CLOUDFLARE

DESCRIPCIÓN GENERAL
DEL PRODUCTO

Cloudflare Access

El acceso a la red Zero Trust (ZTNA) verifica el contexto, como la identidad y el estado del dispositivo, para proteger el acceso en todo tu entorno, sin necesidad de VPN.

Modernización del acceso remoto

Acceso a la red Zero Trust (ZTNA) de manera rápida y confiable

Los entornos de trabajo descentralizado exigen un enfoque distribuido de la seguridad. El "perímetro" ya no existe, y las soluciones tradicionales de acceso remoto, como las VPN, no pueden responder a las expectativas modernas de seguridad o al rendimiento.

El servicio ZTNA de Cloudflare proporciona un acceso sencillo y seguro entre cualquier usuario y recurso, en cualquier dispositivo y en cualquier lugar mediante la comprobación continua del contexto detallado, como la identidad y el estado del dispositivo para cada solicitud. Con un enfoque nativo de nube, ya no hay un "punto de equilibrio" entre la seguridad y la experiencia del usuario. El ZTNA permite que tu empresa acceda de manera eficiente a las aplicaciones y la infraestructura, al mismo tiempo que protege los datos.

También ayuda a las organizaciones a mantenerse ágiles y a adaptarse al cambio con mayor facilidad, ya sea incorporando nuevos contratistas o dispositivos no administrados o gestionando el acceso a través de una migración a la nube o una actividad de fusión y adquisición (M&A). Cloudflare puede convertirse en el núcleo de la estrategia Zero Trust o de modernización de la seguridad de una organización, ofreciendo ZTNA en nuestra conectividad cloud global y programable.

> Cloudflare facilita la implementación de Zero Trust en nuestra organización, y nos ayuda a mitigar riesgos de manera más eficiente y con menos esfuerzo.
>
> **Anthony Moisant**
> VP sénior, CIO y CISO
>
> indeed

Acceso renovado para tu empresa

Refuerza la experiencia del usuario

Mejora la productividad de los equipos con una seguridad modernizada para que las aplicaciones locales parezcan aplicaciones SaaS. Sin VPN complicadas y lentas ni quejas de los empleados.

Elimina el movimiento lateral

Disminuye el riesgo cibernético y reduce la superficie de ataque otorgando un acceso de privilegio mínimo por recurso, basado en el contexto, en lugar del acceso al nivel de red.

Escala fácilmente con Zero Trust

Mejora la eficiencia tecnológica protegiendo las aplicaciones o los grupos de usuarios de alto riesgo, y luego ampliando el ZTNA nativo de Internet para proteger a toda tu organización.

Principales casos de uso de Cloudflare Access

Implementar Zero Trust y un trabajo híbrido

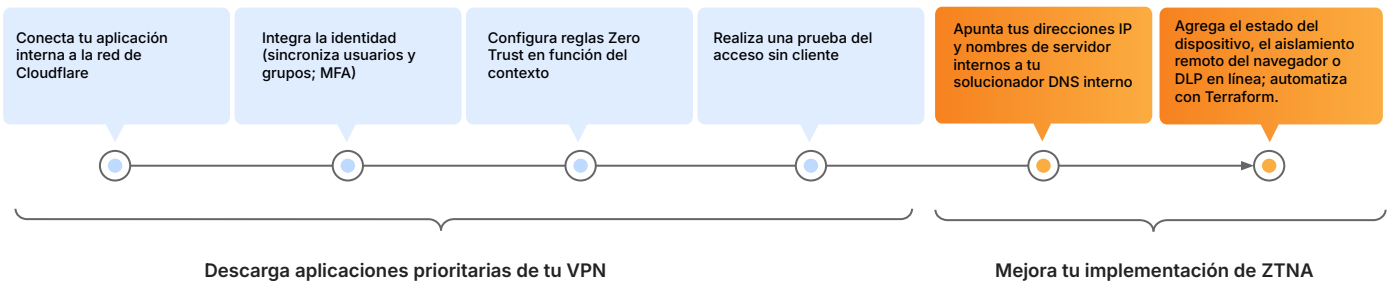
- **Mejora y sustitución de VPN**: Access es más rápido y seguro que las VPN tradicionales. Empieza a descargar usuarios y aplicaciones esenciales para mejorar la seguridad y la experiencia del usuario final.
- **Acceso de contratistas/BYOD**: autoriza a empleados o usuarios de terceros en máquinas personales con opciones de acceso basadas en el navegador.
- **Acceso a la infraestructura**: brinda acceso privilegiado a la infraestructura confidencial, sin interrumpir los flujos de trabajo de los desarrolladores.

Facilitar la modernización digital

- **Acelera las fusiones y adquisiciones**: evita por completo una fusión de red tradicional. Integra con varios proveedores de identidad y brinda acceso interno por aplicación durante las fusiones y adquisiciones.
- **Admite migraciones a la nube:** brinda continuidad de acceso durante los proyectos de modernización de aplicaciones mediante el uso de ZTNA en ambos lados de una migración.
- **Protege los flujos de trabajo de desarrollo y operaciones**: protege los flujos de trabajo de servicio a servicio con conectividad de malla/punto a punto, compatible con el tráfico bidireccional.

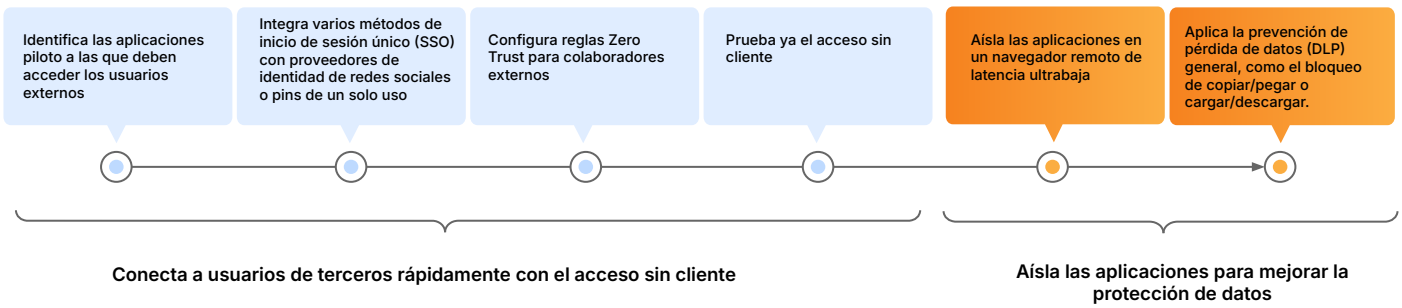
Comenzar: mejora y sustitución de la VPN

Prioriza las aplicaciones críticas o los usuarios de riesgo en una prueba piloto de ZTNA para mejorar tu VPN. Utiliza el acceso sin cliente a las aplicaciones web para acelerar las pruebas. Avanza gradualmente hacia la sustitución total de la VPN con el tiempo, y adopta servicios en línea adicionales para mejorar tu implementación de SSE o SASE con más señales contextuales o controles de datos.



Primeros pasos con el acceso de contratistas/BYOD

Brinda acceso con privilegios mínimos a usuarios de terceros o dispositivos no administrados, al tiempo que mitigas los riesgos de movimiento lateral o exfiltración de datos. Configura opciones de autenticación sencillas para los contratistas, sin necesidad de software de usuario final. Aplica controles de datos dentro de un navegador aislado para mejorar tu implementación.



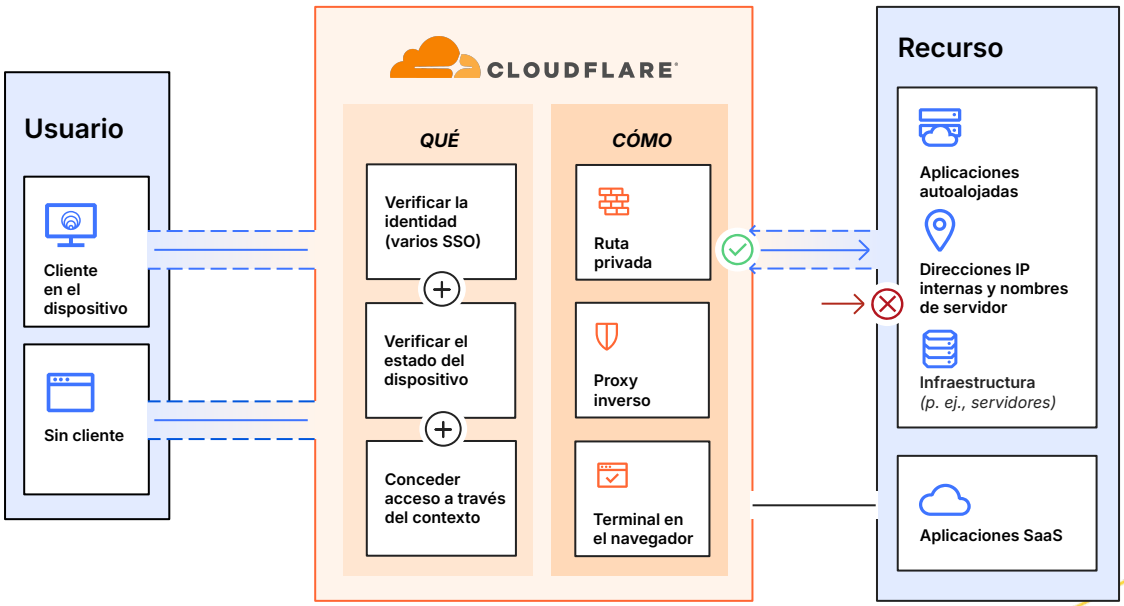
Cómo funciona Cloudflare Access

Simplifica y protege el acceso a todos los recursos de tu organización de forma individual, creando un perímetro definido por software con Cloudflare Access. Nuestro servicio ZTNA es una capa de agregación flexible que verifica continuamente el contexto detallado, como la identidad y el estado del dispositivo. Cuando un usuario se autentica y cumple con todos los criterios de la política de acceso, Cloudflare Access emite un token web JSON (JWT) firmado, válido para una duración de sesión específica. Realizamos una inspección de paso único en todas las solicitudes de los usuarios a través de nuestra plataforma SASE modular, y nuestra experiencia de administración centralizada de políticas aplica los cambios de políticas a nivel global en segundos.

El funcionamiento unificado sin cliente y basado en el cliente gestiona todos los tipos de dispositivos. Utilizamos un dispositivo del cliente a través de nuestra plataforma que cifra el tráfico a nuestra red para mantener la privacidad de los datos de nuestros clientes. También brindamos acceso sencillo y seguro a dispositivos fuera de la empresa mediante nuestra configuración sin cliente. Nuestros servicios de ZTNA, DNS, y los líderes WAF y protección DDoS, trabajan juntos para crear y proteger nombres de host públicos accesibles a usuarios de terceros y equipos híbridos en cualquier dispositivo. Nuestras opciones de autenticación sin usuario (tokens o certificados mTLS) también abordan casos de uso de servicios automatizados y dispositivos IoT.

Para los controles Zero Trust, los recursos utilizan nombres de host públicos para proxy inverso a aplicaciones autoalojadas (nube/locales) o SSH/RDP basados en navegador, proxy de identidad a aplicaciones SaaS o enrutamiento privado basado en cliente/túnel a través de proxy de reenvío de L4-7 a cualquier recurso web o no web (p. ej., objetivo de infraestructura o TCP/UDP arbitrario) dentro de una subred privada. Nuestra red global y nuestro software de conector de aplicaciones combinados admiten cualquier entorno informático (nube pública, incluidos Kubernetes y contenedores o recursos de red locales heredados) sin necesidad de infraestructura de máquina virtual y sin limitaciones de rendimiento.

Mantiene la agilidad y desarrolla con las herramientas que los administradores ya utilizan. Las herramientas de identidad de terceros, punto final, acceso a la red, registro/análisis y SIEM están integradas en el panel de control unificado de Cloudflare, con opciones nativas también proporcionadas para nuestro dispositivo del cliente y análisis.



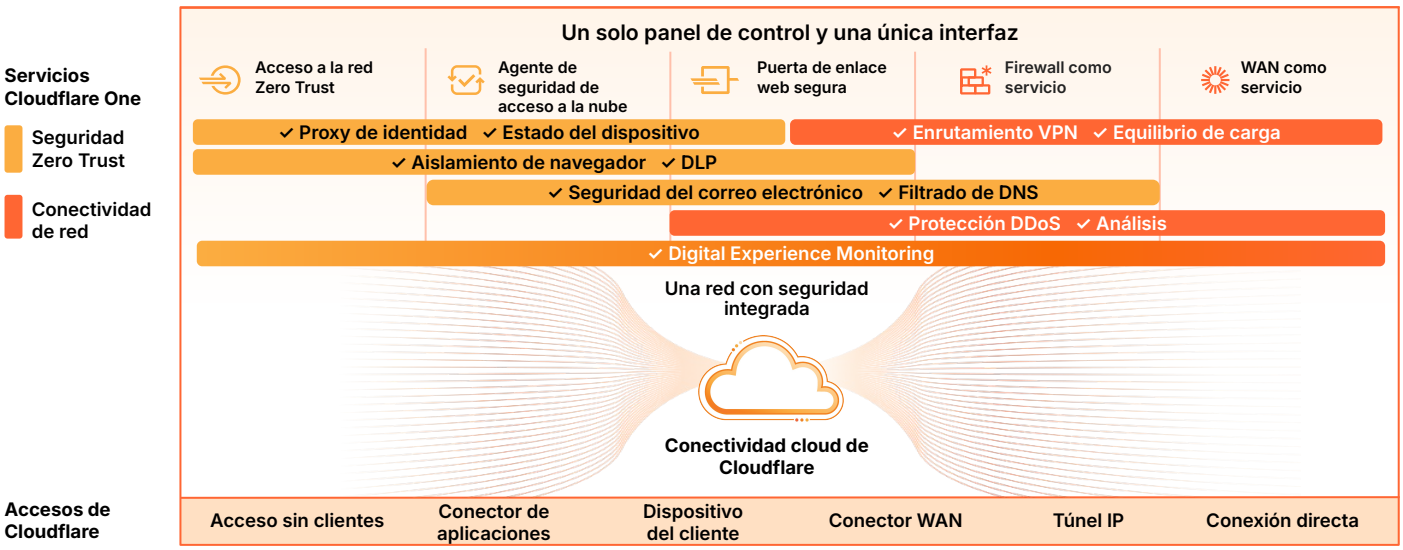
Cloudflare Access, parte de la plataforma SSE y SASE de Cloudflare

SSE y SASE generalmente implican un recorrido estratégico de varios años; sin embargo, las organizaciones suelen empezar con ZTNA para demostrar rápidamente el valor empresarial transversal. Las organizaciones que buscan asegurar el trabajo híbrido, defenderse de las amenazas y proteger sus datos en su recorrido hacia la consolidación eligen cada vez más a Cloudflare como socio de confianza, ya sea que recién estén comenzando a modernizar el acceso remoto o que estén volviendo a encarrilar un proyecto Zero Trust estancado.

La flexibilidad de implementación y la arquitectura modular de Cloudflare permiten a cualquier organización proteger y acelerar el rendimiento de dispositivos, aplicaciones y redes enteras para garantizar la protección y la productividad del trabajo híbrido. Para ello, admitimos la incorporación sin cliente para los usuarios finales, el aislamiento web sin cliente para contener el tráfico peligroso y un panel de gestión unificado que permite la visibilidad de todos los servicios de seguridad y red, independientemente del lugar desde el que se conecten los administradores o los usuarios. La amplitud de la red global de Cloudflare permite que la seguridad se aplique más cerca de los usuarios finales, minimizando la latencia y ofreciendo experiencias ágiles a los usuarios. Nuestra arquitectura Anycast ayuda a sortear las interrupciones de Internet, manteniendo a los equipos en línea y ayudando a garantizar la continuidad operativa.

Refuerza tu estado de seguridad con una implementación y un mantenimiento de políticas simplificados. El contexto compartido entre nuestras políticas ZTNA, CASB, DLP y SWG proporciona flujos de trabajo de administración coherentes; los mismos atributos de identidad y estado del dispositivo pueden informar las decisiones de políticas en todos los servicios.

ZTNA, RBI y la seguridad del correo electrónico también se pueden utilizar juntos para proporcionar acceso condicional a los recursos y aislar a los usuarios del contenido malicioso (enlaces, archivos adjuntos) en el correo electrónico y las herramientas de colaboración. Se puede proporcionar a los contratistas o empleados externos en dispositivos personales acceso con privilegios mínimos a recursos corporativos aislados con controles de datos basados en el navegador (p. ej., políticas DLP o controles amplios como deshabilitar la carga/descarga, copiar/pegar, entrada de teclado).



Estás en buena compañía

Gartner Peer Insights Customers' Choice 2024™

Cloudflare ha sido reconocido como la opción favorita de los clientes (Customers' Choice) en el informe "Voice of the Customer: Zero Trust Network Access" de Gartner® Peer Insights™, 2024.[1]

+100 mil

Fortune 500
Leer el caso práctico

trabajadores híbridos
con acceso seguro a Internet y a las aplicaciones.

+44 000

Delivery Hero
Comercio electrónico
Leer el caso práctico

usuarios protegidos a nivel mundial
sustitución de la VPN por Zero Trust para equipos de trabajo híbridos.

indeed
Sitio web de empleo n.º 1
Leer el caso práctico

3 meses

para reemplazar la VPN
para 13 000 empleados y 2000 contratistas.

THG
Comercio electrónico
Leer el caso práctico

1 semana

para migrar las políticas
y reemplazar Zscaler para más de 7000 trabajadores y simplificar las operaciones.

"Cloudflare Access llegó justo a tiempo para evitar que tuviéramos que implementar una VPN. Fue una elección fácil para nosotros, y su implementación fue sorprendentemente sencilla".

Conor Sherman
Jefe de seguridad
ezcater

"Antes de implementar Cloudflare, preparar una aplicación para una implementación segura implicaba un proyecto de 2 a 4 semanas. Con Cloudflare Zero Trust, nos ahorramos aproximadamente el 90 % de ese tiempo".

Ricardo Girardelli
Responsable de equipo de ingeniería de redes
creditas

Funciones de Access

Creación/edición de políticas Zero Trust para garantizar un acceso seguro	
Políticas de acceso detalladas y personalizadas	La definición unificada de aplicaciones permite una experiencia de administración de políticas uniforme. Las aplicaciones web están protegidas a nivel de subdominio y ruta con comodines y compatibilidad con varios nombres de host, y admiten solicitudes CORS. Los cambios de política se aplican globalmente en segundos. Incluye un evaluador de políticas.
Amplitud de recursos: qué podemos proteger y cómo	Los recursos utilizan nombres de host públicos para proxy inverso a aplicaciones autoalojadas (nube/locales) o SSH/RDP basado en navegador, proxy de identidad a aplicaciones SaaS o enrutamiento privado basado en cliente/túnel a través de proxy de reenvío L4-7 a cualquier web/recurso no web (p. ej., objetivo de infraestructura o TCP / UDP arbitrario) dentro de una subred privada. También admite recursos/flujos de trabajo con tráfico bidireccional (p. ej., VoIP/SIP o canal de CI/CD).
Identidad	Autentica a través de los principales proveedores de identidad (IdP) corporativa y de redes sociales, incluidos varios IdP en simultáneo. También puede utilizar conectores genéricos SAML y OIDC. Admite (y puede aplicar) cualquier método de autenticación proporcionado por el IdP, autenticación temporal, justificación del propósito, intervalos de reautenticación en base a la sesión global o por aplicación/política, y opción de revocación inmediata de la sesión por aplicación o por usuario. Puede utilizar el dispositivo del cliente (WARP) como método de autenticación (identidad en caché por sesión WARP).
Estado del dispositivo	Verifica el estado del dispositivo mediante integraciones de dispositivos del cliente y proveedores de protección de punto final (EPP) de terceros. Utiliza las integraciones de servicio a servicio (o la integración personalizada con cualquier API) para incorporar las puntuaciones de riesgo de EPP en las políticas Zero Trust.
Señales contextuales para políticas	Configura señales como grupo de correo electrónico, rangos de IP, geolocalización, método de inicio de sesión (p. ej., tipo de autenticación multifactor, tipo de IdP), certificado mTLS o SSH válido, token de servicio, lista de números de serie, atributos de estado del dispositivo, dispositivo del cliente instalado, duración de la sesión, aplicación de reglas SWG o señales de llamadas API externas. También puedes consultar de forma directa los contextos de autenticación de acceso condicional de Microsoft Entra ID.
Otro soporte relacionado	• **SCIM:** aprovisiona/desaprovisiona automáticamente a los usuarios para sincronizar los cambios en todos los IdP • **DNS interno:** configura el dominio de reserva local y resuelve las solicitudes de la red privada. • **División de túneles:** incluye/excluye direcciones IP para redes privadas o que funcionan junto a una VPN. • **Autenticación mTLS:** autenticación basada en certificados para IoT y otros casos de uso de mTLS. • **Aislamiento de aplicaciones:** con una sola casilla de verificación, aísla aplicaciones en nuestro navegador remoto ultrarrápido.*
Acceso de entrada y salida	
Conector de aplicaciones	La sencilla organización de nuestro conector de aplicaciones ligero (Cloudflare Tunnel) agiliza la conexión de recursos a Cloudflare, sin necesidad de infraestructura de máquinas virtuales y sin limitaciones de rendimiento. Incluye supervisión, redes virtuales (para solapamientos de direcciones IP) y funciones de redundancia y conmutación por error.
Dispositivo del cliente: cuándo utilizar	• **Sin cliente:** amplía las políticas Zero Trust a usuarios de terceros en dispositivos no gestionados; también se combina con RBI sin cliente para aplicar controles de datos (por ejemplo, bloquear/descargar, copiar/pegar) y políticas DLP de capa 7* a través del navegador. Admite aplicaciones web y SSH, RDP y VNC basados en navegador. • **Basado en el cliente:** nuestro dispositivo cliente (WARP) amplía el acceso seguro a las redes privadas, permite integraciones de estado del dispositivo de servicio a servicio y reconoce la ubicación para aplicar políticas personalizadas para los usuarios de la oficina. Admite el modo multiusuario en dispositivos Windows y utiliza el protocolo MASQUE para un mejor manejo del portal cautivo. Puede conectar dos o más dispositivos que ejecuten WARP para crear redes privadas. Los usuarios pueden autoinscribirse o implementar a través de MDM.
Extensibilidad y visibilidad	
Personalización de páginas	Utiliza un HTML personalizado para que las pantallas de bloqueo y de inicio de aplicaciones se adapten a tu marca o transmitan instrucciones de acceso específicas para agilizar la experiencia del usuario final.
Registro	Registro integral de eventos de autenticación y solicitudes a rutas URI protegidas/objetivos de infraestructura. Incluye registros SSH. Puede utilizar logpush o API para integrarse con las herramientas SIEM, de organización y de análisis existentes. Shadow IT Discovery ofrece visibilidad de las aplicaciones SaaS autorizadas y no autorizadas y de los orígenes de la red privada.
Automatización	API intuitivas y proveedor Terraform disponibles para gestionar mediante una programación todos los aspectos de una implementación Zero Trust. Pueden usar tokens de servicio para sistemas automatizados sin usuarios.

**usar capacidades en otras partes de la plataforma SSE/SASE*

¿Por qué Cloudflare?

Implementación más rápida y sencilla

Empieza a usar ZTNA rápidamente, simplifica la gestión diaria y escala fácilmente en todas las ubicaciones con accesos flexibles y un panel de control y API unificados.

Mejor experiencia del usuario final

Garantiza una aplicación de políticas rápida y uniforme cerca de los usuarios finales gracias a la escala masiva de Cloudflare y a la arquitectura de red Anycast con resiliencia integrada.

Arquitectura ágil para el futuro

Simplifica tu plan de modernización a largo plazo con una red unificada y un plano de control de servicios modulares nativos de nube diseñados para funcionar en conjunto.

Hablemos de un acceso sencillo y seguro para tu organización.

Solicitar seminario

CLOUDFLARE

¿Necesitas más tiempo?

Para más información, consulta nuestra arquitectura de referencia SASE, o comprueba cómo funciona en un recorrido interactivo por nuestra plataforma Zero Trust.

1. Gartner, Voice of the Customer for Zero Trust Network Access, Peer Contributors, 30 de enero de 2024. GARTNER, PEER INSIGHTS y el distintivo Gartner Peer Insights Customers' Choice son marcas comerciales de Gartner, Inc. y/o sus filiales, y se utilizan aquí con permiso. Todos los derechos reservados. El contenido de Gartner Peer Insights se basa en las opiniones de usuarios finales individuales en función de sus propias experiencias con los proveedores enumerados en la plataforma y no se deben interpretar como declaraciones de hecho, ni tampoco representan las opiniones de Gartner o de sus afiliadas. Gartner no respalda a ningún proveedor, producto o servicio descrito en este contenido ni concede ninguna garantía, expresa o implícita, con respecto a este contenido, su precisión o integridad, incluso cualquier garantía de comerciabilidad o idoneidad para un propósito particular.