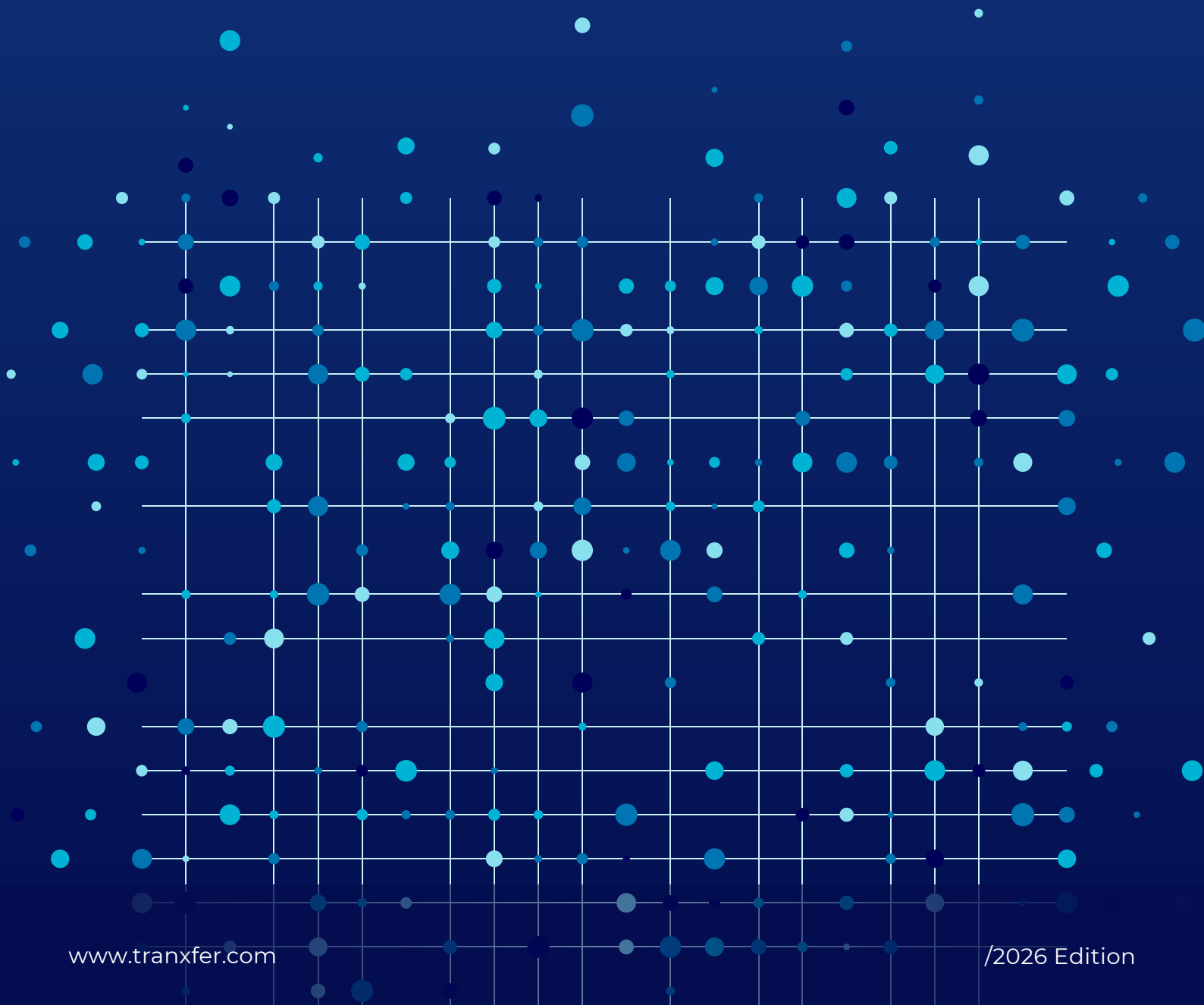
tranxfer

La última milla de la arquitectura SASE

Cómo gobernar el dato en movimiento sin interrumpir el negocio. ***Transición hacia una Infraestructura Unificada de Gobierno del Dato en Movimiento***



Índice

tranxfer

1. Contexto actual

Durante los últimos años, las organizaciones han invertido de forma masiva en arquitecturas SASE, SSE y Cloud Security Platforms para proteger el acceso a aplicaciones y controlar la navegación web.

Las plataformas modernas permiten:

- Controlar acceso a aplicaciones SaaS
- Aplicar políticas de navegación
- Prevenir fuga mediante DLP
- Proteger identidades y endpoints

Sin embargo, incluso en organizaciones con arquitecturas Zero Trust maduras, persiste un último perímetro débil
el gobierno del dato cuando se mueve entre personas, sistemas y organizaciones.

Los intercambios de archivos siguen produciéndose mediante:

- Adjuntos de correo electrónico
- Enlaces compartidos
- FTP heredado
- Plataformas externas de file sharing
- Procesos manuales con terceros

Este problema es estructural.

Diversos estudios muestran que:

94% del malware se distribuye mediante correo electrónico, frecuentemente a través de adjuntos o enlaces.

96% de los ataques de ingeniería social comienzan en el correo electrónico.

94% de los ciberataques exitosos incluyen exfiltración de datos.

Esto refleja una realidad clara:

"el movimiento del dato se ha convertido en uno de los vectores de riesgo más críticos para las organizaciones."

Este documento analiza cómo los CISOs pueden cerrar esta brecha mediante un bundle de seguridad basado en SASE y Secure File Exchange, capaz de gobernar el dato en movimiento sin interrumpir la actividad del negocio.

2. El nuevo perímetro de la ciberseguridad: el movimiento del dato

Durante décadas, la seguridad empresarial se construyó sobre la idea del perímetro. La adopción del cloud y el trabajo distribuido transformó este modelo. Hoy el nuevo paradigma es Zero Trust, donde cada acceso debe ser autenticado y autorizado.

Las plataformas SASE representan la evolución natural de este modelo.

Permiten:

- Proteger el acceso a aplicaciones
- Controlar navegación web
- Aplicar políticas de seguridad en tiempo real
- Prevenir fuga de información

Sin embargo, existe una dimensión crítica que sigue fuera del control estructural: **cómo se mueven los datos entre organizaciones.**

80%

del dato empresarial no estructurado

Este reto es especialmente relevante si consideramos que:

- Más del 80 % del dato empresarial es no estructurado, incluyendo documentos, PDFs, hojas de cálculo o presentaciones.
- Este tipo de información es precisamente la que se intercambia con mayor frecuencia.

Esto convierte al intercambio de archivos en uno de los puntos más sensibles de la arquitectura de seguridad.

3. El problema estructural del intercambio de archivos

El intercambio de archivos es una actividad esencial para el funcionamiento del negocio.

Las organizaciones necesitan compartir información con clientes, proveedores, partners, reguladores, autoridades...

Sin embargo, este intercambio suele realizarse mediante canales fragmentados.

Un estudio de Ponemon muestra que:

- **44 %** de los empleados utilizan herramientas de file sharing en su trabajo diario
- **63 %** de las organizaciones consideran probable haber perdido información sensible en estos entornos

Ponemon INSTITUTE

1. Fragmentación de políticas

Cada herramienta aplica controles distintos o inexistentes.

2. Falta de trazabilidad

Tras un incidente, muchas organizaciones no pueden responder preguntas básicas:

- ¿qué archivo fue enviado?
- ¿a quién?
- ¿cuándo?
- ¿desde qué sistema?

3. Pérdida de control post-envío

Una vez compartido el archivo, el emisor pierde visibilidad sobre:

- descargas
- redistribución
- almacenamiento externo

4. Shadow data exchange

Cuando las herramientas corporativas generan fricción, los usuarios recurren a soluciones externas.

3.1 El reto del intercambio de archivos en cifras

94%	del malware se distribuye mediante correo electrónico, frecuentemente mediante adjuntos o enlaces.	***Fuente:*** *Proofpoint Cybersecurity Report*
96%	de los ataques de ingeniería social comienzan en email.	***Fuente:*** *Proofpoint*
94%	de los ciberataques exitosos implican exfiltración de datos.	***Fuente:*** *Vectra AI Security Research*
44%	de los empleados utilizan plataformas de file sharing en su trabajo diario.	***Fuente:*** *Ponemon Institute*
63%	de las organizaciones creen probable haber perdido información sensible en estas plataformas.	***Fuente:*** *Ponemon Institute*
+80%	del dato empresarial es no estructurado, principalmente archivos y documentos.	***Fuente:*** *IDC / Forbes Tech Council*

4. Limitaciones de las estrategias basadas en bloqueo

Para mitigar estos riesgos, muchas organizaciones aplican políticas de restricción:

- Bloqueo de adjuntos en correo
- Bloqueo de webs de transferencia
- Controles DLP
- Inspección de tráfico web

Estas medidas son necesarias, pero no resuelven el problema.
Bloquear canales de intercambio sin ofrecer alternativas genera tres efectos:

Fricción operativa
Los usuarios necesitan compartir información.

Aparición de Shadow IT
Cuando un canal se bloquea, los usuarios buscan otro.

Falta de gobernanza
Las restricciones no generan un sistema estructural de control. Por tanto, el objetivo no debe ser bloquear el intercambio de información; Debe ser gobernarlo.

tranxfer

5.Aprovechar SASE para habilitar el intercambio seguro

Las plataformas **SASE y SSE** pueden convertirse en una palanca estratégica para habilitar una adopción masiva de intercambio seguro.

Cuando una política detecta situaciones como:

- bloqueo de adjuntos en correo
- intento de subir archivos sensibles
- transferencia de archivos de gran tamaño
- intercambio con dominios externos

la plataforma puede generar **alertas o pop-ups de seguridad.**
Estos pop-ups pueden indicar al usuario que la acción debe completarse mediante un canal corporativo seguro.

Por ejemplo:
"El envío de archivos mediante adjuntos ha sido restringido por política corporativa. Para completar el intercambio de forma segura accede al portal corporativo de transferencia."

El usuario puede entonces continuar la operación mediante una **nueva URL o portal seguro,** autenticándose en una plataforma de intercambio corporativo.

Este enfoque permite:

- mantener la política de seguridad
- evitar la fuga de información
- ofrecer una alternativa inmediata al usuario

En lugar de bloquear el proceso, el sistema redirige al usuario hacia un flujo gobernado. Esto permite una **adopción unificada y masiva de canales seguros de intercambio**, controlados por la organización.

tranxfer

6. Secure Courier Zero Trust

Infraestructura para gobernar el dato en movimiento

Garantizar el Gobierno del Dato en Movimiento
requiere una infraestructura específica.

Una infraestructura Secure Courier Zero Trust permite:

- **Unificar intercambios regulados**
- **Garantizar cumplimiento regulatorio**
- **Generar trazabilidad forense completa**
- **Soportar flujos corporativos de gran volumen**
- **Aplicar control granular sobre el acceso al dato**

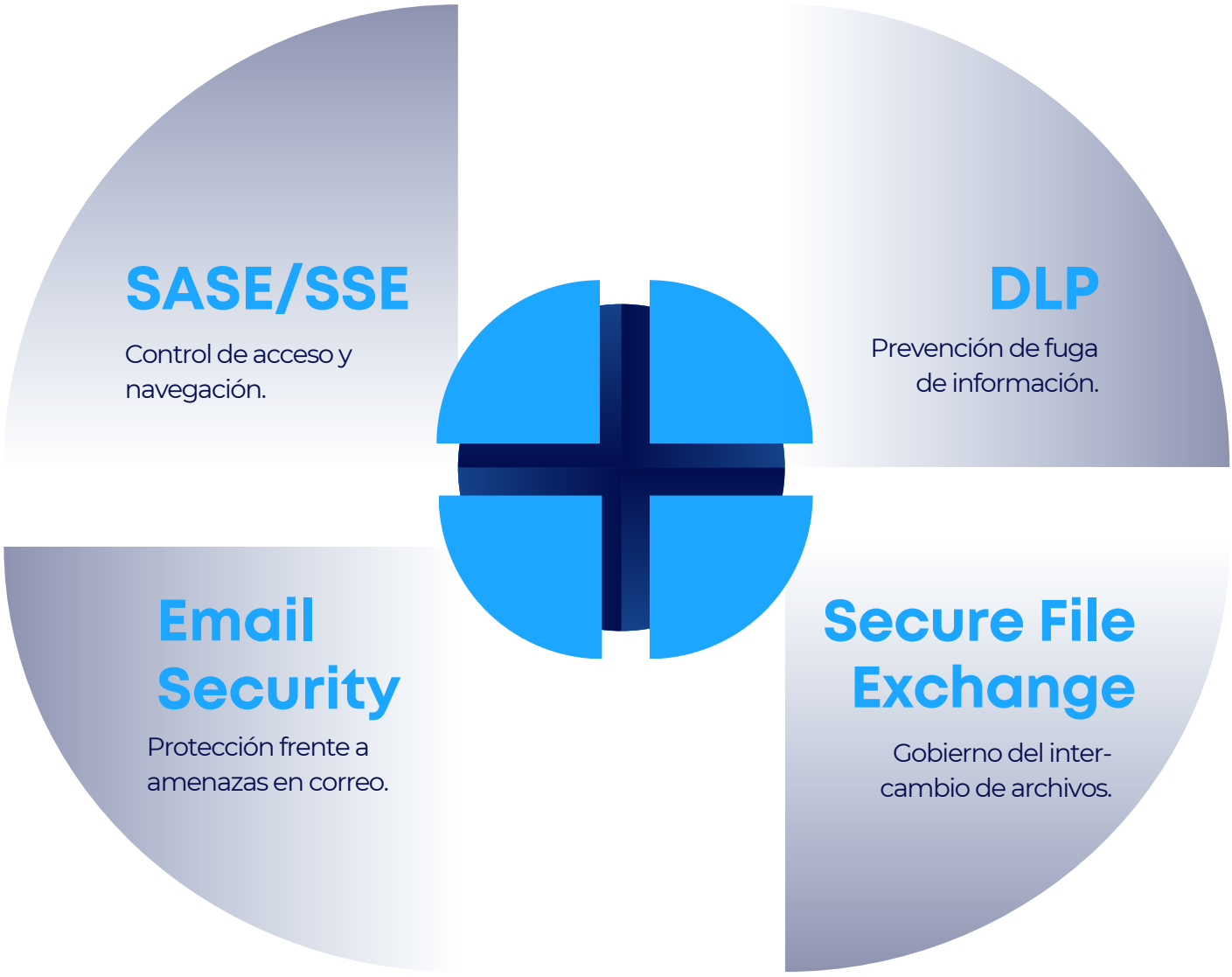
Esta infraestructura permite garantizar el Gobierno del Dato en Movimiento mediante una capa de Secure Courier Zero Trust que unifica intercambios regulados y flujos corporativos de gran volumen bajo una única capa de control, trazabilidad y cumplimiento.

De este modo se soluciona el último perímetro débil de la arquitectura corporativa: El dato en tránsito.

7. El bundle de seguridad que los CISOs deben desplegar

Cerrar la última milla de la arquitectura de seguridad requiere combinar varias capacidades.

Un modelo eficaz se basa en el siguiente bundle:



La combinación de estas tecnologías permite:

- Proteger el acceso
- Controlar navegación
- Prevenir fuga
- Gobernar el movimiento del dato

8. Integración con plataformas SASE y seguridad del correo

Integración con plataformas SASE y seguridad del correo
Las plataformas de Secure File Exchange deben integrarse con la arquitectura de seguridad existente.

Tranxfer, por ejemplo, es compatible con plataformas SASE como:

y soluciones de **Email Security** como:

y otras plataformas equivalentes

Esta integración permite utilizar las políticas de seguridad existentes para redirigir los intercambios hacia canales seguros.

9. Seguridad por diseño y cumplimiento regulatorio

El gobierno del dato en movimiento se encuentra en el centro de múltiples marcos regulatorios:

- NIS2 — Network & Information Systems Directive
- GDPR — General Data Protection Regulation
- DORA — Digital Operational Resilience Act
- ISO 27001 — Information Security Management System
- ens Esquema Nacional de Seguridad — Esquema Nacional de Seguridad

Estas regulaciones exigen:

VISIBILIDAD

TRAZABILIDAD

CONTROL CONTINUO

Una infraestructura diseñada bajo principios de **Security by Design** permite cumplir estos requisitos desde la arquitectura.

10. Impacto estratégico para CISOs

Para los CISOs, gobernar el dato en movimiento representa una de las palancas más eficaces para reducir riesgo.

Permite:

01

Reducir Riesgo Sistémico

Los flujos de datos dejan de depender de canales no gobernados.

02

Extender el modelo Zero Trust

El control se mantiene incluso cuando los datos salen de la organización.

03

Mejorar la respuesta ante incidentes

La trazabilidad permite reconstruir eventos con precisión.

04

Facilitar cumplimiento regulatorio

Las auditorías pueden basarse en evidencia estructurada.

11. Conclusión:

Cerrar la última milla de la arquitectura de seguridad

- Las arquitecturas SASE han transformado la seguridad del acceso.
- Pero la madurez real del modelo Zero Trust exige ir más allá.
- Las organizaciones necesitan gobernar **cómo se mueven sus datos entre personas, sistemas y organizaciones.**
- La combinación de:

SASE y Secure File Exchange permite cerrar esta última milla.

En el nuevo paradigma de seguridad digital:

Gobernar el movimiento del dato es gobernar el riesgo real de la organización.

tranxfer

Comparativa de modelos de intercambio de archivos

¿Porqué el email o los links compartidos no son suficientes?

Característica	Email attachments	Links compartidos (Drive/SharePoint/Dropbox)	Herramientas externas	**Secure File Exchange**
Control de acceso granular	✗ limitado	⚠ parcial	✗ variable	✓ completo
Visibilidad del intercambio	✗	⚠	✗	✓
Trazabilidad forense	✗	⚠	✗	✓
Control post-envío	✗	⚠	✗	✓
Integración con políticas SASE	✗	✗	✗	✓
Cumplimiento regulatorio	⚠	⚠	✗	✓
Gestión de archivos grandes	✗	⚠	⚠	✓
Gobierno del dato en movimiento	✗	✗	✗	✓

tranxfer

El último perímetro débil

Arquitectura de seguridad moderna

Corporate Security Stack

- Identify & Access (IAM / Zero Trust)
- Navigation Security o Web Control (SASE/SSE)
- Endpoint Security
- Email Security
- DLP

DATA LEAVING THE ORGANIZATION

- Files shared with customers
- Files sent to partners
- Regulatory submissions
- Large corporate transfers

Lack Governance Layer

CONCLUSIÓN

La mayoría de organizaciones han invertido en proteger:

- acceso
- navegación
- endpoints
- correo

Pero muchas no tienen visibilidad estructural sobre el intercambio de archivos con terceros.

tranxfer

Evolución de la arquitectura de seguridad

De la seguridad del perímetro al gobierno del dato en movimiento

2000s — Perimeter Security
- Firewalls
- VPN
- Network Segmentation

2010s — Identity Security
- IAM
- SSO
- MFA
- Zero Trust Acces

2020s — Cloud Security
- SASE/ SSE
- CASB
- DLP
- Email Security
- Endpoint Security

NEXT STAGE — Data-in-Motion Governance
- Secure File Exchange
- Traceability
- Secure Collaboration
- Controlled External Flows

CONCLUSIÓN

La seguridad empresarial ha evolucionado desde proteger redes hacia proteger identidades y acceso.

El siguiente paso natural es gobernar cómo se mueven los datos entre organizaciones.

SASE + Tranxfer
Facilita el intercambio seguro

USER ACTION

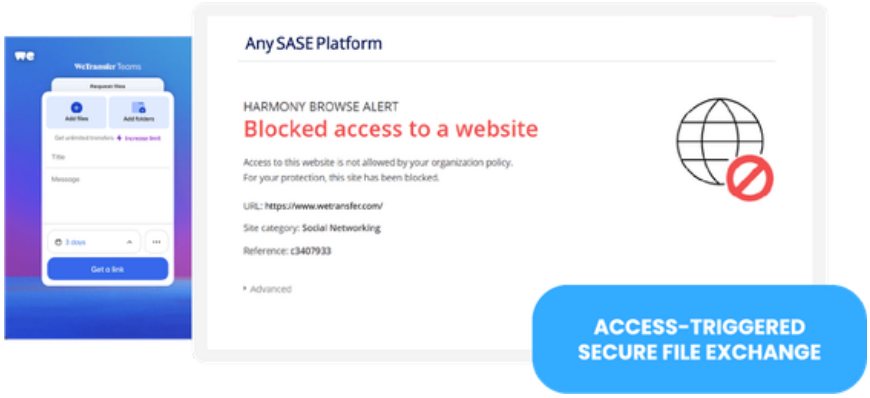
- Attach file to email
- Upload file to external service
- Send large file

SASE / DLP POLICY

- Block attachments
- Restrict external upload

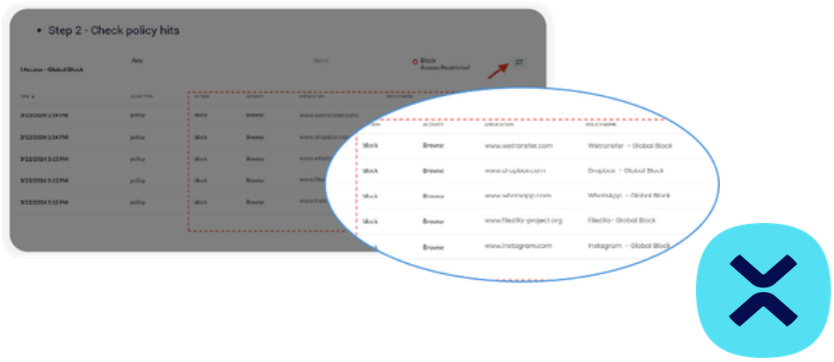
SECURITY NOTIFICATION

"File transfer restricted by corporate policy"



USER REDIRECTED

Access Secure Transfer Portal



SECURE FILE EXCHANGE (Tranxfer)

- Governed transfer
- Traceability
- Access control
- Compliance

CONCLUSIÓN

Las políticas de seguridad no deben bloquear el intercambio.

Deben facilitar el intercambio mediante un canal gobernado.

tranxfer

CISO Self-Assessment

¿Tiene su organización control real sobre el intercambio de archivos?

Sin embargo, la realidad operativa suele ser distinta.

Responda a estas preguntas:

01 ¿Puede saber con precisión qué archivos sensibles se envían a terceros cada día?

- ◯ Sí
- ◯ Parcialmente
- ◯ No

02 ¿Tiene visibilidad completa sobre quién descarga los archivos que su organización comparte externamente?

- ◯ Sí
- ◯ Parcialmente
- ◯ No

03 ¿Puede revocar el acceso a un archivo una vez que ha sido enviado a un partner o cliente?

- ◯ Sí
- ◯ Parcialmente
- ◯ No

04 Cuando se bloquea un adjunto o una subida de archivo, ¿existe un canal seguro alternativo para completar la operación?

- ◯ Sí
- ◯ Parcialmente
- ◯ No

05 ¿Los intercambios de archivos externos generan trazabilidad forense completa?

- ◯ Sí
- ◯ Parcialmente
- ◯ No

06 ¿El intercambio de archivos con terceros está integrado con su arquitectura SASE y DLP?

- ◯ Sí
- ◯ Parcialmente
- ◯ No

Interpretación

Si ha respondido **“No” o “Parcialmente”** a tres o más preguntas, es probable que su organización tenga una **brecha de gobernanza en el movimiento del dato.**

Este es precisamente el punto donde las arquitecturas modernas deben evolucionar.

La mayoría de organizaciones han invertido en:

- proteger el acceso
- controlar la navegación
- prevenir fuga de información

El siguiente paso en la madurez de la arquitectura Zero Trust es: **Gobernar cómo se mueven los datos entre organizaciones.**

tranxfer

ABOUT TRANXFER

Seguridad, trazabilidad y control total en las transferencias de archivos.

Tranxfer es una suite modular de soluciones para la transferencia, recepción, colaboración y almacenamiento seguro de información con terceros, diseñada para entornos corporativos que requieren cumplimiento normativo, control del dato y trazabilidad end-to-end a lo largo de todo el ciclo de vida del archivo.

Gracias a su enfoque modular e integrable, **Tranxfer** permite a las organizaciones proteger su información crítica, reducir riesgos de fuga de datos y optimizar procesos documentales, manteniendo siempre el control sobre quién accede a la información, cómo se utiliza y durante cuánto tiempo.

Más de 10 años siendo la opción de l**as principales entidades bancarias.**

Líderes enbanca de España y Latam

+10mill usuarios

Gartner Peer Insights

Certificaciones y Normativas

Available on cloud **marketplaces**

Microsoft Azure Marketplace · Google Cloud Platform · aws · TD SYNNEX

Secure Access is solved.

Secure Data Movement is the next frontier.

tranxfer

/2026 Edition

www.tranxfer.com