Análisis · 26 de mayo de 2026

← Anterior·Siguiente →

Privacidad real vs aparente: las preguntas que conviene hacerse

Síntesis operativa del ciclo 2: las preguntas que distinguen un servicio con privacidad arquitectónica de uno con privacidad declarativa. Un cuestionario para el profesional europeo antes de adoptar cualquier herramienta digital para datos sensibles.

Para entendernos: Dos servicios con el mismo aviso legal pueden portarse de manera muy distinta. Uno protege por diseño técnico. El otro protege por promesa contractual. La diferencia no se lee en el aviso — se descubre formulando las preguntas concretas. La calidad de las respuestas dice tanto del producto como su propio contenido.

La diferencia entre privacidad arquitectónica y privacidad declarativa

A lo largo de los siete artículos anteriores de este ciclo hemos transitado por capas distintas del mismo asunto. El derecho de las transferencias internacionales con Schrems II. La idea matemática del hash criptográfico que sella cada Cuaderno. La elección arquitectónica del kill switch y la captura institucional que casi siempre lo acompaña. El mecanismo del cifrado de extremo a extremo y la pregunta operativa sobre dónde residen las claves. El alineamiento de incentivos según el modelo de negocio. La identidad criptográfica autosoberana. El autohospedaje como estrategia proporcional. Cada artículo se ocupó de un ángulo. Este, el último del ciclo, los reúne en un cuestionario.

La distinción que conviene retener es sencilla: hay servicios cuya privacidad es *arquitectónica* y hay servicios cuya privacidad es *declarativa*. La primera está incrustada en el diseño técnico: ciertas violaciones del compromiso de privacidad son técnicamente difíciles o imposibles porque la arquitectura no las permite. La segunda está depositada en el texto del aviso legal: ciertas violaciones serían contractualmente sancionables si ocurren, pero técnicamente nada las impide. Los dos modelos pueden cumplir el RGPD; pero uno protege por construcción y el otro protege por promesa, y la diferencia es operativamente enorme.

Las preguntas que siguen están diseñadas para distinguir un caso del otro. No son preguntas técnicas avanzadas. Son las preguntas que cualquier proveedor honesto puede responder en su documentación pública. La calidad y precisión de la respuesta dice tanto del producto como la respuesta misma. Las preguntas se agrupan en seis capas; conviene hacerlas todas antes de adoptar el servicio para datos sensibles, no solo las que el primer instinto identifica.

Capa 1: arquitectura

Conviene fijar un término antes de seguir. Por *operador* entendemos a la empresa que presta el servicio: la entidad que controla los servidores y el software, no una persona concreta. Hecha esa aclaración, la pregunta arquitectónica raíz es: ¿qué hace el operador con el contenido entre el emisor y el destinatario? Hay tres respuestas posibles y conviene saber distinguirlas, porque las tres se publicitan a veces con vocabulario parecido.

- La primera: el contenido pasa por un servidor del operador en claro, donde el operador puede leerlo aunque prometa no hacerlo.
- La segunda: el contenido pasa por un servidor del operador cifrado, donde el operador no puede leerlo si las claves residen exclusivamente en los dispositivos de los usuarios.
- La tercera: el contenido no pasa por ningún servidor del operador, porque no existe servidor del operador en ese flujo concreto.

La diferencia entre estas tres no es de grado: es de tipo.

La pregunta complementaria —ya formulada en el Cuaderno sobre cifrado— es: ¿quién tiene las claves criptográficas que permiten leer el contenido? Si las tiene el usuario y solo el usuario, el cifrado es real. Si las tiene además el operador en cualquier forma —incluso bajo el nombre de «recuperación de cuenta» o «sincronización entre dispositivos»—, el cifrado es nominal. La pregunta no admite respuesta intermedia honesta.

Capa 2: modelo de negocio

La pregunta sobre el modelo de negocio importa tanto como la pregunta arquitectónica, y por la misma razón sustantiva: los incentivos producen, a lo largo del tiempo, productos sistemáticamente distintos aun con propósitos declarados idénticos. ¿Cómo gana dinero hoy el operador? ¿Una sola fuente, dos, mezcla? Si la financiación incluye publicidad o monetización de datos, ¿qué datos se monetizan y sobre qué base jurídica del RGPD se hace? ¿La finalidad declarada en el aviso legal cubre los datos de terceros que el profesional pretende confiar al servicio?

Y la pregunta de segundo orden, no siempre formulada: ¿cuál es la situación financiera del operador a tres o cinco años vista? Una empresa en fase de capital riesgo opera bajo presiones distintas de una empresa en rentabilidad estable. El cambio de modelo de financiación es, repetidamente, el momento en el que el contrato implícito con los usuarios se reescribe sin negociación.

Capa 3: jurisdicción

Para el profesional europeo, la pregunta de la jurisdicción no es retórica. ¿En qué jurisdicción está incorporado el operador? ¿En qué país están físicamente los servidores que procesan los datos? ¿La respuesta a las dos preguntas anteriores es la misma o diferente, y si difiere, qué legislación se aplica? Una región europea operada por una empresa estadounidense no es, para efectos de Schrems II, una respuesta europea: la empresa está sometida a FISA 702 con independencia de dónde estén los servidores.

La pregunta complementaria operativa es: si llegara mañana una orden de inteligencia válida en la jurisdicción del operador pidiendo entregar mis datos o los de mis clientes, ¿qué pasaría? Si la respuesta honesta empieza por «la empresa estaría obligada a entregarlos», el servicio no protege contra esa orden por mucho que la publicidad sugiera lo contrario. Si la respuesta honesta empieza por «la empresa no podría entregarlos porque no los tiene en claro», el servicio sí protege; y la diferencia depende casi enteramente de las dos primeras capas, no de la calidad de la política de privacidad.

Capa 4: operador y kill switch

¿Qué capacidad técnica retiene el operador para suspender, bloquear, eliminar o degradar el servicio a distancia? La pregunta no es paranoica: es operativa. Las plataformas digitales han ejercitado esa capacidad repetidamente en los últimos años, a veces a iniciativa propia, otras bajo orden de Gobiernos, otras tras cambios de propiedad o de política. Si la capacidad existe, conviene saber bajo qué supuestos contractualmente declarados se ejerce, y reservar un margen para los supuestos no declarados que la práctica de los últimos años ha mostrado igual de

relevantes: orden judicial inesperada, sanción internacional, cambio de gobierno corporativo, adquisición por una entidad con otra política.

La pregunta hermana es la del plan de continuidad: si el operador ejerciera la capacidad contra el profesional —por la razón que sea, justa o no—, ¿qué tiempo de actividad seguiría disponible, qué procedimiento de exportación de datos existe, y a qué proveedor alternativo se podría migrar? Si la respuesta empieza por «no debería pasar», no es una respuesta operativa; es una promesa.

Capa 5: identidad y acceso

¿Quién controla las credenciales de acceso al servicio? Si el operador puede restablecer el acceso del usuario sin participación del usuario —procedimiento llamado típicamente «recuperación de cuenta»—, el operador es, técnicamente, el custodio de la cuenta y puede también cederla a quien lo solicite mediante el procedimiento adecuado. Si el operador no puede restablecer el acceso porque la identidad reside criptográficamente en el dispositivo del usuario, el operador no puede tampoco cederla, ni siquiera bajo orden. Las dos modalidades son legítimas según el contexto; pero, una vez más, son distintas, y conviene saber cuál se está adoptando.

¿Qué pasa con los datos del profesional si el profesional pierde el acceso? ¿Existen mecanismos de recuperación —de cuenta, de archivo, de sesión— que dependen del operador? ¿Esos mecanismos son compatibles con la deontología profesional del sector si el operador es coaccionado para usarlos?

Capa 6: futuro

Esta última capa suele descuidarse porque exige proyección. ¿Qué pasaría si el servicio fuera adquirido por otra empresa? Casi todas las adquisiciones llevan aparejada una revisión de términos del servicio en los meses siguientes. ¿Qué pasaría si las exigencias regulatorias cambiaran? El derecho europeo ha incrementado las obligaciones de retirada y bloqueo desde 2022, no las ha reducido. ¿Qué pasaría si el operador desapareciera? Una parte significativa de los servicios cloud no tiene plan de salida documentado para el escenario de cierre del operador; el profesional descubre el problema cuando ya no hay tiempo de prepararlo.

Hay una formulación que conviene retener para esta capa: las arquitecturas que dependen menos del operador son más resilientes ante cambios del operador. El autohospedaje en cualquiera de sus modalidades, la identidad criptográfica autosoberana, las comunicaciones sin servidor en medio, todas estas reducen la superficie de riesgo futura por el procedimiento de reducir la superficie de dependencia presente. No la eliminan; la reducen.

La diferencia entre estructura y promesa

Si tuviéramos que destilar el ciclo en una sola frase, sería esta: las respuestas estructurales se mantienen aunque el operador, la administración o la legislación cambien; las respuestas por promesa se mantienen mientras quien promete pueda y quiera mantenerlas. Las dos pueden ser correctas en el momento de adoptarse. Solo una de las dos se sostiene independientemente del paso del tiempo y del cambio de las circunstancias.

Esto no significa que cada profesional deba exigir respuestas estructurales a todos los servicios que adopta. La proporcionalidad sigue siendo legítima: una hoja de cálculo para contabilidad interna no necesita la misma respuesta que el expediente clínico de un paciente. Significa, sí, que la profesionalidad consiste en saber qué tipo de respuesta se ha aceptado en cada caso, y en haber decidido conscientemente que ese tipo de respuesta es proporcional al dato concreto.

El cuestionario, ordenado

Doce preguntas concretas que sintetizan el ciclo, ordenadas para que la respuesta a cada una informe la siguiente:

1. ¿El contenido pasa por un servidor del operador? Si pasa: ¿en claro, cifrado con claves del operador, o cifrado con claves exclusivas del usuario?
2. Si se invoca cifrado de extremo a extremo, ¿dónde residen las claves criptográficas? ¿El operador conoce o conserva alguna parte de ellas en cualquier forma, incluida la «recuperación»?
3. ¿Qué metadatos genera y conserva el servicio? ¿Cuánto tiempo? ¿A quién son visibles?
4. ¿Cómo se financia el operador? Si la financiación incluye publicidad o monetización de datos, ¿la finalidad declarada cubre datos de terceros confiados por el profesional?
5. ¿Cuál es la situación financiera del operador a tres o cinco años vista? ¿Hay factores que sugieran cambio inminente de modelo (salida a bolsa pendiente, ronda de financiación agotándose, adquisición probable)?
6. ¿En qué jurisdicción está incorporado el operador? ¿En qué país están físicamente los servidores? Si difieren, ¿qué legislación nacional se aplica al tratamiento?
7. ¿Qué pasaría si una orden de inteligencia válida en la jurisdicción del operador pidiera entregar mis datos? ¿La empresa podría cumplirla técnicamente?
8. ¿Qué capacidad técnica retiene el operador para suspender, bloquear o eliminar el servicio? ¿Bajo qué supuestos contractuales? ¿Bajo qué supuestos no contractuales históricamente documentados?
9. ¿Qué plan de salida existe si el operador ejerciera esa capacidad contra mí, justa o injustamente? ¿Hay procedimiento documentado de exportación de datos a un proveedor alternativo?
10. ¿Quién controla las credenciales de acceso? ¿El operador puede restablecerlas sin mi participación? ¿Eso me protege o me expone?
11. ¿Existe una alternativa europea, autohospedada o sin servidor en medio para esta función concreta? ¿Cuál es su coste real, comparado con el riesgo evaluado?
12. Si la decisión de hoy fuera examinada dentro de cinco años por un inspector, un auditor o un cliente afectado por una brecha, ¿la elección actual sería defendible con los argumentos disponibles hoy, o requeriría disculparse por no haber hecho preguntas razonables?

Las preguntas no esperan respuestas perfectas. Esperan respuestas honestas, que el operador honesto sabe dar y el operador menos honesto evita formular con precisión. La diferencia operativa entre las dos clases de operador, lo decimos sin dramatismo, suele percibirse leyendo despacio las respuestas que ofrecen voluntariamente, antes incluso de tener que pedir más.

Con este artículo cerramos el segundo ciclo de Cuadernos Lacre. Empezamos con la editorial debt heredada de Schrems II y terminamos con un cuestionario operativo. Por el camino hemos transitado conceptos —hash, cifrado, identidad— y análisis aplicados —kill switch, modelo de negocio, self-hosting—. La intención editorial declarada de la publicación no era abrumar al lector con la lista exhaustiva de problemas, sino entregarle herramientas para que distinga, ante cualquier servicio nuevo, qué clase de respuesta está aceptando. Esa distinción —entre arquitectura y promesa— es la herramienta. Lo demás cada profesional lo pondrá al servicio de los datos que considere, en su práctica, dignos de la pregunta.

Fuentes y lectura adicional

- Esta publicación, ciclo 2 (mayo de 2026) — *Schrems II cinco años después*, *Qué es realmente SHA-256*, *Kill switch y la captura institucional*, *Cifrado de extremo a extremo explicado de verdad*, *El modelo de negocio como señal de confianza*, *Las 24 palabras: qué es una identidad criptográfica*, *Self-hosting como práctica profesional*. Los siete artículos sobre los que descansa este cuestionario.
- Reglamento (UE) 2016/679 — Reglamento General de Protección de Datos. Marco jurídico de referencia para todas las preguntas que el cuestionario plantea, en particular los artículos 5, 6, 25, 28, 32, 33 y el capítulo V.
- Comité Europeo de Protección de Datos — directrices y dictámenes operativos sobre Schrems II, transferencias internacionales, evaluaciones de impacto y responsabilidad proactiva (publicaciones 2020-2024).
- Agencia Española de Protección de Datos — sanciones publicadas 2022-2024 a responsables del tratamiento por instrumentos inadecuados de transferencia o por evaluaciones de impacto formales sin contenido sustantivo.

- noyb.eu — Centro Europeo para los Derechos Digitales, dirigido por Maximilian Schrems. Repositorio público de denuncias, recursos y análisis sobre el cumplimiento real, no aparente, de las normas europeas de protección de datos.

← AnteriorSelf-hosting como práctica profesionalSiguiente →Lo que una firma no puede arreglar

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 · 25 de mayo de 2026 Self-hosting como práctica profesional

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 8ce8a9814714e9a1f3f2738b8e052df213b9efa30ca93d492d7ef04ab10ad1d8

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