



¿SOLO PARA TUS OJOS?

CLASIFICACIÓN DE 11 EMPRESAS DE TECNOLOGÍA RESPECTO A LA ENCRIPCIÓN Y LOS DERECHOS HUMANOS

*** RESUMEN EJECUTIVO ***

AMNISTÍA
INTERNACIONAL



Amnistía Internacional es un movimiento global de más de 7 millones de personas que trabajan en favor del respeto y la protección de los derechos humanos.

Nuestra visión es la de un mundo en el que todas las personas disfrutan de todos los derechos humanos proclamados en la Declaración Universal de Derechos Humanos y en otras normas internacionales de derechos humanos.

Somos independientes de todo gobierno, ideología política, interés económico y credo religioso. Nuestro trabajo se financia principalmente gracias a nuestra membresía y a donaciones públicas.

© Amnesty International 2016

Salvo cuando se indique lo contrario, el contenido de este documento está protegido por una licencia Creative Commons (atribución, no comercial, sin obra derivada, internacional 4.0).
<https://creativecommons.org/licenses/by-nc-nd/4.0/legalcode>

Si desean más información, visiten la página *Permisos* de nuestro sitio web: www.amnesty.org
El material atribuido a titulares de derechos de autor distintos de Amnistía Internacional no está sujeto a la licencia Creative Commons.

Publicado por primera vez en octubre de 2016
por Amnesty International Ltd.
Peter Benenson House, 1 Easton Street
London WC1X 0DW, Reino Unido

Índice: POL 40/4985/2016

Idioma original: Inglés

amnesty.org



Foto de portada: El uso de servicios de mensajería instantánea forma parte de la vida cotidiana de cientos de millones de personas de todo el mundo, pero sus comunicaciones privadas están realmente amenazadas por la ciberdelincuencia y por la vigilancia de los gobiernos. © iStock

**AMNISTÍA
INTERNACIONAL**



RESUMEN EJECUTIVO

La encriptación ayuda a proteger los derechos humanos de la gente en Internet. Al hacer incomprensibles los datos digitales, la encriptación contribuye a garantizar que la información privada que se envía por Internet siga siendo privada. Además, permite que la gente acceda a espacios online seguros en los que pueden hablar con libertad y expresar sus ideas y opiniones sin temor.

La encriptación impide que los ciberdelincuentes roben nuestra información personal y ayuda a evitar que los gobiernos vigilen ilegalmente nuestras comunicaciones. Es especialmente importante para periodistas y defensores y defensoras de los derechos humanos de todo el mundo —ya sean disidentes en China, activistas bahreiníes en el exilio o periodistas de investigación en Europa—, ya que cualquier brecha en la seguridad de sus datos compromete su fundamental labor y puede tener como consecuencia su arresto y su detención.

Las empresas de tecnología desempeñan un papel crucial a la hora de mantener segura la información digital. En este informe se clasifica a 11 empresas de tecnología atendiendo al cumplimiento de sus responsabilidades en materia de derechos humanos mediante el uso de la encriptación para proteger la seguridad de sus usuarios online. El informe se centra concretamente en los servicios de mensajería instantánea, como Skype, WhatsApp y WeChat, que cientos de millones de personas utilizan en todo el mundo para comunicarse a diario.

Las comunicaciones privadas a través de los servicios de mensajería instantánea están realmente amenazadas por la actividad de ciberdelincuentes y piratas informáticos y por su interceptación ilegítima por parte de las autoridades del Estado. Hemos clasificado a las empresas atendiendo a lo que afirman en sus políticas y a sus prácticas, incluyendo si aplican algún sistema de encriptación eficaz para responder a riesgos identificados en materia de derechos humanos. Amnistía Internacional considera que, como mínimo, las empresas de tecnología deben aplicar encriptación de extremo a extremo por defecto en los servicios de mensajería instantánea, lo cual quiere decir que ni siquiera las propias empresas pueden acceder al contenido de los mensajes.

Las empresas peor clasificadas —Blackberry, Snapchat y Tencent— no aplican un nivel de encriptación adecuado a sus servicios de mensajería instantánea, y por tanto están poniendo en peligro los derechos a la intimidad y a la libertad de expresión de sus usuarios. Además:

- Sólo tres de las empresas evaluadas —Apple, LINE, Viber Media— aplican la encriptación de extremo a extremo por defecto a todos sus servicios de mensajería instantánea, y ninguna de ellas es totalmente transparente respecto al sistema de encriptación que utiliza.

- En cinco casos, Amnistía Internacional encontró incoherencias entre la teoría y la práctica: por ejemplo, Microsoft, a pesar de afirmar claramente su compromiso con los derechos humanos, no aplica ninguna forma de encriptación de extremo a extremo en Skype.
- Todas las empresas, con la excepción de Tencent, han declarado públicamente que no cederán a las peticiones gubernamentales para facilitar el acceso mediante “puertas falsas” a la encriptación de sus servicios de mensajería.

Muchas de las empresas evaluadas han adoptado una firme postura pública en apoyo de la privacidad y la seguridad, y han defendido su uso de herramientas de encriptación ante las presiones de los gobiernos. Pero incluso las que ocupan los mejores puestos en la clasificación aún deben esforzarse más para demostrar que utilizan la encriptación en respuesta a las amenazas contra los derechos humanos. Todas las empresas examinadas también deben ser más transparentes con sus usuarios y con el público en general sobre el uso que hacen de la encriptación.

Ahora es más importante que nunca reconocer la encriptación como un asunto de derechos humanos. Actualmente hay un acalorado debate entre gobiernos, empresas de tecnología y defensores del derecho a la intimidad respecto al uso de herramientas de encriptación en Internet. Los Estados afirman que les preocupa que al proteger mediante la encriptación los datos digitales de presuntos delincuentes y terroristas se esté impidiendo que los servicios de seguridad y los organismos encargados de hacer cumplir la ley lleven a cabo sus investigaciones, un fenómeno que se conoce como “oscurecimiento”.

Los Estados tienen la obligación de proteger a sus habitantes frente al delito, incluido el terrorismo, y la vigilancia electrónica puede utilizarse legítimamente para este fin, siempre que se ajuste al derecho internacional. La encriptación supone un reto para la aplicación de la ley, puesto que, por su propia naturaleza, su eficacia reside en que nadie pueda descifrarla, ni siquiera con intenciones legítimas.

Sin embargo, los Estados también tienen la obligación de proteger los derechos a la intimidad y a la libertad de expresión online. Esto significa que cualquier medida que limite o burle la encriptación debe ajustarse a estrictos requisitos en virtud del derecho internacional.

Países como Pakistán, India, Turquía y China ya han promulgado leyes que limitan el acceso y el uso de la encriptación. Para resolver la preocupación que genera el “oscurecimiento”, algunas autoridades estatales han propuesto que se exija a las empresas de tecnología incluir “puertas traseras” a través de las cuales los organismos encargados de hacer cumplir la ley puedan acceder a la información encriptada.

Sin embargo, prácticamente todos los expertos en tecnología y encriptación están de acuerdo en que es imposible establecer un sistema de acceso especial que sólo puedan utilizar determinadas autoridades estatales. Si hay una puerta trasera, otros –delincuentes, piratas informáticos u otros gobiernos– también podrán acceder a ella. Al socavar la seguridad digital de la inmensa mayoría de la gente que confía en la encriptación como protección, tales medidas son intrínsecamente desproporcionadas y, por tanto no se ajustan al derecho internacional de los derechos humanos.

Además, el debate sobre la encriptación se produce en un momento de gran desconfianza respecto al uso de la vigilancia por parte de los gobiernos. Los documentos de los servicios de inteligencia que Edward Snowden dio a conocer en 2013 mostraron que los servicios de inteligencia de Estados Unidos y Reino Unido realizaban una vigilancia indiscriminada a gran escala, y que empresas como Facebook, Google y Microsoft se enfrentaban a órdenes legales secretas para que entregaran los datos de sus clientes. En octubre de 2016, fuentes internas revelaron que Yahoo había accedido a la exigencia del gobierno estadounidense de rastrear todos los mensajes entrantes de sus usuarios. Además de la

vigilancia masiva, gobiernos de todo el mundo utilizan invasivas herramientas de vigilancia dirigidas específicamente a controlar a activistas y periodistas sin respaldo legal alguno.

En este contexto, las empresas de tecnología deben defender los derechos de sus usuarios aplicando sólidos sistemas de protección de la seguridad de los datos a sus productos y servicios. Las empresas deben resistirse a los intentos de los gobiernos de socavar o restringir el uso de la encriptación, a la vez que satisfacen las legítimas demandas de información de los servicios de seguridad y los organismos encargados de hacer cumplir la ley cuando pueden hacerlo.

Las empresas evaluadas en este informe reconocen la importancia de la encriptación como herramienta para proteger la seguridad online de sus usuarios. Las que se han negado públicamente a los intentos de los gobiernos de acceder a sus servicios mediante puertas traseras, como Apple y Facebook, deben reforzar su postura argumentando que las herramientas de encriptación son fundamentales para la realización de los derechos humanos en un mundo digital. Las que se han quedado atrás, bien sea por utilizar formas de encriptación más débiles, o por no reconocer los peligros existentes en materia de derechos humanos, deben esforzarse por estar a la altura.

CLASIFICACIÓN DE LAS EMPRESAS

Amnistía Internacional envió cartas a las 11 empresas evaluadas para solicitar información sobre la política actual de encriptación de cada una de ellas, así como sobre las políticas y prácticas que aplican para garantizar el cumplimiento de sus responsabilidades en materia de derechos humanos en lo que respecta a sus servicios de mensajería instantánea. Nuestra evaluación se basó en un análisis de la información disponible públicamente y de las respuestas de las empresas, cuando las hubo.

Clasificamos a las empresas según cinco criterios:

- ¿Reconoce las amenazas en línea para la privacidad y la libertad de expresión y el derecho a la intimidad de sus usuarios mediante sus políticas y prácticas?
- ¿Aplica por defecto la encriptación de extremo a extremo?
- ¿Informa a los usuarios de las amenazas a su intimidad y su libertad de expresión y de cómo responde la empresa utilizando la encriptación?
- ¿Revela información sobre los requerimientos del gobierno para que facilite datos de usuarios y sobre la respuesta de la empresa?
- ¿Publica detalles técnicos de sus sistemas de encriptación?

Asignamos hasta 3 puntos por criterio, con una puntuación máxima de 15. Para facilitar la comprensión del resultado, la puntuación total la expresamos sobre 100.

Amnistía Internacional no evaluó la seguridad general de los servicios de mensajería instantánea, ni avala a ninguna de las aplicaciones mencionadas como herramienta segura para las comunicaciones. La organización recomienda que periodistas, activistas, defensores y defensoras de los derechos humanos y otras personas cuyas comunicaciones puedan estar especialmente en riesgo busquen el asesoramiento de expertos en seguridad digital.

Puesto en la clasificación	Empresa	Servicios de mensajería instantánea	¿Contestó a la petición de información de Amnistía?	Puntuación total (sobre 100)
1	Facebook	FB Messenger, WhatsApp	Sí	73
2	Apple	iMessage, FaceTime	No	67
4	Telegram	Telegram Messenger	Sí	67
3	Google	Allo, Duo, Hangouts	No	53
5	Line	Line	Sí	47
7	Viber Media	Viber	Sí	47
8	Kakao Inc	KakaoTalk	Sí	40
6	Microsoft	Skype	Sí	40
10	Snapchat	Snapchat	Sí	26
9	Blackberry	Blackberry Messenger	No	20
11	Tencent	QQ, WeChat	No	0

**AMNISTIA INTERNACIONAL ES
UN MOVIMIENTO GLOBAL DE
DERECHOS HUMANOS.
LAS INJUSTICIAS QUE
AFECTAN A UNA SOLA
PERSONA NOS AFECTAN A
TODAS Y A TODOS.**

Contáctanos



info@amnesty.org



+44 (0)20 7413 5500

Únete a la conversación



www.facebook.com/AmnestyGlobal



[@AmnestyOnline](https://twitter.com/AmnestyOnline)

CLASIFICACIÓN DE LA PRIVACIDAD DE LOS MENSAJES

CLASIFICACIÓN DE 11 EMPRESAS DE TECNOLOGÍA RESPECTO A LA ENCRIPCIÓN Y LOS DERECHOS HUMANOS

La encriptación protege los derechos humanos de la gente en Internet Al hacer incomprensibles los datos digitales, la encriptación contribuye a garantizar que la información privada enviada por Internet siga siendo privada.

La encriptación impide que los ciberdelincuentes roben nuestra información personal y ayuda a evitar que los gobiernos vigilen ilegalmente nuestras comunicaciones. Es especialmente importante para periodistas y defensores y defensoras de los derechos humanos de todo el mundo, ya sean disidentes en China, activistas bahreiníes en el exilio o periodistas de investigación en Europa. Cualquier brecha en la seguridad de los datos de estas personas compromete su fundamental labor y puede tener como consecuencia su arresto y su detención.

Las empresas de tecnología desempeñan un papel crucial a la hora de mantener segura la información digital. En este informe, Amnistía Internacional clasifica a 11 empresas de tecnología atendiendo al cumplimiento de sus responsabilidades en materia de derechos humanos mediante el uso de la encriptación para proteger el derecho a la intimidad de sus usuarios online. El informe se centra concretamente en los servicios de mensajería instantánea, como Skype, WhatsApp y WeChat, que cientos de millones de personas utilizan en todo el mundo para comunicarse a diario.

Amnistía pide a todas las empresas de tecnología que apliquen por defecto la encriptación de extremo a extremo en todos los servicios de mensajería instantánea. Amnistía Internacional halló que todas las empresas evaluadas necesitan ser más transparentes respecto al nivel de protección que ofrecen a los derechos a la intimidad y a la libertad de expresión de sus usuarios en Internet.