Análisis · 16 de mayo de 2026

← Anterior·Siguiente →

Cuando no hay nadie en medio

Cifrar lo que pasa por un servidor protege el contenido. No tener servidor en medio elimina la pregunta. No son lo mismo.

Dos personas, una conversación

Cuando dos personas hablan cara a cara en una habitación, nadie tiene que prometer que no oyó nada. No oyó porque no estaba. Cuando dos personas se pasan un papel de una mano a la otra, nadie en medio tiene que jurar que no lo leyó. No hay nadie en medio.

La mayor parte de las cosas en la vida cotidiana funcionan así. No firmamos acuerdos de confidencialidad con el aire que transmite nuestra voz, ni con el papel que sostenemos. La privacidad de la conversación no descansa sobre la promesa de un intermediario, porque no hay intermediario. Esa es una de las formas más fuertes que existe de ser privado: no porque algo o alguien se comporte bien, sino porque no hay algo o alguien.

Cuando la conversación se traslada a un canal digital, esto cambia por defecto. El modelo habitual es el siguiente: dos personas se conectan a un servidor, el servidor recibe el mensaje, lo cifra o lo guarda cifrado, y se lo entrega al destinatario. El servidor está en medio. El servidor puede ser honesto. Puede estar auditado. Puede operar en una jurisdicción favorable y bajo una política de privacidad estricta. Todo eso puede ser cierto. Pero el servidor está en medio.

La diferencia entre cifrar y no recoger (segunda parte)

En un artículo anterior de esta misma serie sostenemos que cifrar el contenido y no recoger metadatos no son lo mismo. Hay un paso más allá que conviene formular con claridad: cifrar lo que pasa por un servidor y no tener servidor son tampoco lo mismo.

El primer modelo —servidor en medio, contenido cifrado— protege el contenido del operador del servidor, de su personal de mantenimiento, de un atacante externo que comprometa el sistema. Y eso es importante. Pero no elimina al servidor. El servidor sigue ahí. Sigue procesando metadatos. Sigue siendo un punto que puede recibir un requerimiento judicial, una intervención legal, una presión política, o una brecha de seguridad. Sigue siendo un punto que requiere depositar confianza en alguien.

El segundo modelo —no haber servidor entre los dos extremos— no protege mejor el contenido cifrado: si la criptografía es sólida, el contenido va protegido en ambos casos. Lo que cambia no es el contenido. Lo que cambia es que la pregunta *«¿qué pasa con el servidor?»* deja de tener objeto, porque no existe servidor sobre el que preguntar.

Confianza, ausencia, y la diferencia entre ambas

La confianza puede estar bien depositada. Empresas honestas existen. Auditores rigurosos existen. Legislaciones favorables al usuario existen. Servicios serios que cumplen escrupulosamente con todo lo anterior existen. La

confianza, cuando se concede a un operador que la merece, no es un mal arreglo.

Pero la confianza, por sólida que sea, sigue siendo confianza. Es una solución social, no una solución técnica. Una empresa puede cambiar de manos. Una jurisdicción puede cambiar de gobierno. Una orden judicial puede llegar mañana. Una vulnerabilidad nueva puede descubrirse el mes que viene. Nada de esto sucede por mala fe. Sucede porque el operador existe, y todo lo que existe está sujeto a las contingencias del mundo.

La ausencia de un operador no está sujeta a esas mismas contingencias. Una orden judicial no puede pedir datos a un servidor que no existe. Un atacante no puede comprometer un servidor que no existe. Un cambio en la política de una empresa no puede afectar a datos que esa empresa nunca tuvo. La frase clave es sencilla: los datos que no existen no se pueden perder.

Sobre el argumento legítimo del lado del servidor

Quien ofrece un servicio de mensajería profesional con servidor en medio suele formular tres argumentos perfectamente válidos. Primero, que el servidor es necesario para garantizar la entrega cuando el destinatario está desconectado. Segundo, que el cifrado del contenido es robusto y por tanto el operador no puede leerlo. Tercero, que el servicio cumple la legislación europea y que los datos están protegidos por la ley.

Los tres argumentos son ciertos. Ninguno cambia la naturaleza del asunto. Es cierto que un servidor permite almacenar mensajes para entrega diferida; también es cierto que la entrega diferida puede resolverse de otra forma, mediante protocolos de comunicación directa entre dispositivos refinados desde hace décadas y operativos hoy. Es cierto que el cifrado del contenido en tránsito es robusto en los servicios serios. Y es cierto que la legislación europea protege a los usuarios más que la de muchos otros lugares.

La cuestión no es si los servicios con servidor en medio son legales, ni si son seguros, ni si protegen el contenido. Pueden serlo, son legales, y suelen ser seguros. La cuestión es que tener un servidor en medio es una elección arquitectónica, no una imposición técnica. Y cada elección tiene consecuencias. Una arquitectura con servidor en medio genera necesariamente un actor en el que hay que confiar. Una arquitectura sin servidor en medio no.

Lo que la ley dice, y lo que la arquitectura hace

El RGPD no exige un modelo arquitectónico concreto. Exige resultados: minimización de datos, finalidad limitada, protección desde el diseño y por defecto, capacidad de demostrar el cumplimiento. Un servicio con servidor en medio puede cumplir todos estos requisitos. Un servicio sin servidor en medio cumple varios de ellos por construcción, no por declaración. La minimización absoluta —no recoger nada que no sea estrictamente necesario para entregar el mensaje— es trivial cuando no existe un servidor que pueda recoger algo.

Para los usos cotidianos no sensibles, una arquitectura con servidor es perfectamente razonable, y la confianza en un operador serio es un arreglo válido. Para los otros usos —los que llevan secreto profesional reglado, los que conllevan responsabilidad deontológica, los que tocan información especialmente sensible— la ausencia de un punto de confianza no es un lujo, es una ventaja estructural.

Para el lector profesional

Las preguntas que conviene hacerse ante un servicio de comunicación profesional, ya familiares de artículos anteriores en esta misma serie, se completan con una sola pregunta arquitectónica más:

1. ¿Cifra el contenido en tránsito? (Probablemente sí.)
2. ¿Genera y almacena metadatos sobre con quién hablo y cuándo? (Probablemente sí.)
3. ¿Existe un servidor en el camino entre mi dispositivo y el del destinatario?
4. Si existe: ¿quién lo opera, en qué jurisdicción, y qué tendría que ocurrir para que entregara datos sobre mí?

5. Si no existe: las preguntas anteriores no tienen objeto.

La diferencia entre las dos categorías no es de grado, sino de tipo. Llegado el momento de explicárselo a un cliente, a un paciente, o a un colega, la formulación más honesta es también la más sencilla: en una hay alguien en medio; en la otra, no.

Este artículo cierra el ciclo inicial de Cuadernos Lacre. Tras hablar del cifrado, los metadatos y el secreto profesional, completamos el cuadro arquitectónico: cifrar el contenido y no tener servidor en medio son cosas distintas. Las dos pueden ser legales; solo una elimina el punto de confianza.

Fuentes y lectura adicional

- Saltzer, J. H.; Reed, D. P.; Clark, D. D. — *End-to-end arguments in system design*, ACM TOCS, 1984. Texto fundacional del principio según el cual las garantías de un sistema deben implementarse en los extremos, no en el canal intermedio.
- Reglamento (UE) 2016/679, art. 25 — protección de datos desde el diseño y por defecto.
- Reglamento (UE) 2016/679, art. 5.1.c — principio de minimización de datos.
- Schneier, B. — *Data and Goliath: the hidden battles to collect your data and control your world* (2015), W. W. Norton. Capítulos sobre arquitecturas que minimizan la recolección por construcción.

← AnteriorRGPD y mensajería profesional: por qué la mayoría incumple sin saberloSiguiente →Schrems II, cinco años después

Lecturas recientes

- Análisis · 18 de mayo de 2026 Privacidad real vs aparente: las preguntas que conviene hacerse
- Análisis · 18 de mayo de 2026 Self-hosting como práctica profesional
- Concepto · 18 de mayo de 2026 Las 24 palabras: qué es una identidad criptográfica

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 b092bad42c3589efc45044b71c5e984bdd15f8f12dd124e39acb01f0a188a2d5

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