



**Reduzca el riesgo cibernético y, al mismo tiempo, incremente la velocidad de cierre de operaciones de fusiones y adquisiciones en servicios financieros.**

# Introducción

La completa plataforma nativa en la nube de Zscaler conecta de forma segura todos los elementos, simplifica la experiencia del usuario y su incorporación, y reduce la carga de implementación y operación, al tiempo que protege de forma integral los activos frente a las ciberamenazas, de modo que la empresa pueda llevar a cabo operaciones de fusiones, adquisiciones o desinversiones con mayor volumen, velocidad y confianza.

## Retos para las fusiones, adquisiciones y desinversiones en los servicios financieros

El sector bancario, de servicios financieros y de seguros (BFSI) está siendo testigo de amplios cambios que están alterando sus modelos de negocio y, en algunos casos, amenazando su propia existencia. Las bajas tasas de interés, la supervisión regulatoria y una política monetaria incierta combinadas con cambios masivos inducidos por la transformación digital, como las finanzas descentralizadas y FinTech, han hecho que las organizaciones del sector BFSI prioricen estrategias de crecimiento inorgánico, especialmente en los casos en que sus capacidades tecnológicas están rezagadas.

Las fintech con modelos de negocio maduros se están volviendo cada vez más activas en las transacciones. Están surgiendo ocho categorías de transacciones, entre las que se incluyen las siguientes:

1. Banca digital (por ejemplo, la adquisición de EVEN por parte de MoneyLion por 440 millones de dólares)
2. Pagos (por ejemplo, la adquisición de Nets por parte de Mastercard por 3200 millones de dólares)
3. Compre ahora y pague después (BNPL) (por ejemplo, la adquisición de Afterpay por parte de Square para 29 000 millones de dólares)
4. Préstamos (por ejemplo, la adquisición de Truebill por parte de Rocket Companies por 1300 millones de dólares)
5. Gestión patrimonial (por ejemplo, la adquisición de Nutmeg por parte de J. P. Morgan Chase)
6. Seguros (por ejemplo, la adquisición de Metromile por parte de Lemonade para \$500 millón)
7. Plataforma Fintech (por ejemplo, la adquisición de tink por parte de Visa para 2200 millones de dólares)
8. Finanzas descentralizadas (por ejemplo, la adquisición de Blockrize por parte de Gemini)
9. Consolidación de bancos regionales (por ejemplo, la adquisición de First Midwest por parte de Old National Bank por 2500 millones de dólares)

La tesis del acuerdo para las transacciones mencionadas anteriormente parece ser la siguiente:

1. Una gran organización consolidada del sector BFSI que adquiere una empresa Fintech para incorporar capacidades de plataforma impulsadas por la tecnología (por ejemplo, un algoritmo patentado o modelos de ciencia de datos)
2. Una Fintech en crecimiento adquiere otra Fintech para consolidar su posición de liderazgo

Para que la actividad de fusiones y adquisiciones produzca los resultados esperados, los responsables de las operaciones y los directivos deben abordar de forma proactiva aquellas áreas que puedan afectar negativamente a la valoración estimada y a las sinergias.

### **Desequilibrio en la pila tecnológica.**

Las organizaciones del sector BFSI han desarrollado, en las dos últimas décadas, una compleja combinación de sistemas tecnológicos que ha generado una importante deuda técnica. Muchas han adoptado tecnologías digitales sin prestar suficiente atención a la acumulación de deuda técnica y funcional. Esto puede derivar en un riesgo considerable durante las operaciones de fusiones y adquisiciones, ya que resulta difícil evaluar la postura de riesgo de la organización con la que se fusionan. En consecuencia, las organizaciones nunca logran alcanzar las sinergias de ingresos y de costes estimadas.

Las políticas de seguridad de la información de las grandes organizaciones establecidas para una arquitectura de seguridad basada en el perímetro de red tradicional pueden no aplicarse a las Fintech que nacen en la nube. Por ejemplo, una gran institución financiera norteamericana que opera con una arquitectura de seguridad de castillo y foso (por ejemplo, firewalls, VPN) ha tenido dificultades para integrar la plataforma tecnológica nativa de la nube de sus adquisiciones de Fintech, lo que ha dado como resultado una mala experiencia para el usuario final.

### **Amenazas de ciberseguridad y vulnerabilidad de datos.**

Los problemas de ciberseguridad y vulnerabilidad de datos suelen surgir tras el anuncio de cualquier transacción inorgánica, ya que los actores maliciosos buscan capitalizar durante este ambiguo período de transición, cuando los empleados son especialmente vulnerables. En las organizaciones de BFSI, la exigencia de asegurar rápidamente los datos, procesos y ecosistemas regulados de las sedes y los socios es fundamental para cumplir con las normativas y evitar titulares desfavorables. Además, la falta de un proceso exhaustivo de diligencia debida para comprender la postura de riesgo de las empresas adquiridas puede convertirse en una pesadilla regulatoria para las empresas de este sector. Por ejemplo, PayPal tuvo que suspender los servicios de TIO Networks nueve meses después de su adquisición debido a una filtración masiva que no se detectó ni reportó a tiempo.

Según un informe publicado por Kroll, el 13% de todos los ataques cibernéticos se centran en el sector BFSI, que incluye ransomware, ingeniería social y compromiso del correo electrónico empresarial.

### **Zscaler ayuda a que las integraciones de fusiones y adquisiciones se realicen de forma más segura y rápida.**

Zscaler ofrece un enfoque moderno para las integraciones y separaciones en operaciones de fusiones, adquisiciones o desinversiones, basado en el concepto de Zero Trust Exchange suministrado como servicio en una plataforma completamente en la nube. Zero Trust Exchange de Zscaler conecta de forma segura a los usuarios con sistemas, aplicaciones, dispositivos y entre sí, sin conectar ninguno de estos elementos a la red de la empresa adquirente o segregada. La plataforma ofrece acceso instantáneo a los datos y garantiza la disponibilidad, a la vez que protege la red de la empresa frente a posibles riesgos y amenazas cibernéticas. El resultado es un entorno de integración (sandbox) altamente escalable, seguro y transparente que puede reutilizarse una y otra vez.

### **Obtener valor en semanas en lugar de meses o trimestres.**

Zscaler simplifica el proceso de integración con su Zero Trust Exchange suministrado desde la nube, lo que permite optimizar de forma casi instantánea las arquitecturas de red y la estandarización de la seguridad en todo el entorno. Las empresas que utilizan Zscaler pueden integrar tanto como necesiten, o tan poco como deseen, en lugar de verse obligadas a integrar todo por defecto o a quedar limitadas (en tiempo, rendimiento, coste o experiencia) por las complejidades tecnológicas tradicionales de las fusiones y adquisiciones. La prestación como servicio de Zero Trust Exchange crea desde el primer día un estado futuro de red y seguridad. Totalmente operativo en cuestión de días, Zscaler elimina las barreras para actuar, lo que permite a las organizaciones capturar antes las sinergias de valor.

### **Mitigue y controle los riesgos con una política de seguridad común.**

Zscaler protege activamente a la empresa contra ciberamenazas conocidas y en evolución, así como contra riesgos internos, mediante una plataforma en la nube escalable y fácil de usar. Dado que todo el tráfico puede circular a través de nuestra plataforma, las organizaciones pueden centrarse en la protección de su perímetro y no en la de su tráfico. Zscaler proporciona visibilidad detallada y auditabilidad de todos los accesos de la empresa en un único plano de control, a la vez que identifica y mitiga todas las amenazas de la red.

### **Simplifique la integración y optimice los costes mediante la administración, no la ingeniería.**

La plataforma permite que los equipos de TI y de seguridad conecten de forma segura cualquier dispositivo, aplicación o usuario, independientemente de dónde trabajen, viajen o se conecten. Todo el acceso se concede con un esfuerzo mínimo. Mediante políticas basadas en la lógica empresarial, las organizaciones

pueden controlar, conectar y auditar de forma segura el acceso a aplicaciones, usuarios y cargas de trabajo, sin necesidad de una red privada o de una SD-WAN. Además, las empresas pueden aprovechar el poder de Internet y del mayor intercambio global seguro de datos para transportar el tráfico corporativo, y escalar sin interrupciones bajo demanda a medida que crecen y realizan adquisiciones, o mediante un modelo basado en usuarios o en consumo. No existen límites ni capacidades de hardware que la propia organización deba gestionar.

### **Aumente la agilidad y la flexibilidad de su negocio.**

Al eliminar muchos de los componentes de integración técnica complejos y que consumen mucho tiempo, Zscaler ayuda a convertir las operaciones de fusiones y adquisiciones en procesos altamente repetibles. Zscaler simplifica la integración al permitir que los administradores seleccionen qué sistemas son necesarios y puede ayudar a separar los activos desinvertidos sin recurrir al enfoque de «clonar y listo».

## **Cómo Zero Trust Exchange de Zscaler acelera de forma segura las operaciones de fusiones, adquisiciones y desinversiones**

Zero Trust Exchange es el núcleo de la plataforma Zscaler y permite a las empresas acelerar de forma segura su transformación digital. Exchange amplía los entornos de TI para que los empleados puedan trabajar desde cualquier lugar, manteniendo un estándar de seguridad integral. Permite una mayor conectividad y desacopla la seguridad de la red.

**Simplifique las transformaciones de red.** Exchange evoluciona de un enfoque de concentrador y radio a un modelo directo a la nube. Es un enfoque moderno y simplificado que elimina la mayoría de las dificultades asociadas con las integraciones de red, el hardware y el espacio de direcciones. Proporciona un único plano de control para cualquier estrategia de nube (híbrida, multinube, multiinquilino, multiVPC) y permite el acceso directo a aplicaciones para cualquier programa alojado en cualquier lugar.

**Transforme y modernice la seguridad.** El enfoque tradicional de perímetro de castillo y foso se está reemplazando gradualmente por el modelo de confianza cero. Esta confianza proporciona una conexión segura y directa que reduce las posibles vulnerabilidades para el almacenamiento y la transferencia de datos (en SaaS y nubes públicas) y se aplica a prácticamente cualquier tipo de amenaza de seguridad. Con Zscaler, se puede limitar la capacidad de las amenazas para moverse lateralmente, y la escalabilidad de la plataforma reacciona a las amenazas nuevas y en evolución casi en tiempo real.

**Habilite la fuerza laboral moderna y móvil.** La fuerza laboral actual es móvil y está desconectada de los espacios físicos. Zero Trust Exchange facilita esto al brindar acceso basado en políticas a los usuarios dondequiera que estén, independientemente de su ubicación. Atrás quedaron los días de tunelización en las redes, y los problemas se resuelven de forma proactiva con una estrategia de cambio a la izquierda. La plataforma se puede escalar para satisfacer las nuevas demandas de los usuarios, dondequiera o como sea que accedan a internet.

## Zscaler es la forma moderna de integrar

La capacidad inmediata de compartir procesos y datos sin interrupciones desde cualquier lugar es un factor diferenciador clave que Zscaler aporta a las fusiones y adquisiciones del sector BFSI. La simplicidad de Zscaler permite completar las integraciones en mucho menos tiempo y con mínimas interrupciones para el usuario. Zscaler permite a las organizaciones iniciar rápidamente las actividades de captación de valor, al tiempo que aumenta el volumen de operaciones inorgánicas. Póngase en contacto con nosotros hoy mismo para solicitar una [demostración](#).



Experience your world, secured.™

### Acerca de Zscaler

Zscaler (NASDAQ: ZS) acelera la transformación digital para que los clientes puedan ser más ágiles, eficientes, resistentes y seguros. Zscaler Zero Trust Exchange protege a miles de clientes de los ciberataques y la pérdida de datos mediante la conexión segura de usuarios, dispositivos y aplicaciones en cualquier lugar. Distribuida en más de 150 centros de datos en todo el mundo, Zero Trust Exchange basada en SASE es la mayor plataforma de seguridad en la nube en línea del mundo. Obtenga más información en [zscaler.com/es](https://www.zscaler.com/es) o síganos en Twitter [@zscaler](https://twitter.com/zscaler).

©2022 Zscaler, Inc. Todos los derechos reservados. Zscaler™, Zero Trust Exchange™, Zscaler Internet Access™, ZIA™, Zscaler Private Access™ y ZPA™ son (i) marcas comerciales registradas o marcas de servicio o (ii) marcas comerciales o marcas de servicio de Zscaler, Inc. en los Estados Unidos y/o en otros países. Cualquier otra marca registrada es propiedad de sus respectivos dueños.