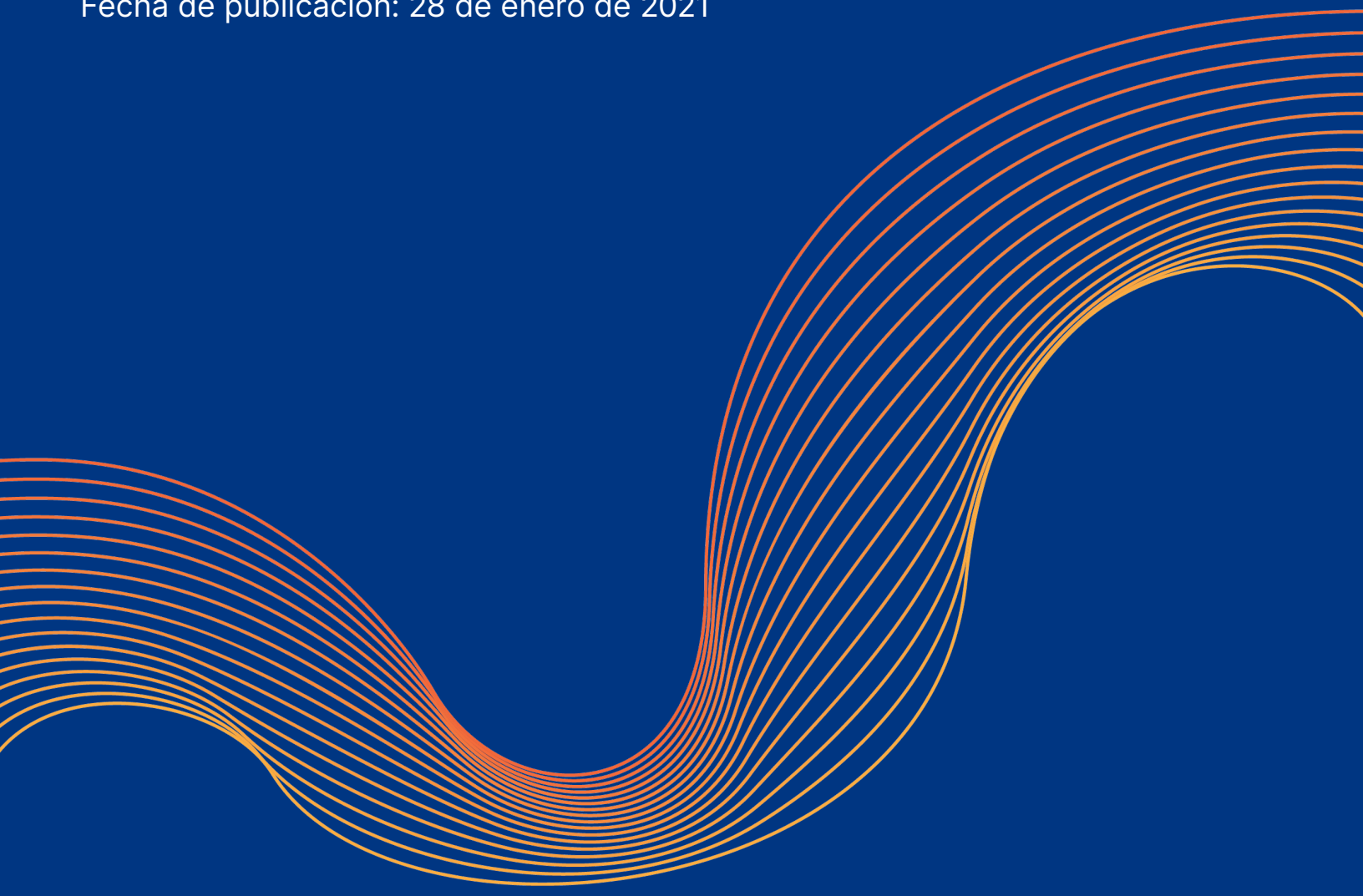
DOCUMENTO TÉCNICO

CLOUDFLARE

Cloudflare: Políticas de privacidad y gestión de las solicitudes gubernamentales de información

Fecha de publicación: 28 de enero de 2021



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

La red y la actividad de Cloudflare se sustentan sobre todo en la confianza de los clientes. Aspiramos a ganar y mantener continuamente esa confianza diseñando e implementando productos que permitan mejorar la seguridad de nuestro sistema, cifrar los datos en reposo o en tránsito y ayudar a nuestros clientes a decidir cómo se inspecciona el tráfico en diferentes lugares del mundo.

Pero la ingeniería no es la solución a todos los problemas. Por esta razón, también tenemos políticas y procedimientos que rigen la gestión de los datos de los clientes y usuarios finales en nuestros sistemas, y también la forma en la que abordamos las solicitudes de datos por parte de los gobiernos y otros organismos legales.

En este documento se describen estas políticas y se ofrecen enlaces a información más detallada sobre diversos aspectos de nuestro enfoque en cuanto a la privacidad de los datos y la conformidad. En concreto, incluye:

- Nuestro punto de vista sobre los cambios que se están produciendo en el panorama de la privacidad de los datos
- Nuestras políticas en torno a la privacidad y las solicitudes de datos

Cambios en el panorama de la privacidad de los datos

El auge de servicios en la nube y el hecho de que los datos puedan almacenarse fuera de los países de residencia de quienes los generaron han supuesto un reto para los gobiernos que llevan a cabo investigaciones policiales. Los proveedores de servicios en línea de todo tipo suelen ser un punto de acceso a esos registros electrónicos.

Para los proveedores de servicios como Cloudflare, las solicitudes gubernamentales de información pueden plantear muchas dificultades. El trabajo que desempeñan las fuerzas del orden público y otras autoridades estatales es importante. Al mismo tiempo, los datos que nos solicitan no nos pertenecen. Al utilizar nuestros servicios, nuestros clientes nos han confiado sus datos y mantener esa confianza es fundamental para nuestro negocio y nuestros valores.

Estas tensiones se ven agravadas por el hecho de que cada gobierno tiene diferentes normas en materia de protección de datos personales. Estados Unidos, por ejemplo, prohíbe a las empresas revelar el contenido de las comunicaciones, incluso a otros gobiernos, salvo en determinadas circunstancias definidas por ley. La Unión Europea, que durante mucho tiempo ha considerado que la privacidad es un derecho humano fundamental, protege todos los datos personales de los ciudadanos de la Unión Europea mediante el Reglamento General de Protección de Datos (RGPD). Aunque estas protecciones se superponen en ciertos aspectos, difieren en lo relativo a su alcance y a quiénes protegen.

Las diferencias entre los distintos marcos jurídicos son importantes, en particular cuando se trata de determinar si las solicitudes legales de información procedentes de gobiernos extranjeros son compatibles con los requerimientos de privacidad. En los últimos años, por ejemplo, el Tribunal de Justicia de la Unión Europea ha concluido en varias ocasiones que las restricciones legales de los Estados Unidos sobre la recogida de datos, así como ciertos compromisos voluntarios como el Escudo de Privacidad o su predecesor, el Puerto Seguro EE. UU.- UE, no se atienen suficientemente a los requisitos de la UE en materia de privacidad, principalmente porque las leyes estadounidenses permiten a las autoridades jurídicas recabar información sobre ciudadanos no estadounidenses para fines de inteligencia extranjera. De hecho, la Junta Europea de Protección de Datos ha adoptado la postura de que las solicitudes de datos personales en virtud del derecho penal de los Estados Unidos, al margen de un proceso jurídico en el que los países de la Unión Europea mantienen cierto control sobre la información que se genera, carece de fundamento legítimo para la transferencia de datos personales sujetos al RGPD.

En el fondo, no son más que conflictos sobre cuándo es apropiado que un gobierno utilice ordenamientos jurídicos u otros procedimientos legales para acceder a los datos de los ciudadanos de otro país. Y estos conflictos no ocurren solo en Europa. Aunque sus respuestas políticas no son coherentes, cada vez más países consideran ahora que el acceso a los datos de sus ciudadanos es una preocupación de seguridad nacional.

Políticas de Cloudflare en torno a la privacidad y las solicitudes de datos

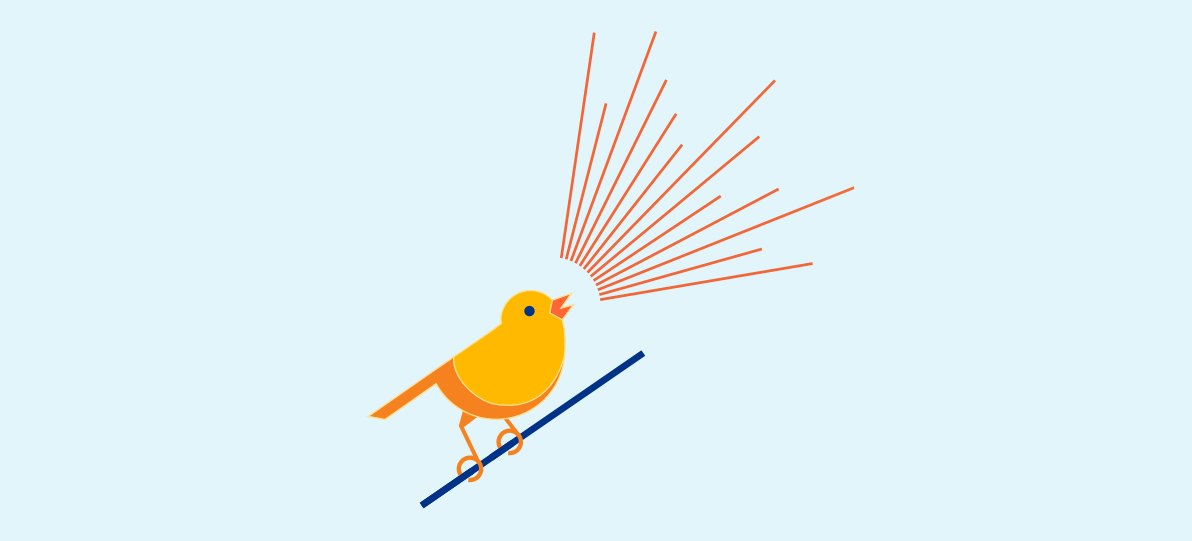
Cloudflare viene aplicando desde hace mucho tiempo políticas para abordar las preocupaciones sobre el acceso a los datos personales, no solo porque creemos que es lo correcto sino porque los conflictos entre jurisdicciones que estamos presenciando hoy en día parecían inevitables. Estas políticas incluyen:

- Compromisos públicos sobre cómo abordamos los datos privados y cómo gestionamos las solicitudes gubernamentales de información
- Cómo informamos a nuestros clientes sobre las solicitudes de datos.

En general, cuando hay un conflicto entre dos normas legales, nos inclinamos por la que protege más la privacidad. Siempre exigimos un procedimiento legal, ya que una vez que se abre la puerta a los datos, puede resultar difícil cerrarla.

Nuestros compromisos públicos en torno a los datos privados y las solicitudes gubernamentales de información

Desde que emitimos nuestro primer informe de transparencia en 2013, que detalla las solicitudes de datos por parte de las autoridades, hemos adquirido compromisos públicos acerca de cómo abordamos las solicitudes de datos y hemos formulado declaraciones públicas sobre las acciones que nunca hemos llevado a cabo. Llamamos a estas declaraciones públicas warrant canaries (alertas de canario), con la idea de que sirvan de señal al mundo exterior.



Estas "alertas de canario" tienen dos funciones. En primer lugar, son un compromiso público en el que indicamos que nunca adoptaríamos estas medidas por elección propia. En segundo lugar, pueden ser un mecanismo para transmitir información, mediante la eliminación de la declaración del sitio web, que de otro modo tal vez no podríamos revelar.

Las entidades reguladoras han empezado a reconocer el valor de los compromisos de privacidad, en particular cuando pueden aplicarse por contrato. De hecho, los compromisos que hemos incluido en nuestros informes de transparencia durante años son exactamente los tipos de compromisos que la Comisión Europea ha recomendado que se incluyan en su proyecto de cláusulas contractuales tipo para el cumplimiento del RGPD.

Entre los principales ejemplos de nuestros compromisos a fecha de publicación de este documento se encuentran los siguientes:

- **Nunca hemos instalado *software* o equipos de las autoridades en nuestra red ni tampoco hemos facilitado ninguna fuente del contenido de los clientes que transitan por la misma.** Como empresa de seguridad sabemos que mantener el control sobre el acceso a nuestras redes es un imperativo absoluto. Por eso nuestro equipo de seguridad se ha centrado en los controles de acceso, registro y supervisión, y es objeto de varias evaluaciones anuales realizadas por terceros. Queremos asegurarnos de que nuestros clientes entiendan que no hay ninguna exención en esos controles para las fuerzas del orden público o autoridades gubernamentales. Es por eso que declaramos que Cloudflare nunca ha instalado *software* o equipos de las autoridades en nuestra red ni tampoco hemos facilitado a ninguna organización gubernamental ninguna fuente del contenido de los clientes que transitan por la misma.
- **Nunca hemos compartido el cifrado de las claves de autenticación.** Cloudflare cree que es necesaria una encriptación sólida, tanto para el contenido como para los metadatos, a fin de asegurar la privacidad en línea. Si un país está tratando de evitar que un servicio de inteligencia extranjero acceda a la información personal de sus ciudadanos, el primer paso debe ser encriptar esa información personal. Sin embargo, los clientes y los reguladores también necesitan estar seguros de que la encriptación en sí misma es digna de confianza. Por tanto, hemos adquirido el compromiso de no entregar nunca a nadie nuestras claves de encriptación o autenticación ni las de nuestros clientes, y nunca hemos debilitado, comprometido o socavado nuestra capacidad de cifrado a petición de las autoridades o de terceros.
- **Nunca hemos cambiado el contenido de los clientes ni las solicitudes de DNS.** No creemos que tengamos que usar nuestros sistemas para atraer a la gente a los sitios web que no tuvieran intención de visitar o para modificar el contenido que ven en línea. Por lo tanto, hemos declarado públicamente que nunca hemos cambiado el contenido de los clientes ni modificado el destino previsto de las respuestas del DNS a petición de las autoridades o terceros.
- **Transparencia en torno a posibles incumplimientos de compromisos.** Nos hemos comprometido a impugnar cualquier ordenamiento jurídico que intente que incumplamos estos compromisos, ante los tribunales si es preciso. Nuestro objetivo era dejar claro, tanto a nuestros clientes como a los gobiernos de todo el mundo, los límites que nos hemos trazado.

Si bien nuestra filosofía general sobre la protección de datos no ha cambiado desde nuestros inicios, de vez en cuando adaptamos nuestros compromisos para reflejar los últimos cambios en nuestros productos y el panorama político. La lista definitiva y actualizada de estos compromisos está disponible en nuestra página Informe de Transparencia.

Notificamos a nuestros clientes sobre las solicitudes gubernamentales de información

Hace tiempo que Cloudflare considera que nuestros clientes merecen saber cuándo alguien, incluido un organismo encargado de velar por el cumplimiento de la ley u otros agentes gubernamentales, utiliza un procedimiento jurídico para solicitar sus datos. Esa notificación permite a nuestros clientes objetar dicha solicitud si tienen dudas.

De hecho, desde nuestros inicios nuestra política ha sido informar a nuestros clientes. En enero de 2013, cuando teníamos una plantilla de menos de 30 empleados, el FBI llamó a nuestra puerta con una carta de seguridad nacional solicitando información sobre un cliente y nos prohibía comentarla con nadie, excepto con nuestros abogados. Las cartas de seguridad nacional, que en ese momento no tenían prácticamente ningún control, podían ser redactadas y aplicadas por cualquier dependencia del Gobierno de Estados Unidos, y silenciaban a los destinatarios para que nunca hicieran mención sobre ellas.

Reconocemos que puede haber algunas circunstancias en las que las autoridades podrían restringir temporalmente la divulgación de manera apropiada para preservar la viabilidad de una investigación. Sin embargo, creemos que el Gobierno debería estar obligado a justificar cualquier disposición de no divulgación y que esta última debería limitarse expresamente al tiempo mínimo necesario para el propósito en cuestión. Así las cosas, trabajamos con la Fundación de Fronteras Electrónicas para recurrir legalmente la carta.

La consiguiente investigación se prolongó varios años y nos prohibieron hablar de ello hasta el 2017, pero finalmente el FBI retiró la carta.

Dado que los tribunales de Estados Unidos han sugerido que las órdenes de no divulgación indefinidas plantean problemas constitucionales, el Departamento de Justicia de Estados Unidos emitió una directriz en 2017 en la que ordenaba a los fiscales federales limitar las órdenes de no divulgación a no más de un año, salvo en circunstancias excepcionales. Eso no ha impedido que las autoridades de Estados Unidos soliciten órdenes de no divulgación indefinidas. Desde 2017 hasta la fecha de la publicación de este documento, hemos recibido al menos 28 órdenes de este tipo que no incluían fecha límite. En colaboración con la ACLU (Asociación americana de defensa de las libertades de los ciudadanos), Cloudflare ha amenazado con iniciar procesos contenciosos para cada orden de no divulgación indefinida que hemos recibido. En cada caso, el Gobierno ha establecido posteriormente plazos en los requisitos de no divulgación en esas órdenes, lo que nos permite informar a nuestros clientes sobre esas solicitudes.

Solución a los conflictos entre legislaciones

Para mantener el cumplimiento de leyes como el RGPD, particularmente frente a los ordenamientos jurídicos que podrían ponernos en la difícil posición de tener que incumplirlo, es necesaria la intervención de los tribunales. Un proveedor de servicios como Cloudflare puede pedir a un tribunal que anule las solicitudes legales debido a un conflicto entre legislaciones, y nos hemos comprometido, tanto en nuestras declaraciones públicas como contractualmente en nuestro anexo de procesamiento de datos, a dar ese paso si es necesario para evitar un conflicto de este tipo. Creemos que el conflicto corresponde a los dos gobiernos que no se ponen de acuerdo sobre quién debe tener derecho a acceder a la información.

Conclusión

Este artículo es solo una introducción a nuestro firme compromiso general con la privacidad de los datos.
Para obtener más información sobre estos compromisos, consulta:

- **Nuestra política general de privacidad:** incluye los datos que recopilamos, cómo los utilizamos, qué datos compartimos, y otras preguntas comunes sobre la privacidad.
- **Nuestro informe de transparencia:** información actualizada sobre las solicitudes legales que hemos recibido para revelar información sobre nuestros clientes.
- **Nuestra página de inicio sobre la privacidad de los datos y conformidad:** los últimos anuncios sobre cómo nuestras políticas y productos apoyan las necesidades de privacidad y conformidad.

En última instancia, operar una red global que protege los datos de los clientes y usuarios finales y cumple con las diferentes legislaciones en materia de privacidad en todo el mundo exige tener presente los valores que hemos defendido desde nuestros inicios como compañía. Entre ellos se incluyen la integridad, la transparencia y el respecto a la privacidad, así como la observancia plena de garantías legales y la obligación de mantener a nuestros clientes informados para que puedan tomar sus propias decisiones respecto a sus datos.