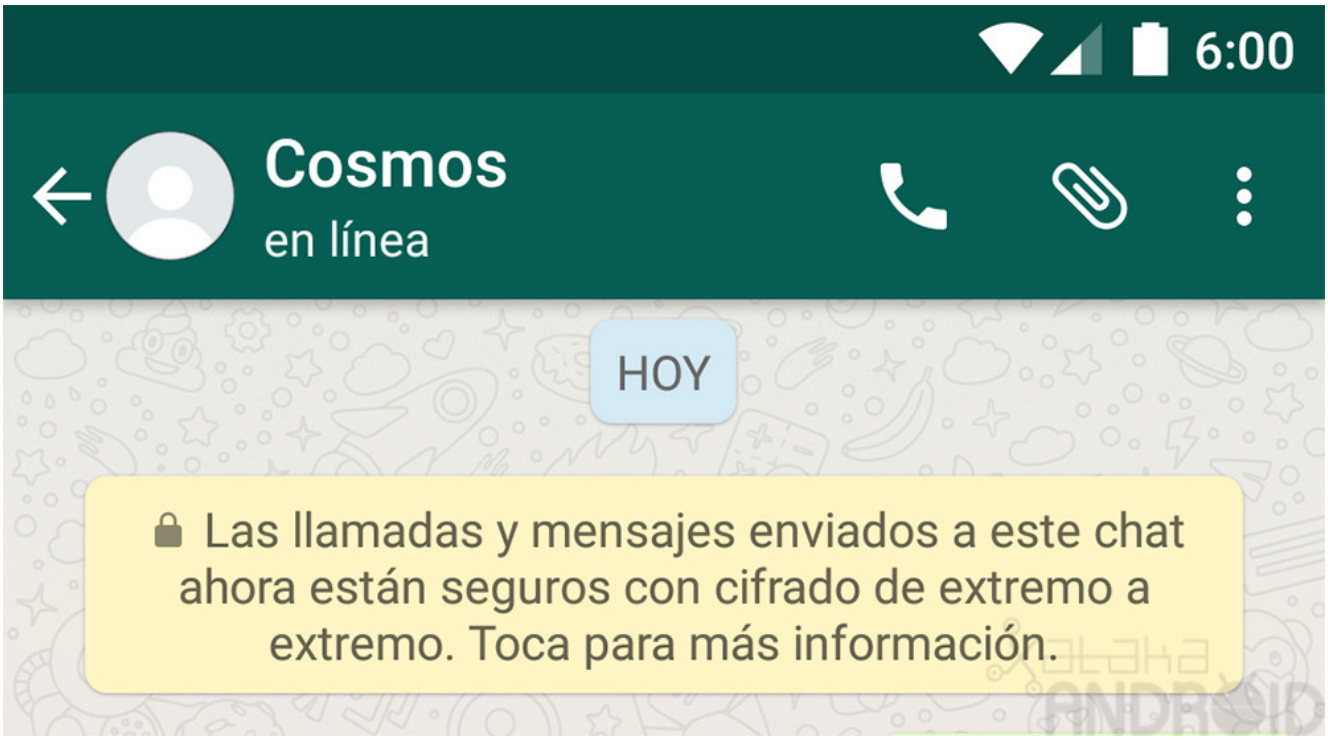
Qué es y cómo funciona el cifrado de extremo a extremo en WhatsApp

05/02/2023



Siempre escuchamos hablar de privacidad y seguridad en las aplicaciones y una de las herramientas que usan las compañías para proteger a sus usuarios es el **cifrado de extremo a extremo.**

Esta tecnología se ha vuelto obligada para todas las plataformas de mensajería y por eso está presente en las que tienen mayor cantidad de usuarios como **WhatsApp, Telegram, Signal, Facebook Messenger, Line** y demás.

Pero cómo funciona el cifrado de extremo a extremo, qué lo hace tan seguro y por qué debe ser una característica que las personas siempre deben exigir en sus aplicaciones de mensajería para cuidar su información.

Así funciona el cifrado de extremo a extremo

Esta es un sistema de comunicación que se basa en el cifrado de los mensajes enviados por un dispositivo, de forma que solamente puedan ser descifrados por el dispositivo al que fue enviado.

Así funciona esta tecnología que aplican WhatsApp, Telegram, Signal, entre otras.

El cifrado consiste en transformar el texto en un sistema de signos, que únicamente pueden ser leídos por el emisor y el receptor, quienes tienen las llaves de acceso a ese proceso. Por lo que ni los servidores de la aplicación ni ningún intermediario tienen cómo ver el contenido enviado.

En otras palabras, los mensajes que se le envían a la pareja por **WhatsApp** van con un cifrado, que solamente el dispositivo de ella o él lo puede descifrar. De esta forma, ni **Meta** o un

ciberdelincuente puede acceder a ellos, a no ser que roben físicamente el teléfono o la cuenta.

“**WhatsApp** no tiene manera de escuchar las llamadas ni ver el contenido de los mensajes que están cifrados de extremo a extremo. Esto se debe a que el cifrado y descifrado de los mensajes enviados y recibidos ocurre completamente en el dispositivo. Antes de que un mensaje salga de él, se asegura con un candado criptográfico, del cual solo el destinatario tiene la clave”, explica la propia aplicación en su blog oficial.

Todo este proceso el usuario nunca lo nota, es decir, no necesita ingresar un código o una clave para ver el mensaje que le envían a diario, sino que la aplicación se encarga del trámite en segundo plano en segundos.

Aunque las personas sí pueden verificar que el cifrado de extremo a extremo está funcionando o que el chat se encuentra encriptado. Esto se puede saber siguiendo estos pasos:

1. Abrir el chat.

2. Tocar en el nombre del contacto para ir a la pantalla de información.

3. Ir a Cifrado para ver el código QR o los 60 dígitos.

4. Con el celular del otro usuario escanear ese código y ahí notificará que el cifrado está funcionando.

Los beneficios del cifrado de extremo a extremo

Que una aplicación tenga esta tecnología quiere decir que las conversaciones, fotos, videos, audios y archivos que se compartan en un chat, nunca van a salir de ahí y que las opciones de robo de información sean casi imposibles.

Esto garantiza que los datos no corren riesgo, que ni siquiera los dueños de las aplicaciones tienen opciones de conocerlos porque no tienen la llave de acceso única del dispositivo al que se la envía ni del que la recibe.

Aunque el cifrado de extremo a extremo no garantiza una protección al 100%, porque ningún sistema lo hace, sí es la forma actual que brinda mayor confianza para mantener la confidencialidad de la información.

Fuente: Infobae