CLOUDFLARE

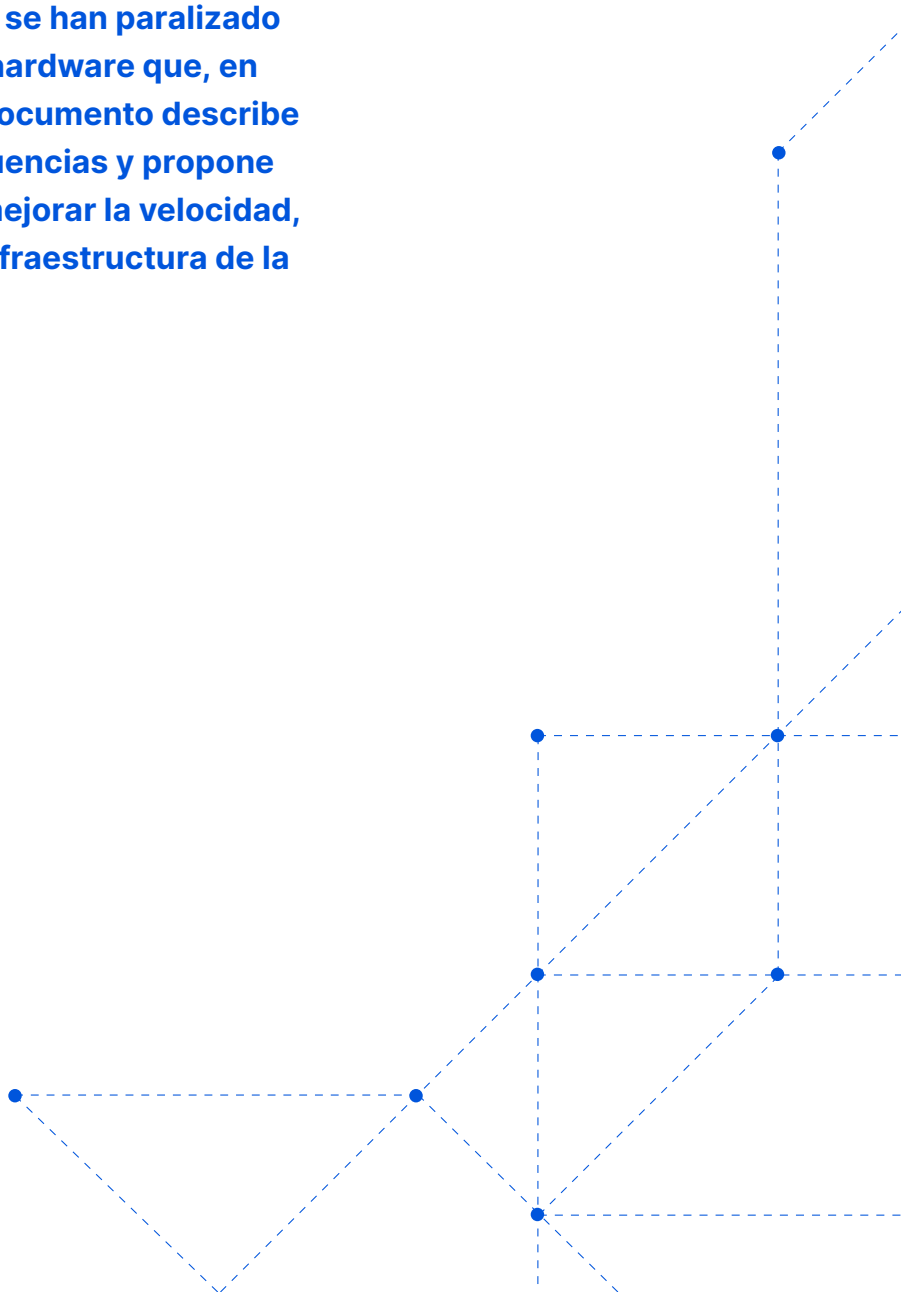
DOCUMENTO TÉCNICO

# La desaparición de los equipos de hardware de red

## ¿Por qué ha llegado el momento de dejar atrás el hardware de red?

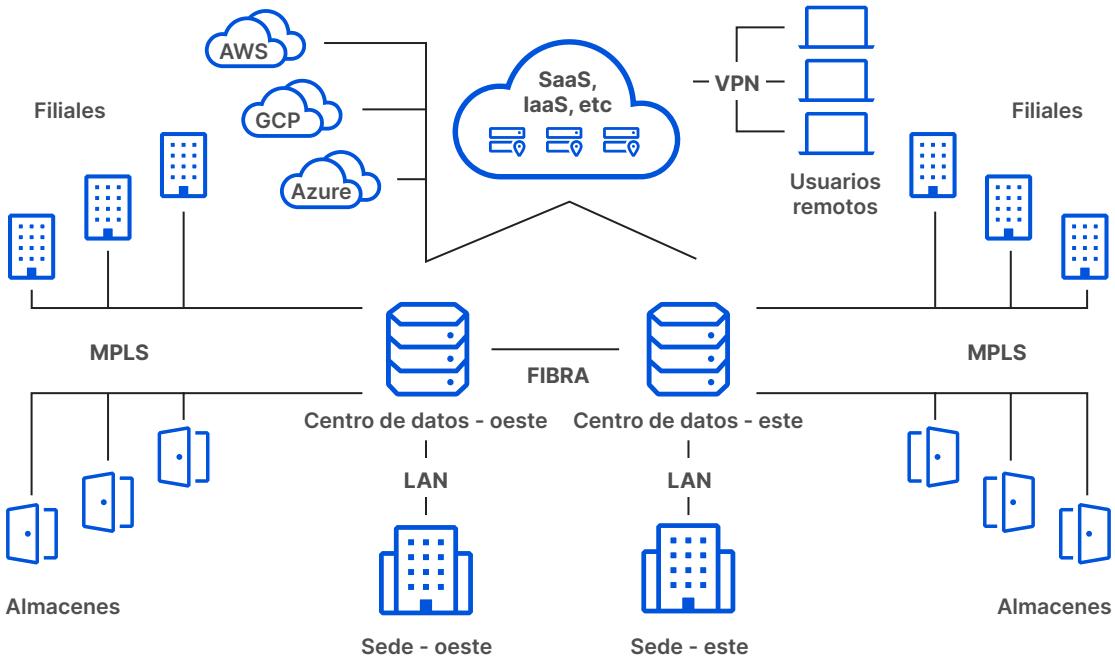
# Resumen ejecutivo

**Si bien el almacenamiento y la informática han migrado a la nube, muchas funciones de red permanecen en entornos locales, lo que limita la capacidad, aumenta el coste total de propiedad, plantea dificultades asociadas al soporte y genera fallos de seguridad. Las organizaciones tienen dificultades para garantizar una capacidad adecuada y una seguridad eficaz conforme el modelo híbrido de trabajo se impone como la nueva norma. Muchos proyectos de transformación se han paralizado debido a retrasos en las entregas de hardware que, en algunos casos, superan el año. Este documento describe esos desafíos, cuantifica sus consecuencias y propone soluciones basadas en la nube para mejorar la velocidad, la accesibilidad y la seguridad de la infraestructura de la nube híbrida.**



# Introducción

La migración a la nube ha demostrado ser una estrategia eficaz para reducir los costes de infraestructura, mejorar la accesibilidad de los datos y aplicaciones, y aumentar la agilidad operacional. Sin embargo, esta migración rara vez ocurre de una sola vez. Muchas grandes organizaciones se encuentran con una combinación compleja de infraestructura multinube y local:




Este tipo de infraestructura híbrida no es necesariamente algo malo, pero sí conlleva complicaciones. En concreto, crea situaciones en las que varias funciones de red, tales como la mitigación de DDoS, el equilibrio de carga, el firewall y las redes VPN, permanecen en entornos locales.

Estos dispositivos de hardware de red heredados no están preparados para proteger y acelerar la infraestructura crítica en un mundo enfocado a la nube. Siempre han sido un engorro, una maraña de equipos caros, a menudo sin orden ni concierto, conectados por madejas de cables. Si a todo esto añadimos la nube, aparecen fácilmente fallos de seguridad, desventajas de rendimiento y otras dificultades asociadas al soporte.

En este documento se exponen los riesgos que entraña el mantenimiento de los equipos de red en un mundo que migra a la nube y que ofrece estrategias para crear una red más segura y eficaz.

# Los riesgos del hardware en el mundo de la nube

Los equipos de hardware de red abarcan una variedad de funciones específicas y, en cierto modo, se utilizan de forma distinta en cada organización.

Entre los ejemplos más comunes están:

### Seguridad

- Protección contra DDoS
- Firewall
- Red privada virtual
- Políticas configurables

### Rendimiento y fiabilidad

- Equilibrio de carga
- Aceleración del tráfico/ Optimización WAN
- Filtrado de paquetes
- Análisis del tráfico

Cuando este hardware se implementa localmente, la arquitectura resultante corre diversos riesgos que se clasifican en cinco categorías: **tensión en la cadena de suministro, limitaciones de capacidad, alto coste total de propiedad, desafíos que atañen al soporte** y **fallos de seguridad**.

Las tres primeras categorías siempre han planteado problemas, incluso para los equipos de red y seguridad más sofisticados. Las otras dos se ven exacerbadas por la migración a la nube.

## Tensión en la cadena de suministro

Como cualquier tipo de producto físico, el hardware de red es vulnerable a una serie de dificultades en la cadena de suministro. Cuando los costes de los materiales suben, es mucho más difícil conseguir ciertos materiales y componentes, los proveedores de transporte se desbordan, y es más complicado adquirir y reemplazar el hardware de red.

Por desgracia, estas dificultades han sido habituales últimamente, en gran parte debido a los efectos de la pandemia de la COVID-19. Según Gartner Research, "antes de la pandemia, era habitual que los plazos de entrega fueran de 4-6 semanas. Ahora, lo normal es que sean de 200-300 días, y hemos visto que algunos clientes han recibido por escrito plazos incluso de más de 430 días".

Estos retrasos se deben a varios factores:

- **Desafíos logísticos:** los modelos tradicionales de la cadena de suministro tienen varios puntos de fallo, equipos de trabajo escasos y una gran dependencia de tecnologías que pueden o no ser seguras. Estos desafíos ya están teniendo repercusiones. Durante la pandemia, muchas fábricas han cerrado, las empresas de transporte están experimentando retrasos, y es más difícil contratar y mantener en nómina a muchos trabajadores de la cadena de suministro. Todos estos desafíos hacen que se tarde más en fabricar y entregar el hardware. Tal vez el aspecto más difícil de recordar en toda actividad logística es que es comparable a una carrera de relevos. Solo porque tu organización no esté experimentando dificultades no significa que no te verás afectado por un eslabón roto en otras fases superiores de la cadena.
- **Costes de materiales más altos:** los dispositivos de hardware de red dependen de una serie de materias primas. Debido a la gran demanda y al suministro limitado, los precios de los materiales se han disparado, lo que significa que las empresas no solo tienen que esperar más tiempo para conseguir lo que necesitan para su red, sino que también tienen que pagar mucho más por ello. Lamentablemente, como consecuencia, Gartner prevé que los plazos de entrega de los dispositivos de hardware seguirán siendo elevados hasta principios de 2023 (fuente).

Todos estos desafíos tienen repercusiones. La atención que se sigue prestando a la adquisición, el mantenimiento y la sustitución del hardware implica más gastos generales, más tiempo dedicado a la planificación en lugar de a la ejecución y más preocupaciones de seguridad en torno a la protección de una cadena de suministro física en tiempos inciertos. En lugar de centrarse en la logística, los plazos de entrega, la adquisición y el almacenamiento del hardware, las organizaciones podrían centrarse en satisfacer las necesidades de sus clientes.

## Limitaciones de capacidad

No debería sorprender que, por su propia naturaleza, los equipos de hardware de red puedan sobrecargarse durante picos de tráfico inesperados, sea o no tráfico legítimo. Pero varias tendencias recientes implican que alcanzar esos límites es una preocupación más común.

Piensa en la mitigación de la denegación de servicio distribuido (DDoS). El mayor ataque DDoS de la historia tuvo lugar en noviembre de 2021, según Microsoft, y se afirma que alcanzó un volumen máximo de 3,47 TB/s (fuente). Los ataques DDoS sobrecargarían muchas veces los módulos de hardware de mitigación DDoS más avanzados del mercado, que suelen proporcionar una parte de la capacidad necesaria para mitigar tales ataques.

**Se afirma que el mayor ataque DDoS de la historia alcanzó un volumen máximo de 3,47 TB/s en noviembre de 2021.**

No todas las organizaciones serán blanco de ataques de tal escala, pero tampoco todas las organizaciones pueden (o no desean) implementan el hardware de mitigación DDoS más avanzado. Un informe de Cloudflare reveló que los ataques volumétricos aumentaron en el primer trimestre de 2022. De hecho, los ataques de más de 10 millones de paquetes por segundo crecieron más de un 300 % en términos intertrimestrales, y los ataques de más de 100 GB/s se alzaron un 645 % en la misma comparación (fuente). No solo es alarmante el pronunciado aumento de los ataques DDoS, sino que este tipo de ataques sobrecargaría muchas soluciones de mitigación basadas en hardware supuestamente de gran capacidad.

Además, el volumen de los ataques no tiene en cuenta el tráfico legítimo que puede llegar a tu centro de datos al mismo tiempo.

Si un ataque de menor envergadura llega durante un pico de tráfico, como el fin de semana de compras del viernes negro, cuando las visitas diarias al comercio electrónico se duplican de manera repentina, en promedio (fuente), el aumento de tráfico resultante podría ser suficiente para llevar al límite al hardware de seguridad.

La mitigación de DDoS es solo un ejemplo de las limitaciones de capacidad de los equipos en las instalaciones.

Entre los ejemplos más comunes están:

**Equilibradores de carga:** los equilibradores de carga individuales en los servidores se pueden sobrecargar fácilmente por picos repentinos de tráfico legítimo. Cuando esto ocurre, se puede necesitar mucho tiempo para suministrar e instalar hardware adicional. La alternativa es mantener la capacidad suficiente para el peor de los casos, pero este enfoque requiere que la organización ejecute continuamente una gran cantidad de hardware a un alto coste.

**Redes privadas virtuales (VPN):** el uso de las VPN se ha vuelto mucho más difícil de predecir con relativa antelación. Para muchas organizaciones, el trabajo totalmente remoto e híbrido es el nuevo paradigma, pero el enfoque tradicional de las VPN requiere una planificación minuciosa, mantenimiento y gestión, ya que muchas VPN no se diseñaron para un uso continuado por parte de toda una organización. Cuando demasiados usuarios utilizan una VPN, la conectividad y la fiabilidad se resienten. Además, pueden surgir problemas de seguridad, simplemente por la naturaleza de cómo se diseñaron las VPN sin ningún tipo de control Zero Trust. Si una VPN se sobrecarga, las organizaciones pueden implementar una tunelización dividida para que el tráfico de la web no pase por la VPN, lo que dificulta el seguimiento y la gestión de la actividad web de los usuarios.

La respuesta a estos problemas suele ser comprar más hardware nuevo y de mayor capacidad. Pero este enfoque entraña otras dificultades.

## Costes de propiedad

Al igual que las limitaciones de capacidad, no debería sorprender que el hardware de los centros de datos sea caro. Por ejemplo, el hardware necesario para alcanzar una capacidad de mitigación de DDoS de aproximadamente 100 GB/s podría tener un coste inicial de entre 400 000 y 500 000 dólares.

Además, estos costes son solo una parte del coste total de propiedad de un equipo de hardware.

Plantéate los siguientes gastos:

- Costes de equipo: la compra, el funcionamiento y el mantenimiento del hardware para defenderse de las amenazas en cada capa del modelo OSI, y para proporcionar el nivel de rendimiento y fiabilidad que se espera de los sitios web y las aplicaciones de Internet modernos, requiere equipos que sean expertos en cada una de esas funciones de red. Formar un equipo con esta amplitud y profundidad de conocimientos es una propuesta costosa, especialmente durante uno de los mercados laborales más ajustados que se han visto nunca. Una encuesta de ISACA de 2022 concluyó que de los 2 000 profesionales de la ciberseguridad que participaron en la encuesta anual, el 63 % tiene puestos de ciberseguridad sin cubrir, un 8 % más que el año anterior (fuente).
- Costes de mantenimiento: en promedio, una pieza de hardware de red local solo tiene una vida útil de 3-5 años, pero las garantías para esos periodos completos suelen requerir un gasto adicional. Si se tiene en cuenta el ritmo de la innovación tecnológica, es inevitable que la vida útil de estos equipos locales siga acortándose. La alternativa pasa por reparaciones imprevistas, y por tanto no presupuestadas, del fabricante original o de un tercero. El mal funcionamiento del hardware también puede causar tiempo de inactividad en los centros de datos, que tiene un coste de oportunidad medio de más de 8 800 dólares por minuto (fuente).
- Costes de sustitución: sustituir un dispositivo de hardware cada tres años exige a las organizaciones no solo amortizar su inversión inicial, sino dedicar recursos al envío e instalación de nuevo hardware. Retrasar estas sustituciones suele dar lugar a averías más frecuentes y, por tanto, a nuevos costes de mantenimiento.

Contrasta este modelo con los servicios de red entregados por la nube. Pueden operar con un equipo más ágil, no suponen costes de mantenimiento y envío, y no obligan a las organizaciones a elegir entre actualizaciones caras y un aumento de los fallos en el funcionamiento.

**Los fallos en el funcionamiento del hardware pueden causar tiempo de inactividad en el centro de datos, que tiene un coste de oportunidad medio de de 8 800 USD por minuto.**

## Desafíos que atañen al soporte

El soporte de los equipos de hardware de red no es solo una propuesta costosa, sino un desafío logístico. La actualización del hardware requiere parches frecuentes con las últimas vulnerabilidades y tácticas de ataque, un proceso que a menudo se basa en la implementación manual y, por lo tanto, es susceptible a errores humanos.

Cuantos más dispositivos de hardware utilice una organización, mayores serán las posibilidades de que acabe olvidando un parche por falta de atención o por temor a que afecte a sistemas necesarios. En una reciente consultoría conjunta sobre ciberseguridad, la Agencia de Seguridad Nacional (NSA), la Agencia de Seguridad de Infraestructura y Ciberseguridad (CISA) y la Oficina Federal de Investigaciones (FBI) informaron de que se habían explotado 16 errores conocidos públicamente en dispositivos de red sin parches en campañas generalizadas (fuente). Las vulnerabilidades afectan a varios dispositivos locales, desde enrutadores de pequeñas empresas hasta VPN empresariales, y potencialmente dan a los atacantes la capacidad de manipular el tráfico de red y filtrar datos fuera de las redes objetivo.

A pesar de que la mayoría de los 16 errores enumerados se clasifican como críticos, la aplicación de parches y su actualización no es una tarea fácil. De hecho, parchear el hardware puede ser tan complejo que existe toda una categoría de software para ayudar a las empresas a estar actualizadas (fuente).

Y las consecuencias de pasar por alto un solo parche pueden ser significativas. El hardware no solo seguirá siendo vulnerable, sino que una vez que se publique un parche, la vulnerabilidad correspondiente se convertirá en un destino de mayor perfil para los atacantes oportunistas. Compara esta situación con los servicios de seguridad basados en la nube, en los que la solución de las vulnerabilidades y la instalación de actualizaciones se realiza automáticamente y de forma predeterminada, y puede tardar tan solo treinta segundos en propagarse, dependiendo de la velocidad de la red del proveedor de la nube.

Entre otros desafíos de mantenimiento del hardware están:

- **Solución de problemas:** en un escenario de solo hardware, la resolución de problemas a menudo obliga a los equipos informáticos a pasar por el arduo proceso de desconectar uno por uno los equilibradores de carga, los firewalls y otros dispositivos locales para identificar dónde está el problema.

  Este proceso se complica aún más por el uso simultáneo de servicios en la nube. Las organizaciones que dependen del hardware suelen gestionar el acceso a esos servicios a través del centro de datos centralizado y todos sus dispositivos individuales. Cuando los usuarios no pueden acceder a un servicio en particular, los equipos informáticos tienen otro lugar que comprobar para diagnosticar los problemas. Si se tiene en cuenta un informe reciente de Productiv que muestra que el 56 % de todas las aplicaciones SaaS entran en la categoría de Shadow IT, o aplicaciones no aprobadas y no gestionadas adquiridas sin el conocimiento de los responsables informáticos, este problema se agrava tanto en alcance como en escala (fuente).
- **Mantenimiento físico:** cuando un dispositivo de hardware se rompe, los equipos informáticos deben desenchufarlo físicamente, pedir un reemplazo, probarlo y volver a instalarlo, otro proceso laborioso. Si tenemos en cuenta la escala de muchas empresas globales, estos dispositivos que necesitan atención podrían estar al otro lado del mundo.

## Fallos de seguridad

Incluso si una organización dispusiera de los recursos necesarios para suministrar y mantener continuamente el hardware más reciente y de mayor capacidad en sus instalaciones, la infraestructura resultante seguiría presentando deficiencias críticas de seguridad, especialmente en un mundo que tiende a la nube.

Considera la gestión de acceso de los empleados. Aunque el hardware de VPN puede establecer túneles encriptados entre los dispositivos de los empleados en remoto y las aplicaciones alojadas en un centro de datos interno, no puede supervisar y proteger la actividad de los usuarios después de establecer este túnel.

Si un ataque de malware pone en riesgo el dispositivo del usuario o si un ataque de phishing compromete sus credenciales VPN, un atacante podría utilizar este acceso VPN para acceder a una amplia variedad de datos confidenciales. Tanto el phishing como el malware siguen planteando graves riesgos y generan importantes ganancias monetarias para los ciberdelincuentes. En 2021, la ciberdelincuencia se tradujo en pérdidas de 6 900 millones de dólares, según el FBI. En concreto, los ataques al correo electrónico corporativo supusieron pérdidas de 2 400 millones de dólares a las empresas (fuente).

**Si un ataque de malware pone en riesgo el dispositivo del usuario o si un ataque de phishing compromete sus credenciales VPN, un atacante podría utilizar este acceso VPN para acceder a una amplia variedad de datos confidenciales.**

Los servicios en la nube y las aplicaciones SaaS complican aún más la seguridad de la infraestructura de hardware. En un modelo de nube híbrida, por ejemplo, una organización cuenta con infraestructura en entornos locales y nube. La organización no puede simplemente enviar el hardware de seguridad a un proveedor de nube. Si desea seguir utilizando hardware local para su propio centro de datos, las diferentes partes de su infraestructura estarán protegidas de diferentes maneras, lo que dará a los equipos de seguridad menos visibilidad y control sobre los ataques entrantes.

Los servicios basados en la nube pueden superar ambos desafíos al unificar los centros de datos y los servicios de la nube bajo una sola capa definida por el software.

Una explicación detallada de este enfoque excede el alcance del presente documento. Para obtener más información, echa un vistazo a los siguientes artículos:

- ¿Qué es la red Zero Trust?
- ¿Qué es el perímetro de servicio de acceso seguro?

# Servicios de seguridad y rendimiento en la nube: ventajas y desafíos

La prestación de servicios de red a través de la nube evita muchos de los problemas asociados al hardware, como la tensión en la cadena de suministro, las limitaciones de capacidad, los costes, las dificultades relacionadas con el soporte y los fallos de seguridad.

- **Cadena de suministro:** muchos proveedores de redes basados en la nube están diseñados para escalar con arquitecturas modernas y globales, lo que hace que los problemas de la cadena de suministro sean menos graves.
- **Capacidad:** debido a la naturaleza distribuida de la nube y la naturaleza definida por el software, las organizaciones pueden proporcionar con facilidad capacidad adicional a medida que su negocio se va ampliando.
- **Coste:** los costes adicionales del hardware son nulos o son más fáciles de planificar con antelación. Además, los servicios en la nube suelen clasificarse como gastos de funcionamiento, no como inversiones, lo que ofrece beneficios fiscales y contables a muchas empresas.
- **Soporte:** las necesidades logísticas y de recursos son gestionadas por el proveedor de servicios. Además, no hay posibilidad de olvidar un parche, ya que las actualizaciones se producen automáticamente.
- **Seguridad:** los servicios de red definidos por software pueden unificar diferentes infraestructuras bajo una única capa protectora.

Sin embargo, los servicios de red en la nube presentan sus propios riesgos si no se implementan con cuidado:

| Riesgo | Descripción |
|---|---|
| **Latencia** | Algunas funciones de red en la nube dependen de centros de datos especializados en la nube, por ejemplo, centros de filtrado para la mitigación de DDoS. El redireccionamiento del tráfico a esos centros de datos puede añadir una latencia significativa dependiendo de su ubicación en relación con el servidor de destino.<br><br>Este problema se agrava cuando una organización utiliza diferentes proveedores para diferentes funciones de red. Cuando el tráfico debe saltar de un proveedor a otro, la latencia se puede medir en cientos de milisegundos. |
| **Soporte** | Cuando una organización utiliza diferentes proveedores para diferentes funciones, la solución de problemas sigue siendo un inconveniente. Puede ser difícil determinar qué proveedor es el causante de la congestión o de las interrupciones. |
| **Costes** | Cuando una organización utiliza diferentes proveedores para diferentes funciones, el tiempo (y, por lo tanto, el dinero) necesario para administrarlas puede seguir siendo elevado. |

## Para evitar estos problemas, ten en cuenta las siguientes estrategias:

- **Busca proveedores que trabajen tanto en la nube como con infraestructura local.**
  Esta capacidad permite a los equipos informáticos y de seguridad establecer controles coherentes y supervisar el tráfico global desde un único lugar. También ayuda a desarrollar una arquitectura más eficaz, una a la que tus usuarios puedan recurrir rápidamente en respuesta a las fluctuaciones de las condiciones del mercado.
- **Busca proveedores de nube que ofrezcan varias funciones de red que trabajen en conjunto.**
  De este modo, se suele reducir el número de saltos de red que debe realizar el tráfico, lo que se traduce en una menor latencia y, por tanto, en una mejor experiencia para el usuario final.
  La resolución de problemas de red también es más fácil cuando solo tienes que contactar a una empresa y no a muchas. Además, la agrupación de varias funciones suele reducir los costes.
- **Busca proveedores de nube que puedan realizar varias funciones desde cualquier lugar de su red.**
  Los proveedores que amplían sus carteras de servicios mediante adquisiciones no siempre integran plenamente esos nuevos servicios, lo que significa que ciertas funciones solo se pueden entregar a través de determinados centros de datos. Contempla los proveedores que ofrezcan estas funciones a través de toda su red para evitar estos problemas.
- **Busca proveedores de nube con una amplia presencia global.**
  Esta capacidad es compatible con la anterior, lo que garantiza que los usuarios finales siempre estén cerca de la red sin importar dónde se encuentren. También crea una gran superficie de red con la que se puede absorber el tráfico DDoS y realizar otras funciones de red que requieran una gran capacidad.

# Cómo puede ayudar Cloudflare

¿Cómo pueden las organizaciones acelerar la transformación de su red sin tener que esperar la llegada de hardware y sin malgastar más dinero en infraestructura que solo durará unos años?
Con Cloudflare.

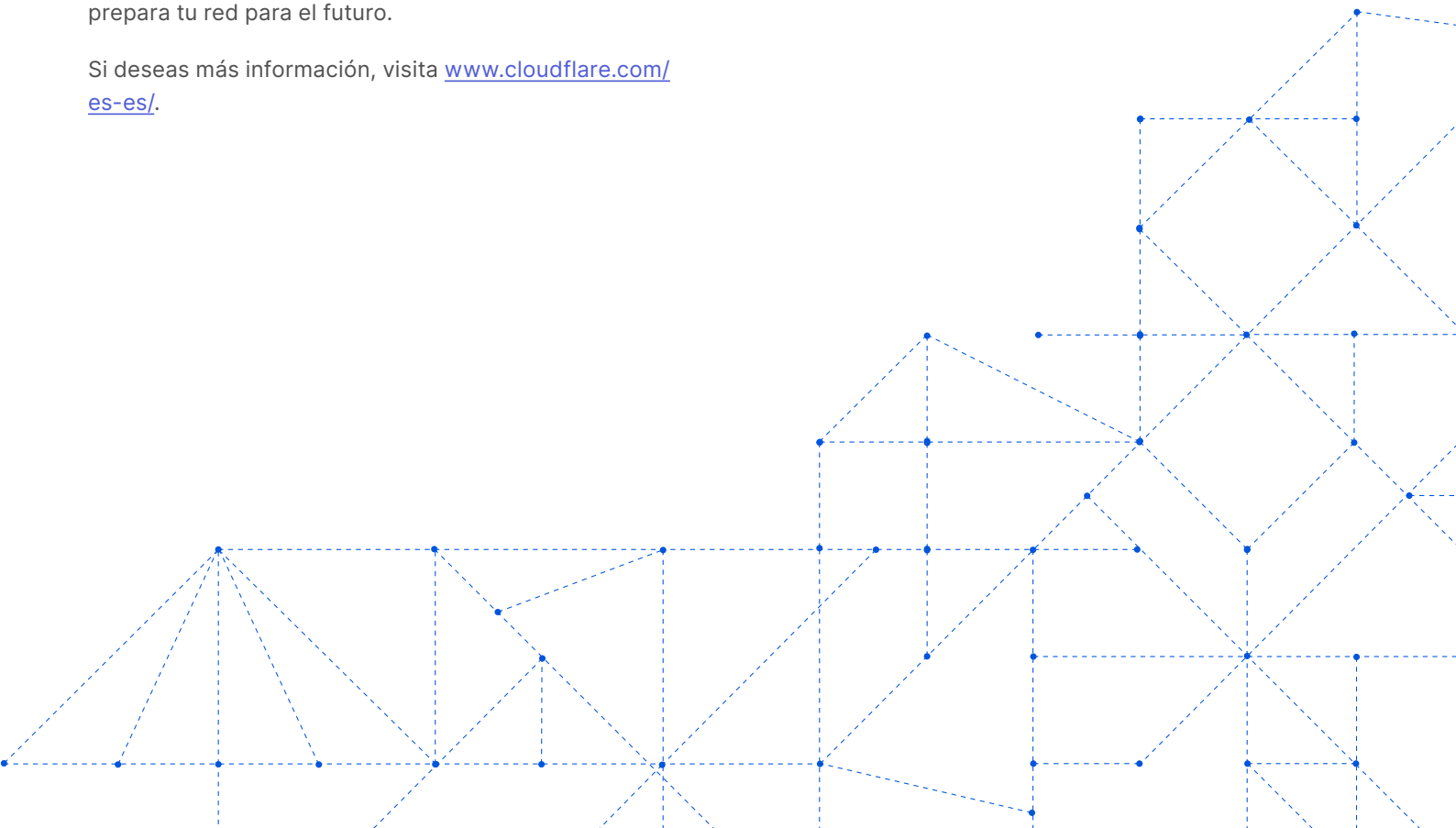
Cloudflare ha creado una plataforma de nube global que proporciona una amplia gama de servicios, que hace que las organizaciones sean más seguras, al mejorar el funcionamiento de sus aplicaciones y eliminar el coste y la complejidad de la administración de hardware de red individual. Esta plataforma sirve como un plano de control unificado, escalable y fácil de usar para brindar seguridad, funcionamiento y fiabilidad a todas las aplicaciones en las instalaciones, en la nube, en nubes híbridas y software como servicio (SaaS).

Y lo que es más importante, todos los centros de datos de la red global de Cloudflare en más de 270 ciudades pueden ofrecer cada uno de estos servicios, reduciendo la latencia que puede complicar las implementaciones en la nube. Agiliza tu pila de red, acelera la transformación y prepara tu red para el futuro.

Si deseas más información, visita www.cloudflare.com/es-es/.

"Dropbox se ha convertido recientemente en una organización que prioriza lo virtual. Hemos estado analizando cómo esta estrategia empresarial afecta a nuestro enfoque de seguridad y arquitectura de red. Agradecemos el soporte de Cloudflare para ayudarnos a nosotros y a otras organizaciones como la nuestra, cuyo plan organizacional incentiva trabajar de manera remota, a aprender a adaptarnos a este "nuevo paradigma".

Konstantin Sinichkin
**Gerente de ingeniería, Dropbox**



+34 518 880 290 | enterprise@cloudflare.com | www.cloudflare.com/es-es/

REV:BDES-3313.10JUN2022