Guía para CISO sobre cómo acelerar la migración a AWS con Zscaler Private Access

Cómo Zscaler Private Access (ZPA) facilita la migración segura a la nube y la modernización de aplicaciones en AWS

LIBRO ELECTRÓNICO



©2026 Zscaler, Inc. Todos los derechos reservados.

Índice



Migración a la nube y modernización en 2026 3

El acceso y la seguridad retrasan la migración a AWS 4

Por qué los modelos heredados de VPN y cortafuegos no son adecuados 5

Zero Trust: una mejor opción para la migración a la nube de AWS 6

¿Qué es Zscaler Private Access (ZPA)? 7

Cómo ayuda ZPA en cada fase de la migración a AWS 8

Cómo ayuda ZPA en los escenarios de migración comunes 10

Por qué esto es importante para la modernización y la IA 11

Conclusión 12

©2026 Zscaler, Inc. Todos los derechos reservados.

Migración a la nube y modernización en 2026

En 2026, la migración a la nube ya no es una iniciativa del futuro. Es un imperativo empresarial para toda compañía. Gartner prevé un crecimiento del 21,3 % en los servicios de nube pública este año, impulsado por las organizaciones que aceleran la migración de cargas de trabajo y adoptan la modernización a gran escala. Sin embargo, a pesar de este impulso, el 42 % de las cargas de trabajo estratégicas siguen estando alojadas en las instalaciones de la empresa en la actualidad.

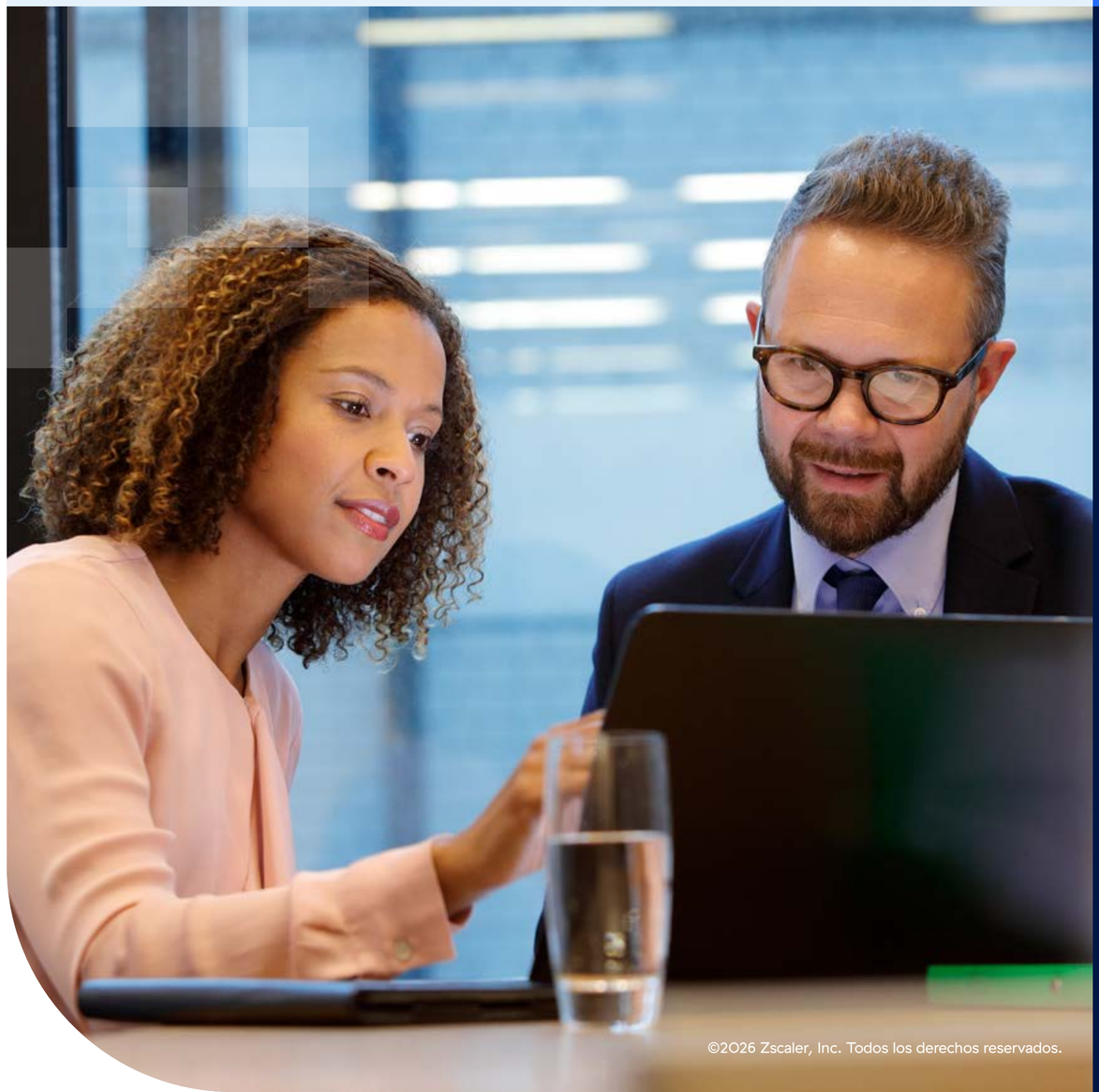
Las cifras cuentan una historia convincente sobre lo que está en juego. Los datos de referencia del marco de adopción de la nube de AWS muestran una reducción del 27 % en el coste por usuario, una disminución del 57 % en el tiempo de inactividad y una disminución del 34 % en los incidentes de seguridad tras la migración. Las organizaciones que participan en el Programa de Aceleración de Migración de AWS alcanzan su primer hito de migración un 41 % más rápido que las que lo hacen por su cuenta. Pero en 2026 el listón se ha puesto aún más alto.

El programa de aceleración de la migración de AWS ahora incluye explícitamente la transformación mediante IA generativa y basada en agentes, junto con la migración tradicional de cargas de trabajo. Migrar a AWS ya no consiste solo en trasladar aplicaciones sin modificar su arquitectura. Se trata de sentar las bases para una empresa preparada para la inteligencia artificial.

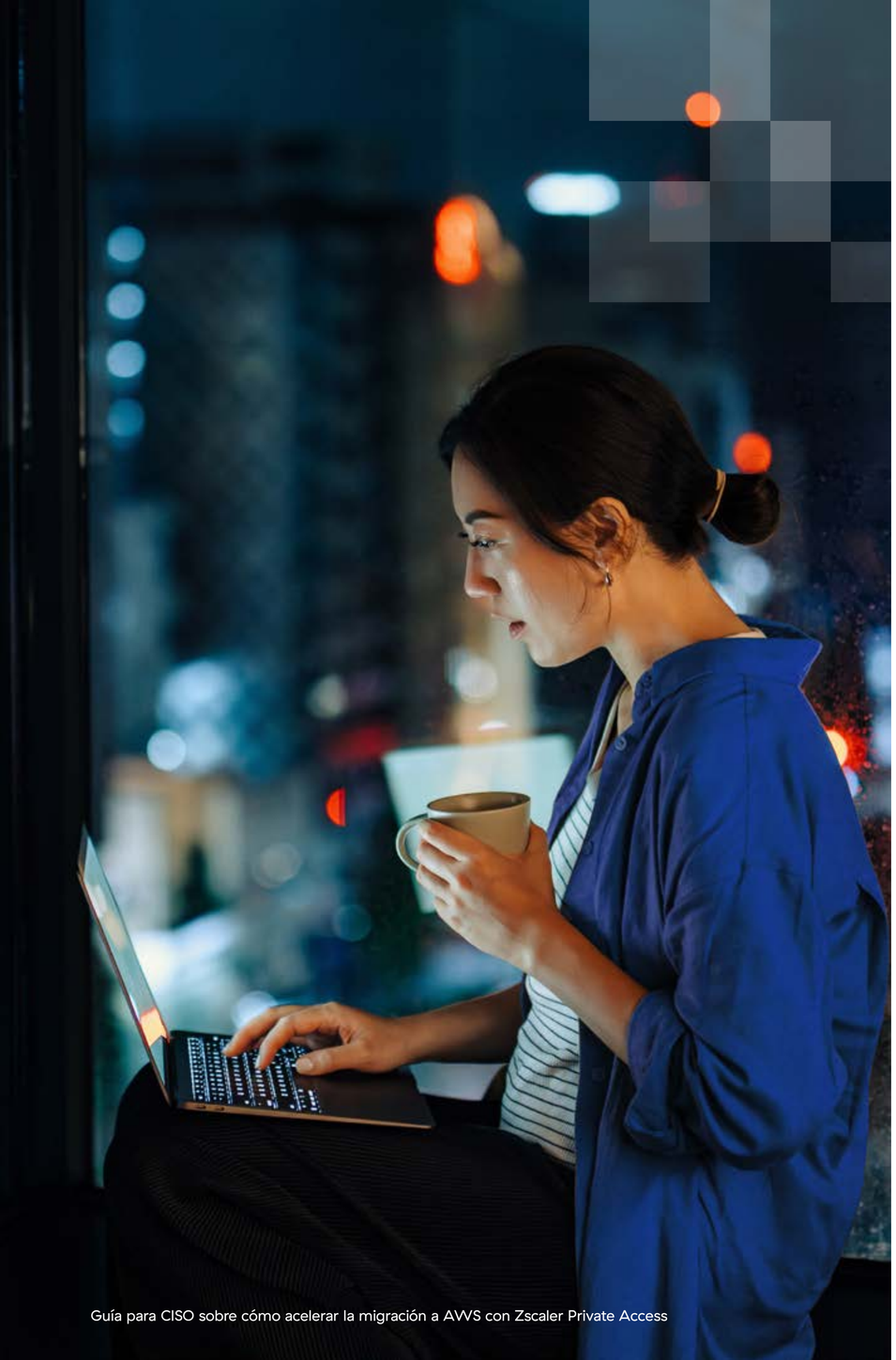
La cuestión ya no es si migrar o no. La clave está en si su arquitectura de seguridad está diseñada para adaptarse a la velocidad que su negocio requiere en la era de la IA.

Sin embargo, muchas migraciones a AWS siguen ralentizándose o retrasándose cuando el acceso seguro se convierte en una limitación. A medida que las aplicaciones se trasladan a través de centros de datos, entornos en la nube y arquitecturas híbridas, las organizaciones suelen considerar el acceso como un desafío de rediseño de la red. Ese enfoque añade complejidad y prolonga los plazos.

Este libro electrónico explora cómo Zscaler Private Access aborda el desafío al reemplazar el acceso remoto centrado en la red con una conectividad basada en la identidad y específica para cada aplicación, y cómo ese enfoque ayuda a reducir la fricción de la migración, respalda la modernización y construye una base más segura para futuras iniciativas de IA a lo largo del proceso de migración a AWS.



©2026 Zscaler, Inc. Todos los derechos reservados.



El acceso y la seguridad retrasan la migración a AWS

Los programas de migración a la nube suelen plantearse como proyectos de aplicaciones e infraestructura. En la práctica, sin embargo, también son proyectos de transformación del acceso y la seguridad. Incluso cuando una carga de trabajo está técnicamente lista para ser transferida, las organizaciones aún necesitan determinar cómo los empleados, contratistas, socios y administradores accederán a ella de forma segura durante la transición. Este desafío suele subestimarse. Los planes de migración pueden tener en cuenta los recursos de computación, el almacenamiento, la arquitectura y las dependencias de las aplicaciones, pero posponen las decisiones sobre el acceso de los usuarios y la segmentación hasta etapas posteriores. Cuando esto sucede, los equipos de seguridad y redes se ven obligados a adaptar los controles heredados a los nuevos modelos de entrega en la nube bajo presión de tiempo. El resultado suele ser la repetición de tareas, retrasos en las aprobaciones y políticas de acceso inconsistentes en los distintos entornos.

Tres cuestiones hacen que esto sea particularmente difícil.

- **En primer lugar,** la migración genera complejidad transitoria. Las aplicaciones rara vez se trasladan de entornos locales a AWS en un solo paso. Lo más frecuente es que las capas de interfaz, middleware y datos se migren en momentos diferentes. Algunos servicios permanecen en el centro de datos, mientras que otros se trasladan a AWS. Durante este período, los usuarios siguen necesitando un acceso fiable y los administradores necesitan visibilidad sobre quién accede a qué.

- **En segundo lugar,** los modelos de acceso tradicionales están estrechamente ligados a la ubicación de la red. Si el acceso depende de la topología de la VPN, las reglas del cortafuegos, los rangos de IP o las suposiciones sobre el enrutamiento interno, cada traslado de una aplicación puede generar trabajo de diseño adicional. Es necesario ajustar las políticas de seguridad, revalidar las rutas de acceso y la experiencia del usuario puede cambiar inesperadamente durante las migraciones.

- **En tercer lugar,** esta complejidad genera riesgos para el negocio. Los retrasos en el diseño del acceso seguro pueden ralentizar los hitos de la migración. Las políticas inconsistentes pueden aumentar la exposición. Una mala experiencia de usuario puede generar resistencia al cambio e incrementar la carga de soporte. En muchos casos, el diseño del acceso se convierte en una dependencia oculta que afecta la velocidad, el coste y la confianza del programa de migración.

Por estas razones, el acceso y la seguridad no deben considerarse como una casilla que se debe marcar al final del proceso. Deben tenerse en cuenta como elementos fundamentales de la estrategia de migración desde el principio. Las organizaciones que lo hagan estarán mejor posicionadas para reducir la fricción, mantener la continuidad y mejorar la seguridad a medida que las cargas de trabajo se trasladen a AWS.

©2026 Zscaler, Inc. Todos los derechos reservados.

Por qué los modelos de VPN y cortafuegos heredados no son adecuados

Las arquitecturas tradicionales de VPN y cortafuegos se diseñaron para extender la confianza en función de la ubicación de la red. Ese modelo podría haber funcionado cuando las aplicaciones se concentraban dentro de un centro de datos corporativo y la mayoría de los usuarios operaban desde un número reducido de ubicaciones de confianza. No se ajusta bien a los programas modernos de migración a AWS.

- **El acceso heredado aumenta el riesgo:** las VPN y herramientas de acceso remoto similares ubican a los usuarios en la red en lugar de limitarlos a aplicaciones específicas. Una vez otorgado el acceso, el usuario o dispositivo puede acceder a amplios segmentos del entorno. Esto incrementa la superficie de ataque y crea oportunidades para el movimiento lateral si las credenciales se ven comprometidas o los dispositivos finales se infectan. En entornos híbridos, el problema se agrava. A medida que las aplicaciones se distribuyen entre entornos locales y en la nube, el amplio acceso a la red dificulta el control preciso sobre qué usuarios pueden acceder a qué cargas de trabajo. La seguridad pasa a depender de capas de segmentación que, a menudo, no fueron diseñadas para un cambio constante.

- **Las arquitecturas heredadas generan costes y demoras:** las reglas de cortafuegos, las listas de control de acceso, los concentradores VPN, las dependencias de enrutamiento y las políticas basadas en IP pueden convertirse en puntos de fricción durante la migración, lo que requiere planificación, coordinación, pruebas y aprobaciones de gobernanza. Durante la migración, estas dependencias pueden multiplicarse, ya que los equipos deben mantener la continuidad del acceso entre los entornos antiguos y nuevos simultáneamente. Muchas organizaciones también operan con múltiples productos de seguridad que han evolucionado con el tiempo. Esto genera fragmentación de políticas y sobrecarga operativa. En lugar de simplificar la migración, la infraestructura de seguridad se convierte en otro dominio que debe conciliarse y reconfigurarse.

- **El enrutamiento heredado degrada la experiencia del usuario:** el acceso remoto tradicional suele depender del enrutamiento de retorno o de la redirección del tráfico a través de ubicaciones centrales de la red antes de que los usuarios lleguen a la aplicación. A medida que las aplicaciones se acercan a los usuarios de la nube, el tráfico puede seguir fluyendo por rutas heredadas ineficientes. El resultado es una mayor latencia, un rendimiento inconsistente y una mayor frustración del usuario. Una mala experiencia de usuario no es solo un inconveniente; puede generar soluciones alternativas, aumentar las solicitudes de soporte y minar la confianza en el proceso de migración.



©2026 Zscaler, Inc. Todos los derechos reservados.



Zero Trust: una opción mejor para la migración a la nube de AWS

La migración a AWS requiere un modelo de acceso que siga al usuario y a la aplicación sin depender de una amplia confianza en la red. Las organizaciones necesitan una forma de mantener un acceso seguro a medida que las aplicaciones se trasladan, las arquitecturas evolucionan y los entornos permanecen híbridos durante períodos prolongados. Ese es el papel que está diseñado para desempeñar un modelo de acceso Zero Trust.

©2026 Zscaler, Inc. Todos los derechos reservados.

¿Qué es Zscaler Private Access (ZPA)?

Zscaler Private Access (ZPA) conecta a los usuarios únicamente con aplicaciones autorizadas, nunca con la red. ZPA verifica la identidad y el contexto, aplica políticas y gestiona conexiones seguras mediante Zero Trust Exchange (ZTE), en lugar de basarse en la ubicación o la confianza por IP. Utilizando marcos de identidad existentes como SAML y MFA, ZPA establece conexiones directas, solo salientes, a través de App Connectors. Este enfoque elimina la necesidad de exponer las aplicaciones a conexiones entrantes, simplificando la arquitectura de seguridad y ocultando las aplicaciones privadas a usuarios no autorizados.

Esta arquitectura transforma la seguridad al desacoplar el acceso de la red. Los usuarios no se conectan a la red y las aplicaciones no quedan expuestas. En cambio, el acceso se concede a nivel de aplicación en función de la identidad y el contexto. Dado que este modelo abstrae el acceso de la infraestructura física o en la nube subyacente, las organizaciones pueden migrar aplicaciones entre centros de datos, VPC y nubes sin necesidad de reconfigurar la conectividad del usuario. En consecuencia, ZPA no solo sirve como solución de acceso remoto, sino también como un elemento clave para la migración a AWS, reduciendo simultáneamente la superficie de ataque y manteniendo el control.

1 App Connector

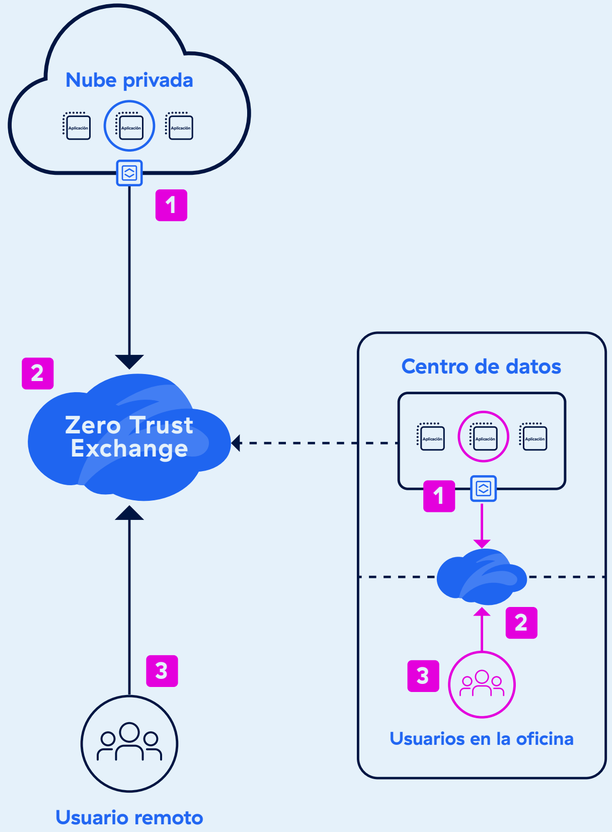
- Desplegado junto a servidores y aplicaciones
- Proporciona una interfaz segura y autenticada entre los servidores de aplicaciones de una organización y la nube de ZPA

2 ZPA Service Edges

- Aplican las políticas de usuario y proporcionan transporte seguro hacia los App Connectors
- Hay Public Service Edges y Private Service Edges disponibles para dar soporte a cualquiera de los dos casos de uso

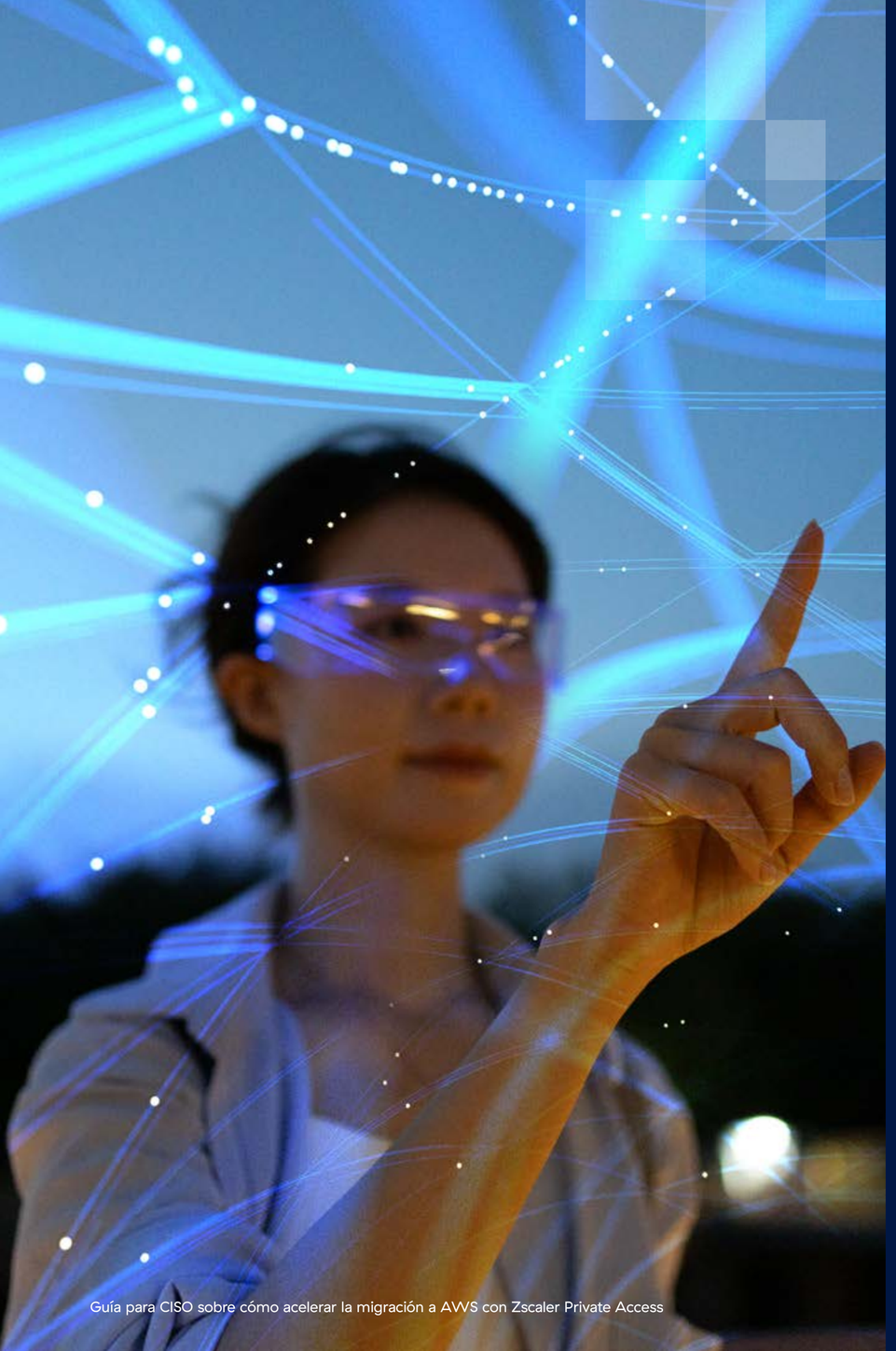
3 Client Connectors

- Una aplicación ligera instalada en su dispositivo
- Garantiza que su tráfico de Internet y el acceso a las aplicaciones internas sean seguros y cumplan las políticas de su organización



Componentes de Zscaler Private Access (ZPA)

©2026 Zscaler, Inc. Todos los derechos reservados.



ZPA ayuda en cada fase de la migración a AWS

Una ventaja clave de ZPA es que da soporte al conjunto de las fases del marco de adopción de la nube de AWS, no solo al estado de acceso final después de que las cargas de trabajo se hayan migrado. Al establecer un modelo de acceso coherente y específico para cada aplicación desde el principio, las organizaciones pueden reducir las fricciones relacionadas con la seguridad en las fases de planificación, transición, puesta en marcha y operaciones continuas.

Fase 1: preparación y planificación

Reto del cliente: Los equipos suelen posponer el diseño de seguridad, asumiendo erróneamente que las VPN y los cortafuegos heredados se extienden fácilmente a AWS. Esto conlleva rediseños costosos cuando los controles heredados no se adaptan al nuevo modelo operativo en la nube.

Cómo ayuda ZPA: ZPA permite el acceso basado en la identidad desde el principio. Al basar las políticas en los usuarios, los dispositivos y las aplicaciones, en lugar de en la ubicación de la red, los equipos pueden definir el acceso y aplicar la autenticación multifactor (MFA) sin esperar a que se concreten los esquemas de direccionamiento IP o las decisiones de enrutamiento. Esto minimiza las interrupciones y la carga de gestión del cambio al mantener los flujos de trabajo habituales de los usuarios.

Resultado para el negocio y la seguridad: Integrar la seguridad como base, en lugar de como un paso posterior, reduce los cambios arquitectónicos de última hora, acelera la planificación y fomenta una mejor alineación entre los equipos de migración y seguridad.

Fase 2: cartera de aplicaciones y descubrimiento

Reto del cliente: Las migraciones a menudo fracasan debido a la visibilidad incompleta del uso de las aplicaciones internas, lo que dificulta determinar qué aplicaciones están activas, sus dependencias y la priorización para la migración.

Cómo ayuda ZPA: ZPA mejora la visibilidad del acceso a aplicaciones privadas y las relaciones entre usuarios, lo que permite a las organizaciones priorizar las cargas de trabajo en función del uso real en lugar de suposiciones. Permite un enfoque por fases, donde se identifican las aplicaciones, se ajustan las políticas y se define la segmentación antes de la migración, minimizando así la exposición y las brechas de políticas durante la transición.

Resultado para el negocio y la seguridad: Las organizaciones logran una planificación más informada, una priorización eficaz de la migración y bases de acceso más sólidas, lo que reduce las sorpresas al detectar las dependencias en las primeras etapas del proceso de migración.



Fase 3: planificación operativa y ejecución

Reto del cliente: La migración de cargas de trabajo a AWS crea entornos mixtos complejos donde las aplicaciones residen en entornos locales, en la nube o en ambos entornos. Adaptar los modelos de acceso a estas arquitecturas cambiantes genera inconsistencia y complejidad operativa.

Cómo ayuda ZPA: ZPA proporciona un marco de políticas coherente, basado en la identidad y la aplicación, independientemente de la ubicación de la aplicación. Los equipos evitan rediseñar el acceso para cada patrón de migración, pasando de la segmentación basada en subredes o IP a un modelo centrado en los derechos y condiciones de acceso del usuario.

Resultado para el negocio y la seguridad:
Planificación operativa simplificada, mayor agilidad en la migración, reducción de las dependencias relacionadas con el acceso y una experiencia de usuario predecible durante toda la transición.

Fase 4: migración y validación

Reto del cliente: Durante la transición, los equipos tienen dificultades para verificar que las migraciones de aplicaciones sean exitosas y seguras sin interrumpir el acceso de los usuarios.

Cómo ayuda ZPA: ZPA desacopla el acceso de la ubicación de la carga de trabajo, lo que permite una migración fluida entre centros de datos y AWS sin que los usuarios tengan que cambiar su forma de conexión. Garantiza que el acceso siga centrado en la aplicación en lugar de en la infraestructura de red, a la vez que proporciona visibilidad fundamental para validar la seguridad y supervisar el comportamiento de las políticas durante la transición.

Resultado para el negocio y la seguridad: Reducción del riesgo de migración y de las interrupciones para los usuarios, a la vez que se mejora la gobernanza. Las organizaciones obtienen la flexibilidad necesaria para trasladar cargas de trabajo sin necesidad de una reconfiguración compleja de la red.

Fase 5: operaciones continuas e inversión futura

Reto del cliente: Tras la migración, las organizaciones necesitan un modelo operativo escalable que admita entornos híbridos sin reintroducir la complejidad de las redes heredadas.

Cómo ayuda ZPA: ZPA facilita la gestión global de políticas por usuario y por aplicación, eliminando la complejidad de la segmentación basada en IP. Permite un control de acceso preciso para empleados, contratistas y terceros en AWS, entornos locales y configuraciones híbridas, garantizando la modernización futura sin necesidad de recurrir a un acceso de red generalizado.

Resultado para el negocio y la seguridad:
Las organizaciones logran un modelo operativo flexible, sostenible y simplificado que respalda la gobernanza y la transformación continuas.

©2026 Zscaler, Inc. Todos los derechos reservados.

Cómo ZPA aborda los escenarios de migración comunes

Los programas de migración varían, desde la migración sin cambios de arquitectura y la modernización parcial hasta los rediseños nativos de la nube. ZPA admite estos diversos patrones de entrega con un paradigma de acceso unificado.

ESCENARIO 1

Migración sin cambios de arquitectura manteniendo las aplicaciones privadas

Muchas aplicaciones, especialmente las cargas de trabajo empresariales complejas, se migran a AWS de forma incremental con cambios arquitectónicos mínimos. En estos escenarios, las capas de interfaz, aplicación y datos pueden moverse por fases. Es posible que algunos componentes permanezcan en las instalaciones durante un tiempo, mientras que otros se trasladan a AWS. ZPA respalda este modelo al preservar el acceso privado y específico de la aplicación durante toda la transición.

Los usuarios continúan conectándose a la aplicación mediante los mismos controles basados en la identidad, incluso cuando cambia la ubicación de alojamiento subyacente. Esto reduce la necesidad de exponer aplicaciones sensibles o de depender de un amplio acceso a la red para preservar la continuidad. Para las organizaciones que trasladan aplicaciones de alto valor o sujetas a controles estrictos, esto puede hacer que la migración sin cambios de arquitectura sea más manejable y menos disruptiva.

ESCENARIO 2

Acceso externo selectivo con controles Zero Trust

Algunas aplicaciones deben ser accesibles a un conjunto más amplio de usuarios por razones comerciales, para usuarios externos, socios, contratistas u otros equipos externos. Con frecuencia, estos usuarios necesitan acceder desde dispositivos que no son gestionados por la organización. En estos casos, las organizaciones desean ampliar el acceso a la propia aplicación, y no a la red, sin exponer la aplicación a internet ni debilitar su nivel de seguridad de datos.

ZPA permite el acceso Zero Trust basado en el navegador, conectando a los usuarios únicamente con la aplicación específica que están autorizados a usar, sin necesidad de un agente en su dispositivo. Los usuarios se autentican a través del proveedor de identidad de la organización, y el acceso se controla mediante políticas basadas en la identidad y el contexto. El acceso se establece mediante una conexión intermediada de adentro hacia afuera entre el navegador del usuario y la aplicación, lo que ayuda a mantener la aplicación oculta de la internet pública.

ESCENARIO 3

Reestructuración nativa de la nube con preservación del acceso privado

No todas las aplicaciones se migran a AWS en su formato original. Muchas se rediseñan para convertirse en servicios nativos de la nube que pueden abarcar EC2, contenedores, funciones sin servidor, bases de datos administradas y componentes de aplicaciones distribuidas. Esto aumenta la flexibilidad arquitectónica, pero también puede dificultar la gestión del control de acceso tradicional basado en la red. ZPA ayuda al mantener el acceso centrado en la identidad y el contexto de la aplicación, en lugar de en la topología de red en constante evolución que hay detrás de la aplicación.

Los sistemas empresariales sensibles, los entornos de desarrollo y las interfaces administrativas pueden seguir siendo accesibles de forma privada mediante políticas granulares, incluso a medida que la arquitectura de la aplicación se vuelve más dinámica. Esto es especialmente relevante para las cargas de trabajo reguladas, las plataformas empresariales y los programas de modernización en los que la seguridad debe evolucionar a la par de la arquitectura, no quedarse rezagada con respecto a ella.

©2026 Zscaler, Inc. Todos los derechos reservados.



Por qué es importante

La migración de cargas de trabajo a AWS forma parte cada vez más de la agenda de modernización más amplia de las empresas. Las organizaciones no se limitan a reubicar su infraestructura; están actualizando las arquitecturas de sus aplicaciones, optimizando sus modelos operativos, adoptando servicios nativos de la nube y expandiéndose a nuevas áreas como las plataformas de datos, la automatización y la inteligencia artificial. Esto aumenta la importancia del diseño de accesos en lugar de disminuirla.

Los entornos modernizados suelen estar más distribuidos que los sistemas a los que sustituyen. Pueden implicar múltiples servicios, procesos de desarrollo, dependencias híbridas y una mayor diversidad de usuarios. En estos entornos, resulta aún más difícil justificar y mantener una confianza amplia centrada en la red. El acceso debe ser más granular, tener más en cuenta el contexto y ser más fácil de gestionar en arquitecturas cambiantes.

Lo mismo ocurre con las iniciativas de IA. A medida que las organizaciones incorporan aplicaciones relacionadas con la IA, entornos de desarrollo y flujos de trabajo de datos confidenciales a AWS, necesitan un control más estricto sobre quién puede acceder a esos recursos, desde qué dispositivos y bajo qué condiciones. Estos entornos suelen involucrar equipos multidisciplinarios, terceros y flujos de trabajo en constante evolución. Por lo tanto, el modelo Zero Trust no es simplemente una mejora de la seguridad; es un requisito de gobernanza que aplica el mismo modelo de acceso específico para cada aplicación en entornos de migración, modernización y entornos relacionados con la IA.

©2026 Zscaler, Inc. Todos los derechos reservados.

Conclusión

La migración a AWS a menudo se ralentiza porque el acceso seguro se convierte en una fuente oculta de complejidad. Cuando los usuarios, las aplicaciones y las políticas siguen vinculados a modelos heredados de VPN y cortafuegos, cada paso de la migración se vuelve más difícil de planificar, validar y escalar.

Zscaler ofrece un enfoque diferente. Al sustituir el acceso centrado en la red por una conectividad basada en la identidad y específica para cada aplicación, Zscaler Private Access (ZPA) ayuda a las organizaciones a reducir la superficie de ataque, simplificar las políticas y mantener una experiencia de usuario más coherente a lo largo del ciclo de vida de la migración. Permite la planificación, el descubrimiento, la entrega, la validación y las operaciones continuas con un modelo que se adapta mejor a los entornos de AWS.

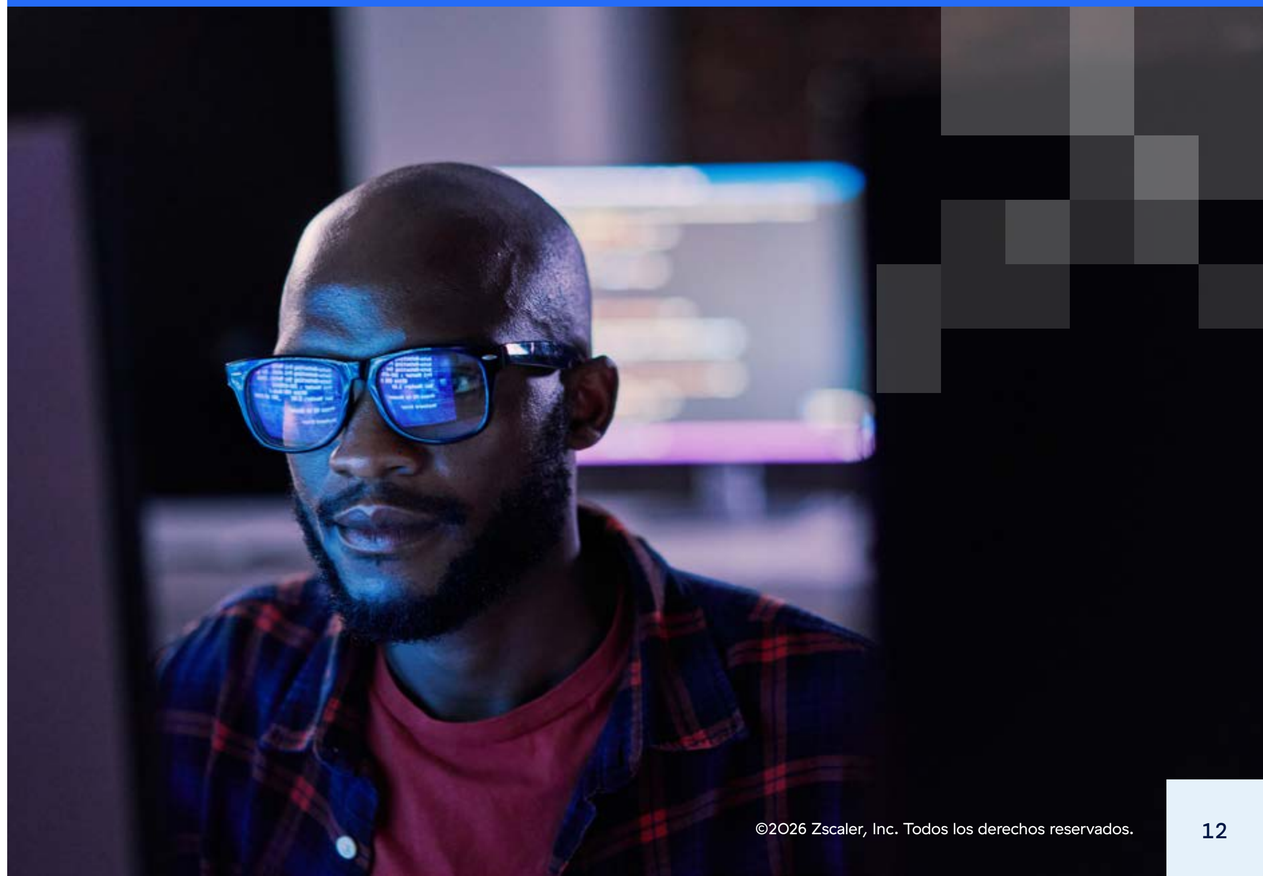
Esto va más allá de la mera migración. A medida que las organizaciones avanzan en la modernización, la transformación nativa de la nube y las iniciativas impulsadas por la IA, la necesidad de un acceso preciso y con privilegios mínimos no hace más que aumentar. Por lo tanto, un modelo de acceso Zero Trust no es solo una mejora de la seguridad. Es un elemento fundamental que permite la agilidad operativa en la nube. Para las organizaciones que migran y se modernizan en AWS, el acceso seguro no debe ser una cuestión secundaria. Debería formar parte de la arquitectura desde el principio. Zscaler ayuda a que eso sea posible.

Fuentes:
Migre a AWS de forma sencilla y segura con Zscaler
Marco de adopción de la nube de AWS
Gartner®
Página de socios de Zscaler para AWS

ZPA está disponible en AWS Marketplace

ZPA está disponible en AWS Marketplace, lo que facilita a las organizaciones la adquisición, implementación y gestión del acceso seguro a las aplicaciones dentro de sus entornos AWS existentes. Para obtener información detallada sobre la solución, solicitar una demostración o consultar las opciones de compra, visite la **página de ZPA en el Marketplace**.

Para obtener más información sobre Zscaler en AWS Marketplace, visite nuestro **perfil de vendedor**.



©2026 Zscaler, Inc. Todos los derechos reservados.

Actúe con rapidez.
Manténgase seguro.

Acerca de Zscaler

Zscaler (NASDAQ: ZS) es pionera y líder mundial en seguridad Zero Trust. Las mayores empresas del mundo, organizaciones de infraestructuras críticas y organismos gubernamentales confían en Zscaler para proteger usuarios, sucursales, aplicaciones, datos y dispositivos, y para acelerar sus iniciativas de transformación digital. Distribuida en más de 160 centros de datos en todo el mundo, la plataforma Zscaler Zero Trust Exchange™, combinada con IA avanzada, combate cada día miles de millones de ciberamenazas e infracciones de políticas y ayuda a las empresas modernas a aumentar la productividad reduciendo los costes y la complejidad.

© 2026 Zscaler, Inc. Todos los derechos reservados. Zscaler™ y otras marcas comerciales enumeradas en **zscaler.com/es/legal/trademarks** 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/u otros países. Cualquier otra marca registrada es propiedad de sus respectivos dueños.

+1 408.533.0288 **Zscaler, Inc. (HQ) • 120 Holger Way • San Jose, CA 95134** **zscaler.com/es**