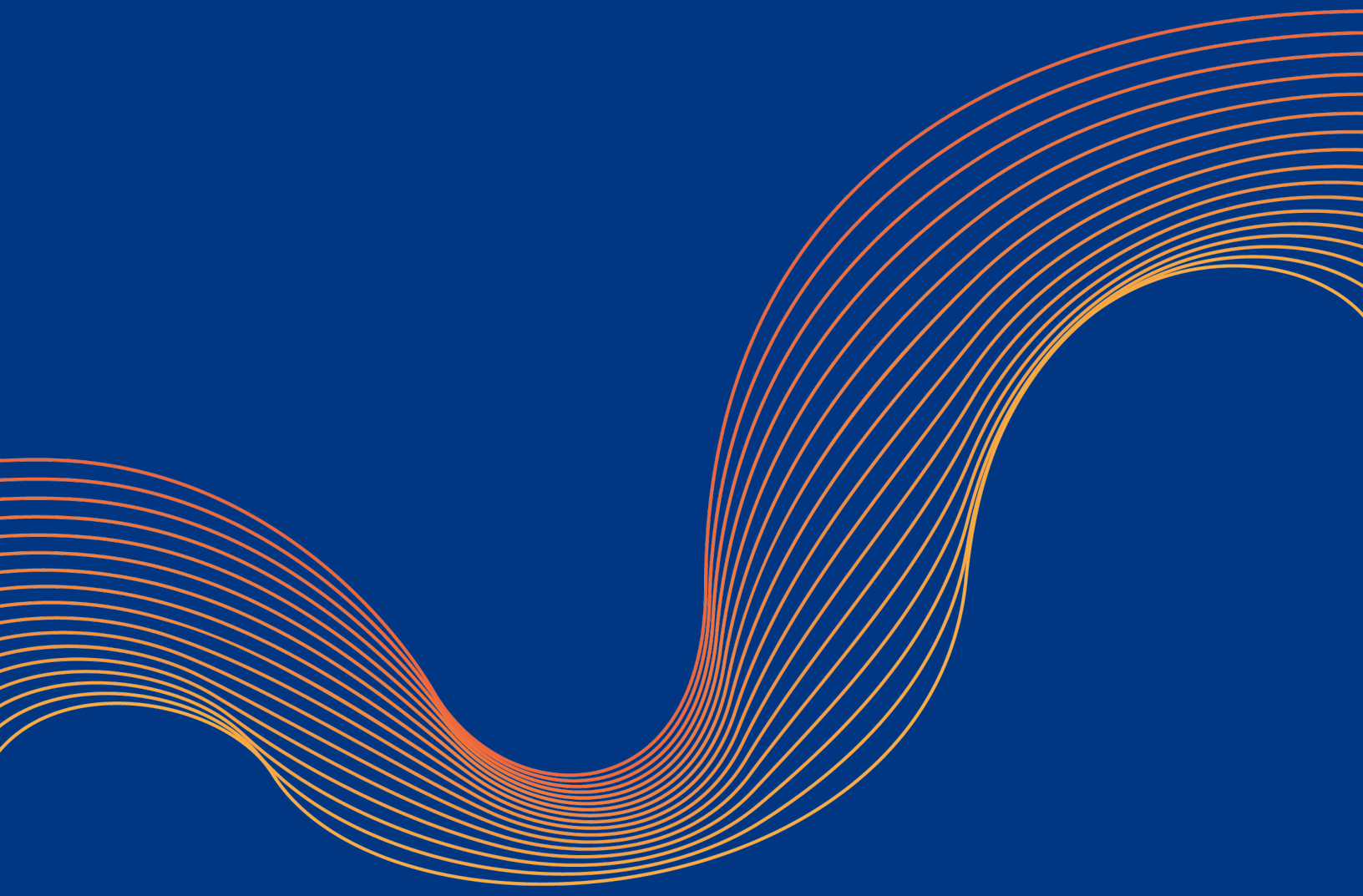
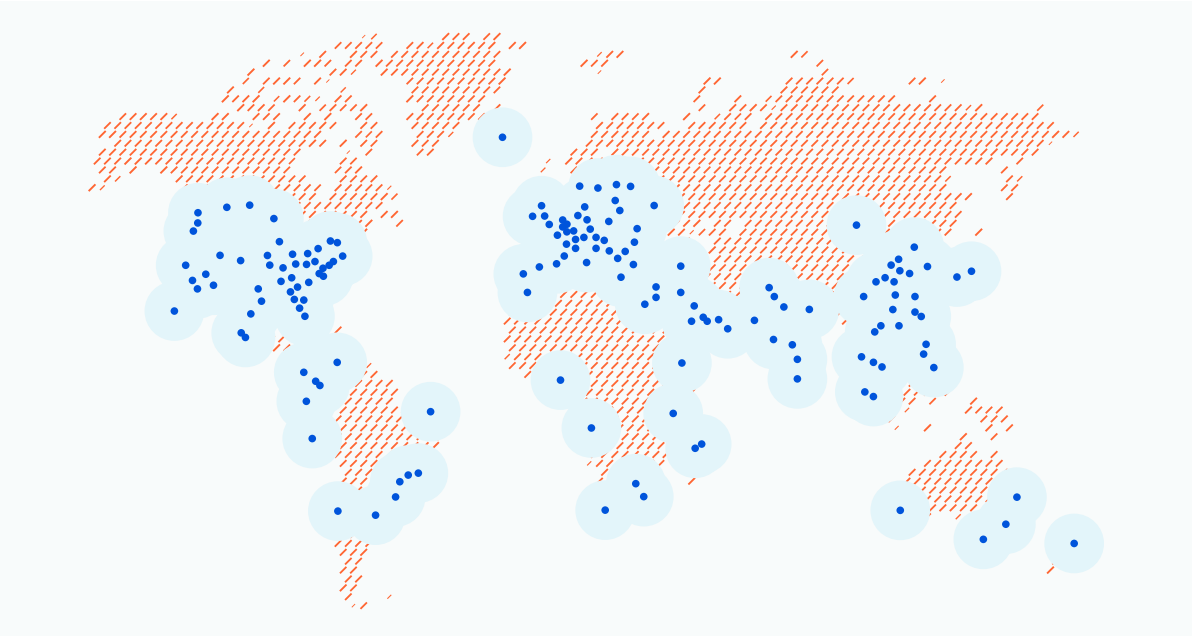
DOCUMENTO TÉCNICO

CLOUDFLARE

Cómo ayuda Cloudflare a abordar la ubicación de los datos y las obligaciones de privacidad en Europa



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



La exclusiva red global en la nube de Cloudflare cuenta con una presencia física de más de 200 puntos en más de 100 países. Cloudflare ofrece herramientas para administrar la manera en que tus datos confidenciales circulan alrededor de estos centros de datos, de modo que puedas personalizar tu tráfico para satisfacer tus necesidades de seguridad, privacidad y funcionamiento.

Cloudflare y la confianza del cliente

La misión de Cloudflare es ayudar a crear un Internet mejor. Brindamos una plataforma global en la nube que ofrece una amplia gama de servicios de red a particulares y empresas de todos los tamaños en todo el mundo. La red de Cloudflare y su creciente cartera de productos mejoran la seguridad, el funcionamiento y la fiabilidad de todo lo que está conectado a Internet. Además de prestar servicio a nuestros clientes, la misión de Cloudflare también es ayudar a mejorar el propio Internet, siempre activo, siempre rápido, siempre seguro, siempre privado y disponible para todos.

La red, la comunidad de desarrolladores y el negocio de Cloudflare se sustentan, en última instancia, en la confianza de nuestros clientes. Tratamos permanentemente de ganarnos y mantener la confianza de los clientes siendo claros en cuanto a nuestro compromiso con la privacidad de los datos y la manera en que gestionamos los datos de los clientes y los usuarios finales en nuestros sistemas. También creamos confianza construyendo e implementando productos que (i) ayudan a mejorar la seguridad de nuestros sistemas, (ii) encriptan los datos en reposo o en tránsito, y (iii) permiten a nuestros clientes determinar cómo se inspecciona el tráfico en diferentes ubicaciones en el mundo. Por último, conquistamos la confianza de los clientes asegurando y manteniendo las certificaciones establecidas por el sector (por ejemplo, SSAE 18 SOC 2 Tipo II) y proporcionando mecanismos de contratación (por ejemplo, Acuerdos de procesamiento de datos) que comunican nuestro modelo de responsabilidad compartida con nuestros clientes para garantizar la privacidad.

Cloudflare en Europa

Hoy en día, más de 25 millones de propiedades mundiales de Internet utilizan Cloudflare. Esta lista incluye muchas de las empresas más grandes y de crecimiento más rápido de Europa, entre ellas Eurovisión, L'Oreal, AO.com, AllSaints y muchas otras marcas conocidas. También comprende una lista cada vez más amplia de instituciones importantes de Europa, entre ellas INSEAD, Börse Stuttgart, IATA y Great Rail Journeys. A medida que las empresas y organizaciones de todos los tamaños confían cada vez más en Internet como plataforma fundamental para atender a sus clientes, usuarios y partes interesadas, están adoptando con rapidez redes en la nube seguras y fiables como Cloudflare para ayudar a proteger sus aplicaciones, infraestructuras y a las personas frente a amenazas de todo tipo en Internet.

La plataforma de Internet de Cloudflare se ha diseñado para apoyar a los sectores europeos regulados y más sensibles a la protección de la privacidad, entre los que se encuentran los servicios financieros, el sector público, la energía, los servicios públicos, el comercio minorista, los videojuegos y la atención sanitaria. En Cloudflare desarrollamos nuestros productos conforme a las normas más exigentes de seguridad y privacidad del usuario, y colaboramos estrechamente con cada uno de nuestros clientes europeos para ayudarles a cumplir con las obligaciones de protección de datos asociadas a su ubicación específica y a su segmento empresarial.

El compromiso corporativo distintivo de Cloudflare con la privacidad

Cloudflare se ha diseñado para ayudarte a ti y a tus clientes a estar más seguros en Internet. Nuestra red y todos nuestros productos se han diseñado con la protección de datos en mente. Somos una empresa que prima la privacidad; en nuestra Política de privacidad nos comprometemos a no vender los datos personales que procesamos en tu nombre, ni a utilizarlos para ningún otro propósito que no sea el de proporcionarte nuestros servicios. A lo largo de nuestra historia, nunca hemos incumplido esta promesa. De hecho, nuestra postura sobre la privacidad estaba definida mucho antes de que los gobiernos comenzarán a regular la privacidad de manera que se obligaba a muchas otras empresas de tecnología a actualizar sus prácticas para dar la prioridad adecuada a la privacidad de los clientes y usuarios. No generamos ingresos por publicidad y, por lo tanto, nos abstenemos de recopilar y retener los datos personales que procesamos en tu nombre.

Como procesador de datos y proveedor de servicios, Cloudflare procesa los datos de registro de los usuarios finales en nombre de nuestros clientes cuando sus usuarios finales acceden a nuestros servicios conforme a la autorización de nuestros clientes. Estos datos de registro procesados pueden incluir, entre otros, direcciones IP, información de configuración del sistema y otra información sobre el tráfico hacia y desde los sitios web, dispositivos, aplicaciones o redes de nuestros clientes. Nuestra Política de privacidad describe la información que recopilamos y cómo la utilizamos. Además, en nuestro papel de controlador de datos, Cloudflare recopila y almacena datos y registros de actividad del servidor y de la red en el curso de la operación del servicio y hace observaciones y análisis de los datos de tráfico (llamamos a estos datos “métricas operativas”). Entre los ejemplos de métricas operativas se incluyen las métricas de tiempo de actividad y disponibilidad del servicio, volúmenes de solicitud, tasas de error, tasas de caché y puntuaciones de amenaza de IP.

Cuando recopilamos y almacenamos datos de la actividad en nuestra red, lo hacemos solo para mejorar nuestros productos para ti, para nuestros otros clientes y para la comunidad de Internet en general. No buscamos monetizar estos datos de ninguna manera que pensemos que te pudiera sorprender. Por ejemplo, podemos almacenar y analizar temporalmente los datos de tráfico de la red de todos nuestros clientes en el mundo para poder dirigir de manera inteligente a los usuarios finales por las rutas menos congestionadas y más fiables de Internet. También podemos almacenar y analizar los datos de la red para detectar e identificar los vectores de amenazas emergentes que podemos utilizar inmediatamente para actualizar la manera en que nuestros productos protegen tus propiedades de Internet. Por último, podemos agregar datos de red de segmentos considerablemente grandes de nuestros clientes (pero nunca de usuarios o clientes identificables individualmente) para ayudar a la comunidad de Internet a comprender los conocimientos, las amenazas y las tendencias en toda la red (consulta el servicio Radar de Cloudflare). En última instancia, los datos de la red que recopilamos y almacenamos solo se utilizan para mejorar nuestra red y los productos que ofrecemos a nuestros clientes, o para compartir las tendencias globales de la red con la comunidad de Internet en general.

A continuación presentamos algunos de los compromisos de privacidad que asumimos y que nos diferencian de muchos otros proveedores de servicios en la nube:

- Cloudflare no vende datos personales.
- Cloudflare no rastrea a los usuarios finales de nuestros clientes a través de las propiedades de Internet.
- Cloudflare no elabora perfiles de los usuarios finales de nuestros clientes para vender anuncios.
- Cloudflare solo conserva los datos personales necesarios para proporcionar ofertas de Cloudflare a nuestros clientes.
- Cloudflare nunca ha proporcionado ni a terceros ni a gobiernos las claves de encriptación de nuestros clientes o cualquier otra fuente de contenido de los clientes que transitan por nuestra red. Tenemos el compromiso desde hace mucho tiempo de que agotaremos todos los recursos legales antes de cumplir con tal solicitud.
- Cloudflare se ha comprometido públicamente a buscar los recursos legales para impugnar cualquier solicitud de datos del Gobierno de los EE. UU. que identifiquemos como sujetos al RGPD (Reglamento General de Protección de Datos).
- La política de Cloudflare es notificar a nuestros clientes cualquier proceso legal en el que se solicite su información antes de revelarla, a menos que esté legalmente prohibido.

Funciones del producto Cloudflare diseñadas para reforzar la protección de datos

Nuestros clientes europeos suelen utilizar las siguientes funciones para configurar su implementación de Cloudflare con el fin de ayudar a cumplir sus obligaciones legales en cuanto a la manera en que deben manejarse los datos:

Seguridad del panel de control y del portal:
El panel de control de Cloudflare ofrece una interfaz de usuario fácil de usar para que los clientes configuren y administren todos los productos que utilizan y que se ejecutan en la red de Cloudflare. Los clientes inician sesión en el panel de control de Cloudflare a través de los portales web seguros de Cloudflare. Para ayudar a los clientes a garantizar un acceso seguro y autorizado a las cuentas y datos de los clientes de Cloudflare, hemos incorporado funciones de seguridad estandarizadas en nuestros portales y en el panel de control. Hemos observado que muchas empresas y organizaciones se esfuerzan por asegurar el acceso a sus diferentes dispositivos, productos y servicios de seguridad. En cambio, los productos de Cloudflare se desarrollan sobre una plataforma única, unificada y segura, por lo que los clientes de Cloudflare se benefician de un acceso a la cuenta permanente y sumamente seguro para todos sus productos de seguridad, funcionamiento y fiabilidad.

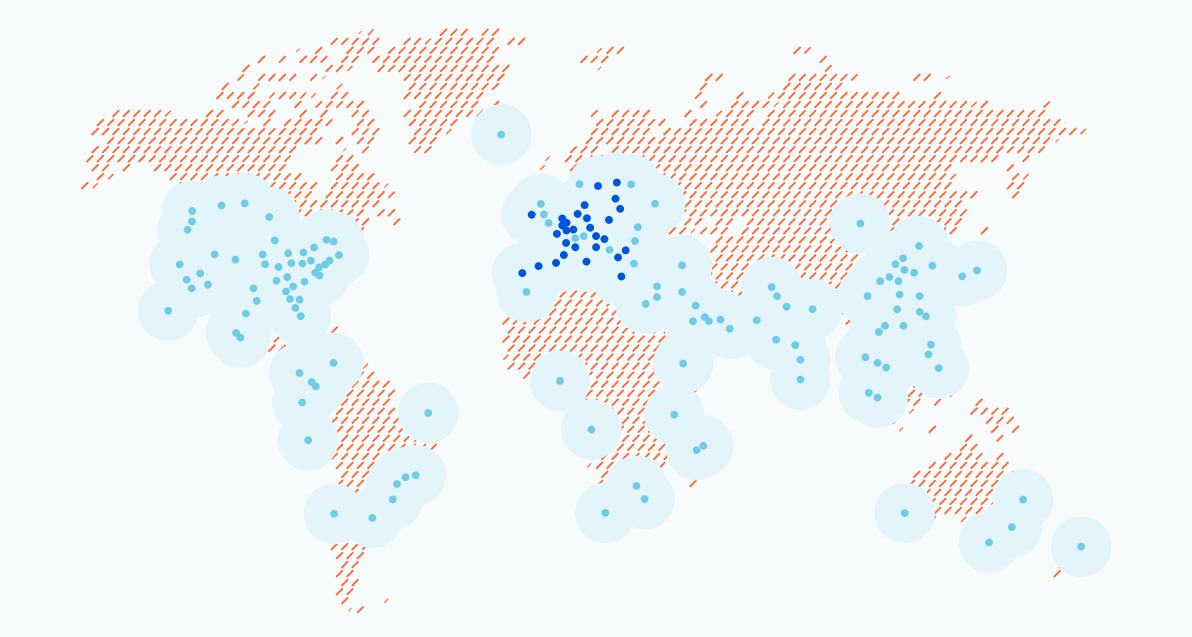
- La **autenticación en dos fases** (2FA) aumenta la seguridad de la cuenta mediante la solicitud de un segundo dato para validar la identidad del usuario al iniciar la sesión. La 2FA de Cloudflare admite tokens de hardware y aplicaciones móviles TOTP (Time-based One Time Password, contraseña temporal de un solo uso).
- Las funciones de **inicio de sesión único** (cuando están habilitadas) permiten a los clientes utilizar un proveedor de identidad local o alojado en la nube para el control de acceso. Consulta la lista completa de proveedores admitidos aquí.
- Los **registros de auditoría** resumen el historial de acceso y los cambios realizados en la configuración de Cloudflare de un cliente. Los registros de auditoría incluyen acciones a nivel de la cuenta como iniciar y cerrar sesión, así como la aplicación de cambios en las funciones de DNS, Crypto, Firewall, Speed, Caching, reglas de página, Network, Traffic, etc. Los registros de auditoría están disponibles en todos los tipos de planes y se capturan tanto para usuarios individuales como para organizaciones de múltiples usuarios.

Encriptación:
La encriptación es una forma de codificar los datos de manera que solo las partes autorizadas puedan comprender la información. Los datos se pueden encriptar “en reposo” cuando se almacenan o “en tránsito” mientras se están transmitiendo a otra ubicación. La encriptación de los datos transmitidos por una red requiere el uso de una clave de encriptación: un conjunto de valores matemáticos que conocen tanto el remitente como el destinatario de un mensaje encriptado.

La encriptación impide que partes no autorizadas, ya sean atacantes, redes publicitarias, proveedores de servicios de Internet o agentes extranjeros hostiles, intercepten y lean datos confidenciales. Las comunicaciones encriptadas permiten a las partes comunicantes intercambiar datos confidenciales sin que se produzcan filtraciones. La encriptación también ayuda a prevenir comportamientos maliciosos como los ataques en ruta. Muchas regulaciones del sector y gubernamentales requieren que las compañías que manejan los datos de los usuarios mantengan esos datos encriptados. Entre los ejemplos de normas reglamentarias y de cumplimiento que exigen la encriptación se incluyen la Ley de portabilidad y responsabilidad del seguro médico (HIPAA) de 1996, el Estándar de seguridad de datos de la industria de las tarjetas de pago (PCI DSS) y el RGPD.

Cloudflare ofrece los productos de “red como servicio” más seguros y de mayor funcionamiento porque utilizamos servidores proxy para la totalidad de tu tráfico directamente desde el extremo de nuestra red. Como servidor proxy autorizado de tu tráfico, lo inspeccionamos de manera segura para identificar las amenazas a la seguridad y enrutarlo desde cualquier ubicación de nuestra red global. Cloudflare te otorga el control completo sobre dónde y cómo se inspecciona el tráfico. Cloudflare es uno de los únicos proveedores de la nube diseñados como una plataforma global unificada que también puede configurarse para responder a requisitos regionales específicos.

> Los servicios regionales ceden a las organizaciones el control sobre dónde se inspecciona su tráfico. Con los servicios regionales habilitados, el tráfico de contenido se incorpora a la red global Anycast de Cloudflare en la ubicación más próxima al cliente. En lugar de ser inspeccionado en ese punto de presencia (PoP), este tráfico se transmite de manera segura a los PoP de Cloudflare dentro de la región o regiones seleccionadas por el cliente, donde luego se le presta servicio. Si también se aplica la función Geo Key Manager, las TLS keys del cliente solo se almacenan y se utilizan para manejar el tráfico de contenido dentro de esas regiones. Los servicios regionales ayudan a los clientes que desean mantener el control local sobre su tráfico, conservando al mismo tiempo las ventajas de seguridad de una red global.



Por ejemplo, un cliente de Cloudflare en Alemania podría permitir a los servicios regionales limitar la prestación de servicios a la UE. Sus clientes finales se conectarán a la ubicación de Cloudflare más próxima en cualquier parte del mundo, pero si esa ubicación está fuera de la UE, el tráfico se pasa a una ubicación de Cloudflare en la UE antes de ser inspeccionado. El cliente sigue recibiendo el beneficio de nuestra red global de baja latencia y alta capacidad, que es capaz de soportar incluso los mayores ataques DDoS. No obstante, los servicios regionales también otorgan a los clientes el control local; solo los centros de datos dentro de la UE tendrán el acceso necesario para aplicar las políticas de seguridad. Este enfoque permite a Cloudflare seleccionar la ruta más rápida hacia la UE y el punto de presencia más próximo disponible para el procesamiento.

Además de especificar dónde se inspecciona el tráfico, Cloudflare ayuda a las empresas a proteger a los usuarios y los datos utilizando técnicas y tecnologías de encriptación líderes en el sector. Las funciones Geo Key Manager y SSL sin clave otorgan a los clientes un control total sobre dónde se almacenan las claves y qué PoP tienen acceso a esas claves.

SSL sin clave permite al cliente almacenar y administrar sus propias claves privadas SSL para su uso con Cloudflare. Los clientes pueden utilizar una variedad de sistemas para su depósito de claves, incluidos módulos de seguridad de hardware ("HSM"), servidores virtuales y hardware compatible con Unix/Linux y Windows y que esté alojado en entornos controlados por los clientes. SSL sin clave emplea varios métodos para crear una conexión segura para la transmisión de la clave del cliente a Cloudflare, y permite la persistencia de la sesión, lo que normalmente acelera la velocidad general de la transacción SSL.

La función Geo Key Manager otorga a los clientes un control granular sobre dónde se almacenan sus claves. Por ejemplo, un cliente puede elegir que las claves privadas solo sean accesibles dentro de los PoP ubicados en la UE.

Con Cloudflare, los clientes tienen un amplio control no solo sobre la ubicación de las claves privadas, sino también sobre la ubicación donde se inspecciona realmente el tráfico en busca de amenazas a la seguridad. Si el cliente lo elige, solo podrán inspeccionar el tráfico los PoP ubicados dentro de los estados miembros de la UE.

Certificaciones de seguridad de Cloudflare en Europa y en el mundo

Cloudflare cumple las principales normativas del sector en materia de seguridad y privacidad, y valida anualmente esos compromisos con auditores externos. Cloudflare cumple la norma ISO 27001/27002, el estándar PCI DSS y la SSAE 18 SOC 2 Tipo II. Hemos firmado acuerdos de asociación comercial y podemos respaldar a las empresas sujetas a la HIPAA. Estas validaciones ofrecen garantías a las organizaciones que transfieren sus datos más confidenciales a través de nuestros servicios, y también les ayudan a cumplir y mantener sus propias obligaciones de cumplimiento.

Además de las evaluaciones periódicas de terceros con respecto a las normativas del sector, Cloudflare se considera un "Operador de servicios esenciales" en virtud de la Directiva de la UE sobre la seguridad de las redes y los sistemas de información (Directiva NIS). Además de registrarse bajo esta directiva con la ICO y Ofcom en el Reino Unido, BSI en Alemania, y CNCS en Portugal, Cloudflare también ha sido evaluado con respecto a requisitos regionales específicos, como la Ley BSI en Alemania (BSIG). Mantenemos nuestras relaciones con los reguladores regionales europeos y trabajamos en estrecha colaboración con ellos en lo que respecta al cumplimiento, a la vez que facilitamos información sobre cómo estamos abordando los requisitos de protección de datos.

A nivel práctico, el RGPD de Europa era una codificación de muchos de los pasos que ya estábamos dando:

- Cloudflare solo recoge los datos personales que necesitamos para proporcionar el servicio que ofrecemos.
- Cloudflare no vende información personal.
- Cloudflare otorga a los usuarios la capacidad de acceder, corregir y eliminar su información personal.
- En consonancia con nuestro papel como procesador de datos, Cloudflare cede a los clientes el control sobre la información que, por ejemplo, se almacena en la caché de nuestra red de entrega de contenido (CDN), en el almacén de valores clave de Workers o en nuestro firewall de aplicaciones web (WAF).

Puedes leer nuestras Preguntas frecuentes sobre el RGPD aquí: cloudflare.com/gdpr/introduction.

Dado que nos preocupamos por la protección de los datos, no nos limitamos a auditar cuando la ley nos obliga a hacerlo o cuando disponemos de certificaciones. Nuestro equipo responsable de la seguridad realiza rigurosas pruebas de penetración internas y externas, dirigimos un programa de recompensas por errores a través de HackerOne y contamos con auditores externos para validar nuestros compromisos de privacidad. Un ejemplo claro son las auditorías centradas en la privacidad, como la que realizamos a principios de este año en relación con nuestros compromisos para nuestra solución de DNS pública 1.1.1.1. Siempre estamos abiertos a la obtención de validaciones adicionales que aporten seguridad a nuestro programa, políticas y prácticas de privacidad para el procesamiento y almacenamiento de datos personales de la UE.

Mecanismos de transferencia de datos de Cloudflare

Los tipos de datos personales que Cloudflare procesa en nombre de un cliente dependen de qué servicios de Cloudflare haya implementado. La gran mayoría de los datos que transitan por la red de Cloudflare permanecen en los servidores perimetrales de Cloudflare, mientras que los datos de registro sobre esta actividad pueden ser procesados en nombre de nuestros clientes en nuestro centro principal de datos en los Estados Unidos, incluso cuando los clientes habilitan los servicios regionales.

Algunos de estos datos de registro incluirán información sobre los visitantes y usuarios autorizados de los dominios, redes, sitios web, interfaces de programación de aplicaciones ("API") o aplicaciones de nuestros clientes. Estos metadatos contienen datos personales extremadamente limitados, la mayoría de las veces en forma de direcciones IP. Procesamos este tipo de información en nombre de nuestros clientes en nuestro centro principal de datos en los EE. UU. durante un periodo de tiempo limitado.

Puesto que algunos datos personales limitados se transfieren a los Estados Unidos, hemos facilitado a las empresas el mantenimiento de un mecanismo válido de transferencia de datos cuando utilizan los servicios de Cloudflare. Nuestro Acuerdo de procesamiento de datos (DPA) se incorpora a nuestro Acuerdo de servicio de empresa, y el DPA incorpora las Cláusulas contractuales estándar (SCC) de la UE en lo relativo a los datos sujetos al RGPD. En conjunto, los términos de Cloudflare aseguran un nivel de protección de los datos personales equivalente al garantizado por el RGPD. Puedes encontrar más información sobre nuestro compromiso con el RGPD y sobre nuestro DPA aquí.

El 16 de julio de 2020, el Tribunal de Justicia de la Unión Europea ("TJUE") emitió una decisión que invalidaba el paradigma del marco del Escudo de Privacidad entre la UE y los EE.UU. en el caso "Schrems II". Como resultado, algunos de nuestros clientes que procesan los datos de residentes en la UE nos han preguntado qué implica esta decisión para la legalidad de la transferencia de los procesos de datos de Cloudflare en su nombre a los Estados Unidos. En primer lugar, la invalidación del Escudo de Privacidad no cambia las rigurosas protecciones de privacidad de datos que Cloudflare tiene en vigor para los datos personales que procesamos en nombre de nuestros clientes, y continuaremos aplicando los principios de protección de datos a los que nos comprometimos cuando obtuvimos la certificación del Escudo de Privacidad.

En virtud de la decisión de Schrems II, las SCC aprobadas por la Unión Europea siguen siendo un mecanismo de transferencia válido en el marco del RGPD, en el que también se aplican medidas de protección adicionales a los datos transferidos a los Estados Unidos. Cloudflare seguirá utilizando el mecanismo de las SCC para las transferencias de datos, y hemos actualizado nuestro DPA estandarizado de clientes para incorporar medidas de protección adicionales como compromisos contractuales. Por ejemplo, nos comprometemos a buscar recursos legales para impugnar cualquier solicitud del Gobierno de los Estados Unidos de datos que identifiquemos como sujetos al RGPD, y nos comprometemos a notificar a nuestros clientes cualquier proceso legal en el que se solicite su información antes de divulgarla, a menos que esté legalmente prohibido. Puedes consultar las medidas de protección adicionales que hemos añadido como compromisos contractuales en la sección 7 de nuestro DPA.

Los reglamentos y directrices de protección de datos están en constante evolución, por lo que vigilamos de cerca el panorama normativo y legislativo. Nos mantenemos atentos a las nuevas directrices para garantizar que nuestros clientes y socios puedan seguir disfrutando de los beneficios de Cloudflare en toda Europa.

Oportunidades y responsabilidades compartidas

Puesto que sabemos que todas las organizaciones europeas necesitan integrar los principios de privacidad y seguridad en cada fase de su actividad, hemos preparado este cuadro para que puedas comprender fácilmente quién es responsable de estos requisitos de privacidad habitualmente solicitados:

Principio	Responsabilidad	Información sobre la responsabilidad
Protección de datos por diseño	Compartido	Cloudflare tiene la responsabilidad de entregar productos y servicios teniendo en cuenta la privacidad. El equipo responsable de la privacidad proporciona revisiones, evaluaciones y formación para asegurar que la privacidad se inculque en nuestra manera de trabajar. Los clientes son responsables del uso y la configuración de sus servicios Cloudflare, y deben revisar periódicamente su uso y la configuración de estos servicios para validar que se hayan observado los principios de protección de datos en el diseño y la implementación.
Solicitud de acceso del interesado	Compartido	Cloudflare otorga a los sujetos de los datos el derecho de acceso, corrección y eliminación de la información personal, independientemente de su jurisdicción de residencia. El interesado puede enviar sus solicitudes a sar@cloudflare.com. En caso de recibir una solicitud de una persona que parezca ser un usuario final de uno de nuestros clientes, le indicaremos que se ponga en contacto con nuestro cliente directamente.

Principio	Responsabilidad	Información sobre la responsabilidad
Seguridad eficiente	Compartido	Cloudflare mantiene un programa de seguridad conforme a las normas del sector. El programa de seguridad incluye el mantenimiento de políticas y procedimientos de seguridad formales, el establecimiento de controles de acceso lógico y físico adecuados, la implementación de medidas técnicas de protección en entornos corporativos y de producción (incluidos el establecimiento de configuraciones, transmisiones y conexiones seguras, registro y monitorización) y la existencia de tecnologías de encriptación idóneas para los datos personales. Los clientes son responsables de revisar las medidas de seguridad de sus proveedores de la nube como Cloudflare, y pueden hacerlo revisando nuestras validaciones e informes de cumplimiento. También animamos a nuestros clientes a que revisen la configuración de seguridad de sus paneles de control para asegurarse de que se adhieren a sus políticas y procedimientos de seguridad.
Fundamentos jurídicos para el procesamiento	Compartido	Cloudflare procesa los datos de acuerdo con las instrucciones de nuestros clientes, es decir, los controladores de datos, y funciona como un procesador de datos conforme al RGPD. Los clientes son responsables de garantizar que tienen un fundamento jurídico adecuado para procesar los datos de sus usuarios finales.
Fuga de datos personales	Compartido	Cloudflare notificará a los clientes tan pronto como tengamos conocimiento cualquier vulneración de la seguridad que dé lugar a la pérdida, divulgación no autorizada o acceso a los datos personales procesados por Cloudflare o sus procesadores subsidiarios. Cloudflare también es responsable de proporcionar a nuestros clientes cooperación y asistencia razonables en relación con la vulneración, lo que incluye facilitar a los clientes la información razonable que obre en poder de Cloudflare sobre las circunstancias de la vulneración y los datos personales afectados. Los clientes son responsables de cumplir con los requisitos regulatorios o contractuales para notificar a sus usuarios finales y las autoridades gubernamentales cualquier vulneración de datos personales.

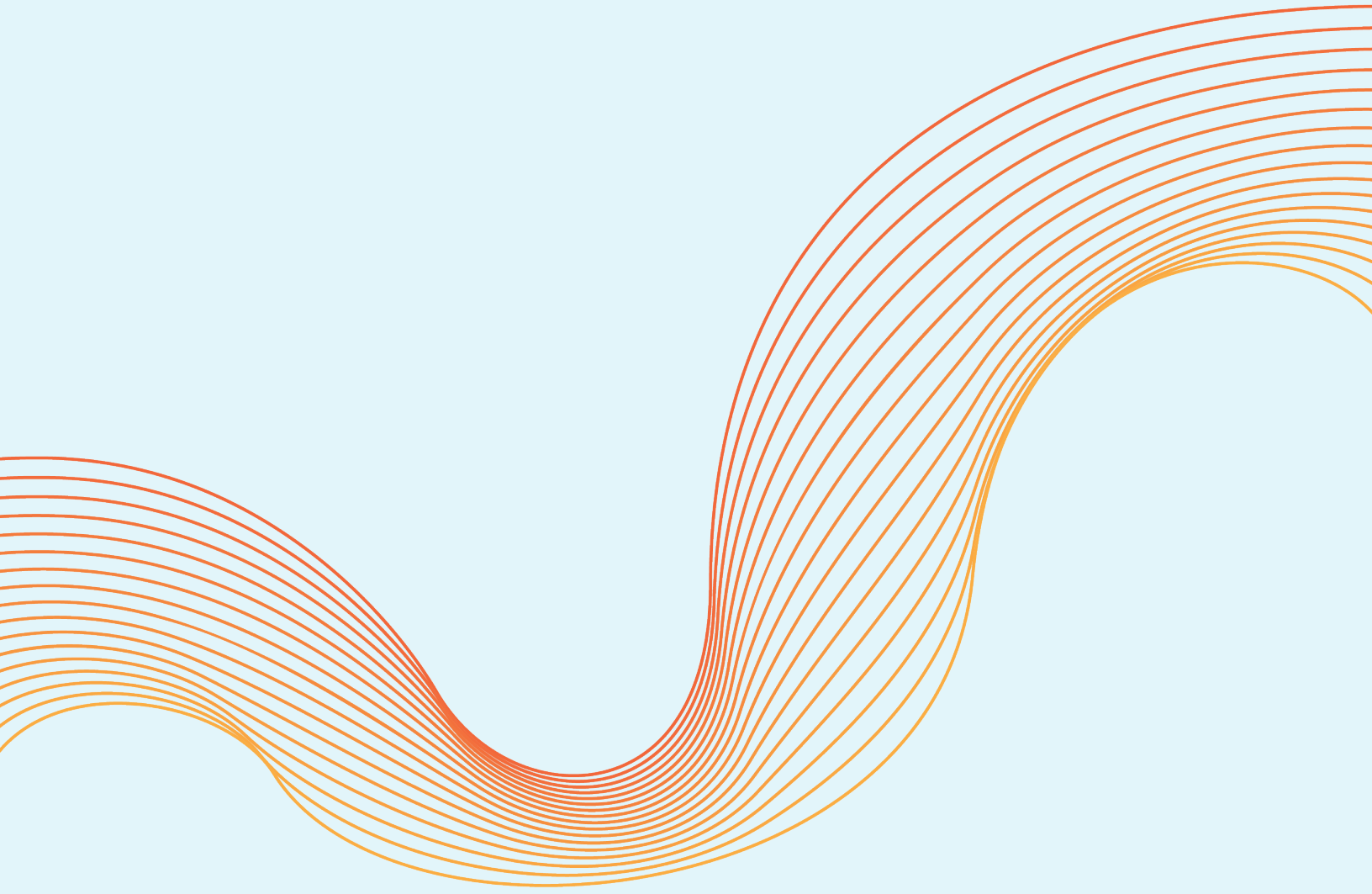
Una red global en la nube construida sobre la confianza de los clientes

La principal prioridad de Cloudflare es ganarse la confianza de los clientes y mantenerla. Entendemos que la transparencia en los compromisos de privacidad de Cloudflare, así como en nuestro enfoque para la construcción de medidas de protección de la privacidad y la ubicación de los datos en nuestra red y productos, ayuda a los clientes a cumplir con sus propias obligaciones. También entendemos que las certificaciones del sector de Cloudflare y los mecanismos de contratación bien diseñados nos ayudan a crear una sólida relación de confianza con nuestros clientes europeos.

Los equipos responsables de la privacidad y la seguridad de Cloudflare están aquí para colaborar contigo y abordar los requisitos más estrictos a los que te puedes enfrentar en tu país, región o sector. Nuestros experimentados ejecutivos de cuentas, responsables de satisfacción del cliente y técnicos de ventas colaboran regularmente con nuestros equipos de cumplimiento de la privacidad y la seguridad para ayudar a nuestros clientes a configurar los productos de Cloudflare que utilizan para responder a sus obligaciones de cumplimiento específicas. Si deseas solicitar una demostración o una sesión especializada sobre la configuración de tus servicios para cumplir con tus obligaciones específicas, ponte en contacto con nosotros hoy mismo. Envíanos un correo electrónico a privacyquestions@cloudflare.com o security@cloudflare.com.

MÁS INFORMACIÓN

1. **Descripción de los servicios de registro de Cloudflare**
2. **Administración y análisis de los registros**
3. **Preguntas frecuentes sobre los registros**
4. **Ponte en contacto con nosotros** para habilitar los servicios regionales



© 2020 Cloudflare Inc. Todos los derechos reservados. El logotipo de Cloudflare es una marca comercial de Cloudflare. Todos los demás nombres de empresas y productos pueden ser marcas comerciales de las respectivas empresas a las que están asociados.