Resolver delitos sin debilitar el cifrado

Por qué un cifrado fuerte y la seguridad pública van de la mano

Junio de 2026

Resumen ejecutivo

En un mundo cada vez más digital, las agencias de aplicación de la ley se enfrentan a desafíos crecientes para determinar cómo encontrar y acceder a las pruebas necesarias para sus investigaciones. A su vez, los formuladores de políticas debaten cómo regular este acceso sin comprometer la seguridad y la privacidad de las comunicaciones en línea. Reconociendo que el cifrado es una herramienta fundamental que hace que Internet sea segura y confiable, las propuestas que exigen acceso legalmente autorizado por diseño harían que Internet fuera inherentemente menos segura para todas las personas.

Si bien el cifrado limita el acceso al contenido de determinadas comunicaciones, las agencias de aplicación de la ley hoy tienen acceso a más datos que nunca, incluidos historiales de ubicaciones, metadatos y registros de transacciones. En este documento describimos algunas herramientas que permiten realizar investigaciones eficaces sin comprometer el cifrado. Muchas veces el problema no es la falta de información, sino la capacidad de extraer, de manera legal, eficaz y proporcional, información útil de los grandes volúmenes de datos que ya están disponibles. Por lo tanto, el enfoque debería centrarse en fortalecer la capacidad de investigación, mejorar la cooperación transfronteriza, potenciar la informática forense, apoyar el análisis de metadatos específicos y fomentar una cooperación voluntaria y transparente con los proveedores de servicios, no en aumentar la cantidad de pruebas mediante la introducción de fallas de seguridad sistémicas.

El cifrado es una tecnología fundamental que protege la confidencialidad y la integridad de los datos, las comunicaciones, los dispositivos y los servicios. Es esencial para una Internet segura y confiable que proteja a las personas, los niños, las empresas, los gobiernos, los servicios públicos, la infraestructura crítica, los periodistas, los defensores de los derechos humanos y las comunidades vulnerables. Las propuestas que imponen el escaneo del lado del cliente, puertas traseras u otras formas de acceso excepcional debilitarían esta base y harían que Internet fuera inherentemente menos segura para todos.

Los intentos de crear puertas traseras o introducir el escaneo del lado del cliente en dispositivos o sistemas de cifrado son técnicamente inviables y jurídicamente cuestionables. Cualquier debilitamiento intencional de las comunicaciones cifradas no puede limitarse a objetivos específicos. Estos enfoques crean riesgos sistémicos, no superan las pruebas de necesidad y proporcionalidad y amenazan la Internet abierta, globalmente conectada, segura y confiable.

Por lo tanto, los formuladores de políticas deberían emprender tres acciones prioritarias. En primer lugar, las leyes y políticas relacionadas con la investigación de delitos deberían proteger el cifrado fuerte y rechazar las medidas que lo debiliten. En segundo lugar, los gobiernos deberían invertir en la capacidad y la formación de las agencias encargadas de aplicar la ley, de modo que los investigadores puedan utilizar con eficacia herramientas legales, específicas y proporcionales que preserven la seguridad y la privacidad de los demás usuarios. En tercer lugar, los marcos de políticas deberían permitir una cooperación voluntaria y transparente con los proveedores de servicios en investigaciones de delitos graves, con el respaldo de garantías procesales, rendición de cuentas y respeto de los derechos humanos.

Proteger el cifrado fuerte no es un obstáculo para la seguridad pública, la protección de la infancia ni la prevención de los delitos. Es un requisito previo para las tres cosas y una condición necesaria para una Internet segura y confiable.

El cifrado es un pilar fundamental de la seguridad, la confianza y la seguridad pública

El cifrado es una tecnología fundamental para la sociedad moderna. Asegura las comunicaciones en línea, posibilita el comercio y el gobierno electrónico, protege la infraestructura crítica y sustenta la confianza en los sistemas digitales de los que dependen tanto las personas como las empresas y los gobiernos. Sin un cifrado fuerte, no habría banca en línea segura, ni servicios sanitarios o públicos confidenciales, ni una defensa eficaz contra el ciberdelito, las filtraciones de datos, el robo de identidad o el espionaje.

Las propuestas para imponer el acceso a las comunicaciones cifradas mediante mecanismos como el escaneo del lado del cliente o las puertas traseras parten de una interpretación equivocada de cómo funciona el cifrado y de lo que está en juego. **Cualquier debilitamiento intencional del cifrado — independientemente de su finalidad— genera inevitablemente vulnerabilidades sistémicas que no pueden limitarse a jurisdicciones, investigaciones u objetivos específicos. Una vez introducidas, estas vulnerabilidades pueden ser descubiertas, replicadas o aprovechadas por delincuentes, estados hostiles y otros actores malintencionados.**

Si bien el cifrado puede limitar el acceso al contenido de algunas comunicaciones, no deja a las agencias de aplicación de la ley sin recursos. Por el contrario, hoy en día los investigadores disponen de

más datos sobre el comportamiento, los desplazamientos y las interacciones de las personas que en cualquier otro momento de la historia. Por lo tanto, la pregunta clave relacionada con las políticas no es si las investigaciones son posibles en un mundo con un cifrado fuerte, sino cómo garantizar que las fuerzas del orden puedan hacer un uso eficaz, lícito y proporcional de la gran cantidad de herramientas de investigación y datos ya disponibles sin poner en riesgo la seguridad de todos los demás.

Los proveedores de servicios desempeñan un papel fundamental en este desafío. Ellos diseñan y operan muchos de los servicios de comunicaciones, plataformas, sistemas de denuncia y procesos de tratamiento de datos que los usuarios utilizan todos los días. Además, desempeñan un papel importante a la hora de responder a las solicitudes lícitas de datos que no sean contenido, mantener medidas de seguridad sólidas y respaldar los mecanismos de denuncia de los usuarios. Por lo tanto, una política eficaz debería apoyar una cooperación clara, transparente y respetuosa con los derechos entre las fuerzas del orden y los proveedores de servicios y, a la vez, preservar un cifrado fuerte y evitar obligaciones que introduzcan debilidades sistémicas.

Proteger el cifrado fuerte no es un obstáculo para la seguridad pública, la protección de la infancia ni la prevención de los delitos. Es un requisito previo para las tres cosas. El cifrado permite una Internet segura y confiable. Reduce las oportunidades para el ciberdelito, protege a las víctimas y a las comunidades vulnerables y respalda el estado de derecho al garantizar que las medidas de investigación sigan siendo específicas, necesarias, proporcionales y sujetas a rendición de cuentas.

El kit de herramientas de investigación: propuestas de políticas sobre acceso a los datos

Los organismos de aplicación de la ley ya tienen acceso a un kit de herramientas de investigación amplio y diverso que no requiere debilitar el cifrado ni socavar las bases técnicas de Internet. Estas medidas varían significativamente en su impacto sobre la seguridad, la privacidad y la integridad de los sistemas digitales.

La siguiente matriz de propuestas de políticas de acceso a los datos ilustra esta variedad de opciones, ordenadas según su impacto en las bases técnicas de Internet. Las medidas que se muestran en verde operan dentro de la estructura existente de una Internet conectada globalmente, segura y confiable. Preservan el cifrado y al mismo tiempo permiten investigaciones eficaces. Las medidas que se muestran en rojo requieren debilitar el cifrado o comprometer los dispositivos, introduciendo vulnerabilidades sistémicas que no pueden limitarse a sospechosos o jurisdicciones específicas.

Esta comparación visual destaca una elección crítica en materia de políticas: los gobiernos pueden fortalecer la capacidad de investigación y a la vez preservar la seguridad de Internet o bien pueden adoptar medidas intrusivas que debiliten la infraestructura de la que dependen la seguridad pública, la estabilidad económica y las instituciones democráticas.

Los riesgos de las medidas intrusivas

Algunas técnicas de investigación plantean riesgos mucho mayores para la ciberseguridad, los derechos humanos y la confianza pública que otras. Los riesgos que plantean estas medidas intrusivas superan con creces sus potenciales beneficios para las investigaciones. Estos riesgos deben enfrentarse de manera directa.

Software forense remoto y explotación de vulnerabilidades de día cero. Las herramientas forenses remotas, también conocidas como *spyware*, permiten un acceso remoto profundo y continuo a los contenidos y funciones de un dispositivo. Su uso suele aprovechar vulnerabilidades de software no divulgadas (vulnerabilidades "de día cero"), lo que genera incentivos para no divulgar estas vulnerabilidades y deja a todos los usuarios expuestos a su explotación. Muchas veces estas herramientas se han asociado con abusos, incluida la vigilancia de periodistas, defensores de los derechos humanos y opositores políticos. Incluso cuando se utilizan con autorización, los daños sistémicos a la ciberseguridad son profundos.

Escaneo del lado del cliente y puertas traseras de cifrado. El escaneo del lado del cliente y las puertas traseras de cifrado alteran radicalmente el modelo de seguridad de los sistemas cifrados. Introducen un monitoreo continuo, socavan la confidencialidad y crean nuevas superficies de ataque. Una vez que se crean las puertas traseras, las vulnerabilidades pueden ser descubiertas, replicadas o aprovechadas por delincuentes, estados hostiles y otros actores malintencionados. Estas medidas no son compatibles con una Internet segura y confiable y no pueden limitarse a un uso lícito. Los daños que generan son intrínsecos e inevitables.

Opciones existentes para los organismos de aplicación de la ley que preservan el cifrado

Análisis de metadatos. Incluso cuando el contenido de las comunicaciones está cifrado, los metadatos asociados (por ejemplo, marcas de tiempo, identificadores de remitente y destinatario, datos de ubicación y del dispositivo, registros de transacciones y patrones de uso) suelen seguir estando disponibles a través de procesos legales. Con ayuda de las herramientas analíticas modernas, los metadatos se pueden utilizar para reconstruir cronologías, identificar redes, detectar patrones y localizar sospechosos. Dirigido apropiadamente y sujeto al debido proceso, el análisis de metadatos puede ser una herramienta de investigación poderosa y proporcional y debería ser una condición previa antes de considerar cualquier medida más intrusiva.

Informática forense digital en dispositivos incautados. Cuando los dispositivos se incautan legalmente, los investigadores pueden acceder a los datos almacenados utilizando técnicas forenses digitales como la extracción de memoria, la recuperación de contraseñas o la reconstrucción de datos. La inversión en

capacitación y capacidad forense puede mejorar de forma significativa el acceso a las pruebas sin debilitar los sistemas de cifrado. Estos métodos deben ser estrictamente controlados y dirigidos y estar sujetos a autorización judicial.

Técnicas de investigación encubiertas. Los métodos de investigación tradicionales como las operaciones encubiertas y la inteligencia humana siguen siendo eficaces en los entornos digitales. Los organismos de aplicación de la ley han adaptado con éxito estas técnicas para aplicarlas en sus investigaciones en línea, incluso en el caso de delitos graves como la distribución de material de abuso sexual infantil (MASI), mediante el uso de cuentas señuelo y participación encubierta. Estos enfoques son, por su propia naturaleza, dirigidos y evitan riesgos sistémicos para la seguridad digital.

Cooperación, denuncias y pruebas digitales directas

Cooperación voluntaria con los proveedores de servicios. Muchos proveedores ya facilitan el acceso legal a datos que no son contenido, como información de las cuentas, historiales de inicio de sesión y patrones de uso. A diferencia de los mandatos de acceso obligatorios, la cooperación voluntaria basada en la confianza puede mejorar los resultados de las investigaciones y a la vez respetar la privacidad de los usuarios y el debido proceso. La transparencia, la rendición de cuentas y la supervisión son fundamentales para garantizar que esta cooperación siga siendo coherente con los derechos humanos y el estado de derecho.

Mecanismos de denuncia para los usuarios. Las herramientas de denuncia eficaces permiten a los usuarios denunciar actividades ilegales o dañinas directamente a las plataformas. Lineamientos claros, un seguimiento receptivo y procesos transparentes aumentan la confianza y mejoran la calidad de las líneas de investigación. Los sistemas de denuncia robustos son especialmente importantes para la seguridad infantil y los problemas relacionados con el abuso.

Pruebas digitales directas de víctimas y testigos. Muchas veces se pueden obtener pruebas directamente de las personas implicadas o afectadas por la actividad delictiva. Simplificar los procesos para enviar pruebas digitales y apoyar a las víctimas para que lo hagan puede fortalecer significativamente las investigaciones sin introducir nuevos riesgos de seguridad.

Desmintamos algunos mitos persistentes

- **El "acceso legalmente autorizado por diseño" es factible desde el punto de vista técnico**. Ningún sistema puede permitir el acceso excepcional sin debilitar la seguridad de todos. Los mecanismos de acceso técnico no pueden distinguir entre un uso legítimo y uno malicioso.
- **Un "apagón digital" impide que las fuerzas del orden detengan los delitos**. Aunque parte del contenido está cifrado, los datos sobre los comportamientos, las redes y la ubicación son más abundantes que nunca. Los organismos de aplicación de la ley no se enfrentan a un

apagón digital, sino que están operando en una era de disponibilidad de datos sin precedentes.

- **Se puede crear una puerta trasera segura exclusivamente para las fuerzas del orden**. Las puertas traseras son indiscriminadas por naturaleza e imponen un daño social generalizado para abordar las acciones de una minoría delictiva.

Recomendaciones

Para los formuladores de políticas:

- Desarrollar una comprensión básica del cifrado y de por qué es importante. Entender el papel técnico básico que desempeña el cifrado en la protección de la confidencialidad, la integridad y la seguridad de los datos, las comunicaciones, los dispositivos y los servicios de los usuarios. Esta comprensión es esencial para asegurar que las leyes destinadas a mejorar la seguridad pública no hagan que todos los usuarios de Internet estén menos seguros de forma involuntaria.
- Las leyes y políticas relacionadas con la investigación de delitos deberían proteger el cifrado fuerte, no debilitarlo.
- Los organismos de aplicación de la ley deberían tener capacidad y capacitación suficientes para utilizar una variedad de medidas de investigación que no afecten la seguridad, la protección y la privacidad de otros usuarios. Estas medidas deberían aplicarse únicamente cuando sea necesario y proporcional y bajo suficiente supervisión.
- Las políticas deberían permitir la cooperación voluntaria con los proveedores de servicios en investigaciones de delitos graves, siempre con el respaldo de garantías procesales, rendición de cuentas y respeto por los derechos humanos.
- Las políticas deberían aumentar el financiamiento para la capacitación en informática forense digital y otras capacidades de investigación que preserven el cifrado.

Para los proveedores de servicios:

- Mantener y desplegar un cifrado fuerte por defecto; no introducir puertas traseras ni debilidades sistémicas.
- Responder de manera eficaz y transparente a las solicitudes lícitas de datos que no son contenido, de acuerdo con el debido proceso.
- Fortalecer la cooperación voluntaria con los organismos de aplicación de la ley a través de canales operativos claros y puntos de contacto de confianza.
- Invertir en mecanismos de denuncia eficaces y fáciles de usar, en particular para la seguridad infantil y los problemas relacionados con el abuso.
- Interactuar regularmente con los formuladores de políticas, las agencias de aplicación de la ley y la sociedad civil para explicar las realidades técnicas y los impactos en la seguridad.

Para otras partes interesadas (sociedad civil, academia, comunidad técnica, educadores):

- Monitorear y evaluar los impactos de las medidas de investigación sobre los derechos humanos y la seguridad.
- Ofrecer experiencia independiente basada en evidencia para contrarrestar afirmaciones engañosas sobre el cifrado y el apagón digital (también conocido como "quedarse a oscuras").
- Promover la alfabetización digital y la educación sobre seguridad en línea para niños, padres y cuidadores.
- Apoyar las iniciativas de denuncia temprana y prevención que reduzcan los daños y mejoren los resultados de las investigaciones.
- Fomentar el diálogo de múltiples partes interesadas para garantizar que las políticas fortalezcan la confianza, la protección y la seguridad pública en línea.

Otros recursos

Enlaces a lecturas adicionales y materiales de Internet Society:

- Qué es el cifrado: https://www.internetsociety.org/issues/encryption/what-is/
- Proteja el cifrado, protéjase a usted mismo: https://www.internetsociety.org/issues/encryption/protect-encryption-protect-yourself/
- El cifrado protege a los menores en Internet: https://www.internetsociety.org/blog/2023/05/encryption-keeps-kids-safe-online/
- Hoja informativa: Cómo el cifrado puede proteger a los periodistas y la prensa libre: https://www.internetsociety.org/resources/doc/2020/fact-sheet-how-encryption-can-protect-journalists-and-the-free-press/
- El impacto económico de las leyes que debilitan el cifrado: https://www.internetsociety.org/es/resources/doc/2021/el-impacto-economico-de-las-leyes-que-debilitan-el-cifrado/
- Mantener a los niños y niñas seguros en línea: Guía sobre el cifrado para padres y madres: https://www.internetsociety.org/blog/2024/01/keeping-kids-safe-online-navigating-the-new-parents-guide-to-encryption/
- Curso de aprendizaje sobre cifrado: https://www.internetsociety.org/es/learning/encryption/