchufas en casa o en el despacho, y es tuyo. No pagas una cuota cada mes; lo pagas una vez y te pertenece, como cualquier herramienta de tu negocio. Lo enciendes, lo apagas, te lo llevas a otro sitio si quieres. Y como es tuyo, nada impide tener dos —uno en casa, otro en la oficina— o tres, añadiendo uno en un lugar seguro, sincronizados entre sí: tu propia redundancia, sin depender de que un tercero la mantenga. El autohospedaje, al final, no es una sola cosa: es una combinación de equipos, de propiedad, de ubicaciones y de software.

Aquí es inevitable nombrar lo que hacemos, y lo hacemos sin disfraz: en Solo2 ese puente lo tiende la propia aplicación. El ordenador de tu oficina queda accesible solo para tus dispositivos de confianza, y siempre bajo cifrado, y tus demás aparatos se reconectan a él solos. Cuando un cliente habla contigo, es tu ordenador —no el de un tercero— el que habla con el cliente. No resolvemos el corte de luz; resolvemos el puente. Y no somos los únicos: para casi cada necesidad existen hoy programas —libres o propietarios— que permiten justo esto, tener los datos en tu equipo y llegar a ellos desde fuera. Lo nuestro es un ejemplo; lo importante es la idea, no la marca.

La redundancia no es un superpoder

Aquí surge la objeción inmediata, y es razonable: si lo tengo todo en el ordenador de mi oficina, ¿qué pasa si se rompe? La pregunta es buena. La respuesta es que la red de seguridad que imaginamos en los grandes proveedores es más modesta —y más imitable— de lo que parece.

Cuando dejo mis datos en el centro de datos de una multinacional, confío en que tenga copias en varios sitios. Y probablemente las tenga: en un segundo emplazamiento, quizá en un tercero. Pero esa redundancia no es infinita y, sobre todo, no es mía: sigue siendo un disco duro del que no soy el dueño, gestionado por alguien en quien deposito una fe que casi nunca verifico.

Esa misma red la puedo tejer yo, y con una ventaja decisiva. Mi servicio diario vive en el ordenador de la oficina. De ahí guardo una copia cifrada en el ordenador de una empresa amiga —un compañero de profesión, otra oficina de confianza— y otra copia cifrada, si quiero, en ese mismo proveedor europeo del que hablábamos. La diferencia lo es todo: lo que dejo fuera no es mi servicio ni mis datos en claro, sino una copia cifrada que solo yo puedo abrir. El proveedor externo guarda un cofre cerrado cuya llave no tiene. No le confío mi información: le confío unos bytes que, sin mí, no significan nada.

Estaba a salvo hasta que dejó de estarlo

Permíteme una historia propia, porque ilustra esto mejor que cualquier argumento. Durante más de diez años fui cliente devoto de CrashPlan, un servicio de copias de seguridad técnicamente extraordinario. Respaldaba en su nube todos mis ordenadores y los de mi familia —los de la empresa y los de casa, todo—, con versiones que podía recuperar a la frecuencia que quisiera, viajando hacia atrás en el tiempo hasta un archivo concreto de hacía meses. Tras la primera copia solo transmitía las diferencias, cifradas y comprimidas, de modo que mantenía al día un respaldo enorme sin apenas esfuerzo. Me salvó muchas veces, desde un documento tonto hasta un disco entero. El precio fue subiendo con los años y me daba igual: pagaba feliz.

Lo que yo no sabía es que CrashPlan había cometido un error de cálculo: había prometido por contrato almacenamiento ilimitado, en espacio y en tiempo. Y el espacio multiplicado por el tiempo —años de historia, versiones cada pocos minutos— crece hasta volverse insostenible. Un día nos comunicaron a todos que el servicio terminaba. Lo hicieron con elegancia y con un plazo generoso, casi un año, y nos dieron medios para descargar lo nuestro. Pero ¿a dónde se va uno con más de diez años de copias versionadas de todos sus discos? Ahí descubres que no tienes ni cómo bajarlo todo ni dónde meterlo, y que, aun pudiendo, el nuevo almacén costaría una fortuna.

Salvé cuatro cosas imprescindibles. El resto se fue cuando apagaron el interruptor. Yo estaba tranquilo, mi información estaba a salvo... hasta que dejó de estarlo. Y no por una traición: CrashPlan se portó de forma impecable —al contrario que Evernote, que años después se portó de forma vergonzosa—; sencillamente, mi ángel de la guarda en la nube decidió, con todo el derecho, dejar de serlo. El resultado, para mí, fue idéntico: lo que creía seguro, desapareció.

Lo que de verdad enseña esta historia tiene más de naturaleza humana que de tecnología. Cuando uno siente que algo es responsabilidad suya, actúa de forma preventiva: hace copias, se cubre las espaldas, desconfía con buen

criterio. Cuando cree —equivocadamente— que la responsabilidad la sostiene un tercero grande y solvente, se relaja y deja hacer. Esa tranquilidad delegada no es prudencia: es, sin maquillaje, una forma de irresponsabilidad.

Pagar no es lo mismo que cumplir

Esa irresponsabilidad tranquila se parece mucho a la de unos padres que matriculan a su hijo en el colegio más caro, le pagan después un máster, y con eso creen haber cumplido. No han cumplido. Ser padre es preocuparse de qué aprendió hoy, de lo que no entiende, de sus valores, de su seguridad en sí mismo. Si a los veinticinco años ese hijo no sabe trabajar ni comportarse, la culpa no es del colegio que cobró: es de quien delegó y pagó creyendo que con eso bastaba. Pagar a un tercero no exime de responsabilidad. Nunca lo ha hecho.

Con los datos pasa igual, y la historia reciente lo confirma. Hace cincuenta o cien años un profesional guardaba lo de sus clientes en carpetas, en su despacho o en su casa, y se sentía responsable de ellas. Rara vez se perdía nada. Hemos pasado al mundo digital y, con una facilidad pasmosa, lo subimos todo a «la nube» —que no es más que el ordenador de una multinacional— y dejamos de preocuparnos. Y con frecuencia hay accidentes, y hay empresas que lo pierden todo, y entonces se dice: la culpa fue de Google, la culpa fue de Microsoft. No. La información es tuya, o la de tus clientes, pero el responsable eres tú.

Hospedar lo tuyo no es un capricho técnico: es recuperar esa serenidad de hace décadas, la de saber dónde está cada cosa y por qué. La protección de datos, mientras tanto, ha vivido un péndulo brusco —de no haber norma ninguna, cuando cualquiera exhibía los datos de un cliente sin pensarlo, a una exigencia que recae con dureza desproporcionada sobre el más pequeño, el autónomo que pasa el teléfono de un cliente al repartidor—. No discuto el fin; observo el desajuste. Pero el desajuste no nos exime: el día en que la administración tenga medios para rastrear y sancionar a escala, el tamaño dejará de proteger a nadie, y conviene no esperar a ese día con la casa sin ordenar. Tener el dato bajo control propio ayuda a cumplir y ayuda a demostrarlo. Y, sobre todo, devuelve las cosas a su sitio: cuando la información es tuya, la responsabilidad es enteramente tuya —no hay un tercero a quien culpar, ni tampoco un tercero cuyo fallo te exponga—.

La responsabilidad también protege

Sería deshonesto pintar esto sin sombras. Ocupar el lugar del intermediario significa cargar con lo suyo: mantener copias al día, aplicar actualizaciones y una responsabilidad legal —la del RGPD— que, en realidad, nunca dejó de ser del todo tuya (las referencias al pie detallan los artículos). Hay trabajo, y hay un día en que algo falla a deshora. No lo escondemos.

Pero el miedo que rodea a esa palabra, responsabilidad, está mal calibrado. Es mucho más fácil perder tus archivos en un servicio de la nube que cierra, o tus fotos en Google Fotos, que perder esa carpeta de documentos importantes que tienes en tu propio ordenador: la que sabes dónde está y que notarías que falta en cuanto desapareciera. Lo que sientes tuyo, lo cuidas; lo que crees a salvo en manos de otro, lo descuidas.

Piensa en los álbumes de fotos de antes, los de papel revelado guardados en un cajón. ¿Has oído alguna vez a alguien decir que «perdió» su álbum familiar? Se oye lo de la casa que ardió con el álbum dentro; perderlo sin más, no. Y en cambio, gente que tenía todas sus fotos en Google Fotos o en Apple Fotos y se quedó sin nada: esa historia vuelve cada pocos meses, porque creían que estaba a salvo. Google Fotos cuida tus fotos, claro que sí; pero no las cuida como unos padres cuidan el álbum donde están sus hijos y sus nietos. Esa diferencia no la arregla ningún centro de datos: la responsabilidad, cuando es tuya, no es solo una carga; es también la mejor garantía.

Cuatro preguntas antes de decidir

Si te planteas dar el paso, en cualquiera de sus formas, conviene responder antes a cuatro preguntas con desapasionada honestidad:

1. ¿Qué parte de tus datos te dolería perder, o no poder llevarte? Y cuidado con descartar lo «rutinario»: el histórico de facturas parece lo más prosaico del mundo hasta que cambias de programa y descubres que esas facturas eran del proveedor, no tuyas —que, como mucho, te las puedes imprimir en PDF, sin poder ya buscar dentro de ellas—. No es solo cuestión de sensibilidad: es de a quién pertenece de verdad lo que necesitas conservar.
2. ¿Qué opción es proporcional a tu capacidad técnica real? Un ordenador propio bien cuidado está al alcance de cualquiera; administrar un servidor entero, no tanto. Sé honesto sobre lo que sabes y lo que no. Y recuerda que entre montarte un servidor entero y delegarlo todo hay un terreno intermedio muy razonable: programas —libres o propietarios— que guardan tus datos en tu propio equipo y te dejan llegar a ellos desde fuera. Para mucha gente es el mejor equilibrio.
3. ¿Qué plan tienes para el peor día? Una brecha, un disco que muere, un proveedor que cierra, el técnico de baja. Si el plan empieza por «no debería pasar», no es un plan.
4. ¿Sabrías demostrar que cumples si mañana te inspeccionan? Hacerlo bien y poder probar que lo haces bien no son lo mismo. La ley pide lo segundo.

No hay respuesta universal. Hay una respuesta proporcional, asumida con honestidad sobre lo que se gana y lo que se hereda. Y, por encima de la técnica, una certeza sencilla: tus datos viven en el ordenador de alguien. La única pregunta que de verdad importa es de quién quieres que sea ese ordenador.

El autohospedaje no es ni virtud ni vicio: es una herramienta con una huella concreta de capacidades y de responsabilidades. La pregunta nunca fue si hospedar lo tuyo, sino qué, cómo y con qué red de apoyo. Recuperar el control de los datos no es volver al sótano ni desconfiar de todo: es volver a sentirse responsable de lo que es nuestro, como cuando aquello vivía en una carpeta sobre la mesa. Esa responsabilidad, bien entendida, es el verdadero servicio que un profesional presta a sus clientes.

Fuentes y lectura adicional

- Reglamento (UE) 2016/679 — artículo 28 (encargado del tratamiento), artículo 32 (seguridad del tratamiento), artículo 33 (notificación de brechas), artículo 37 (designación del Delegado de Protección de Datos).
- Agencia Española de Protección de Datos — *Guía práctica para análisis de riesgos en el tratamiento de datos personales* (revisión vigente). Marco para responsables del tratamiento que asumen funciones técnicas propias.
- European Data Protection Board — *Guidelines 1/2024 on processing of personal data based on legitimate interests*. Aplicable también al examen de proporcionalidad en decisiones de infraestructura propia.
- Comisión Europea — directorio público de proveedores de servicios de la información establecidos en jurisdicción europea. Punto de partida administrativo para identificar opciones de hosting gestionado europeo.
- Nextcloud GmbH (Alemania) — *Nextcloud Enterprise architecture and compliance documentation*. Caso documentado de software libre con modalidades autohospedada y gestionada por proveedor europeo; útil como referencia técnica de un proyecto sostenido en jurisdicción europea desde 2016.

← AnteriorLas 24 palabras: qué es una identidad criptográficaSiguiente →Privacidad real vs aparente: las preguntas que conviene hacerse

Lecturas recientes

- Reflexión · 29 de junio de 2026 No eres anónimo
- Reflexión · 27 de mayo de 2026 Lo que una firma no puede arreglar
- Análisis · 26 de mayo de 2026 Privacidad real vs aparente: las preguntas que conviene hacerse

Llévate este artículo donde lo necesites.

↓ Markdown ↓ Texto plano ↓ PDF

El archivo se descarga a tu dispositivo. Desde ahí puedes guardarlo, importarlo a Solo2, o compartirlo donde quieras. Cuadernos no decide el destino por ti.

Sello de lacre · SHA-256 2e5573cbc7a8b417bbe572949c9563b8660b65dd3f5535ef909037e8ee14e27f

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