Flujos e-mail: sobre el papel, todo está bajo control

Cómo los sistemas “que funcionan” ocultan dependencias jurídicas, operativas y estratégicas

Enterprise E-Mail Report 2026 — Soberanía

retarus

Índice

01	Resumen	Pág. 03
02	El control de los flujos: más allá de la percepción técnica	Pág. 05
03	La soberanía cambia de terreno: de lo jurídico a lo estratégico	Pág. 08
04	Alojar los datos en Europa no basta para mantener el control	Pág. 12
05	Un control operativo más fragmentado de lo que parece	Pág. 16
06	Transparencia, presentación de informes y pruebas: la prueba de resistencia del control	Pág. 20
07	El soporte local: una expresión concreta de la soberanía	Pág. 24
08	Flexibilidad o dependencia: la falsa libertad de las arquitecturas de correo electrónico	Pág. 28
09	Por qué las empresas cambian realmente de proveedor	Pág. 32
10	¿Controla realmente sus flujos?	Pág. 37

Resumen

Para la mayoría de las empresas españolas, los flujos de correo electrónico (e-mail) son el engranaje esencial del funcionamiento diario. Pedidos, facturas, contratos, alertas: miles de datos e información circulan a través de flujos invisibles dentro y fuera de la organización... Sin embargo, lo que escapa a la vista también escapa al control. Y ahí es donde aparece el riesgo.

Una encuesta reciente de Researchscape para Retarus revela que el 80 % de las organizaciones considera tener bajo control casi todos sus flujos e-mail. Sin embargo, el 45 % depende de proveedores extracomunitarios y el 56 % teme una exposición de sus datos a legislaciones extraterritoriales como el Cloud Act. Esta diferencia refleja una realidad sencilla: muchas empresas confunden funcionamiento con control.

En realidad, el control de los flujos e-mail suele percibirse a través de elementos visibles: la continuidad de los intercambios, la estabilidad de los sistemas y la ausencia de incidentes importantes. Pero eso es solo la superficie. No dice prácticamente nada sobre el marco jurídico aplicable, la dependencia de proveedores fuera de la Unión Europea o el cumplimiento de los requisitos de reporting.

Sin embargo, con normativas como NIS2 o DORA, ya no basta con implementar dispositivos de seguridad. Ahora las empresas deben demostrar su eficacia, trazar la ejecución y documentar minuciosamente los resultados. El control ya no depende únicamente de la gestión de la infraestructura.

Según la encuesta, el 92 % de las organizaciones considera indispensable disponer de un reporting completo y explotable. La soberanía ya no es un debate ideológico: el 89 % de los encuestados la considera estratégica y el 94 % la ve como un criterio determinante en la elección de proveedores.

Proteger ya no es suficiente. Ahora es necesario poder actuar, demostrar y recuperar el control. El punto de fricción es operativo:

El 61 % de las organizaciones declara poder aplicar sus políticas de forma autónoma. **61 %**

Solo el 49 % indica poder gestionar o migrar sus cuentas sin depender de su proveedor. **49 %**

Estas cifras reflejan una realidad concreta: la capacidad de actuación, como modificar una configuración, evolucionar un flujo o recuperar el control de un perímetro, sigue siendo parcial.

La razón es sencilla: las arquitecturas han explotado en complejidad. Los flujos ya no circulan dentro de un único sistema, sino a través de una superposición de capas: plataformas cloud, aplicaciones de negocio, herramientas internas y servicios de terceros. Cada componente funciona. Pero el conjunto se vuelve más difícil de interpretar, gestionar y evolucionar sin dependencia.

Ahí reside el verdadero desafío. Un entorno puede ser estable en el día a día y, al mismo tiempo, volverse rígido cuando hay que adaptarlo, auditarlo o justificar su funcionamiento. Lo que parece controlado en la operación diaria rara vez supera la primera prueba real.

El control ya no consiste únicamente en hacer circular correos electrónicos. Hoy, controlar significa algo distinto: poder gobernar, verificar y hacer evolucionar los flujos sin una dependencia excesiva.

02

El control de los flujos: más allá de la percepción técnica

El control de los flujos frente a la realidad

Durante mucho tiempo, el control se medía principalmente por la estabilidad técnica: mientras los flujos funcionaran, los filtros resistieran y los incidentes fueran poco frecuentes, el sistema se consideraba bajo control. Ese enfoque ya no es suficiente. Porque hoy un entorno técnicamente estable puede ocultar otras vulnerabilidades: dependencias invisibles, restricciones jurídicas o falta de capacidad de reacción cuando es necesario intervenir.

Esta diferencia de percepción no se debe a una falta de vigilancia, sino al propio diseño de las arquitecturas. Los correos electrónicos transitan a través de una sucesión de capas en entornos híbridos: cloud, aplicaciones de negocio, componentes de seguridad, herramientas internas y sistemas de seguridad superpuestos a lo largo del tiempo. Cada componente es operativo. Pero el conjunto se vuelve más opaco, más rígido y difícil de recuperar bajo control.

El control ya no puede evaluarse por intuición. Las expectativas de las empresas lo confirman:

92 %

El 92 % considera esencial o muy importante disponer de un reporting completo y explotable.

88 %

El 88 % considera esencial o muy importante controlar las reglas que gestionan los flujos e-mail.

88 %

El 88 % desea poder desplegar sus servicios progresivamente con un proveedor europeo.

Así, un sistema aparentemente funcional ya no es suficiente. También es necesario poder gestionarlo y hacerlo evolucionar sin una dependencia excesiva.

Actualmente, el control se juega en tres niveles.

01 El control jurídico

La primera pregunta importante es: ¿qué normas se aplican realmente a los datos y a los flujos? Alojar los datos en Europa ya no basta para garantizar una protección total. Lo que importa es el marco jurídico al que está sometido el proveedor y las condiciones en las que un tercero puede acceder a los datos. En otras palabras: hasta qué punto los datos permanecen protegidos y en qué situaciones dejan de estarlo.

02 El control operativo

La segunda pregunta que debe plantearse es: ¿quién gestiona los flujos? ¿Quién define las reglas? ¿Quién puede modificarlas sin depender de un tercero? En entornos fragmentados, esta capacidad rara vez está en manos de una sola parte. Está dispersa, a veces compartida y, con frecuencia, condicionada. El problema no es tanto el reparto, sino sus consecuencias. Cuando es necesario actuar, aumentan los plazos, se crean dependencias y se reduce el margen de maniobra.

03 Un reporting relevante

La tercera cuestión esencial es: ¿qué datos están disponibles? ¿Pueden explotarse rápidamente? ¿Permiten responder con precisión a una auditoría, una exigencia de cumplimiento o una investigación? La transparencia solo tiene valor si permite aportar elementos fiables, explotables y jurídicamente válidos. Ver no basta. Hay que explicar y demostrar.

03

La soberanía cambia de terreno: de lo jurídico a lo estratégico

La soberanía se convierte en un desafío operativo

La soberanía ha cambiado de naturaleza. Ya no es un principio que defender, sino un margen de maniobra que preservar. La soberanía se incorpora ahora a decisiones concretas: elección del proveedor, nivel de dependencia aceptable, riesgo jurídico, condiciones contractuales, soporte y capacidad para salir de un modelo que se ha vuelto restrictivo.

Las cifras de la encuesta lo confirman:

94 %

El 94 % de las organizaciones indica que la soberanía desempeña un papel clave en la elección de los proveedores.

89 %

El 89 % la considera una prioridad estratégica.

88 %

El 88 % considera esencial que su proveedor esté jurídicamente establecido en Europa.

La soberanía ya no es una bandera. Es una palanca de decisión. Y este cambio no tiene nada de abstracto.

En primer lugar, el marco regulatorio se está endureciendo. Con NIS2, proteger los flujos ya no es suficiente. Las empresas deben justificar sus decisiones, trazar sus prácticas y documentar sus mecanismos a lo largo del tiempo. Ya no basta con cumplir sobre el papel: también hay que poder demostrarlo.

Además, el contexto geopolítico está redefiniendo las reglas jurídicas. El riesgo de quedar sometido a leyes extraterritoriales se vuelve muy real. Alojar los datos en Europa ya no basta para sentirse protegido. Las empresas quieren saber cuáles son las normas realmente aplicables y cuáles son los riesgos de perder el control de sus datos, e incluso de espionaje.

Por último, la realidad operativa alcanza a las arquitecturas. A medida que las capas se acumulan, las dependencias se refuerzan. Proveedores difíciles de cuestionar, contratos rígidos y soporte remoto: todas estas limitaciones, acumuladas, reducen de forma concreta los márgenes de maniobra.

La soberanía se convierte así en un tema tangible. No se limita a la ubicación de los datos. Abarca todo lo que condiciona el control real de los flujos: exposición a jurisdicciones extranjeras, margen de negociación contractual, dependencia del proveedor, calidad del soporte, capacidad para evolucionar la arquitectura y, en última instancia, posibilidad de recuperar el control mediante verdaderas cláusulas de reversibilidad.

En España, esta visión está especialmente marcada. La soberanía se aborda menos como un principio y más como una cuestión pragmática: ¿hasta qué punto la organización conserva el control de sus decisiones, sus datos y sus márgenes de maniobra?

Este cambio de enfoque tiene un impacto concreto sobre el terreno:

Orienta las decisiones de arquitectura hacia modelos más modulares y menos cerrados.

Reconfigura la relación con los proveedores, con una mayor atención a las condiciones contractuales y a la reversibilidad.

También influye en las decisiones de inversión, introduciendo criterios que van más allá del mero rendimiento técnico.

> **La soberanía se convierte así en un criterio de decisión por derecho propio.**

04

Alojar los datos en Europa no basta para mantener el control

La soberanía no depende únicamente del alojamiento

Es una de las ideas preconcebidas más persistentes: creer que alojar los datos en Europa basta para mantener el control. Pero las cifras de la encuesta muestran otra realidad.

56 %

El 56 % de las organizaciones considera probable que leyes estadounidenses puedan obligar a dar acceso a sus datos de correo electrónico.

45 %

El 45 % sigue utilizando soluciones alojadas fuera de Europa.

El problema está identificado, pero todavía no se ha resuelto.

01 El mito de “alojado en Europa”

La creencia común es que, si los datos se almacenan en Europa, están protegidos. En la práctica, la realidad es mucho más compleja. El alojamiento, por sí solo, no determina el marco jurídico aplicable. Un proveedor puede operar infraestructuras en Europa y, aun así, seguir sujeto a obligaciones extraterritoriales. Las organizaciones empiezan a comprender esta amenaza, pero todavía se subestima y la cuestión del alojamiento sigue influyendo de forma predominante en las decisiones estratégicas.

02 La verdadera cuestión: la jurisdicción

La verdadera pregunta es: ¿a qué normas está realmente sometido el proveedor? ¿Quién puede solicitar acceso a los datos? ¿En qué marco jurídico? ¿Con qué obligaciones de respuesta? Son estas respuestas concretas las que determinan el nivel real de protección. El control jurídico no depende únicamente del lugar donde se almacenan los datos, sino de las normas a las que está sujeto el proveedor.

03 Garantías que deben resistir la prueba de la realidad

El 77 % de las organizaciones afirma disponer de garantías contractuales certificadas y verificables relativas a la localización de sus datos, las condiciones de acceso y el marco jurídico aplicable.

77 %

Sin embargo, el 22 % indica que estas garantías siguen siendo parciales.

22 %

En otras palabras: los compromisos existen, pero no siempre cubren todos los escenarios. Y una garantía solo tiene valor si resiste la prueba de la realidad.

Por tanto, la localización noequivale automáticamente a protección.

05

Un control operativo más fragmentado de lo que parece

Más capas, menos control

En las grandes organizaciones, los flujos e-mail no siguen una trayectoria lineal. Circulan por una red cada vez más densa, con desvíos, intersecciones y puntos de congestión. A medida que la arquitectura se enriquece, el control se vuelve más difícil de identificar.

Ahí es donde nace la ilusión de control. Mientras los correos electrónicos circulan, el sistema se considera bajo control. Pero un flujo que funciona no es necesariamente un flujo controlado. Las cifras de la encuesta lo confirman:

61 %

El 61 % de las organizaciones declara poder aplicar sus políticas de forma autónoma.

49 %

Solo el 49 % puede gestionar o migrar sus cuentas sin depender de su proveedor.

En otras palabras: la autonomía existe, pero tiene límites rápidos.

El problema está identificado, pero sigue sin resolverse

01 Una arquitectura más compleja de lo que parece

Sobre el papel, los flujos e-mail parecen estar controlados. En la práctica, utilizan una superposición de sistemas: cloud, ERP, CRM, herramientas internas, soluciones de seguridad, archivos, entornos heredados y múltiples proveedores. Esta complejidad se ha construido con el tiempo, a través de proyectos e integraciones. Y sigue intensificándose con la aceleración de los flujos automatizados procedentes de las aplicaciones de negocio, que multiplican los puntos de paso y las dependencias.

En el terreno, hay una constatación recurrente: las organizaciones subestiman el número real de aplicaciones que envían correos electrónicos y el fenómeno del “shadow IT”. Los proyectos revelan casi siempre la misma realidad: más flujos, más dependencias y más puntos ciegos de lo previsto.

Las fusiones y adquisiciones acentúan todavía más este fenómeno. Cada entidad aporta sus herramientas, sus reglas y sus excepciones. La arquitectura se amplía, pero no necesariamente se simplifica.

02 Dependencias difusas, pero muy reales

En este entorno, el control no desaparece. Se fragmenta. Algunos componentes siguen gestionándose internamente. Otros dependen de proveedores o soluciones de terceros. Sin embargo, la aparente estabilidad oculta a veces una dependencia muy concreta.

Es cuando hay que actuar, cuando las empresas se enfrentan a la realidad: aplicar una regla, ajustar un flujo, migrar un perímetro o gestionar una excepción... Acciones aparentemente simples se vuelven más lentas, más restrictivas y, en ocasiones, dependientes de terceros.

La dependencia no se percibe en el funcionamiento diario. Se revela en el momento en que es necesario recuperar el control.

03 Consecuencias muy concretas en las operaciones

Esta fragmentación no se limita al área de IT. Tiene efectos muy concretos sobre el terreno: aumentan los tiempos de procesamiento, las facturas no llegan, los pedidos se bloquean y la atención al cliente se ralentiza. A esto se suma el tiempo que los equipos dedican a verificar, insistir y corregir.

Tomados de forma aislada, estos problemas parecen menores. Pero acumulados, generan una fricción continua. Lo que parece fluido suele ocultar un coste operativo permanente.

06

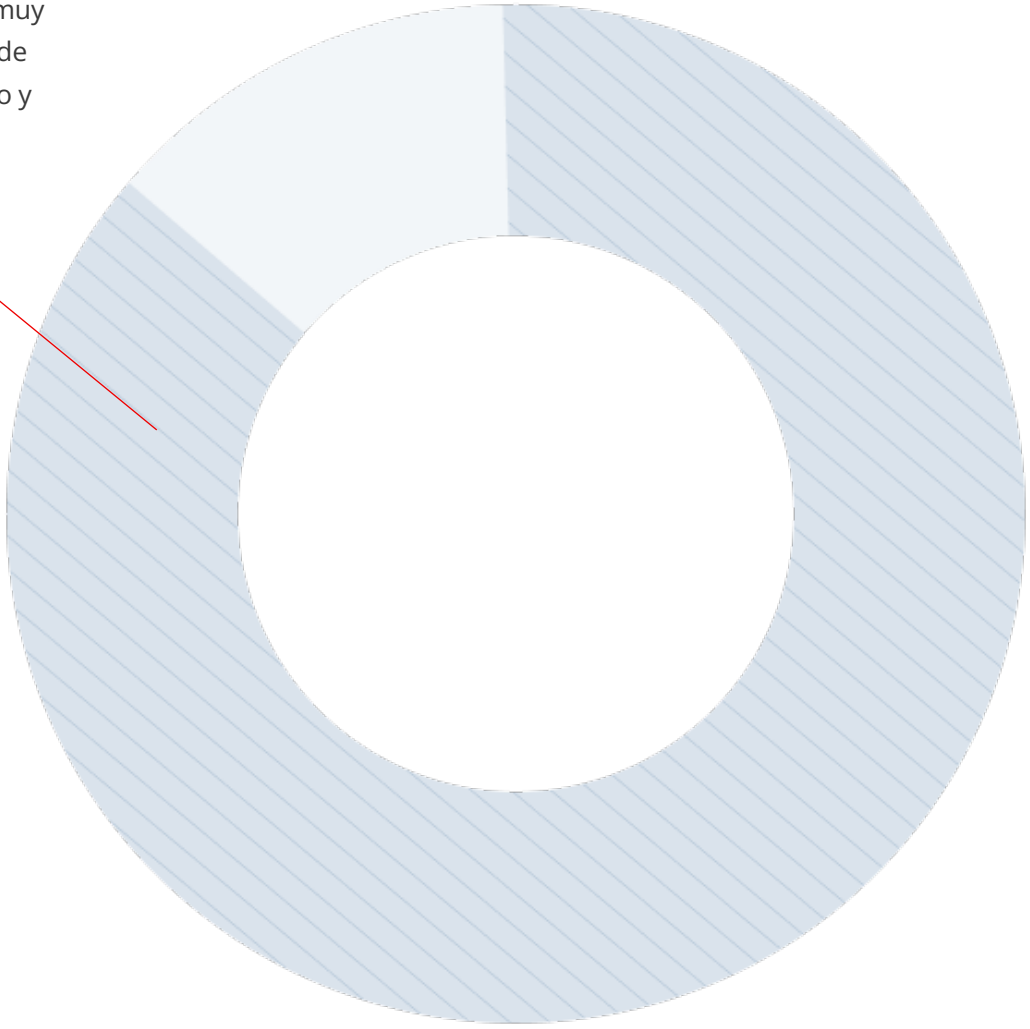
Transparencia, presentación de informes y pruebas: la prueba de resistencia del control

La visibilidad informa. La prueba tranquiliza. La trazabilidad protege.

Explicar, rastrear y demostrar lo cambia todo. La visibilidad informa. La prueba aporta confianza. La trazabilidad protege. Cuadros de mando, métricas, indicadores: la visibilidad se ha convertido en un requisito previo.

92 %

El 92 % de las organizaciones considera esencial o muy importante disponer de un reporting completo y transparente.



01 Ver los flujos ya no es suficiente

Aunque hoy la mayoría de las empresas cree poder supervisar sus flujos de correo electrónico (volúmenes enviados, tasas de entrega, incidentes detectados, alertas de seguridad), estos indicadores solo ofrecen una visión global y permiten identificar rápidamente una anomalía o un aumento del tráfico.

Pero detectar un problema no significa poder resolverlo. También es necesario reconstruir con precisión qué ocurrió, en qué momento y en qué nivel. Ahí reside la diferencia: entre constatar un incidente y ser capaz de explicarlo.

02 El verdadero desafío: la capacidad de demostración

La presión regulatoria sobre el cumplimiento normativo sigue aumentando. NIS2, controles internos, auditorías de clientes: las solicitudes de acceso a los datos se vuelven recurrentes. El 52 % de las organizaciones declara haber tenido que acceder a sus datos o auditarlos entre tres y cinco veces al año.

En estas situaciones, la cuestión es: ¿puede acceder rápidamente a los datos, extraerlos, reconstruir los flujos, contextualizarlos y proporcionar información utilizable?

Una información visible pero difícil de explotar no es suficiente. Tener acceso a los datos no sirve de nada si siguen siendo difíciles de utilizar. Sin acceso rápido, sin trazabilidad clara y sin capacidad para documentar con precisión lo sucedido, no existe verdadera transparencia.

Sin posibilidad de auditoría, no hay control.

03 El momento de la verdad: la auditoría

Sobre el papel, las herramientas de control y auditoría existen.

41 %

Sin embargo, solo el 41 % de las organizaciones afirma ser capaz de responder a una auditoría sin demora.

En los demás casos, necesitan una preparación laboriosa: cruzar datos, reconstruir flujos y verificar información para poder cumplir con sus obligaciones.

En la práctica, esto significa horas dedicadas a localizar un correo electrónico, comprender su recorrido y explicar un incidente bajo presión de plazos.

La visibilidad no tiene valor si no conduce a pruebas utilizables.

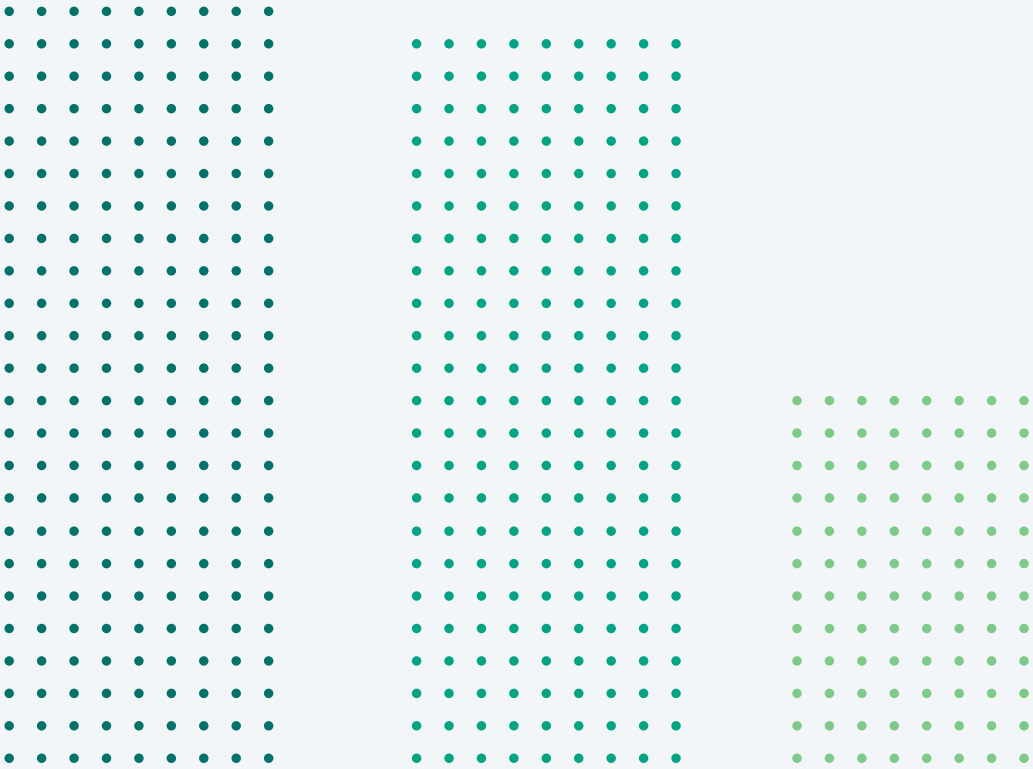
07

El soporte local: una expresión concreta de la soberanía

El soporte se convierte en un asunto de soberanía

El soporte ya no es un simple criterio de calidad de servicio. Ahora influye directamente en la capacidad para gestionar un incidente, ajustar un flujo o tomar una decisión rápida.

Los datos de la encuesta son claros:



84 %

El 84 % de las organizaciones considera esencial o muy importante disponer de un soporte local.

83 %

El 83 % espera un proveedor accesible y reactivo.

46 %

Y cerca del 46 % indica que este criterio puede influir en la decisión de cambiar de proveedor.

Para muchas empresas, la soberanía también se juega ahí: en la capacidad de hablar rápidamente con alguien que pueda actuar.

01 Cuando todo depende del tiempo de reacción

La capacidad de reacción se vuelve realmente visible cuando algo deja de funcionar. Mientras todo va bien, pasa a un segundo plano. Pero en cuanto un flujo se bloquea, una configuración debe modificarse o se produce un incidente, la capacidad de intervenir se vuelve crítica.

En estas circunstancias, ¿cuánto tiempo se necesita para comprender, decidir y corregir? Si cada acción requiere varios intermediarios, varios equipos o distintos husos horarios, los plazos se alargan. Y las consecuencias no son menores.

02 Un incidente, y todo se convierte en una cuestión de coordinación

Los incidentes ya no son una excepción. Pueden surgir en cualquier nivel: seguridad, mensajería, aplicaciones de negocio o servicios de terceros. Identificar el origen del problema requiere poder orientarse rápidamente en este laberinto. Intervenir se convierte en un ejercicio de coordinación. Cuantos más intermediarios haya, más lenta será la resolución. La cuestión clave es: ¿quién puede intervenir y con qué nivel de rapidez?

03 Lo que realmente importa en el momento crítico

Las empresas esperan soluciones muy concretas por parte de su proveedor:

- Poder dirigirse a alguien que conozca el tema.
- Obtener rápidamente una respuesta útil y aplicable.
- Evitar intercambios innecesarios que retrasen la resolución.

Estas exigencias muy concretas permiten contener un incidente, limitar su impacto y mantener la continuidad de los flujos. El soporte local ya no es un valor añadido. Es lo que evita que un incidente común se convierta en un problema costoso.

08

Flexibilidad o dependencia: la falsa libertad de las arquitecturas de correo electrónico

La modularidad no garantiza la independencia

Las empresas no buscan necesariamente sustituir todos sus sistemas de una vez. Quieren avanzar por etapas, según sus prioridades y limitaciones, sin perder el control de su entorno. Los datos de la encuesta lo confirman:

71 %

El 71 % de los encuestados considera fácil modificar o añadir módulos.

49 %

El 49 % indica que la independencia o la flexibilidad influye directamente en su decisión de cambiar de proveedor.

88 %

El 88 % considera esencial o muy importante poder integrar los servicios de correo electrónico de forma progresiva con un proveedor europeo.

76 %

El 76 % de las organizaciones describe su entorno como flexible.

Sin embargo, flexibilidad no significa independencia. La verdadera pregunta es: ¿esa flexibilidad le aporta libertad o solo la ilusión de tenerla?

01 Avanzar por etapas, sin romperlo todo

Las arquitecturas evolucionan ahora de forma incremental. Añadir un componente, activar un servicio o conectar un nuevo uso debe poder hacerse sin una sustitución completa ni un compromiso irreversible. Esta lógica permite convivir con los sistemas existentes, integrar progresivamente nuevos servicios y adaptar las decisiones a las limitaciones presupuestarias y operativas.

02 La flexibilidad no debe reforzar la dependencia

No todas las formas de flexibilidad son iguales. Añadir componentes es una cosa. Poder sustituirlos, reconfigurarlos o desvincularse de ellos es otra muy distinta. Esa es la verdadera diferencia entre una flexibilidad real y una flexibilidad de fachada.

Si cada evolución refuerza la dependencia, si aumentan los costes de salida y si se reducen los márgenes de maniobra, la flexibilidad acaba volviéndose prácticamente imposible.

03 El verdadero riesgo: una trayectoria impuesta

La dependencia del proveedor no aparece en el momento de firmar el contrato. Se instala con el tiempo, a través de decisiones condicionadas, interdependencias entre componentes, complejidad de migración y elevados costes de salida.

A partir de cierto nivel de antigüedad y compromiso, la trayectoria deja de decidirse y pasa a sufrirse. A menudo queda condicionada por las evoluciones técnicas.

Por tanto, la flexibilidad solo tiene valor si va acompañada de una verdadera reversibilidad. Solo así la flexibilidad se convierte en una palanca de control y no en un factor de dependencia.

La flexibilidad sin reversibilidad es un bloqueo encubierto

09

Por qué las empresas cambian realmente de proveedor

La elección de un proveedor se convierte en una elección de control

Las organizaciones no revisan su estrategia de correo electrónico para obtener una funcionalidad adicional. Buscan recuperar el control. Estos son los criterios clave que influyen en la decisión.

01 Soberanía y jurisdicción

La soberanía se impone como un criterio estructurante. El 94 % de las organizaciones indica que influye fuertemente en la elección del proveedor. La soberanía se traduce en cuestiones muy concretas:

¿Hasta qué punto sus datos pueden quedar sometidos a jurisdicciones extranjeras?

¿Qué margen real de negociación tienen sobre las condiciones contractuales?

¿En qué medida pueden actuar sobre sus flujos sin depender completamente del proveedor?

02 Experiencia y soporte local

La proximidad operativa se convierte en un factor clave de decisión. El 84 % de las empresas considera el soporte local como crítico o muy importante. Este criterio refleja una expectativa sencilla: poder actuar rápidamente, sin depender de cadenas de intermediación largas u opacas.

03 Transparencia, reporting, cumplimiento y capacidad de demostración

La capacidad para supervisar, comprender y documentar los flujos adquiere cada vez más peso en las decisiones.

65 %

El 65 % de las empresas indica que las certificaciones de cumplimiento o el acceso a auditorías influyen en su decisión de cambiar de proveedor.

Más allá de las certificaciones, lo determinante pasa a ser la capacidad de proporcionar rápidamente información fiable y verificable.

04 Flexibilidad, independencia y reversibilidad

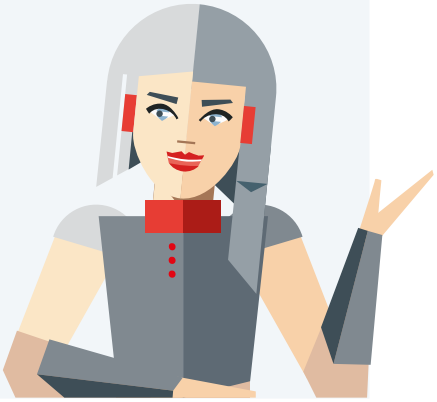
La flexibilidad se convierte en un criterio estratégico:

49 %

El 49 % de las organizaciones indica que la flexibilidad o la independencia respecto al proveedor influye en su decisión.

88 %

El 88 % considera también esencial o muy importante poder integrar los servicios de forma progresiva con un proveedor europeo.



Las empresas no buscan una amplia variedad de opciones, sino la posibilidad de evolucionar sin quedar condicionadas por una arquitectura o por la relación con el proveedor.

05 Una jerarquía implícita de prioridades

Algunos criterios destacan de manera más precisa en la evaluación de las soluciones. La capacidad de reacción y la continuidad bajo control local, así como la aplicación de políticas gestionadas mediante reglas, figuran entre los criterios mejor valorados (con una puntuación media en torno a 2,2).

En otras palabras, la prioridad no es añadir funcionalidades, sino garantizar un funcionamiento fiable, gobernable y coherente a largo plazo.

La elección de un proveedor de correo electrónico es, en realidad, una decisión sobre el grado de control que la organización acepta o rechaza delegar.

10

¿Controla realmente sus flujos?

Evaluar su nivel real de control

En la mayoría de las organizaciones, los flujos e-mail son globalmente funcionales. Los mensajes circulan, los incidentes siguen siendo limitados y los equipos se adaptan. Es en las situaciones donde hay que intervenir cuando todo se vuelve más lento, más opaco y dependiente.

Estas fricciones suelen permanecer difusas. No ponen en cuestión el funcionamiento global, pero se acumulan: tiempo perdido, decisiones retrasadas y dependencias mal identificadas. Por lo general, es al tomar distancia cuando estas fricciones se vuelven visibles. No observando simplemente si “funciona”, sino comparando el nivel de control con el de organizaciones del mismo tamaño y sector, enfrentadas a las mismas limitaciones.

Ese es precisamente el interés de un benchmark. Permite evaluar y situar su nivel de control. Tres dimensiones estructuran este análisis:

- **la exposición jurídica,**
- **el control operativo,**
- **la capacidad de verificación.**

Evalúe su nivel de control

01

Importancia estratégica

- ¿Qué importancia tiene la soberanía del correo electrónico en su organización?
- ¿Hasta qué punto influye en la elección de sus proveedores?

02

Riesgo jurídico (jurisdicción)

- ¿Qué importancia concede al hecho de que su proveedor esté establecido en Europa, especialmente frente a leyes como el Cloud Act?

03

Control operativo

- ¿Hasta qué punto sus flujos de correo electrónico están realmente bajo su control directo?

04

Auditoría, transparencia y capacidad de verificación

- ¿Está en condiciones de realizar una auditoría de cumplimiento sin demora?
- ¿Qué nivel de transparencia y acceso a los datos le ofrece su proveedor?
- ¿Podría proporcionar rápidamente las justificaciones necesarias en caso de una inspección por parte de una autoridad como la CNMC?

05

Flexibilidad y dependencia del proveedor

- ¿Su arquitectura de correo electrónico es flexible?
- ¿Hasta qué punto puede cambiar de proveedor con facilidad?

Estas preguntas ponen de manifiesto el nivel real de control. A medida que aumentan las exigencias regulatorias, operativas y reputacionales, cada área no controlada se convierte en un punto ciego estratégico.

A medida que aumentan los flujos, las arquitecturas se superponen y las exigencias se refuerzan, algunas organizaciones siguen absorbiendo la complejidad. Otras empiezan a percibir sus límites: dependencias difíciles de evitar, falta de visibilidad e intervenciones cada vez más costosas en tiempo y coordinación.

Este punto de inflexión suele ser discreto. Nada se rompe realmente. Pero cada ajuste se vuelve más lento, cada evolución más condicionada y cada incidente más difícil de explicar.

Por lo general, es en ese momento cuando las empresas dejan de soportar la situación y buscan recuperar el control.

El benchmark permite identificar con precisión ese punto. Y, sobre todo, determinar dónde actuar prioritariamente.

También es ahí donde algunas organizaciones evolucionan su enfoque: recuperando el control sobre los componentes críticos de su infraestructura de correo electrónico, reduciendo dependencias y apoyándose en actores capaces de aportar al mismo tiempo claridad jurídica, control operativo y capacidad de demostración. Esa es precisamente la misión de Retarus.

Retarus es un líder mundial en comunicaciones seguras

Desde hace más de 33 años, acompañamos a las empresas frente a la evolución y las exigencias crecientes relacionadas con las soluciones de mensajería y los flujos de datos críticos, especialmente en sectores altamente regulados.

Hemos adquirido una profunda experiencia en mercados internacionales y locales, así como en normativas y requisitos de cumplimiento. Gracias a un enfoque tecnológico preciso y controlado, ayudamos a las empresas a mantener el control de sus comunicaciones críticas.

www.retarus.com/es/

+49 89 5528 0000

C/ Cedaceros nº10, 4ª Izq. 28014 Madrid

retarus