Informe de políticas: Perspectivas sobre el bloqueo de contenido en Internet

Septiembre de 2025

Resumen ejecutivo

Imagine intentar impedir la entrada a un edificio en una ciudad cerrando toda una calle. En esa calle podría haber hospitales, escuelas y viviendas, por lo que al cerrarla se interrumpirían múltiples servicios esenciales para muchas personas. De todos modos, quienes decidan hacerlo encontrarán la forma de acceder. Algo parecido ocurre cuando los gobiernos intentan bloquear el acceso a determinados sitios web o contenidos en línea específicos cerrando partes de Internet usando métodos de bloqueo basados en el Sistema de Nombres de Dominio (DNS) o direcciones del Protocolo de Internet (IP). Aunque este enfoque pueda parecer rápido y sencillo, suele tener un impacto mayor del previsto: suele interrumpir otros servicios y no resuelve el problema de fondo.

El bloqueo basado en direcciones IP y DNS se ha convertido en uno de los métodos más propuestos debido a su aparente simplicidad y facilidad de implementación[1]. Cada vez con más frecuencia, los gobiernos de todo el mundo instruyen a los proveedores de servicios de Internet (ISP) y a los resolvedores de DNS que bloqueen el acceso a contenido de Internet que consideran ilegal u objetable, como juegos de azar no autorizados, material de abuso infantil, infracciones de derechos de autor y amenazas a la seguridad nacional. Sin embargo, estos métodos rara vez abordan con eficacia las causas de fondo y pueden provocar importantes interrupciones técnicas y daños sociales.

Si bien el bloqueo de contenido puede parecer una solución rápida para restringir el acceso a material ilegal, en la práctica suele resultar ineficaz y con frecuencia termina bloqueando servicios legítimos, lo que afecta tanto a usuarios como a empresas. Además, el bloqueo por DNS o IP no elimina el contenido de Internet, lo que permite que el material siga siendo accesible para determinadas personas. Los intentos de eludir el bloqueo pueden poner en riesgo la privacidad y la seguridad de los usuarios.

Internet Society presentó un análisis técnico de los métodos de bloqueo más comunes, destacando sus limitaciones y potenciales riesgos. Este

[1] i2Coalition. DNS at Risk: How Network Blocking and Fragmentation Undermine the Global Internet, 3 de junio de 2025. Disponible en: https://i2coalition.com/i2coalition-launches-dns-at-risk-report-and-website-to-spotlight-rising-global-internet-infrastructure-abuse/

análisis muestra que ambas técnicas se pueden eludir fácilmente, son imprecisas y propensas a provocar daños colaterales. Internet Society alienta a los formuladores de políticas a priorizar soluciones que aborden el contenido dañino en su origen, en lugar de depender de medidas técnicas restrictivas que pueden generar externalidades negativas para la naturaleza abierta y global de Internet.

Consideraciones clave

El bloqueo por DNS y direcciones IP interfiere, por diseño, con los mecanismos básicos que permiten a los usuarios encontrar y acceder a información en Internet. Su implementación implica más que una simple ejecución técnica. Estos enfoques afectan el funcionamiento fundamental de Internet y su uso puede generar importantes consecuencias operativas, legales y sociales. En esta sección se describen los factores críticos que deben guiar cualquier consideración sobre políticas de bloqueo de contenido.

El **bloqueo basado en direcciones IP** deniega el acceso al contenido al impedir el establecimiento de conexiones TCP/IP a direcciones IP específicas, interrumpiendo así la comunicación con los servidores que se desea bloquear. En cambio, el **bloqueo basado en DNS** manipula el Sistema de Nombres de Dominio (DNS) al devolver respuestas falsas o engañosas cuando un usuario intenta acceder a un dominio bloqueado, haciendo que el contenido parezca inaccesible.

Ambos enfoques generalmente se imponen a nivel nacional y suelen implementarse dentro de la red del Proveedor de Servicios de Internet (ISP). Son populares en ciertos círculos por su aparente simplicidad y escalabilidad. Sin embargo, estas técnicas pueden carecer de precisión y los usuarios las evaden fácilmente a través de las VPN (redes privadas virtuales) o modificando los resolvedores DNS, mientras que los proveedores de contenido pueden cambiar la infraestructura donde se aloja el contenido.

El verdadero problema radica en la discrepancia entre los resultados previstos y los efectos técnicos reales de las políticas. Estos métodos no eliminan el contenido de Internet ni atacan su origen. En cambio, imponen barreras de acceso poco confiables y propensas a causar daños colaterales. Esta discrepancia entre los objetivos de las políticas y las realidades técnicas subraya la necesidad de respuestas más matizadas, eficaces y menos disruptivas.

Desafíos

La implementación de bloqueos basados en DNS y direcciones IP plantea una serie de desafíos técnicos, sociales, económicos y políticos complejos. A nivel técnico, estas medidas son herramientas intrínsecamente poco precisas que dificultan distinguir entre contenido ilegal y legítimo cuando ambos

se alojan en la misma dirección IP o dominio. Como resultado, los servicios legítimos suelen quedar atrapados en el fuego cruzado, lo que provoca un bloqueo excesivo y el riesgo de interrupción del acceso a información y plataformas esenciales.

Imagine un servidor que aloja tanto un sitio de *streaming* pirata como un pequeño sitio de comercio electrónico bajo una misma dirección IP. Si se ordena bloquear esa IP, también se bloqueará el acceso al sitio de comercio electrónico, interrumpiendo así las actividades comerciales legítimas aunque el sitio no haya estado involucrado en la piratería[2]. Este ejemplo ilustra cómo el bloqueo a nivel de IP puede generar interrupciones significativas, muy alejadas de su propósito original.

Para intentar recuperar el acceso, los usuarios podrían recurrir a herramientas como las VPN o resolvedores DNS alternativos. El riesgo es que, al intentar eludir el bloqueo de contenido, sin darse cuenta, los usuarios elijan VPN o resolvedores DNS que prometen acceso, pero ofrecen menor seguridad y protección de la privacidad, con lo cual la experiencia en Internet de esos usuarios podría ser menos segura. Las empresas legítimas podrían verse obligadas a migrar sus servicios a una dirección IP o dominio que no esté bloqueado, o a cambiar de proveedor de alojamiento.

Entre 2024 y 2025, Italia implementó su sistema Escudo contra la piratería , un plan agresivo que obliga a los proveedores de servicios de Internet (ISP), servicios de DNS y proveedores de VPN a bloquear dominios y direcciones IP vinculados a la transmisión ilegal de deportes en un plazo máximo de treinta minutos desde la solicitud de los titulares de derechos3. Sin embargo, esta política bloqueó repetidamente servicios legítimos, entre ellos dominios de Google, sitios alojados en Cloudflare y Google Drive, lo que causó interrupciones generalizadas que afectaron a empresas, usuarios de Internet y servicios en la nube4.

El bloqueo de dominios a nivel de los resolvedores DNS públicos puede tener consecuencias imprevistas que van más allá del control de contenido y afectan directamente a la seguridad en línea de los usuarios en los países donde operan estos servicios. Por ejemplo, los resolvedores recursivos públicos como Quad9[5] desempeñan una función fundamental en la protección de los usuarios contra malware, phishing y otras ciberamenazas, ya que filtran los dominios dañinos basándose en fuentes de inteligencia de amenazas globales.

Cuando los gobiernos exigen a estos resolvedores que desvíen recursos técnicos y operativos para implementar bloqueos de contenido, corren el riesgo de erosionar sus funciones básicas de seguridad. Esto no solo debilita la protección de personas y empresas, sino que también puede reducir la

[2] The i2Coalition, *DNS at Risk: How Network Blocking and Fragmentation Undermine the Global Internet*, mayo de 2025, p. 8, disponible en: https://i2coalition.com/wp-content/uploads/2025/05/DNS-at-Risk-How-Network-Blocking-and-Fragmentation-Undermine-the-Global-Internet.pdf.

[3] TechRadar, *Italy's Piracy Shield may be breaching EU law...*, 10 de julio de 2025

[4] DediRock, *Report Highlights Risks of Government DNS Blocking*, junio de 2025

[5] Quad9. *About Quad9*. Disponible en: https://quad9.net/about

ciberresiliencia general de un país al eliminar o deteriorar una capa de infraestructura confiable. El riesgo es que, al implementar medidas de control específicas para un sitio, las autoridades erosionen inadvertidamente un servicio defensivo que beneficia a millones de usuarios, dejándolos más expuestos al fraude en línea, el robo de identidad y los ataques a la red.

Desde una **perspectiva económica,** las medidas de bloqueo por DNS y direcciones IP pueden imponer costos sustanciales tanto a los proveedores de servicios de Internet como a los operadores de red. Estos costos incluyen gastos operativos asociados a la implementación y el mantenimiento de sistemas de bloqueo, pérdidas de ingresos para las plataformas y los negocios en línea afectados por el bloqueo excesivo, e ineficiencias económicas más amplias causadas por la reducción de la confianza en la infraestructura de Internet[6].

Principios rectores y recomendaciones

Internet Society considera que la forma más apropiada de contrarrestar el contenido y las actividades ilegales en Internet es abordarlos desde su origen. El uso de bloqueo por DNS o direcciones IP para limitar el acceso a contenido en línea no solo puede resultar ineficaz, sino que también puede causar daños colaterales que afecten a usuarios inocentes. Por estas razones, y en línea con los desafíos expuestos, desaconsejamos el bloqueo de contenido. Sin embargo, estas técnicas aún se utilizan. Reconociendo esta realidad, sugerimos dos estrategias principales para los formuladores de políticas preocupados por el contenido ilegal en Internet:

- **Abordar el problema en el origen.** El enfoque menos perjudicial para Internet es atacar el contenido y las actividades ilegales en su origen. Eliminar el contenido ilegal desde su origen y aplicar medidas de control contra quienes lo generan evita los efectos negativos del bloqueo y es más eficaz para eliminar el contenido ilegal. Dado que el contenido ilegal en línea trasciende las fronteras y las legislaciones nacionales, la cooperación entre jurisdicciones y partes interesadas es un requisito previo para el éxito.
- **Priorizar y utilizar enfoques alternativos.** Por ejemplo:
    - Una cooperación eficaz entre los proveedores de servicios, las fuerzas del orden y las autoridades nacionales puede proporcionar otros medios para ayudar a las víctimas de contenido ilegal y para aplicar medidas de control.
    - Crear un entorno de confianza donde los usuarios reciban información sobre qué es legal y qué no lo es puede mejorar la autorregulación. En algunos casos (por ejemplo, el control parental), empoderar a los usuarios para que usen filtros en sus

[6] Analysys Mason, *The economic cost of network blocking*, informe para Cloudflare, 28 de julio de 2025. Disponible en: https://www.analysysmason.com/consulting/reports/network-blocking-economic-impact-jul25/

propios dispositivos, con su consentimiento, puede ser eficaz y menos perjudicial para Internet.

Además, ofrecemos los siguientes lineamientos específicos para minimizar los impactos negativos del bloqueo de contenido:

- **Agotar primero todas las opciones que no impliquen bloqueo.** En primer lugar, agotar todas las opciones prácticas para abordar el contenido en su origen o cualquier otra alternativa al bloqueo. El bloqueo de contenido no debe considerarse simplemente porque sea más fácil. Debe ser necesario y proporcional.
- **Ser transparentes.** Debe existir transparencia tanto sobre la aplicación del bloqueo como sobre el objetivo subyacente y las políticas de bloqueo de contenido. Los gobiernos deben garantizar que los usuarios afectados puedan plantear sus inquietudes con respecto a los impactos negativos en sus derechos, intereses y oportunidades.
- **Empoderar a los usuarios**. Los usuarios deben poder filtrar el contenido ilegal o no deseado en sus propios dispositivos o redes, garantizando el acceso a herramientas de seguridad en línea y capacitación en habilidades digitales.
- **Limitar el alcance.** Bloquear el contenido lo más localmente posible para minimizar el impacto global.
- **Involucrar a las partes interesadas.** El desarrollo y la implementación de políticas relacionadas con el contenido en línea deben involucrar a un amplio conjunto de partes interesadas, incluidos expertos en tecnología, economía, derechos del consumidor y otras áreas. Esto garantiza que se tomen medidas adecuadas para minimizar los efectos secundarios negativos de las políticas adoptadas para abordar dicho contenido.
- **Seguir el debido proceso legal.** Toda orden de bloqueo de contenido ilegal debe estar respaldada por la ley, sujeta a revisión independiente y específicamente orientada a lograr un objetivo legítimo. Se deben priorizar los medios menos restrictivos disponibles para abordar la actividad ilegal. Los proveedores de servicios de Internet u otros intermediarios no deben convertirse en agentes de facto encargados de hacer cumplir la ley: no se les debe exigir que determinen cuándo una conducta o un contenido es ilegal.
- **Limitarlo en el tiempo.** Todas las medidas de bloqueo deben ser temporales y levantarse tan pronto como deje de existir el motivo del bloqueo. Si bien es común que el contenido ilegal se traslade para evadir las medidas de bloqueo, estas suelen mantenerse mucho después de que el contenido ya no se encuentra en la ubicación original.

La oposición de Internet Society a los bloqueos basados en DNS y direcciones IP se fundamenta en que estas técnicas socavan las propiedades fundamentales de Internet, tal como se definen en el **modo Internet de interconectarse (IWN, por sus siglas en inglés).** Estos métodos de bloqueo alteran la arquitectura técnica que hace que Internet sea abierta, globalmente accesible y resiliente.

Internet Society ha desarrollado una descripción técnica de estos principios fundamentales que denominamos "el modo Internet de interconectarse", un marco que explica lo que distingue a Internet de otras redes. Para ayudar a nuestra comunidad de expertos técnicos, en políticas y de otras áreas a utilizar este marco, Creamos el Kit de herramientas para la evaluación del impacto sobre Internet[7]. Estas herramientas pueden ayudar a identificar cómo las políticas, las decisiones empresariales, las regulaciones o las tendencias pueden afectar los cimientos únicos de Internet o las mejores prácticas que la sustentan.

[7] Internet Society. *Kit de herramientas para la evaluación del impacto sobre Internet*, 2020. Disponible en: https://www.internetsociety.org/es/resources/internet-impact-assessment-toolkit/