Anàlisi · 26 de maig del 2026

← Anterior·Següent →

# Privadesa real vs aparent: les preguntes que convé fer-se

Síntesi operativa del cicle 2: les preguntes que distingeixen un servei amb privadesa arquitectònica d'un amb privadesa declarativa. Un qüestionari per al professional europeu abans d'adoptar qualsevol eina digital per a dades sensibles.

**Per entendre'ns:** Dos serveis amb el mateix avís legal poden comportar-se de manera molt distinta. Un protegeix per disseny tècnic. L'altre protegeix per promesa contractual. La diferència no es llegeix en l'avís — es descobreix formulant les preguntes concretes. La qualitat de les respostes diu tant del producte com el seu propi contingut.

## La diferència entre privadesa arquitectònica i privadesa declarativa

Al llarg dels set articles anteriors d'aquest cicle hem transitat per capes distintes del mateix assumpte. El dret de les transferències internacionals amb Schrems II. La idea matemàtica del hash criptogràfic que segella cada Cuaderno. L'elecció arquitectònica del kill switch i la captura institucional que gairebé sempre l'acompanya. El mecanisme del xifratge d'extrem a extrem i la pregunta operativa sobre on resideixen les claus. L'alineament d'incentius segons el model de negoci. La identitat criptogràfica autosobirana. L'autoallotjament com a estratègia proporcional. Cada article es va ocupar d'un angle. Aquest, l'últim del cicle, els reuneix en un qüestionari.

La distinció que convé retenir és senzilla: hi ha serveis la privadesa dels quals és *arquitectònica* i hi ha serveis la privadesa dels quals és *declarativa*. La primera està incrustada en el disseny tècnic: certes violacions del compromís de privadesa són tècnicament difícils o impossibles perquè l'arquitectura no les permet. La segona està dipositada en el text de l'avís legal: certes violacions serien contractualment sancionables si es produeixen, però tècnicament res no les impedeix. Els dos models poden complir el RGPD; però un protegeix per construcció i l'altre protegeix per promesa, i la diferència és operativament enorme.

Les preguntes que segueixen estan dissenyades per distingir un cas de l'altre. No són preguntes tècniques avançades. Són les preguntes que qualsevol proveïdor honest pot respondre en la seva documentació pública. La qualitat i precisió de la resposta diu tant del producte com la resposta mateixa. Les preguntes s'agrupen en sis capes; convé fer-les totes abans d'adoptar el servei per a dades sensibles, no només les que el primer instint identifica.

## Capa 1: arquitectura

Convé fixar un terme abans de continuar. Per *operador* entenem l'empresa que presta el servei: l'entitat que controla els servidors i el programari, no una persona concreta. Feta aquesta aclaració, la pregunta arquitectònica d'arrel és: què fa l'operador amb el contingut entre l'emissor i el destinatari? Hi ha tres respostes possibles i convé saber distingir-les, perquè totes tres es publiciten de vegades amb un vocabulari semblant.

- La primera: el contingut passa per un servidor de l'operador en clar, on l'operador pot llegir-lo encara que prometi no fer-ho.

- La segona: el contingut passa per un servidor de l'operador xifrat, on l'operador no pot llegir-lo si les claus resideixen exclusivament en els dispositius dels usuaris.
- La tercera: el contingut no passa per cap servidor de l'operador, perquè no existeix servidor de l'operador en aquest flux concret.

La diferència entre aquestes tres no és de grau: és de tipus.

La pregunta complementària —ja formulada al Cuaderno sobre xifratge— és: qui té les claus criptogràfiques que permeten llegir el contingut? Si les té l'usuari i només l'usuari, el xifratge és real. Si les té a més l'operador en qualsevol forma —fins i tot sota el nom de «recuperació de compte» o «sincronització entre dispositius»—, el xifratge és nominal. La pregunta no admet resposta intermèdia honesta.

# Capa 2: model de negoci

La pregunta sobre el model de negoci importa tant com la pregunta arquitectònica, i per la mateixa raó substantiva: els incentius produeixen, al llarg del temps, productes sistemàticament distints encara que amb propòsits declarats idèntics. Com guanya diners avui l'operador? Una sola font, dues, barreja? Si el finançament inclou publicitat o monetització de dades, quines dades es monetitzen i sobre quina base jurídica del RGPD es fa? La finalitat declarada en l'avís legal cobreix les dades de tercers que el professional pretén confiar al servei?

I la pregunta de segon ordre, no sempre formulada: quina és la situació financera de l'operador a tres o cinc anys vista? Una empresa en fase de capital de risc opera sota pressions distintes d'una empresa en rendibilitat estable. El canvi de model de finançament és, repetidament, el moment en què el contracte implícit amb els usuaris es reescriu sense negociació.

# Capa 3: jurisdicció

Per al professional europeu, la pregunta de la jurisdicció no és retòrica. En quina jurisdicció està incorporat l'operador? En quin país estan físicament els servidors que processen les dades? La resposta a les dues preguntes anteriors és la mateixa o diferent, i si difereix, quina legislació s'aplica? Una regió europea operada per una empresa nord-americana no és, a efectes de Schrems II, una resposta europea: l'empresa està sotmesa a FISA 702 amb independència d'on estiguin els servidors.

La pregunta complementària operativa és: si arribés demà una ordre d'intel·ligència vàlida en la jurisdicció de l'operador demanant lliurar les meves dades o les dels meus clients, què passaria? Si la resposta honesta comença per «l'empresa estaria obligada a lliurar-les», el servei no protegeix contra aquesta ordre per molt que la publicitat suggereixi el contrari. Si la resposta honesta comença per «l'empresa no podria lliurar-les perquè no les té en clar», el servei sí que protegeix; i la diferència depèn gairebé enterament de les dues primeres capes, no de la qualitat de la política de privadesa.

# Capa 4: operador i kill switch

Quina capacitat tècnica reté l'operador per suspendre, bloquejar, eliminar o degradar el servei a distància? La pregunta no és paranoica: és operativa. Les plataformes digitals han exercit aquesta capacitat repetidament en els últims anys, de vegades per iniciativa pròpia, d'altres sota ordre de Governs, d'altres després de canvis de propietat o de política. Si la capacitat existeix, convé saber sota quins supòsits contractualment declarats s'exerceix, i reservar un marge per als supòsits no declarats que la pràctica dels últims anys ha mostrat igual de rellevants: ordre judicial inesperada, sanció internacional, canvi de govern corporatiu, adquisició per una entitat amb una altra política.

La pregunta germana és la del pla de continuïtat: si l'operador exercís la capacitat contra el professional —per la raó que sigui, justa o no—, quant temps d'activitat continuaria disponible, quin procediment d'exportació de

dades existeix, i a quin proveïdor alternatiu es podria migrar? Si la resposta comença per «no hauria de passar», no és una resposta operativa; és una promesa.

## Capa 5: identitat i accés

Qui controla les credencials d'accés al servei? Si l'operador pot restablir l'accés de l'usuari sense la participació de l'usuari —procediment anomenat típicament «recuperació de compte»—, l'operador és, tècnicament, el custodi del compte i pot també cedir-lo a qui ho sol·liciti mitjançant el procediment adequat. Si l'operador no pot restablir l'accés perquè la identitat resideix criptogràficament en el dispositiu de l'usuari, l'operador tampoc no pot cedir-lo, ni tan sols sota ordre. Les dues modalitats són legítimes segons el context; però, una vegada més, són distintes, i convé saber quina s'està adoptant.

Què passa amb les dades del professional si el professional perd l'accés? Existeixen mecanismes de recuperació —de compte, d'arxiu, de sessió— que depenen de l'operador? Aquests mecanismes són compatibles amb la deontologia professional del sector si l'operador és coaccionat per usar-los?

## Capa 6: futur

Aquesta última capa sol descurar-se perquè exigeix projecció. Què passaria si el servei fos adquirit per una altra empresa? Gairebé totes les adquisicions porten aparellada una revisió dels termes del servei en els mesos següents. Què passaria si les exigències regulatòries canviessin? El dret europeu ha incrementat les obligacions de retirada i bloqueig des de 2022, no les ha reduït. Què passaria si l'operador desaparegués? Una part significativa dels serveis al núvol no té un pla de sortida documentat per a l'escenari de tancament de l'operador; el professional descobreix el problema quan ja no hi ha temps de preparar-lo.

Hi ha una formulació que convé retenir per a aquesta capa: les arquitectures que depenen menys de l'operador són més resilients davant de canvis de l'operador. L'autoallotjament en qualsevol de les seves modalitats, la identitat criptogràfica autosobirana, les comunicacions sense servidor pel mig, totes aquestes redueixen la superfície de risc futura mitjançant el procediment de reduir la superfície de dependència present. No l'eliminen; la redueixen.

## La diferència entre estructura i promesa

Si haguéssim de destil·lar el cicle en una sola frase, seria aquesta: les respostes estructurals es mantenen encara que l'operador, l'administració o la legislació canviïn; les respostes per promesa es mantenen mentre qui promet pugui i vulgui mantenir-les. Les dues poden ser correctes en el moment d'adoptar-se. Només una de les dues se sosté independentment del pas del temps i del canvi de les circumstàncies.

Això no significa que cada professional hagi d'exigir respostes estructurals a tots els serveis que adopta. La proporcionalitat continua sent legítima: un full de càlcul per a comptabilitat interna no necessita la mateixa resposta que l'expedient clínic d'un pacient. Significa, sí, que la professionalitat consisteix a saber quin tipus de resposta s'ha acceptat en cada cas, i a haver decidit conscientment que aquest tipus de resposta és proporcional a la dada concreta.

## El qüestionari, ordenat

Dotze preguntes concretes que sintetitzen el cicle, ordenades perquè la resposta a cadascuna informi la següent:

1. El contingut passa per un servidor de l'operador? Si passa: en clar, xifrat amb claus de l'operador, o xifrat amb claus exclusives de l'usuari?
2. Si s'invoca xifratge d'extrem a extrem, on resideixen les claus criptogràfiques? L'operador coneix o conserva alguna part d'elles en qualsevol forma, inclosa la «recuperació»?

3. Quines metadades genera i conserva el servei? Quant de temps? A qui són visibles?
4. Com es finança l'operador? Si el finançament inclou publicitat o monetització de dades, la finalitat declarada cobreix dades de tercers confiades pel professional?
5. Quina és la situació financera de l'operador a tres o cinc anys vista? Hi ha factors que suggereixin un canvi imminent de model (sortida a borsa pendent, ronda de finançament esgotant-se, adquisició probable)?
6. En quina jurisdicció està incorporat l'operador? En quin país estan físicament els servidors? Si difereixen, quina legislació nacional s'aplica al tractament?
7. Què passaria si una ordre d'intel·ligència vàlida en la jurisdicció de l'operador demanés lliurar les meves dades? L'empresa podria complir-la tècnicament?
8. Quina capacitat tècnica reté l'operador per suspendre, bloquejar o eliminar el servei? Sota quins supòsits contractuals? Sota quins supòsits no contractuals històricament documentats?
9. Quin pla de sortida existeix si l'operador exercís aquesta capacitat contra mi, justament o injustament? Hi ha un procediment documentat d'exportació de dades a un proveïdor alternatiu?
10. Qui controla les credencials d'accés? L'operador pot restablir-les sense la meva participació? Això em protegeix o m'exposa?
11. Existeix una alternativa europea, autoallotjada o sense servidor pel mig per a aquesta funció concreta? Quin és el seu cost real, comparat amb el risc avaluat?
12. Si la decisió d'avui fos examinada d'aquí a cinc anys per un inspector, un auditor o un client afectat per una bretxa, l'elecció actual seria defensable amb els arguments disponibles avui, o requeriria disculpar-se per no haver fet preguntes raonables?

Les preguntes no esperen respostes perfectes. Esperen respostes honestes, que l'operador honest sap donar i l'operador menys honest evita formular amb precisió. La diferència operativa entre les dues classes d'operador, ho diem sense dramatisme, sol percebre's llegint a poc a poc les respostes que ofereixen voluntàriament, abans fins i tot d'haver de demanar més.

---

*Amb aquest article tanquem el segon cicle de Cuadernos Lacre. Vam començar amb el deute editorial heretat de Schrems II i acabem amb un qüestionari operatiu. Pel camí hem transitat conceptes —hash, xifratge, identitat— i anàlisis aplicades —kill switch, model de negoci, self-hosting—. La intenció editorial declarada de la publicació no era aclaparar el lector amb la llista exhaustiva de problemes, sinó lliurar-li eines perquè distingeixi, davant de qualsevol servei nou, quina mena de resposta està acceptant. Aquesta distinció —entre arquitectura i promesa— és l'eina. La resta cada professional la posarà al servei de les dades que consideri, en la seva pràctica, dignes de la pregunta.*

## Fonts i lectura addicional


- Aquesta publicació, cicle 2 (maig de 2026) — *Schrems II, cinc anys després*, *Què és realment SHA-256*, *Kill switch i la captura institucional*, *Xifratge d'extrem a extrem explicat de debò*, *El model de negoci com a senyal de confiança*, *Les 24 paraules: què és una identitat criptogràfica*, *Self-hosting com a pràctica professional*. Els set articles sobre els quals descansa aquest qüestionari.
- Reglament (UE) 2016/679 — Reglament General de Protecció de Dades. Marc jurídic de referència per a totes les preguntes que el qüestionari planteja, en particular els articles 5, 6, 25, 28, 32, 33 i el capítol V.
- Comitè Europeu de Protecció de Dades — directrius i dictàmens operatius sobre Schrems II, transferències internacionals, avaluacions d'impacte i responsabilitat proactiva (publicacions 2020-2024).
- Agència Espanyola de Protecció de Dades — sancions publicades 2022-2024 a responsables del tractament per instruments inadequats de transferència o per avaluacions d'impacte formals sense contingut substantiu.
- noyb.eu — Centre Europeu per als Drets Digitals, dirigit per Maximilian Schrems. Repositori públic de denúncies, recursos i anàlisis sobre el compliment real, no aparent, de les normes europees de protecció de dades.


← AnteriorSelf-hosting com a pràctica professionalSegüent →El que una signatura no pot arreglar

## Lectures recents

- Reflexió · 29 de juny del 2026 No ets anònim
- Reflexió · 27 de maig del 2026 El que una signatura no pot arreglar
- Anàlisi · 25 de maig del 2026 Self-hosting com a pràctica professional

Emporta't aquest article on el necessitis.

↓ Markdown ↓ Text pla ↓ PDF

L'arxiu es descarrega al teu dispositiu. Des d'allà pots guardar-lo, importar-lo a Solo2, o compartir-lo on vulguis. Cuadernos no decideix el destí per tu.

Segell de lacre · SHA-256 aec6b4a171f78ea532b6078d15ed566e4c708185ba3aa9e0e97c6964eb397641



Cuadernos Lacre · Una publicació de Menzuri Gestión S.L. ·
escrita per R.Eugenio · editada per l'equip de Solo2.