

¿Qué es la censura en Internet?

La censura en Internet es la supresión o **control intencional** de lo que se puede acceder, publicar o ver en Internet.

OONI mide la censura a nivel de red, que incluye el **bloqueo de sitios web y aplicaciones**.

¿Por qué medir la censura en Internet?

- 1 Comprobar/confirmar informes
- 2 Descubrir controles de información
- 3 Transparencia y supervisión
- 4 Recopilar evidencias de controles de la información



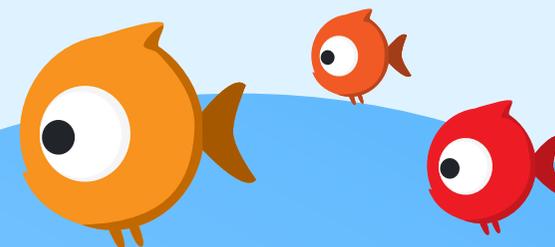
Fundado en 2012, el Observatorio Abierto de Interferencias en la Red (OONI, por sus siglas en inglés) es un proyecto de software libre sin ánimo de lucro que documenta la censura en Internet alrededor del mundo.

Conoce más sobre OONI: ooni.org



Entendiendo la censura en Internet

Explorando restricciones y control de acceso en la web



¿Quién implementa la censura en Internet?

Los proveedores de servicios de Internet (ISPs) pueden utilizar diversas técnicas de censura como la **manipulación de DNS, bloqueo de IP, filtrado SNI**, entre otras.

“¿Cómo se implementa la censura en Internet?”

Los **proveedores de servicios de Internet (ISP) bloquean el acceso a determinados sitios web y/o aplicaciones** basados en órdenes gubernamentales y/o en cumplimiento de la legislación nacional.

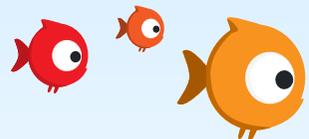
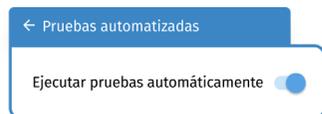
¿Cómo medir la censura en Internet?

Obtén la aplicación **OOONI Probe** para móvil y escritorio.

Escanea para instalar OONI Probe →



¡Activa las **pruebas automatizadas** en la configuración para que se ejecuten todos los días automáticamente!



Manipulación del DNS

La manipulación de DNS se produce cuando los proveedores de servicios de internet (ISP) interfieren en la resolución DNS de un determinado nombre de servidor, impidiéndote acceder a él (p. ej., devolviendo la IP incorrecta).

Bloqueo HTTP

“El bloqueo HTTP se produce cuando un ISP **interfiere en la conexión entre su ordenador y el servidor que aloja el sitio web** al que intentas acceder”

Esto puede implementarse interceptando su petición HTTP (en algunos casos, redirigiéndole a una página bloqueada) o cerrando la conexión (impidiendo así el intercambio normal entre su computador y el servidor del sitio web).

Bloqueo IP

El bloqueo IP ocurre cuando proveedores de servicios de Internet (ISP) **bloquean las conexiones a la dirección IP** de un sitio web.



Filtrado SNI

SNI es una extensión para el protocolo TLS (utilizado para sitios web alojados en HTTPS), diseñada para especificar con qué nombre de host debe establecerse la conexión cifrada.

Como el campo SNI no está cifrado, los ISP pueden ver si estás intentando acceder a un sitio web prohibido y restringir el acceso (p. ej., cerrando la conexión).

La censura informada por el **campo SNI** se caracteriza como filtrado SNI

Método de detección	Método de bloqueo					
	Cierre de la conexión (RST o FIN)	Pérdida de paquetes	Ralentización del tráfico	Ataque de intermediario	Respuesta HTTP no válida	Respuesta DNS no válida
IP de destino (+puerto)	✓	✓	✓	✓		
Dominio en consulta de DNS						✓
Cabecera del servidor HTTP	✓	✓	✓	✓	✓	
Campo SNI en el apretón de manos TLS	✓	✓	✓	✓		