Cómo proteger el trabajo híbrido

Reduce el riesgo y aumenta la visibilidad de todos los usuarios, tanto dentro como fuera de la red

Protege las conexiones de cualquier usuario y dispositivo, en cualquier lugar.

Nuestro futuro del teletrabajo: tras años de pandemia mundial y con una recesión en ciernes, el trabajo híbrido parece una realidad. Los equipos informáticos y de seguridad deben ofrecer protección y experiencias coherentes a todos los usuarios y dispositivos, remotos o en la oficina, y las herramientas tradicionales centradas en la ubicación (como las VPN y los controles basados en la IP) no pueden hacerlo.

Seguridad moderna para equipos modernos: en respuesta, muchas organizaciones están renovando sus arquitecturas informáticas y de seguridad y adoptando una seguridad en la nube que se adapta a las necesidades de los equipos descentralizados y que aplica las prácticas recomendadas del modelo de seguridad Zero Trust.

Cloudflare facilita la seguridad de cualquier conexión para que los usuarios de cualquier dispositivo o en cualquier lugar estén seguros y sean productivos cuando accedan a las aplicaciones o a Internet.

Según Gartner®:

> *Para el 2026, el 75 % de los trabajadores seguirá dividiendo su tiempo entre el trabajo presencial de siempre y el teletrabajo, lo que supone un ligero descenso con respecto al 77 % en el momento más difícil de la pandemia en 2021.*[1]

> *Los diseños de seguridad de red basados en un conjunto de dispositivos de seguridad perimetral no son adecuados para abordar las necesidades dinámicas de una empresa digital moderna y su equipo de trabajo híbrido en cualquier momento y en cualquier lugar.*[2]

Tabla de contenidos por página

Oportunidades para la modernización de la seguridad

Protege el acceso a las aplicaciones sin una VPN

Con la descentralización de los usuarios, el redireccionamiento del tráfico a través de dispositivos locales, como las VPN, ralentiza el rendimiento y plantea el riesgo de que las amenazas se propaguen lateralmente por la red corporativa.

Como alternativa, recupera la visibilidad de todas las solicitudes y aplica controles basados en la identidad que se entregan más cerca de los usuarios para garantizar la productividad. Sin redireccionamientos.

Optimiza la seguridad de SaaS

Más que nunca, los usuarios dependen de las aplicaciones SaaS fuera de los controles de las redes corporativas tradicionales.

En respuesta, las organizaciones necesitan visibilidad y controles integrales sobre sus aplicaciones SaaS para crear políticas de acceso, aplicar controles de protección de datos, mitigar los elementos de Shadow IT y analizar las aplicaciones en busca de configuraciones erróneas.

Protege a los usuarios y los datos de las amenazas de Internet

El ransomware, el phishing y otras amenazas de Internet están siempre presentes y son cada vez más sofisticadas.

La adopción de la inspección y el aislamiento del tráfico de salida en la nube protege a los usuarios del malware. Además, los administradores pueden aplicar controles para evitar que los datos confidenciales lleguen a los dispositivos locales no administrados.

Trabajo híbrido para empresas maduras

Para las empresas maduras, moderniza la seguridad del trabajo híbrido con confianza

Desafío: entornos complejos y heredados

Las organizaciones están experimentando con los modelos de trabajo en la oficina, pero mantener protecciones y experiencias de usuario coherentes es un reto en estos escenarios híbridos.

Estas empresas suelen estar más consolidadas y cuentan con importantes planes de inversión preexistentes (a menudo complejos) locales y heredados. Empezar un nuevo proyecto de seguridad ante las presiones recesionistas puede parecer demasiado arriesgado y difícil.

Oportunidad: un recorrido más sencillo hacia la modernización

Las organizaciones merecen llevar a cabo la transformación digital a su propio ritmo, sin necesidad de presupuestos infinitos, "pruebas de concepto" costosas, fases de implementación complejas o servicios en cadena.

Para ayudar a estas empresas maduras a abordar sus necesidades de trabajo híbrido, Cloudflare está diseñado para que su implementación sea más fácil y rápida que la de otros proveedores de servicios Zero Trust, como Zscaler.

Ejemplos de casos de uso

Telecomunicaciones

Contexto: una empresa de telecomunicaciones europea con más de 100 años de antigüedad y más de 20 000 millones de dólares de ingresos anuales quería un único proveedor para implementar el filtrado de Internet y autenticar el acceso a las aplicaciones heredadas que se habían migrado recientemente a varios entornos en la nube.

Solución: la empresa seleccionó a Cloudflare para consolidar los servicios y utilizar una plataforma unificada para proteger tanto el acceso a las aplicaciones como a Internet de sus más de 100 000 usuarios.

Gobierno federal

Contexto: el Departamento de Seguridad Nacional (DHS) de EE. UU. está realizando inversiones en protección contra las amenazas de Internet en todas las oficinas, ubicaciones e infraestructuras federales.

Solución: el DHS seleccionó a Cloudflare y Accenture Federal Services para desarrollar una solución conjunta que permitiera filtrar las consultas de DNS a destinos maliciosos y peligrosos que se utilizarán en todas las agencias federales.

Medios de comunicación y publicidad

Contexto: un conglomerado de medios de comunicación (con ingresos superiores a 10 000 millones de dólares y más de 100 000 empleados en todo el mundo) se enfrenta a ciberataques en la infraestructura interna, incluida una nota de rescate.

Solución: Cloudflare protege cientos de aplicaciones web y no web con reglas Zero Trust basadas en la identidad. La empresa despliega protección para 50 000 empleados en 3 meses y prevé ampliarla a toda la plantilla en 9 meses.

Energía

Contexto: un proveedor de gas natural de la lista Fortune 500 buscaba una mayor protección frente al aumento de las ciberamenazas contra el sector, tanto para sus centros de datos distribuidos como para sus más de 1500 empleados.

Solución: la empresa seleccionó a Cloudflare para sustituir a Zscaler por su mayor fiabilidad y consistencia en la protección de las aplicaciones y el acceso a Internet y, a más largo plazo, por su mayor facilidad para adoptar controles avanzados con aislamiento del navegador remoto.

TESTIMONIOS DE CLIENTES

> *Cloudflare es un multiplicador de fuerza en nuestro recorrido Zero Trust.*

John McLeod
Director de seguridad de la información, National Oilwell Varco

> *Cloudflare ha permitido a Ziff Media Group ofrecer nuestro conjunto de herramientas internas a usuarios de todo el mundo en cualquier dispositivo, sin necesidad de configuraciones de red complicadas.*

Josh Butts
Vicepresidente sénior de producto y tecnología, Ziff Media Group

> *Con Cloudflare, hemos podido reducir nuestra dependencia de las VPN y la elaboración de listas de direcciones IP permitidas para los entornos de desarrollo.*

Alexandre Papadopoulos
Director de ciberseguridad, INSEAD

Usuarios remotos para empresas nativas digitales

Para las empresas nativas digitales, prioriza un modelo de seguridad ágil para apoyar la flexibilidad del teletrabajo

Desafío: escalar y automatizar la seguridad en la nube

Muchas organizaciones están adoptando la contratación de personal remoto. Suelen ser empresas jóvenes, usuarios pioneros de la nube, que cuentan con una infraestructura local limitada y modelos de negocio basados en servicios digitales seguros, rápidos y fiables.

Permitir la flexibilidad del trabajo desde cualquier lugar puede ser un elemento diferenciador, pero exige herramientas de seguridad que sean igualmente flexibles, ya que los usuarios trabajan desde cualquier lugar y dependen de sus dispositivos personales.

Oportunidad: seguridad modular apta para escalar

Estas empresas nativas digitales, que tienen menos sistemas informáticos heredados obsoletos, pueden aprovechar nuestra arquitectura nativa de Internet y la flexibilidad de implementación para seguir siendo ágiles en su proceso de modernización de la seguridad.

Nuestros servicios modulares, nuestro enfoque que "prioriza las API" y la gestión a través de un único panel facilitan la puesta en marcha y la adaptación de la seguridad. La velocidad, la escala y la fiabilidad de nuestra red global satisfacen las necesidades de una plantilla 100 % remota.

Ejemplos de casos de uso

SaaS B2B

Contexto: la plataforma australiana de diseño gráfico Canva (valorada en 40 000 millones de dólares en 2021) implementó Cloudflare antes de la pandemia para agilizar el acceso de terceros y evitar las molestias de implementar una VPN.

Solución: con el tiempo, Canva ha implementado políticas de acceso a aplicaciones Zero Trust en toda su plantilla en aumento, además de haber ampliado el filtrado y la inspección de Internet.

Tecnología financiera y cadena de bloques

Contexto: BlockFi, una plataforma de gestión de capitales de serie D que funciona con la tecnología de cadena de bloques, necesitaba aumentar la seguridad en vista de las amenazas cibernéticas contra sus crecientes activos administrados y sus usuarios remotos.

Solución: Cloudflare facilitó a BlockFi la transición a la autenticación basada en la identidad para el acceso a las aplicaciones que le permitió dejar de lado el lento proceso de creación de controles basados en la IP.

Medios sociales

Contexto: una plataforma global de medios sociales experimentó una brecha de alto perfil que explotaba el acceso a aplicaciones internas y las configuraciones de la VPN.

Solución: en respuesta, la empresa decidió revisar su enfoque de acceso remoto adoptando la solución de acceso a la red Zero Trust (ZTNA) de Cloudflare para 13 000 empleados y proveedores y retiró sus implementaciones de VPN.

Comercio electrónico

Contexto: una plataforma global de comercio electrónico (con ingresos de más de 4000 millones de dólares y más de 15 000 empleados) buscaba una mejor protección para los usuarios remotos que navegan por Internet y acceden a aplicaciones SaaS confidenciales mientras están fuera de la red.

Solución: la empresa implementa Cloudflare para sumar capacidades de protección contra amenazas, como el filtrado de DNS, a la vez que mejora la visibilidad del uso de las aplicaciones SaaS.

TESTIMONIOS DE CLIENTES

> *En Delivery Hero, nuestro objetivo es ofrecer experiencias increíbles a nuestros clientes. Cloudflare nos ayuda a hacer lo mismo con nuestros equipos internos, permitiéndonos ofrecerles un entorno de trabajo seguro en todo el mundo y una forma fácil de crear aplicaciones rápidas, fiables y que respeten la privacidad.*

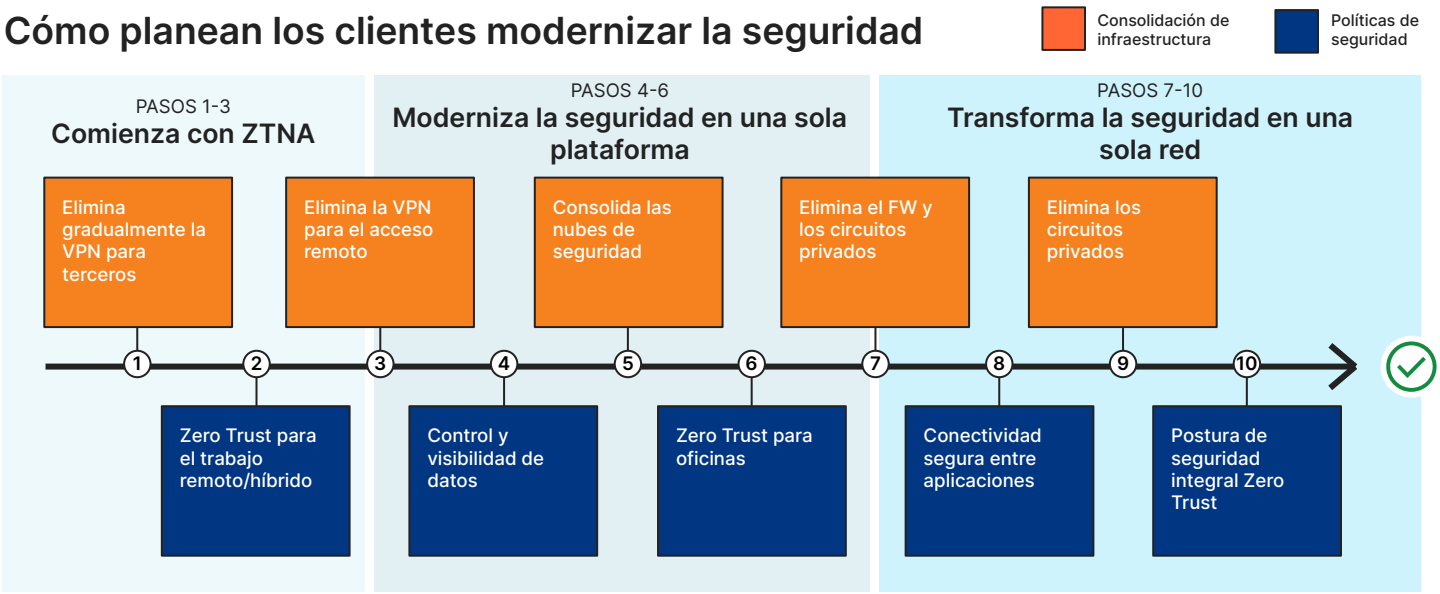
Christina von Hardenberg
Directora técnica,
Delivery Hero

> *Cloudflare es esencial para la seguridad de nuestra creciente plantilla remota. La adopción de Zero Trust para el acceso a las aplicaciones proporcionó a nuestros administradores mayor visibilidad y controles granulares que nunca pudieron conseguir con las herramientas anteriores.*

Marccio Alcaide
Responsable de seguridad informática, Facily

Plan de desarrollo ilustrativo del trabajo híbrido

Cómo planean los clientes modernizar la seguridad



Plan de desarrollo para la modernización de la seguridad

El plan de desarrollo anterior muestra el enfoque que vemos que están adoptando las organizaciones para modernizar su seguridad y adaptarse al trabajo híbrido. Este plan de desarrollo tiene dos objetivos clave:

1) **Fila superior (en naranja):** consolidar la infraestructura de conectividad y seguridad en una plataforma nativa en la nube, dejando de lado los productos específicos y el hardware.
2) **Fila inferior (en azul):** obtener visibilidad y controles para adoptar el modelo de seguridad Zero Trust entre usuarios y recursos en cualquier dispositivo, en cualquier lugar.

Fases 1 - 5: proteger el acceso a las aplicaciones y a Internet

Para muchos, adaptarse al trabajo híbrido significa primero modernizar la forma en que los usuarios llegan a los recursos corporativos.

Fase 1: a menudo el primer paso es empezar a descargar el tráfico VPN y preparar la transición a controles nativos de Internet para usuarios seleccionados, como proveedores, desarrolladores, socios o equipos que se acaban de incorporar tras una adquisición. Cloudflare hace que sea especialmente fácil proteger las aplicaciones autoalojadas accesibles a través de un navegador sin necesidad de implementar software en los puntos finales.

Fase 2: esta moderna herramienta permite la visibilidad necesaria para crear políticas por aplicación basadas en la función, los requisitos de la autenticación multifactor (MFA) y clave segura, y la postura de la identidad y el dispositivo.

Fase 3: a medida que los equipos adquieren confianza en este enfoque, pasan a eliminar por completo su VPN y a proteger las redes privadas no web y heredadas con Zero Trust.

Fase 4: la atención se centra después en mejorar la visibilidad y los controles de las aplicaciones SaaS, incluida la mitigación de elementos de Shadow IT, la gestión de inquilinos y la prevención de la exfiltración de datos.

Fase 5: las aplicaciones internas y SaaS ahora se gestionan desde una única plataforma, por lo que las organizaciones buscan ampliar los controles para el acceso saliente a Internet y consolidar las herramientas de protección contra amenazas, como filtros DNS y puertas de enlace web seguras.

Fases 6-10: trasladar la conectividad a la nube

Las demás fases del plan de desarrollo están en fase de planificación para la mayoría de las organizaciones, pero aspiran a migrar toda la conectividad y seguridad de la red a una red unificada en la nube.

Fase 6: aquí, las organizaciones buscan ampliar la seguridad Zero Trust coherente a cualquier ubicación de la red, como la sede central, las filiales, los centros de datos y las oficinas satélite, para dar soporte al trabajo híbrido.

Fase 7: conforme aumenta el envío de tráfico de las oficinas a Cloudflare para su seguridad, las organizaciones pueden eliminar gradualmente los firewalls locales tradicionales y otros dispositivos de red privada.

Fase 8: estos casos de uso avanzados se centran en proteger la conectividad entre aplicaciones en entornos híbridos multinube, lo que prepara al equipo de infraestructura de red para poner fin a los contratos de comunicaciones MPLS en la **Fase 9**.

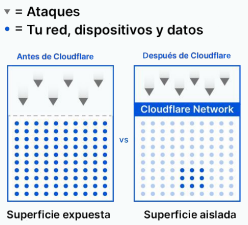
Fase 10: Aunque la modernización nunca termina realmente, la aspiración es que la seguridad Zero Trust se extienda ahora a todos los usuarios, dispositivos, datos, aplicaciones y entornos.

Resultados empresariales y de seguridad

5 formas para ahorrar tiempo y dinero a tu empresa con Zero Trust

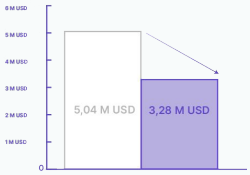
Reduce la superficie de ataque

91 %↓



Reduce los costes de fugas

35 %↓



Acelera el proceso de incorporación de usuarios

60 %↑

Reduce las incidencias informáticas

80 %↓

Reduce la latencia de los usuarios

39 %↓

Otros factores claves para el negocio

Promueve la productividad de la plantilla

Para los administradores

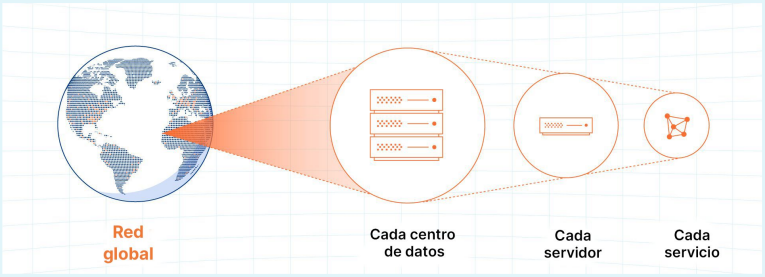
- Simplifica la configuración con una única interfaz de gestión para establecer políticas para el acceso a las aplicaciones e Internet.
- Configura todas las integraciones con proveedores de identidad, de soluciones de protección de puntos finales, de soluciones en la nube y de acceso a la red desde esa misma interfaz de gestión.

Para los usuarios finales

- Autenticación eficaz y experiencias de navegación nativas con una seguridad que no estorba.

Reduce los costes de los servicios heredados

- Reemplaza o mejora tus dispositivos de red privada virtual (VPN) y adopta en su lugar el acceso a la red Zero Trust (ZTNA).
- Cambia tu proxy web o firewall local por los servicios de seguridad de capa 3 y 7 nativos de la nube.
- Descarga los casos de uso de la infraestructura de escritorio virtual con el aislamiento remoto del navegador (RBI).
- Cambia la tradicional puerta de correo electrónico segura por la moderna seguridad del correo electrónico en la nube.



Velocidad y escala coherentes para proteger a todos los usuarios remotos o presenciales

Todas las funciones de seguridad, rendimiento y fiabilidad están diseñadas para ejecutarse en cada uno de los servidores de todos los centros de datos de Cloudflare en nuestra red, que actualmente abarca más 275 ciudades.

Acelera tu recorrido Zero Trust **Probar ahora** **Te ayudamos**

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

REV: PMM-JUL2022

[1] *Top Network Practices to Support Hybrid Work,* Gartner, Karen Brown, Andrew Lerner, Mike Toussaint, 08/04/2022
[2] *2022 Strategic Roadmap for SASE Convergence,* Gartner, Neil MacDonald, Andrew Lerner, John Watts 24/06/2022