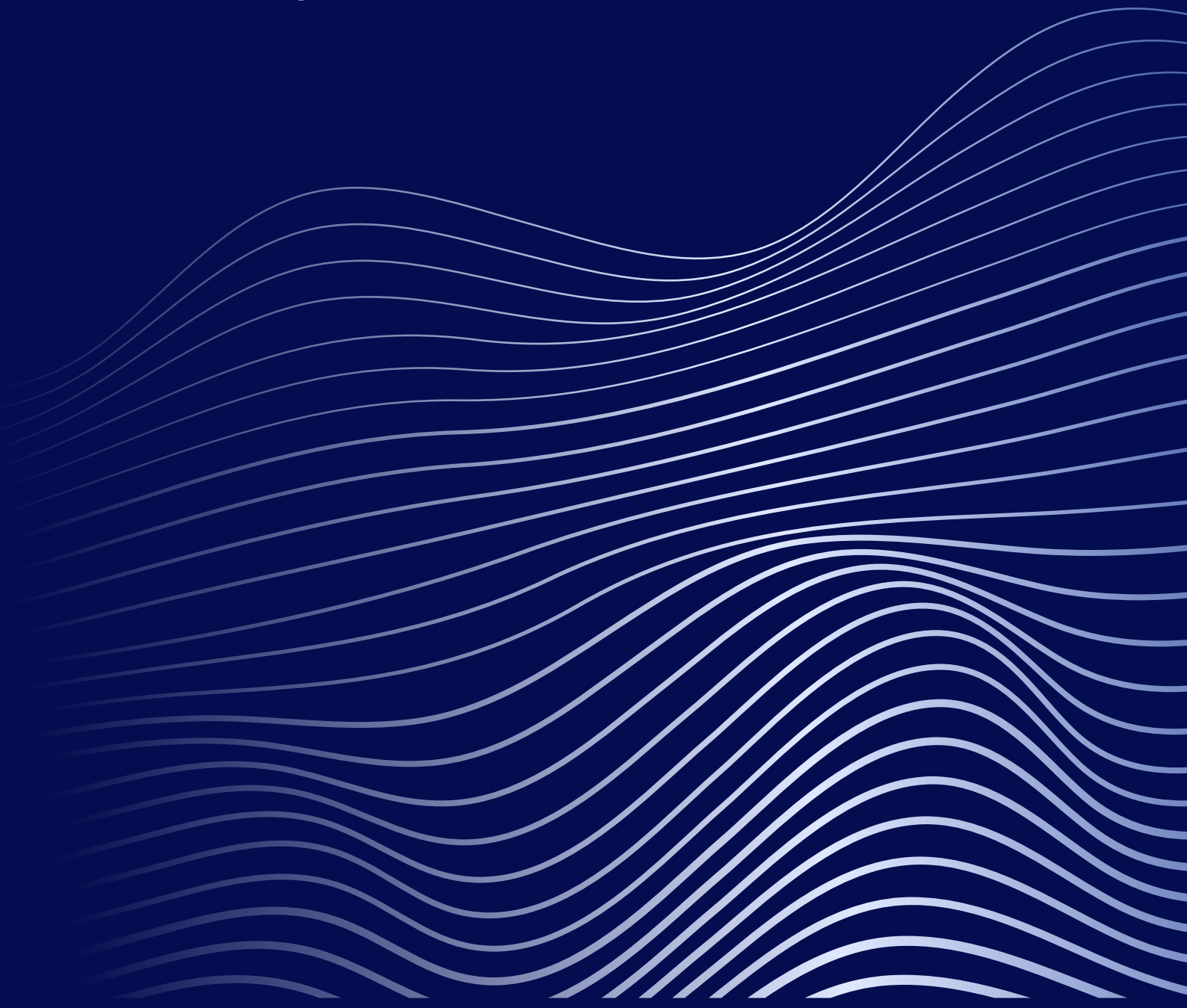
/2026 Edition

tranxfer

Gobernar el dato en movimiento:

El gran reto estructural de la ciberseguridad moderna



www.tranxfer.com

Tabla de contenidos

tranxfer

Las predicciones de Gartner sobre el rol del CISO ante este desafío

Resumen ejecutivo

En un entorno de hiperconectividad permanente, el dato ya no reside: **circula.** Se mueve entre empleados, partners, proveedores, filiales, clientes y plataformas cloud a una velocidad y escala sin precedentes. Sin embargo, mientras las organizaciones han invertido de forma sostenida en proteger el dato en reposo, el **dato en tránsito sigue siendo el gran ángulo muerto de la ciberseguridad moderna.**

Hoy, **más del 82% de las brechas de seguridad involucran datos alojados o procesados en la nube**, y una parte significativa de estas brechas se produce **durante la transferencia de información**, cuando los controles tradicionales pierden eficacia y la visibilidad se fragmenta.

Este riesgo se amplifica de forma exponencial con la adopción de inteligencia artificial, tanto defensiva como ofensiva

Gartner®

Según Gartner, para 2030 existirán más de 1 millón de vulnerabilidades documentadas (CVEs), lo que supone un incremento superior al 300% respecto a 2025, impulsado en gran parte por nuevos vectores de ataque asociados al uso de IA.

Este whitepaper analiza por qué el **gobierno del dato en movimiento** se ha convertido en un imperativo estratégico para CISOs y Consejos de Administración, cómo la convergencia regulatoria (NIS2, GDPR, DORA) lo sitúa en el centro de la responsabilidad ejecutiva y qué hoja de ruta deben seguir las organizaciones para abordarlo de forma realista, efectiva y sostenible.

1. Introducción:

Cuando la ciberseguridad deja de ser perimetral

La entrada en vigor plena de la **Directiva NIS2** en octubre de 2024 marca un punto de inflexión histórico en Europa. Por primera vez, la ciberseguridad deja de ser un dominio puramente técnico para convertirse en una **responsabilidad explícita de la alta dirección.**

Sin embargo, en la práctica, muchas organizaciones han abordado NIS2 reforzando controles tradicionales: firewalls, segmentación de red, protección de endpoints, cifrado de bases de datos. Todo ello es necesario, pero insuficiente.

El dato en movimiento —archivos que se envían, comparten, descargan, reenvían o almacenan temporalmente fuera del perímetro— sigue escapando a una gobernanza efectiva.

4,88mill
en 2024

El coste medio de una brecha de datos alcanzó los **4,88 millones de dólares en 2024,** un incremento del 10% interanual. Más allá del impacto económico, el daño reputacional, la interrupción operativa y la pérdida de confianza del cliente son cada vez más difíciles de cuantificar... y de revertir.

2. El problema invisible:

cuando los datos abandonan el perímetro

2.1 La falsa sensación de control

Durante décadas, la ciberseguridad empresarial se ha construido sobre la metáfora del "castillo": proteger el perímetro y asumir que el interior es seguro. Esta mentalidad ya no se corresponde con la realidad operativa. Hoy, los flujos de información atraviesan:

- Herramientas de colaboración cloud
- Transferencias ad-hoc entre empleados y terceros
- Plataformas legacy como FTP
- Servicios externos no siempre gobernados (shadow IT)

En este contexto, la transferencia de archivos se convierte en un vector de ataque silencioso pero extremadamente eficaz. **Gartner predice que, para 2028, los agentes de IA automatizarán el robo de credenciales y la explotación de canales de autenticación, reduciendo en un 50% el tiempo necesario para comprometer cuentas expuestas.**

Cuando estas credenciales se utilizan para acceder a flujos de transferencia no gobernados, el impacto se multiplica sin necesidad de exploits sofisticados.

2.2 La pérdida de visibilidad como multiplicador de riesgo

El riesgo no proviene únicamente de la transferencia en sí, sino de la **pérdida de contexto** asociada a ella.
Diversos estudios muestran que:

- Un porcentaje significativo de archi-vos sensibles es accesible de forma excesivamente amplia

- Muchas organizaciones no pueden responder con precisión a preguntas básicas tras un incidente:
  - ¿Qué datos se transfirieron?
  - ¿A quién?
  - ¿Durante cuánto tiempo?
  - ¿Desde qué ubicaciones?

Esta falta de trazabilidad es especialmente crítica en un entorno regulado.

3. La ecuación de riesgo del dato en tránsito

El dato en movimiento es estructuralmente más vulnerable que el dato en reposo por cuatro factores clave:

01 **Exposición temporal extendida**
Cada transferencia crea una ventana de oportunidad para interceptación o abuso.

02 **Fragmentación de canales**
Email, FTP, plataformas cloud, mensajería... cada canal añade complejidad y debilita la coherencia de las políticas.

03 **Factor humano y shadow IT**
Cuando la seguridad introduce fricción, los usuarios buscan atajos.

04 **Pérdida de control post-envío**
Una vez compartido, el dato puede ser descargado, reenviado o almacenado indefinidamente sin conocimiento del emisor.

A este escenario se suma una amenaza emergente:

Según Gartner, para 2026, los incidentes impulsados por deepfakes generados por IA llevarán a muchas organizaciones a cuestionar la fiabilidad de los sistemas biométricos tradicionales.

La identidad, por sí sola, deja de ser garantía suficiente.

4. El imperativo regulatorio:

NIS2 y la responsabilidad del Board

4.1 De cumplimiento técnico a gobernanza ejecutiva

NIS2 introduce un cambio radical: **la alta dirección es responsable directa del riesgo cibernético.** Esto implica supervisión activa, aprobación de me-didas y capacidad de rendición de cuentas.

Este cambio converge con una transformación más amplia del modelo de defensa:

> **Gartner estima que, para 2030, las soluciones de ciberseguridad preventiva representarán el 50% del gasto en seguridad IT, frente a menos del 5% en 2024, sustituyendo a los enfoques reactivos.**

El gobierno del dato en mov-imiento es una de las palancas más claras para esta transición hacia la prevención.

4.2 Convergencia regulatoria

NIS2 no actúa de forma aislada.
Se superpone con:

GDRP
protección de datos personales

DORA
resiliencia operativa digital en servicios financieros

ISO 27001 / ENS
controles de referencia

El resultado es una exigencia clara sobre los flujos de información sensible:

- **VISIBILIDAD**
- **TRAZABILIDAD**
- **CONTROL CONTINUO**

5. Metadata y documentación:

La infraestructura invisible del control

El gobierno del dato en movimiento no puede sostenerse sin **metadata de calidad.**

Gartner®

Gartner advierte que las organizaciones sin un enfoque de modernización basado en metadata pueden gastar hasta un 40% más en gestión de datos.

Además:

- **Para 2026,** más del 35% de las organizaciones **adoptarán prácticas activas de metadata.**
- **Hasta 2026, la GenAI** reducirá los costes manuales de gestión de datos hasta un 20% anual, habilitando cuatro veces más casos de uso.

Sin metadata, no hay clasificación automática, no hay auditoría fiable y no hay IA segura.

6. Arquitectura de control:

Los cinco pilares del gobierno del dato en movimiento

1.

Cifrado end-to-end como estándar mínimo

2.

Permisos granulares y temporales

3.

Trazabilidad forense completa

4.

Integración con IAM, SIEM y DLP

5.

IA para detección de anomalías

Gartner®

Gartner señala que las organizaciones que utilizan IA en seguridad detectan y contienen brechas hasta 108 días antes que aquellas que no lo hacen.

7. Roadmap ejecutivo para CISOs:

Cómo superar las barreras reales

Barrera 1: Dirección no percibe urgencia

Traducir riesgo técnico en impacto financiero, regulatorio y reputacional.

Gartner indica que en el 52% de las organizaciones los CISOs lideran la definición de la estrategia de riesgo en IA.

Barrera 2: Fricción con el usuario final

Diseñar seguridad usable por defecto.

Gartner advierte que los empleados no priorizan formarse en riesgos de IA y necesitan soporte automatizado y contextual.

Barrera 3: Saturación operativa

Automatizar controles y priorizar prevención.

Gartner destaca que la presión operativa impide a los equipos mantenerse al día de los riesgos emergentes sin automatización.

8. Conclusión:

Gobernar el dato en movimiento es gobernar el negocio

El gobierno del dato en movimiento ha dejado de ser un “nice to have”. Es una **capacidad estructural** que define la madurez real de una organización frente a la ciberseguridad moderna.

Las organizaciones que actúan de forma proactiva no solo cumplen:

- Protegen su reputación
- Reducen riesgo sistémico
- Habilitan colaboración segura
- Construyen confianza digital sostenible

El tiempo de las aproximaciones parciales ha terminado.

La pregunta ya no es si gobernar el dato en movimiento, sino cuándo y con qué rigor hacerlo.

tranxfer

Predicciones de Gartner para CISOs

el nuevo contrato de responsabilidad

El rol del CISO está experimentando una transformación estructural impulsada por la adopción de inteligencia artificial, la aceleración del riesgo y la presión regulatoria. Según Gartner, esta evolución redefine tanto las **prioridades operativas** como la **responsabilidad ejecutiva** del CISO en los próximos años.

Lo que Gartner anticipa para el rol del CISO

Gartner señala que **las demandas operativas continuas en ciberseguridad están alejando a los CISOs** y a sus equipos del tiempo necesario para comprender, evaluar y gobernar los riesgos asociados al uso de IA en la empresa.

Esto obliga a pasar de modelos manuales y reactivos a controles automatizados y preventivos, especialmente en áreas como el dato en movimiento.

Casi el **100%** de los participantes

En el Gartner Cybersecurity Innovations in AI Risk Management and Use Survey 2025 **afirmaron estar involucrados en la gestión de riesgos asociados al uso de IA.**
La gestión del riesgo ya no es opcional ni delegable: es transversal y permanente.

Según Gartner, **los empleados no priorizan la formación para gestionar los riesgos de ciberseguridad asociados a la IA**, y requieren soporte eficiente, contextual y automatizado.

La concienciación tradicional deja de ser suficiente; la seguridad debe integrarse en los flujos operativos por diseño.

Gartner advierte que los **métodos convencionales de gestión del riesgo cibernético no se adaptan** a la naturaleza dinámica y probabilística de la IA y la GenAI.

Los modelos estáticos de control y cumplimiento no escalan frente a flujos de datos automatizados y decisiones algorítmicas.

Gartner **identifica una falta crítica de visibilidad de los equipos de seguridad** sobre las decisiones de riesgo independientes que toman usuarios, desarrolladores y propietarios de IA en la organización.

Esto amplifica el riesgo en entornos donde los datos se mueven libremente entre sistemas, equipos y terceros.

La investigación de Gartner muestra que, en el **52%** de las organizaciones.

Los CISOs son los principales responsables de definir la estrategia de gestión de riesgos de IA y de establecer los controles de ciberseguridad como miembros de los comités de gobernanza de IA.

El CISO se consolida como figura clave entre tecnología, riesgo, cumplimiento y dirección.

Implicación directa para el gobierno del dato en movimiento

Estas predicciones convergen en una conclusión clara:
El gobierno del dato en movimiento se convierte en una de las pocas palancas reales que permiten al CISO escalar control sin escalar fricción ni carga operativa.

Para los CISOs, esto implica:

- **Pasar de concienciación a control sistémico**
- **De detección reactiva a prevención automatizada**
- **De seguridad explicada a seguridad integrada**
- **De responsabilidad técnica a responsabilidad ejecutiva demostrable**

En el nuevo contexto descrito por Gartner, **gobernar cómo se mueven los datos es gobernar el riesgo real de la organización.**

tranxfer

Recursos

- Directiva NIS2 - Sitio oficial de la Comisión Europea
- ENISA - Guía técnica de implementación NIS2
- ISO/IEC 27001:2022 - Gestión de Seguridad de la Información
- CCN-CERT - Esquema Nacional de Seguridad
- Tranxfer - Descubre cómo gobernar tus datos en movimiento

tranxfer

/2026 Edition

www.tranxfer.com