Análisis · 18 de mayo de 2026

← Anterior·Siguiente →

Self-hosting como práctica profesional

Cuándo el autohospedaje es prudencia profesional y cuándo es exceso. El RGPD aplicado al propio servidor: lo que se gana al eliminar al intermediario y lo que se hereda al ocupar su lugar.

Para entendernos: Montar tus propios servidores te quita al intermediario que tenía tus datos. Pero al sustituirlo heredas todo lo suyo: copias de seguridad, actualizaciones, responsabilidad legal del RGPD. Para algunos despachos profesionales es lo proporcional. Para otros, lo proporcional es pagar a un intermediario europeo y dormir tranquilo.

La pregunta entre la nube y el sótano

El profesional europeo que se preocupa por el control real de los datos de sus clientes acaba antes o después en una elección que se le presenta más sencilla de lo que es. De un lado, la nube comercial de los grandes proveedores estadounidenses, donde la herramienta ya está montada y el coste es la cuota mensual y la incomodidad ya descrita en otro Cuaderno. Del otro, lo que la jerga del sector llama *self-hosting*, autohospedaje: montar uno mismo los servidores donde se procesan los datos profesionales. La conversación pública tiende a presentar las dos opciones como contrapuestas, casi morales. La realidad, leída despacio, es más fina y más exigente.

Este artículo se ocupa de eso: cuándo el autohospedaje tiene sentido para un despacho profesional, cuándo es un compromiso excesivo, qué se hereda al asumirlo, y qué soluciones intermedias cubren el terreno entre el sótano y la nube transatlántica. La respuesta corta es la previsible —depende—; la respuesta larga merece formularse en serio.

Qué cuenta como autohospedaje

El término admite gradaciones. En su forma más pura, autohospedaje significa servidores físicos propios, en una sala propia, conectados a la red mediante una conexión propia. Solo el profesional o su equipo accede al hardware. Es la modalidad del aficionado a la informática y de un puñado de despachos especialmente sensibles. En su forma más común, autohospedaje significa el alquiler de un servidor virtual o físico en un centro de datos profesional, en el que el profesional instala el software que considera oportuno y administra él el resultado. El hardware no es suyo, pero la administración sí. En su forma más laxa —que el sector llama a veces «BYO» o «bring your own»— autohospedaje significa usar una instalación gestionada por un tercero de un software que en otro contexto se autohospedaría, como Nextcloud o Mattermost ofrecidos por un proveedor europeo bajo modelo SaaS. El control aquí es parcial: el software es libre y conocido, el operador es un tercero europeo, pero los datos los procesa el tercero.

Las tres modalidades comparten una propiedad central: el dato no termina en una empresa transatlántica sometida a FISA 702. Las tres difieren en otra propiedad igual de central: el peso técnico y jurídico que el profesional asume al elegirla. Una cosa es saber qué se quiere; otra es saber a qué se está dispuesto a comprometerse para tenerlo.

El argumento estructural a favor

El argumento a favor del autohospedaje, en cualquiera de sus formas, es estructural antes que ideológico. Cuando los datos del cliente residen físicamente en hardware controlado por el profesional —o por un proveedor europeo claramente identificado—, la cuestión de las transferencias internacionales del Cuaderno Schrems II deja de aplicarse. La pregunta del proveedor estadounidense subyacente desaparece. La pregunta del modelo de negocio del proveedor de herramientas también: el profesional sabe quién paga por qué, porque es él quien paga, y por una hora servidor que ese coste documenta. La pregunta del kill switch se reduce drásticamente: el proveedor europeo del centro de datos puede, técnicamente, apagar el servidor del cliente; pero la jurisdicción europea limita los supuestos y las órdenes legales para hacerlo, y existe en cualquier caso un plan de salida convencional (migrar los datos a otro proveedor europeo) que no depende de la buena voluntad del actual.

A esto se añade, para algunas profesiones, una consideración deontológica explícita. El abogado europeo sujeto a secreto profesional reglado, el médico con historia clínica bajo deber de custodia particular, el periodista que protege fuentes, llevan operando con archivos físicos durante décadas y manejan la lógica del control directo del dato con relativa naturalidad. La transición a autohospedaje, en sus formas razonables, es una continuidad operativa de esa lógica, no una ruptura.

El argumento proporcional en contra

El argumento en contra es proporcional y conviene formularlo sin paternalismo. El autohospedaje, en cualquiera de sus modalidades, traslada responsabilidades técnicas al profesional. Mantener un servidor implica actualizaciones de seguridad, copias de respaldo verificadas, monitorización, gestión de incidencias, planes de recuperación ante desastres. Mantener un servidor mal implica el peor escenario posible: la falsa sensación de control sobre datos que, en realidad, están más expuestos por la insuficiencia técnica del custodio que lo estarían en manos de un proveedor competente, aunque transatlántico.

El paralelismo con la caja fuerte es útil. Una caja fuerte mal cerrada protege menos que un sobre certificado depositado en una sucursal bancaria; el sobre certificado es una solución de bajo umbral técnico que funciona. Una caja fuerte bien cerrada, en cambio, protege bastante más que el sobre. El umbral técnico necesario para que la caja fuerte sea efectivamente protección y no engaño existe, y conviene medirlo antes de comprar la caja.

El RGPD aplicado al propio servidor

El cambio jurídico más importante al autohospedar no es la desaparición del problema. Es su consolidación en otro punto. Cuando el profesional procesa datos en infraestructura gestionada por él mismo, deja de tener un encargado del tratamiento externo en el sentido del artículo 28 del RGPD: él mismo combina ambas figuras. El artículo 32 del Reglamento, que exige medidas técnicas y organizativas adecuadas, recae enteramente sobre el profesional. Las notificaciones de brecha del artículo 33 son su responsabilidad. La obligación de demostrar cumplimiento del artículo 5.2 también. Si la escala del tratamiento o la sensibilidad de los datos cruza ciertos umbrales, puede aparecer la obligación de designar un Delegado de Protección de Datos (DPD), figura del artículo 37.

La autoridad española de protección de datos, la AEPD, mantiene guías específicas para responsables del tratamiento que asumen también las funciones técnicas: pautas para evaluaciones de impacto, para gestión de brechas, para registros de actividades. Esas guías existen porque la AEPD entiende que el sector tiene profesionales en esa situación y la valora como legítima. No la presupone fácil.

Las tres figuras intermedias

Entre la nube transatlántica y el servidor propio existen tres figuras intermedias que un profesional realista debería conocer. La primera, el alojamiento gestionado europeo: proveedores como OVHcloud (Francia),

Hetzner (Alemania), Scaleway (Francia), Aruba (Italia), Open Telekom Cloud (Alemania) o Sovereign Cloud (varias jurisdicciones nórdicas) ofrecen servidores en jurisdicción europea sin dependencia jurídica directa de empresas estadounidenses. El profesional alquila el servidor y administra el software. La complejidad técnica es la del autohospedaje sin la complicación adicional del hardware propio.

La segunda, el software libre sobre nube europea gestionado por el proveedor europeo: una variante donde el proveedor europeo no solo alquila el servidor sino que mantiene también la instalación del software. Nextcloud en versión gestionada, ProtonMail, Tuta, Mailfence ofrecen modalidades de este tipo. El profesional renuncia a parte del control sobre la administración a cambio de delegar la carga técnica; mantiene a cambio el control sobre la jurisdicción (europea) y sobre el modelo de negocio del proveedor (suscripción transparente).

La tercera, las arquitecturas sin servidor: comunicaciones cifradas peer-to-peer, ciertos modos de almacenamiento descentralizado, identidad criptográfica autosoberana. Estas arquitecturas no resuelven todo —no almacenan toda la infraestructura profesional, no sustituyen a la contabilidad ni a la gestión documental masiva—, pero eliminan completamente las preguntas del Schrems II, del modelo de negocio y del kill switch para los datos que sí gestionan. El despacho mixto contemporáneo combina, sin culpa, varias de estas tres figuras según el tipo de dato.

La pregunta del coste real

Una conversación honesta sobre autohospedaje incluye su coste, y el coste rara vez es el del hardware. El hardware actual cuesta menos cada año y un servidor sólido para un despacho mediano se puede adquirir hoy por menos de mil quinientos euros, alquilarlo por cuarenta o cincuenta euros al mes. El coste real son las horas de tiempo profesional dedicadas al mantenimiento, la guardia técnica para incidencias fuera de hora, los conocimientos necesarios para diagnosticar problemas, y, sobre todo, la valoración honesta del peor escenario: ¿qué pasa cuando algo falla un viernes por la tarde, el técnico que lo monta está de vacaciones y el lunes hay vista?

La modalidad gestionada por proveedor europeo —segunda figura intermedia— resuelve gran parte de ese coste a cambio de una cuota mensual razonable, perdiendo a cambio el último 10% de control sobre la administración. Para la mayoría de despachos profesionales medianos, esa relación coste-beneficio es la más sensata. El autohospedaje puro queda como opción para los pocos casos donde el último 10% justifica el coste técnico entero.

Para el lector profesional

Cuatro preguntas que conviene formularse antes de adoptar autohospedaje en cualquiera de sus modalidades:

1. ¿Qué proporción de los datos profesionales merece esta exigencia? La contabilidad del despacho, probablemente no. El expediente penal de un cliente bajo prisión preventiva, probablemente sí. La asignación proporcional es la primera decisión a tomar.
2. ¿Qué modalidad de autohospedaje es proporcional a la capacidad técnica disponible? Servidor propio en sala propia requiere conocimientos que pocos despachos pequeños tienen; alojamiento europeo gestionado es asequible para casi cualquiera.
3. ¿Qué plan de continuidad existe para el peor escenario? Brecha de seguridad, fallo de hardware, indisponibilidad del proveedor, baja del personal técnico. Si el plan empieza con «no debería pasar», no es plan.
4. ¿La capacidad propia incluye documentar el cumplimiento del RGPD —registros de actividades, evaluaciones de impacto, gestión de brechas— en caso de inspección? La AEPD audita; la respuesta «sé que lo hago bien» no demuestra cumplimiento por sí sola.

No hay respuesta universal. Hay una respuesta proporcional, asumida con honestidad sobre lo que se gana y lo que se hereda. El profesional que adopta autohospedaje sin haber respondido a las cuatro preguntas con

desapasionada precisión hace algo distinto y peor que el profesional que se queda en la nube transatlántica con plena conciencia de los riesgos: ofrece una falsa garantía a sus clientes, sin la conciencia que tendría el segundo de qué exactamente está delegando.

El autohospedaje no es virtud ni vicio. Es una herramienta con una huella concreta de capacidades y responsabilidades. La pregunta no es si autohospedar; es qué autohospedar, cómo, con qué red de soporte. La industria europea —proveedores de centro de datos, software libre maduro, comunidad técnica profesional— ofrece hoy un terreno intermedio mucho más razonable que el dilema simplificado entre el sótano y la nube de las grandes plataformas. Aprovechar ese terreno con realismo es trabajo profesional. Lo demás —el atajo entusiasta, la nube de oficio, el sótano amateur— son posiciones que cuestan más de lo que parece a quien las adopta sin medir.

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

- Análisis · 18 de mayo de 2026 Privacidad real vs aparente: las preguntas que conviene hacerse
- Concepto · 18 de mayo de 2026 Las 24 palabras: qué es una identidad criptográfica
- Análisis · 18 de mayo de 2026 El modelo de negocio como señal de confianza

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 a124e35e5ba2215f3b304d0de5287c004ab4f471611d4f4664a5a259ad04227e

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