Análise · 26 de maio de 2026

← Anterior·Seguinte →

Privacidade real vs aparente: as preguntas que convén facerse

Síntese operativa do ciclo 2: as preguntas que distinguen un servizo con privacidade arquitectónica dun con privacidade declarativa. Un cuestionario para o profesional europeo antes de adoptar calquera ferramenta dixital para datos sensibles.

Para entendérmonos: Dous servizos co mesmo aviso legal poden comportarse de maneira moi distinta. Un protexe por deseño técnico. O outro protexe por promesa contractual. A diferenza non se le no aviso — descóbrese formulando as preguntas concretas. A calidade das respostas di tanto do produto como o seu propio contido.

A diferenza entre privacidade arquitectónica e privacidade declarativa

Ao longo dos sete artigos anteriores deste ciclo transitamos por capas distintas do mesmo asunto. O dereito das transferencias internacionais con Schrems II. A idea matemática do hash criptográfico que sela cada Cuaderno. A elección arquitectónica do kill switch e a captura institucional que case sempre o acompaña. O mecanismo do cifrado de extremo a extremo e a pregunta operativa sobre onde residen as chaves. O aliñamento de incentivos segundo o modelo de negocio. A identidade criptográfica autosoberana. O autoaloxamento como estratexia proporcional. Cada artigo ocupouse dun ángulo. Este, o último do ciclo, reúneos nun cuestionario.

A distinción que convén reter é sinxela: hai servizos cuxa privacidade é *arquitectónica* e hai servizos cuxa privacidade é *declarativa*. A primeira está incrustada no deseño técnico: certas violacións do compromiso de privacidade son tecnicamente difíciles ou imposibles porque a arquitectura non as permite. A segunda está depositada no texto do aviso legal: certas violacións serían contractualmente sancionables se ocorren, pero tecnicamente nada as impide. Os dous modelos poden cumprir o RGPD; pero un protexe por construción e o outro protexe por promesa, e a diferenza é operativamente enorme.

As preguntas que seguen están deseñadas para distinguir un caso do outro. Non son preguntas técnicas avanzadas. Son as preguntas que calquera provedor honesto pode responder na súa documentación pública. A calidade e precisión da resposta di tanto do produto como a propia resposta. As preguntas agrúpanse en seis capas; convén facelas todas antes de adoptar o servizo para datos sensibles, non só as que o primeiro instinto identifica.

Capa 1: arquitectura

Convén fixar un termo antes de seguir. Por *operador* entendemos a empresa que presta o servizo: a entidade que controla os servidores e o software, non unha persoa concreta. Feita esa aclaración, a pregunta arquitectónica de raíz é: que fai o operador co contido entre o emisor e o destinatario? Hai tres respostas posibles e convén sabelas distinguir, porque as tres anúncianse ás veces cun vocabulario semellante.

- A primeira: o contido pasa por un servidor do operador en claro, onde o operador pode lelo aínda que prometa non facelo.

- A segunda: o contido pasa por un servidor do operador cifrado, onde o operador non pode lelo se as chaves residen exclusivamente nos dispositivos dos usuarios.
- A terceira: o contido non pasa por ningún servidor do operador, porque non existe servidor do operador nese fluxo concreto.

A diferenza entre estas tres non é de grao: é de tipo.

A pregunta complementaria —xa formulada no Cuaderno sobre cifrado— é: quen ten as chaves criptográficas que permiten ler o contido? Se as ten o usuario e só o usuario, o cifrado é real. Se as ten ademais o operador en calquera forma —mesmo baixo o nome de «recuperación de conta» ou «sincronización entre dispositivos»—, o cifrado é nominal. A pregunta non admite resposta intermedia honesta.

Capa 2: modelo de negocio

A pregunta sobre o modelo de negocio importa tanto como a pregunta arquitectónica, e pola mesma razón substantiva: os incentivos producen, ao longo do tempo, produtos sistematicamente distintos aínda con propósitos declarados idénticos. Como gaña diñeiro hoxe o operador? Unha soa fonte, dúas, mestura? Se o financiamento inclúe publicidade ou monetización de datos, que datos se monetizan e sobre que base xurídica do RGPD se fai? A finalidade declarada no aviso legal cobre os datos de terceiros que o profesional pretende confiar ao servizo?

E a pregunta de segunda orde, non sempre formulada: cal é a situación financeira do operador a tres ou cinco anos vista? Unha empresa en fase de capital risco opera baixo presións distintas dunha empresa en rendibilidade estable. O cambio de modelo de financiamento é, repetidamente, o momento no que o contrato implícito cos usuarios se reescribe sen negociación.

Capa 3: xurisdición

Para o profesional europeo, a pregunta da xurisdición non é retórica. En que xurisdición está incorporado o operador? En que país están fisicamente os servidores que procesan os datos? A resposta ás dúas preguntas anteriores é a mesma ou diferente, e se difire, que lexislación se aplica? Unha rexión europea operada por unha empresa estadounidense non é, para efectos de Schrems II, unha resposta europea: a empresa está sometida a FISA 702 con independencia de onde estean os servidores.

A pregunta complementaria operativa é: se chegase mañá unha orde de intelixencia válida na xurisdición do operador pedindo entregar os meus datos ou os dos meus clientes, que pasaría? Se a resposta honesta comeza por «a empresa estaría obrigada a entregalos», o servizo non protexe contra esa orde por moito que a publicidade suxira o contrario. Se a resposta honesta comeza por «a empresa non podería entregalos porque non os ten en claro», o servizo si protexe; e a diferenza depende case enteiramente das dúas primeiras capas, non da calidade da política de privacidade.

Capa 4: operador e kill switch

Que capacidade técnica retén o operador para suspender, bloquear, eliminar ou degradar o servizo a distancia? A pregunta non é paranoica: é operativa. As plataformas dixitais exerceron esa capacidade repetidamente nos últimos anos, ás veces por iniciativa propia, outras baixo orde de Gobernos, outras tras cambios de propiedade ou de política. Se a capacidade existe, convén saber baixo que supostos contractualmente declarados se exerce, e reservar unha marxe para os supostos non declarados que a práctica dos últimos anos mostrou igual de relevantes: orde xudicial inesperada, sanción internacional, cambio de goberno corporativo, adquisición por unha entidade con outra política.

A pregunta irmá é a do plan de continuidade: se o operador exercese a capacidade contra o profesional —pola razón que sexa, xusta ou non—, que tempo de actividade seguiría dispoñible, que procedemento de exportación de datos existe, e a que provedor alternativo se podería migrar? Se a resposta comeza por «non debería pasar», non é unha resposta operativa; é unha promesa.

Capa 5: identidade e acceso

Quen controla as credenciais de acceso ao servizo? Se o operador pode restablecer o acceso do usuario sen a participación do usuario —procedemento chamado tipicamente «recuperación de conta»—, o operador é, tecnicamente, o custodio da conta e pode tamén cedela a quen o solicite mediante o procedemento adecuado. Se o operador non pode restablecer o acceso porque a identidade reside criptograficamente no dispositivo do usuario, o operador tampouco pode cedela, nin sequera baixo orde. As dúas modalidades son lexítimas segundo o contexto; pero, unha vez máis, son distintas, e convén saber cal se está adoptando.

Que pasa cos datos do profesional se o profesional perde o acceso? Existen mecanismos de recuperación —de conta, de arquivo, de sesión— que dependen do operador? Eses mecanismos son compatibles coa deontoloxía profesional do sector se o operador é coaccionado para usalos?

Capa 6: futuro

Esta última capa adoita descoidarse porque esixe proxección. Que pasaría se o servizo fose adquirido por outra empresa? Case todas as adquisicións levan aparellada unha revisión dos termos do servizo nos meses seguintes. Que pasaría se as esixencias regulatorias cambiasen? O dereito europeo incrementou as obrigas de retirada e bloqueo desde 2022, non as reduciu. Que pasaría se o operador desaparecese? Unha parte significativa dos servizos na nube non ten un plan de saída documentado para o escenario de peche do operador; o profesional descobre o problema cando xa non hai tempo de preparalo.

Hai unha formulación que convén reter para esta capa: as arquitecturas que dependen menos do operador son máis resilientes ante cambios do operador. O autoaloxamento en calquera das súas modalidades, a identidade criptográfica autosoberana, as comunicacións sen servidor polo medio, todas estas reducen a superficie de risco futura mediante o procedemento de reducir a superficie de dependencia presente. Non a eliminan; redúcena.

A diferenza entre estrutura e promesa

Se tivésemos que destilar o ciclo nunha soa frase, sería esta: as respostas estruturais mantéñense aínda que o operador, a administración ou a lexislación cambien; as respostas por promesa mantéñense mentres quen promete poida e queira mantelas. As dúas poden ser correctas no momento de adoptarse. Só unha das dúas se sostén independentemente do paso do tempo e do cambio das circunstancias.

Isto non significa que cada profesional deba esixir respostas estruturais a todos os servizos que adopta. A proporcionalidade segue sendo lexítima: unha folla de cálculo para contabilidade interna non precisa a mesma resposta que o expediente clínico dun paciente. Significa, si, que a profesionalidade consiste en saber que tipo de resposta se aceptou en cada caso, e en ter decidido conscientemente que ese tipo de resposta é proporcional ao dato concreto.

O cuestionario, ordenado

Doce preguntas concretas que sintetizan o ciclo, ordenadas para que a resposta a cada unha informe a seguinte:

1. O contido pasa por un servidor do operador? Se pasa: en claro, cifrado con chaves do operador, ou cifrado con chaves exclusivas do usuario?

2. Se se invoca cifrado de extremo a extremo, onde residen as chaves criptográficas? O operador coñece ou conserva algunha parte delas en calquera forma, incluída a «recuperación»?
3. Que metadatos xera e conserva o servizo? Canto tempo? A quen son visibles?
4. Como se financia o operador? Se o financiamento inclúe publicidade ou monetización de datos, a finalidade declarada cobre datos de terceiros confiados polo profesional?
5. Cal é a situación financeira do operador a tres ou cinco anos vista? Hai factores que suxiran un cambio inminente de modelo (saída a bolsa pendente, rolda de financiamento esgotándose, adquisición probable)?
6. En que xurisdición está incorporado o operador? En que país están fisicamente os servidores? Se difiren, que lexislación nacional se aplica ao tratamento?
7. Que pasaría se unha orde de intelixencia válida na xurisdición do operador pedise entregar os meus datos? A empresa podería cumprila tecnicamente?
8. Que capacidade técnica retén o operador para suspender, bloquear ou eliminar o servizo? Baixo que supostos contractuais? Baixo que supostos non contractuais historicamente documentados?
9. Que plan de saída existe se o operador exercese esa capacidade contra min, xusta ou inxustamente? Hai un procedemento documentado de exportación de datos a un provedor alternativo?
10. Quen controla as credenciais de acceso? O operador pode restablecelas sen a miña participación? Iso protéxeme ou exponme?
11. Existe unha alternativa europea, autoaloxada ou sen servidor polo medio para esta función concreta? Cal é o seu custo real, comparado co risco avaliado?
12. Se a decisión de hoxe fose examinada dentro de cinco anos por un inspector, un auditor ou un cliente afectado por unha brecha, a elección actual sería defendible cos argumentos dispoñibles hoxe, ou requiriría desculparse por non ter feito preguntas razoables?

As preguntas non esperan respostas perfectas. Esperan respostas honestas, que o operador honesto sabe dar e o operador menos honesto evita formular con precisión. A diferenza operativa entre as dúas clases de operador, dicímolo sen dramatismo, adoita percibirse lendo amodo as respostas que ofrecen voluntariamente, antes mesmo de ter que pedir máis.

Con este artigo pechamos o segundo ciclo de Cuadernos Lacre. Comezamos coa débeda editorial herdada de Schrems II e rematamos cun cuestionario operativo. Polo camiño transitamos conceptos —hash, cifrado, identidade— e análises aplicadas —kill switch, modelo de negocio, self-hosting—. A intención editorial declarada da publicación non era abafar o lector coa lista exhaustiva de problemas, senón entregarlle ferramentas para que distinga, ante calquera servizo novo, que clase de resposta está aceptando. Esa distinción —entre arquitectura e promesa— é a ferramenta. O demais cada profesional poñerao ao servizo dos datos que considere, na súa práctica, dignos da pregunta.

Fontes e lectura adicional

- Esta publicación, ciclo 2 (maio de 2026) — *Schrems II, cinco anos despois*, *Que é realmente SHA-256*, *Kill switch e a captura institucional*, *Cifrado de extremo a extremo explicado de verdade*, *O modelo de negocio como sinal de confianza*, *As 24 palabras: que é unha identidade criptográfica*, *Self-hosting como práctica profesional*. Os sete artigos sobre os que descansa este cuestionario.
- Regulamento (UE) 2016/679 — Regulamento Xeral de Protección de Datos. Marco xurídico de referencia para todas as preguntas que o cuestionario formula, en particular os artigos 5, 6, 25, 28, 32, 33 e o capítulo V.
- Comité Europeo de Protección de Datos — directrices e ditames operativos sobre Schrems II, transferencias internacionais, avaliacións de impacto e responsabilidade proactiva (publicacións 2020-2024).
- Axencia Española de Protección de Datos — sancións publicadas 2022-2024 a responsables do tratamento por instrumentos inadecuados de transferencia ou por avaliacións de impacto formais sen contido substantivo.
- noyb.eu — Centro Europeo para os Dereitos Dixitais, dirixido por Maximilian Schrems. Repositorio público de denuncias, recursos e análises sobre o cumprimento real, non aparente, das normas europeas de

protección de datos.

← AnteriorSelf-hosting como práctica profesionalSeguinte →O que unha firma non pode arranxar

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

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 33c2e46a336e53e6a29db484a7f9427c6156bebfb4fe5c95690667c6b8c8ab90

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