plan EU



LIBRO BLANCO · OCTUBRE DE 2026

La dependencia digital es un riesgo empresarial

Por qué toda organización europea debe saber dónde están su software, sus datos y sus pagos, y necesita un plan de salida para los servicios de los que no puede prescindir.

RESUMEN

En resumen

Para el correo, los documentos, la contabilidad, los pagos y el alojamiento, las organizaciones europeas dependen en gran medida de servicios de proveedores no europeos. Eso suele funcionar muy bien, hasta que una decisión tomada fuera de Europa hace que un servicio se restrinja, se corte o resulte jurídicamente insostenible.

PUNTOS CLAVE

- **El riesgo no es técnico, sino jurídico y político.** Las leyes, sanciones y normas de exportación del país del proveedor pueden determinar si su servicio sigue funcionando.
- **La mayoría de las dependencias son invisibles.** Están en sus proveedores de servicios y sus subcontratistas, no solo en su propia informática.
- **La regulación ya lo exige.** DORA obliga a las entidades financieras a tener estrategias de salida; NIS2 y el RGPD exigen conocer la cadena; la Data Act facilita el cambio entre servicios en la nube.
- **Cambiar no siempre es necesario; estar preparado, sí.** Un plan de salida para cada servicio crítico marca la diferencia entre una semana difícil y semanas de parálisis.

Este libro blanco describe dónde están esas dependencias, qué mecanismos las convierten en un riesgo, qué exige la regulación y cómo pasar en cinco pasos del conocimiento a un plan de salida viable.

¿Para quién? Consejeros, directivos y responsables de cumplimiento y de TI de organizaciones europeas de todos los sectores, con especial atención a las entidades financieras sujetas a DORA.

1 La dependencia silenciosa

Pregunte a cualquier organización qué software utiliza y la respuesta llega rápido: un paquete ofimático, un programa de contabilidad, un CRM, un proveedor de pagos. Pregunte después dónde funcionan esos servicios, a qué legislación está sujeto el proveedor y qué ocurre si el servicio deja de estar disponible mañana, y se hace el silencio.

Es comprensible. Los servicios en la nube son populares precisamente porque no hay que pensar en ellos. Pero así, en poco tiempo, se ha llegado a una situación en la que la actividad diaria de muchas organizaciones europeas depende de un pequeño número de proveedores de fuera de Europa, sin que nadie lo haya decidido conscientemente.

> **El problema no es que utilice servicios no europeos. El problema es que no sabe qué hacer si desaparecen.**

Un ejemplo que caló

En 2025 se informó ampliamente de que el fiscal jefe de la Corte Penal Internacional en La Haya, tras las sanciones estadounidenses contra la Corte, dejó de tener acceso a su correo en un proveedor estadounidense. Sobre lo ocurrido exactamente hay versiones distintas. Pero para muchas organizaciones el principio se volvió de pronto concreto: la decisión de un gobierno extranjero puede, a través de un proveedor, afectar directamente a una organización europea, aunque esta no haya hecho nada mal.

Lo mismo puede ocurrir por causas menos dramáticas: una subida de precio que hace inasumible un servicio, un producto que se retira, una cuenta bloqueada por un control automatizado o un proveedor que es adquirido.

2 Tres mecanismos detrás del riesgo

La dependencia de un proveedor no europeo se convierte en un riesgo por tres vías. No tienen que ver con la calidad ni con las buenas intenciones del proveedor.

01

Jurisdicción

Un proveedor está sujeto a la legislación del país donde está establecido. La CLOUD Act estadounidense (2018), por ejemplo, permite a las autoridades de EE. UU. solicitar datos a proveedores estadounidenses aunque estén almacenados en Europa. Eso puede chocar con el RGPD.

02

Sanciones y normas de exportación

Los gobiernos pueden obligar a las empresas a dejar de prestar servicios a determinadas personas, organizaciones o países. El proveedor no tiene entonces elección. Para usted, eso puede significar perder un servicio o no poder llegar a un cliente o contraparte.

03

Control técnico

En los servicios en la nube y los dispositivos conectados, el proveedor tiene las llaves técnicas. Actualizaciones, comprobaciones de licencia o la desactivación de funciones pueden hacerse a distancia, con o sin mala intención.

No solo Estados Unidos

El debate suele centrarse en las grandes tecnológicas estadounidenses, porque atienden a la mayor parte del mercado. Pero lo mismo ocurre con proveedores de otros países. Un ejemplo claro son los vehículos conectados, los puntos de recarga, los inversores y otros equipos cuyo software puede actualizarse o desactivarse a distancia. En enero de 2025 Estados Unidos aprobó normas que excluyen el software chino y ruso de los vehículos conectados a partir del año modelo 2027, precisamente por ese motivo. Para las empresas europeas con flotas, logística o instalaciones energéticas, la pregunta es directa: ¿quién puede manejar sus equipos a distancia?

¿Por qué ahora?

Estos riesgos siempre han existido, pero tres tendencias los hacen más urgentes: las relaciones geopolíticas se han vuelto menos previsibles, cada vez más procesos de negocio funcionan exclusivamente en la nube y la regulación europea espera ya que las organizaciones gestionen estos riesgos de forma demostrable.

3 La cadena oculta

Las mayores dependencias a menudo no están en su propia informática, sino en sus proveedores de servicios. Su gestoría, su proveedor de nóminas, su proveedor de TI o su auditor también utilizan software y alojamiento, y esas decisiones usted no las ve.

Ejemplo: la cadena financiera

Una gestora de fondos suele externalizar la administración de los fondos a un administrador especializado, trabaja con un depositario o trustee y con una firma externa de cumplimiento. Cada una de esas partes funciona con sus propios sistemas: un programa de administración, una plataforma documental, un entorno de correo, un proveedor de alojamiento. La gestora sigue siendo la responsable última, pero a menudo no sabe qué partes están fuera de Europa.

ESLABÓN	PREGUNTA TÍPICA QUE QUEDA SIN RESPUESTA
Su organización	¿Qué servicios utilizamos y cuáles son críticos?
Proveedor directo	¿Sobre qué software y qué alojamiento funciona el servicio que nos presta?
Subcontratistas (subencargados)	¿Dónde están los datos y a qué legislación están sujetas estas partes?
Contrato	¿Qué se ha acordado sobre terminación, transferencia de datos y salida?

La respuesta a esas preguntas suele existir, en contratos de encargo del tratamiento, listas de subencargados y cláusulas contractuales, pero está dispersa y cuesta mucho tiempo reunirla. Ahí es precisamente donde falla en la práctica.

Consejo. Pida a sus proveedores más importantes su lista actualizada de subencargados, con el país de establecimiento y la ubicación de los datos. Según el RGPD, un encargado no puede recurrir a un subencargado sin su autorización y debe informarle previamente de cualquier cambio.

4 Qué exige la regulación

Las normas europeas no obligan a nadie a utilizar solo proveedores europeos. Sí exigen que las organizaciones conozcan sus dependencias, gestionen los riesgos y puedan cambiar cuando sea necesario.

NORMA	PARA QUIÉN	QUÉ ES RELEVANTE
DORA Reglamento (UE) 2022/2554, aplicable desde el 17 de enero de 2025	Bancos, aseguradoras, empresas de servicios de inversión, gestoras de fondos autorizadas y otras entidades financieras (solo quedan excluidas las gestoras de FIA meramente registradas)	Registro de todos los contratos de servicios TIC; evaluación de riesgos antes de contratar; estrategias de salida obligatorias para los servicios TIC que soportan funciones críticas o importantes; atención al riesgo de concentración.
NIS2 Directiva (UE) 2022/2555	Entidades esenciales e importantes, entre otros en energía, transporte, sanidad, infraestructura digital y administración pública	Deber de diligencia en la seguridad de la cadena de suministro, incluida la evaluación de proveedores y prestadores de servicios.
RGPD Reglamento (UE) 2016/679	Toda organización que trate datos personales	Transferencias fuera del EEE solo con garantías adecuadas; desde la sentencia Schrems II (2020) debe evaluarse caso por caso si la legislación del país receptor socava esas garantías.
Data Act Reglamento (UE) 2023/2854, aplicable desde el 12 de septiembre de 2025	Clientes y proveedores de servicios en la nube	Derecho a cambiar de proveedor; los costes de cambio se reducen y desaparecen a partir de enero de 2027. Eso hace que un plan de salida sea más viable en la práctica.

Atención. Esta tabla es un resumen simplificado y no constituye asesoramiento jurídico. Las obligaciones exactas que se aplican a su organización dependen de su sector, su tamaño y sus licencias. Para cada norma puede comprobar en las páginas de legislación si le afecta.

5 Del conocimiento al plan de salida

Plan EU trabaja con un enfoque fijo en cinco pasos. Los primeros puede hacerlos usted mismo con el análisis; para la profundización y el plan de salida le acompañamos.

1

Dominio

A partir de su nombre de dominio identificamos los servicios visibles públicamente, como los proveedores de correo y de alojamiento.

2

Sector

Su sector determina qué regulación y qué dependencias típicas son relevantes.

3

Preguntas por área

Preguntas breves de opción múltiple por área: ofimática, contabilidad, pagos, alojamiento, comunicación, proveedores de servicios.

4

Informe

Para cada respuesta, una posición en la escala de riesgo de Plan EU, con explicación y alternativas europeas.

5

Plan de salida y asesoramiento

Un plan paso a paso para cada servicio no europeo. Si lo desea, revisamos contratos, recopilamos las respuestas de los proveedores y acompañamos el cambio.

La escala de riesgo

● Soberano	◐ Controlable	○ Vulnerable	■ Crítico
Proveedor europeo, datos y gestión dentro de la UE.	No europeo, pero no crítico para el negocio o fácil de sustituir.	No europeo e importante para la actividad.	No europeo, crítico para el negocio y difícil de sustituir.

El análisis no guarda datos que no sean necesarios para el informe. Evaluamos situaciones, no proveedores: el informe describe de forma objetiva dónde está establecido un servicio y qué significa para usted. Más información en nuestra metodología.

6 Qué contiene un buen plan de salida

Un plan de salida no es un plan de mudanza. Es una preparación que le permite cambiar cuando sea necesario, de forma planificada o bajo presión. Para cada servicio clasificado como vulnerable o crítico, deje constancia al menos de lo siguiente:

- **Función y responsable.** ¿Qué proceso de negocio depende del servicio y quién es el responsable?
- **Datos.** ¿Qué datos hay, en qué formato puede exportarlos y con qué frecuencia lo hace?
- **Alternativa.** Al menos una alternativa europea, con una estimación aproximada de coste y plazo.
- **Contrato.** Plazo de preaviso, acuerdos sobre transferencia de datos, asistencia en la salida y sus derechos según la Data Act.
- **Escenario de emergencia.** ¿Qué hace en las primeras 48 horas si el servicio desaparece de repente?
- **Dependencias.** ¿Qué otros sistemas o integraciones se detienen también?
- **Revisión.** ¿Cuándo se revisa y se ensaya el plan?

Para decenas de servicios de uso habitual, ese plan ya está listo en nuestros planes de salida.

Cinco cosas que puede hacer este mes

1. Haga una lista de los diez servicios sin los cuales su organización se paralizaría en un día.
2. Anote para cada servicio el país de establecimiento del proveedor y la ubicación de los datos.
3. Pida a sus proveedores más importantes su lista de subencargados.
4. Compruebe si realmente puede exportar sus datos más importantes en un formato utilizable.
5. Haga el análisis en plan-eu.eu para tener una primera visión general.

Fuentes

- Reglamento (UE) 2022/2554 sobre la resiliencia operativa digital del sector financiero (DORA), en particular el artículo 28.
- Directiva (UE) 2022/2555 (NIS2), en particular el artículo 21 sobre la seguridad de la cadena de suministro.
- Reglamento (UE) 2016/679 (RGPD), capítulo V; TJUE, 16 de julio de 2020, C-311/18 (Schrems II).
- Reglamento (UE) 2023/2854 (Data Act), capítulo VI sobre el cambio entre servicios de tratamiento de datos.
- Clarifying Lawful Overseas Use of Data Act (CLOUD Act), Estados Unidos, 2018.

plan EU

PLAN-EU.EU

Acerca de Plan EU

Plan EU ayuda a las organizaciones europeas a identificar sus dependencias digitales y a elaborar un plan de salida viable. Con un análisis en línea, un informe claro y asesoramiento a medida, desde una segunda opinión DORA hasta el acompañamiento en el cambio a una alternativa europea.

plan-eu.eu

info@plan-eu.eu

Plan EU es una iniciativa de Luce Holding B.V. Este libro blanco se ha elaborado con cuidado a partir de información pública disponible en octubre de 2026 y tiene carácter informativo general. No genera derechos y no constituye asesoramiento jurídico, fiscal ni de inversión. Plan EU no es una institución de la Unión Europea.