THE internet SHUTDOWN GAME

MANUAL DEL JUEGO

APC
ASOCIACIÓN PARA
EL PROGRESO DE
LAS COMUNICACIONES

Publicado por APC en 2023 en inglés - versión en español del 2025
ISBN 978-92-95113-75-6
APC-202510-APC-T-ES-DIGITAL-365

ÍNDICE

ACERCA DE ESTE JUEGO

Hemos creado las instrucciones de este juego con el objetivo de ayudar a organizar una actividad de capacitación atractiva e informativa que arroje luz sobre los diversos métodos de bloqueo de internet y las formas de contrarrestarlos.

Los gobiernos recurren a los apagones de internet con fines muy diversos. Estos van desde la adopción de medidas cautelares y preventivas para frenar la difusión de información no verificada en situaciones turbulentas, hasta la defensa de la seguridad nacional y el mantenimiento del orden público. Los apagones de internet son un fenómeno preocupante que no solo interrumpe la conectividad digital, sino que también supone una amenaza significativa para los derechos humanos. Comprender las motivaciones y los distintos métodos empleados para bloquear el acceso a internet es fundamental para las personas y organizaciones que luchan por salvaguardar la libertad en internet y proteger los derechos humanos en la era digital.

Diseñado como un juego de creative commons que se puede adoptar y adaptar, este documento proporciona instrucciones detalladas para los facilitadores del juego y sugerencias sobre la dinámica del mismo, así como un mapa y cartas para jugar tanto en persona como en un entorno en línea.
Creemos que este juego puede ser jugado por una variedad de públicos y puede servir como una herramienta valiosa para crear conciencia sobre las diferentes tácticas empleadas para restringir el acceso a internet, así como para mejorar la comprensión de quienes participan sobre la infraestructura de internet, los procedimientos de bloqueo y el uso de diversas herramientas para eludirlos.

Las instrucciones del juego pueden ser utilizadas por cualquier persona, tanto si se planea facilitarlo en persona como en un entorno en línea. El público objetivo de este juego abarca a personas dedicadas a la defensa de los derechos humanos, ciudadanos/as preocupados/as por la temática, profesionales del derecho y cualquier persona que se haya enfrentado al control gubernamental del acceso a internet y desee profundizar sus conocimientos en esta área.

A lo largo de un juego de 120 minutos, profundizaremos en las complejidades técnicas de varios modelos de bloqueos de internet. Al incorporar escenarios del mundo real y tarjetas de «elusión», quienes juegan obtendrán información sobre los mecanismos técnicos que hay detrás de los apagones y comprenderán mejor las diferentes estrategias que pueden utilizar para sortearlos.

Confiamos en que el juego te resulte entretenido y que las instrucciones te resulten útiles para ampliar tus conocimientos sobre los bloqueos de internet y los mecanismos de elusión. Nuestro compromiso es seguir mejorando esta herramienta para la comunidad en general. Esperamos poder compartir versiones actualizadas para garantizar su continua utilidad para todos; consulta la última versión en el sitio web del juego.

Envíanos tus comentarios, ideas de mejora y nuevos escenarios, o avisanos si deseas traducir el juego a otros idiomas, a shutdowngame@apc.org.

¡A disfrutar del juego!

El equipo técnico de APC: Avi, Igu, Maja, Mirto, Adolfo, Liz y Roxana.

https://shutdowngame.apc.org

Versión del juego 1.12 en español, Octubre de 2025

CONCEPTOS BÁSICOS DEL JUEGO

Este documento describe la organización y ejecución del Juego de los apagones de internet, una sesión de capacitación interactiva dirigida por personas que puede realizarse en persona o en línea. Este juego depende de quienes lo facilitan, siendo esenciales para su éxito. Son las personas que poseen los conocimientos necesarios para adaptar el contenido, el estilo, los escenarios elegidos, los niveles de dificultad y la dinámica del juego a las necesidades de quienes participan.

Quienes facilitan deben tener un conocimiento sólido de la infraestructura de internet y su funcionamiento. También deben estar atentos/as a las preguntas y dudas de quienes participan y garantizar un entorno inclusivo y participativo para todas las personas.

El juego utiliza un mapa que sirve como representación simplificada de la infraestructura nacional de telecomunicaciones de un país imaginario, en el que las personas que juegan pueden situarse a sí mismas y a sus dispositivos. Este mapa sirve como ayuda visual para explicar conceptos fundamentales relacionados con los principios básicos de la transmisión de datos, el funcionamiento de internet y los retos que plantea el diseño de las infraestructuras nacionales de telecomunicaciones.

Posteriormente, este mismo mapa se utiliza para presentar un escenario en el que el acceso a internet está bloqueado de cierta manera, basándose en ejemplos del mundo real, indicando los componentes específicos del mapa que han sido afectados para restringir el acceso a internet. El conjunto de herramientas del juego ofrece 13 escenarios de diferentes niveles de dificultad entre los que el equipo de facilitación puede elegir, según el perfil, la ubicación y los intereses de sus participantes.

Durante el juego, el grupo de participantes en equipos, analizan el escenario y seleccionan una tarjeta de elusión para intentar sortear el bloqueo. Los equipos compiten por puntos, pero lo realmente divertido es deliberar sobre las distintas soluciones y su eficacia dentro de los escenarios elegidos.

Después de haber realizado el juego con públicos diversos, hemos llegado a apreciar que cada sesión de juego representa una oportunidad para compartir y aprender. Cada sesión puede ser disfrutada como una experiencia única y enriquecedora para todas las personas involucradas y, con suerte, cada una de ellas también generará un conocimiento más preciso desde el punto de vista técnico sobre los bloqueos de internet y cómo sortearlos de manera más eficaz.

REQUISITOS DEL JUEGO: VERSIÓN PRESENCIAL

La versión presencial del juego está diseñada para un tamaño de grupo óptimo de entre 6 y 20 participantes, organizados en 2 o 3 grupos. Su duración suele oscilar entre 90 y 120 minutos.

Para facilitar esta versión, necesitarás los siguientes materiales:

1. Una superficie, tablero o tela en la que se dibuje el mapa de la red del país imaginario. Este mapa puede estar dibujado a mano, impreso o creado imprimiendo componentes individuales en papel y ensamblándolos en el suelo o la pared, conectándolos con líneas o hilos. También se puede proyectar el mapa en una pantalla grande.

2. Tarjetas de bloqueo: son varias tarjetas con una X roja, preferiblemente de material transparente. Estas tarjetas se utilizan para indicar qué componentes del mapa no funcionan cuando se juegan los diferentes escenarios de bloqueo.

3. Un juego de cartas con métodos de elusión para cada equipo jugador. Estas cartas son fundamentales en el juego y ayudan a los equipos a elaborar estrategias para sortear los bloqueos.

Con estos materiales y directrices, además de tus conocimientos e imaginación, podrás llevar a cabo con éxito una sesión presencial atractiva y educativa del Juego de los apagones de internet.

REQUISITOS DEL JUEGO: VERSIÓN EN LÍNEA

La versión en línea del juego es adecuada para entre 6 y 20 participantes, idealmente organizados en 2 o 3 grupos que utilizarán salas grupales privadas para sus debates y decisiones. La duración del juego en línea oscila entre 90 y 120 minutos.

Debido a las complejidades del juego a distancia, es recomendable contar con al menos dos personas facilitadoras que hayan coordinado el trabajo previamente y dividido las distintas tareas. Sus funciones incluirán la gestión de la presentación, la configuración de las salas grupales, el apoyo al uso de la plataforma en línea, la supervisión del desarrollo del juego y la respuesta a las preguntas y consultas de quienes participan.

Para facilitar esta versión, necesitarás lo siguiente:

1. Presentación del juego: prepara una presentación del juego en formato PDF. Debes proporcionar una visión general del juego, instrucciones y cualquier información básica necesaria. La que utilizamos está disponible aquí como parte de nuestro kit, en varios formatos.

2. Presentación para los/as jugadores/as: crea una presentación para quienes juegan que incluya los diferentes escenarios, el mapa del juego y las cartas que los equipos pueden utilizar durante el juego. Esta presentación debe estar disponible para todas las personas que participan y se puede compartir a través de una plataforma digital. También disponible aquí como parte de nuestro kit, en varios formatos.

3. Configuración de la reunión: necesitarás una sala de reuniones principal y salas grupales privadas, con una sala privada dedicada por equipo. Precarga la presentación para los/as participantes en cada sala grupal. Debe contener el diseño y las tarjetas para todos los escenarios, y estas salas deben permanecer accesibles durante toda la sesión. También se puede utilizar una pizarra compartida para el ejercicio de trazar la ruta sobre el mapa del juego.

4. Selección de cartas: implementa una forma para que cada equipo envíe de forma privada su carta seleccionada a la persona que facilita. Esto se puede hacer, por ejemplo, a través de una función de mensajes privados dentro de la plataforma en línea para garantizar que nadie más vea la carta elegida.

Si se tienen en cuenta cuidadosamente estos elementos y preparativos, la versión en línea del Juego de los apagones de internet se puede ejecutar con éxito, manteniendo el interés y el valor educativo, al tiempo que se adaptan los retos particulares de este juego operado a distancia y en línea.

INTRODUCCIÓN A LOS APAGONES Y AL MAPA DEL JUEGO

OBJETIVOS

Es recomendable comenzar el juego acordando los objetivos y las reglas del mismo.
Los objetivos del juego se pueden resumir de la siguiente manera:

1. Comprender mejor la infraestructura de internet: proporcionar a quienes juegan una comprensión integral de los conceptos técnicos fundamentales que rigen la infraestructura de internet. Esto incluye presentar los componentes de la infraestructura nacional de internet y debatir las diversas variaciones que existen. De este modo, obtendrán información sobre cómo se logran ejecutan técnicamente los distintos tipos de bloqueos.

2. Eludir los bloqueos: mejorar los conocimientos de quienes participan sobre los mecanismos y estrategias que se pueden emplear para eludir los bloqueos de internet. Esto incluye explorar formas de protegerse de posibles represalias gubernamentales, dotando así a las personas de las habilidades y la conciencia necesarias para navegar y mitigar el impacto de los bloqueos de manera eficaz.

> Consejo: Si trabajas con un grupo específico de participantes con un perfil determinado (por ejemplo, defensa de los derechos humanos, profesionales del derecho) o de una organización, país o región específicos, o si participas en un evento, probablemente puedas añadir otros objetivos más concretos a tu juego.

3. Facilitar el aprendizaje en un entorno seguro en el cual la gente pueda participar y se respeten todas las opiniones.

INTRODUCCIÓN A LOS APAGONES, SU RELACIÓN CON LA INFRAESTRUCTURA DE INTERNET Y SU IMPACTO EN LOS DERECHOS HUMANOS

Un apagón o bloqueo de internet puede definirse como «una interrupción intencionada de las comunicaciones basadas en Internet, que las hace inaccesibles o efectivamente no disponibles para una población, ubicación o modo de acceso específicos, a menudo con el fin de ejercer control sobre el flujo de información».[1]

Los gobiernos emplean una gran variedad de técnicas con diferentes nombres para ejercer control sobre internet. Estos métodos se pueden denominar cortes, interrupciones, apagones, bloqueos, toques de queda, limitaciones de acceso, prohibición de uso, censura, desvío de tráfico, secuestro de DNS, bloqueo geográfico, cierre, fragmentación, entre otros términos utilizados. La proliferación de estas diversas tácticas de bloqueo subraya la necesidad de dotar a los/as defensores/as de una mejor preparación para poder comprender y eludir estos mecanismos.

Los gobiernos recurren a los bloqueos, apagones y cierres de internet con una amplia variedad de fines. Estos van desde la adopción de medidas cautelares y preventivas para frenar la difusión de información no verificada en situaciones turbulentas, hasta la defensa de la seguridad nacional y la garantía del mantenimiento del orden público.

Los bloqueos de internet son un fenómeno preocupante que no solo interrumpe la conectividad digital, sino que también supone una amenaza significativa para los derechos humanos. Los cortes suelen producirse en lugares donde los gobiernos desean ejercer control sobre el flujo de información y reprimir la disidencia, lo que restringe de manera efectiva la libertad de expresión y el acceso a la información y los servicios. Estas acciones violan el derecho humano fundamental a la libertad de expresión y el derecho a la libertad de reunión, consagrados en acuerdos internacionales como la Declaración Universal de los Derechos Humanos. Pero los apagones de internet tienen consecuencias de gran alcance, que van más allá de la libertad de expresión y de reunión. Impiden el acceso a servicios esenciales como la salud, los recursos educativos, los recursos empresariales e incluso las comunicaciones de emergencia, lo que repercute directamente en el derecho a la educación y el derecho a la vida en casos de crisis, guerras o desastres naturales. Esta relación que existe entre la infraestructura de internet y la forma en que se ejecutan los cortes de la misma subraya la necesidad de un ecosistema de internet más robusto, descentralizado y resistente, una relación que puede quedar muy clara al jugar a este juego.

[1] https://www.internetsociety.org/policybriefs/internet-shutdowns

Cuando se producen apagones, la mayoría de los gobiernos no reconocen que estos están ocurriendo y, en cambio, culpan de la interrupción a fallos técnicos, congestiones de la red o ciberataques. Pero todos los cortes son en realidad posibles gracias al nivel de control que los gobiernos tienen sobre diferentes componentes de su infraestructura nacional de telecomunicaciones. El control gubernamental sobre las redes de telecomunicaciones y los componentes clave de la infraestructura, como los proveedores de servicios de internet (ISP), los puntos de intercambio de internet (IXP), las conexiones internacionales (llamadas *gateways*), los reguladores de telecomunicaciones y/o los servidores de nombres de dominio de nivel superior (DNS), facilita a las autoridades la aplicación de estos cortes, convirtiendo a internet - que ahora se considera un servicio básico - en una herramienta que puede utilizarse como arma contra las mismas personas a las que se supone que debe empoderar. Todo ello hace que los cierres, en sus múltiples formas, sean también casi imposibles de demostrar.

La protección de los derechos humanos en la era digital requiere el compromiso de garantizar que internet siga siendo abierta y accesible para todas las personas, independientemente de las circunstancias políticas o sociales, y que su infraestructura esté diseñada para resistir el control y la censura indebidos de los gobiernos.

Comprender cómo se producen los apagones y bloqueos, qué componentes de la infraestructura de internet se ven amenazados y cómo eludir estos bloqueos es fundamental para las personas y organizaciones que luchan por salvaguardar la libertad en internet y proteger los derechos humanos en la era digital.

Si deseas obtener más información sobre los bloqueos y sus consecuencias, o remitir a participantes que puedan estar interesados en referencias adicionales para profundizar en su comprensión de los bloqueos y sus consecuencias, puedes encontrar un conjunto de recursos comentados y lecturas recomendadas en el anexo 3.

INTRODUCCIÓN AL MAPA DEL JUEGO Y AL FUNCIONAMIENTO DE INTERNET

En la versión en línea, este mapa se puede compartir a través de diapositivas, mientras que para las sesiones presenciales se puede imprimir, dibujar en tela o crear de forma dinámica utilizando trozos de papel e hilo para representar y conectar los componentes individuales

El juego emplea un mapa que representa la infraestructura de internet de un país imaginario. Este mapa sirve como punto de referencia visual compartido, situando a quienes participan en un espacio común y ayudándoles a comprender los conceptos fundamentales de la conectividad.

Antes de comenzar el juego, es esencial aclarar que el mapa es una herramienta simulada, que representa una infraestructura simplificada de telecomunicaciones de un país imaginario. Se debe informar a quienes participan de que la infraestructura del mundo real varía significativamente de un país a otro y que su diseño se ve influido por múltiples factores, entre los que se incluyen las normas técnicas, los marcos legales, las políticas gubernamentales, la topología del terreno, los monopolios existentes, los intereses comerciales, las presiones geopolíticas, el deseo de control y muchos otros.

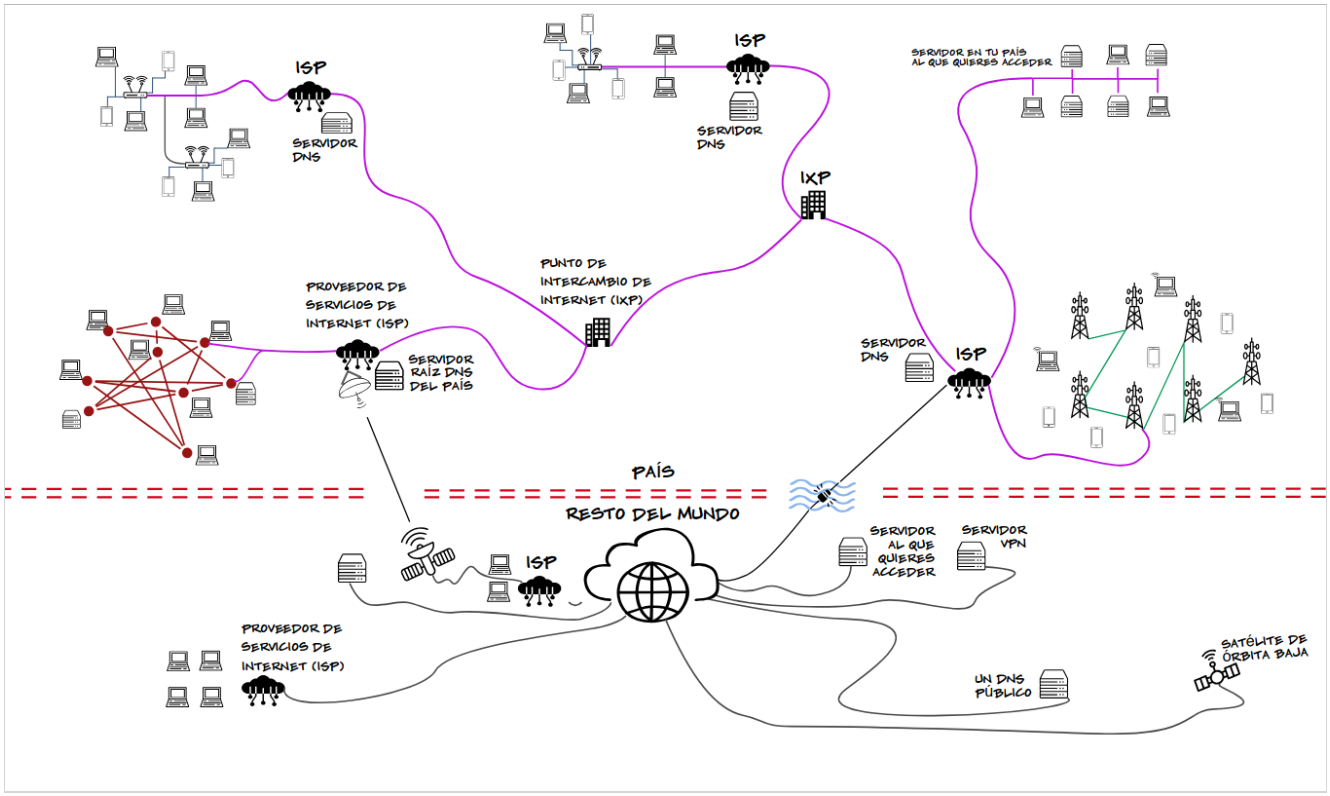
Para presentar el juego, puedes utilizar el mapa para explicar el funcionamiento de internet.

- En la versión en línea, esto se puede lograr utilizando diferentes diapositivas para añadir gradualmente componentes al mapa, culminando con la presentación del mapa completo. Consulta nuestras diapositivas de ejemplo.

- En el entorno presencial, se puede emplear un enfoque similar utilizando piezas impresas y construyendo el mapa de forma colaborativa con quienes participan, añadiendo las partes a medida que se introducen los conceptos, de forma similar a lo que se hace en la presentación en línea.

Esta fase introductoria ayuda a establecer una comprensión básica de cómo funciona internet en el contexto del juego. Requiere entre 20 y 30 minutos, incluyendo un par de ejercicios realizados sobre el mismo mapa.

Componentes del mapa



Analicemos los componentes del mapa y proporcionemos descripciones de cada uno de ellos para ayudarte a facilitar la sección introductoria del juego:

Límite del país (línea punteada)

La línea punteada roja en la parte inferior del mapa representa la frontera territorial del país. Todo lo que se encuentra por encima de esta línea es componente de la infraestructura nacional de internet, que puede ser influenciada y controlada por el gobierno. Por el contrario, todo lo que se encuentra por debajo de esta línea representa la infraestructura de internet más amplia, fuera del control del gobierno.

Proveedores de servicios de internet (ISP)

Son empresas responsables de gestionar la infraestructura de acceso a internet para individuos y organizaciones. Nuestro mapa muestra varios tipos de ISP, incluidos los que ofrecen acceso de banda ancha (como cable, ADSL, fibra óptica), uno que ofrece telefonía móvil y banda ancha, y otro que conecta una red en malla (o *mesh network*). Cada una de estas redes, bajo el control de una sola entidad, también se denominan técnicamente *sistemas autónomos*.

Puntos de intercambio de internet (IXP):

Los IXP son lugares donde los ISP conectan sus redes con otras, lo que facilita el intercambio de tráfico local de internet. El número y la calidad de los IXP en un país pueden influir significativamente en la eficiencia del tráfico nacional y reducir la latencia (retrasos en la llegada de los datos a su destino) y los costos de telecomunicaciones. En nuestro ejemplo, hay dos IXP que conectan a los ISP entre sí. Los IXP pueden ser de propiedad privada, cooperativa o estar gestionados por organizaciones gubernamentales.

Conexiones internacionales

Nuestro país de ejemplo tiene dos puntos de conexión internacional a la red global de internet, también llamados enlaces o *gateways*. Estas conexiones están representadas por un enlace satelital y un cable submarino, cada uno gestionado por un ISP diferente. Los países también pueden tener conexiones internacionales fijas (a través de cables o radio).

El número y el tipo de puntos de conexión internacional dependen de factores como el deseo de control del gobierno, los recursos económicos, la ubicación geográfica, la topografía, el mercado monopólico, etc., y pueden variar desde uno hasta cientos de puntos de conexión con el mundo «exterior».

También existe una tercera opción, el uso de conexiones de satélites geoestacionarios para el acceso internacional directo por el espacio.

El resto de la nube de internet

Más allá de las fronteras del país, representamos el resto de internet, conocido como la «nube de internet». Esto abarca diversos recursos, como servidores y otros servicios en línea que utilizaremos en este juego. Recuerde a los participantes que todo lo que se encuentra fuera de la infraestructura nacional de nuestro país imaginario (es decir, por encima de la linea roja) NO está bajo el control del gobierno.

Opciones de conectividad

En nuestro mapa de país imaginario hay varias formas de conectarse a internet:

Red de telefonía celular: puede conectarse a través de un dispositivo que conecta con una antena celular, con los datos viajando a través de la red celular y

conectándose finalmente a la red nacional de internet a través de un proveedor de servicios de internet. Destaca que las antenas están conectadas de forma jerárquica.

Banda ancha: incluye conexiones como fibra óptica, DSL y cable, que suelen dar servicio a una zona geográfica limitada con una alta densidad de gente usando el servicio.

Red en malla (mesh): redes especializadas en las que los nodos de acceso están interconectados, que se utilizan a menudo en redes comunitarias. Se trata de una infraestructura muy resiliente debido a la multiplicidad de conexiones.

Acceso por satélite: una conexión directa a una constelación de satélites de órbita baja (LEO) evita la infraestructura nacional, conectándose directamente a los satélites en órbita y retransmitiendo los datos a una estación terrestre en otro país. (Ejemplos: Starlink, Project Kuiper, Oneweb, IRIS).

Wi-Fi: los puntos de acceso Wi-Fi proporcionan conectividad inalámbrica de corto alcance, que normalmente cubre un área limitada y se conecta a uno de los otros métodos de conexión.

Direcciones IP

Es importante explicar que todos los dispositivos conectados a internet, como computadoras, teléfonos y tabletas, deben tener un identificador único conocido como dirección IP. Todos los servidores que ofrecen contenido también tienen una dirección IP.
Las direcciones IP son esenciales para que los datos viajen desde su origen hasta su destino en internet: los paquetes de datos llevan la dirección IP de su origen y su destino.

Ejercicio: Seguimiento de las rutas de datos

Este ejercicio no solo ayuda a visualizar las rutas de los datos, sino que también sirve como una forma práctica e interactiva de reforzar los conceptos presentados en el mapa del juego. Fomenta la participación y garantiza que la gente se sienta cómoda con el mapa y sus componentes antes de continuar con el juego.

Para jugar en línea, utilizando un tablero compartido

Activar el tablero compartido con el mapa completo: asegúrate de que la herramienta del tablero compartido esté accesible y lista para que los equipos participantes la utilicen. En muchas plataformas de reuniones en línea se puede utilizar una pizarra digital o una herramienta externa.

Explica el ejercicio: informa a los equipos que simularán las rutas de los datos desde diferentes lugares de acceso a un servidor, tanto dentro del país como en el extranjero. Este ejercicio tiene como objetivo reforzar los conceptos y familiarizar a la gente con el mapa del juego.

- **Seleccionar ubicaciones:** pide a los equipos que se imaginen en una de las ubicaciones de acceso del mapa del juego (por ejemplo, un dispositivo conectado por Wi-Fi, red celular, banda ancha o red en malla). Pueden elegir cualquier ubicación.

- **Dibujo de la ruta de datos:** con una herramienta de lápices de colores, pide que dibujen la ruta que seguirían sus datos desde la ubicación de acceso elegida hasta el servidor resaltado en el país (parte superior derecha del mapa). Anima a seguir los componentes de la infraestructura que se muestran en el mapa.

- **Debate y revisión:** mientras dibujan sus rutas de datos, modera un debate. Pide que expliquen sus elecciones y la ruta que han dibujado. Esta es una oportunidad para revisar conceptos y aclarar cualquier idea errónea. Comparte cómo la ruta que siguen los datos no puede ser controlada por individuos, y que incluso diferentes paquetes siguen diferentes rutas en función del costo, el tiempo, la velocidad, etc. Una vez que sientan comodidad con el ejercicio, repítelo con un servidor ubicado en el extranjero.

- **Reitera los conceptos clave:** a lo largo del ejercicio y mientras la gente dibuja sus rutas de datos, refuerza los conceptos clave, como las direcciones IP, la participación de los ISP, la conexión de las redes celulares a internet y el papel de los IXP.

- **Fomenta la participación:** anima la participación activa y a hacer preguntas. Asegúrate de que toda la concurrencia tenga la oportunidad de contribuir y comprender mejor la infraestructura de internet.

Para jugar en persona, marca, indica o camina sobre el mapa del juego.

- **Explica el ejercicio:** informa a quienes participan que simularán rutas de datos desde diferentes ubicaciones de acceso a un servidor, tanto dentro del país como en el extranjero. El objetivo de este ejercicio es reforzar los conceptos y familiarizar a la gente con el mapa del juego.

- **Seleccionar ubicaciones:** pide que se sitúen en una de las ubicaciones de acceso del mapa del juego (por ejemplo, un dispositivo conectado a la red Wi-Fi, red celular, banda ancha o red en malla). Los equipos pueden elegir cualquier ubicación.

- **Dibujo de la ruta de datos:** indica que marquen la ruta que seguirían sus datos desde la ubicación de acceso elegida hasta el servidor resaltado en el país (parte superior derecha del mapa). Anímales a seguir los componentes de la infraestructura que se muestran en el mapa, utilizando los dedos para indicar cómo viajan los datos.

- **Debate y revisión:** mientras indican sus rutas de datos, modera un debate. Pídeles que expliquen sus elecciones y la ruta que están utilizando. Esta es una oportunidad para revisar conceptos y aclarar cualquier idea errónea. Una vez que las personas se sientan cómodas con el ejercicio, repítelo con un servidor ubicado en el extranjero.

- **Reitera los conceptos clave:** a lo largo del ejercicio y mientras dibujan sus rutas de datos, refuerza los conceptos clave, como las direcciones IP, la participación de los proveedores de servicios de Internet, la conexión de las redes de telefonía móvil a Internet y el papel de los IXP.

- **Fomenta la participación:** anima a la gente a participar activamente y a hacer preguntas. Asegúrate de que tengan la oportunidad de contribuir y comprender mejor la infraestructura de internet.

Resolución del DNS (servidor de nombres de dominio)

Una vez que se sientan en comodidad con la estructura del mapa, presentaremos el último componente fundamental.

La resolución del DNS es un paso preliminar fundamental en cualquier intercambio de datos por internet. Permite que su dispositivo encuentre la dirección IP del servidor que aloja el sitio web, el contenido o el servicio al que desea acceder. Una vez conocida esta dirección IP, los datos pueden enrutarse a su destino en internet.

Como paso final explica que, antes de que los datos puedan viajar desde su dispositivo hasta su destino previsto en internet, se produce un paso crucial denominado resolución del sistema de nombres de dominio (DNS). Recuerda a los/as participantes que, para que los datos viajen a través de internet, es necesario disponer de la dirección IP del servidor de destino. El proceso DNS traduce los nombres de dominio fáciles de recordar para los humanos (como www.apc.org) a direcciones IP legibles por las máquinas. Este proceso es automático, transparente y necesario para que cualquier dato pueda viajar.

A continuación se ofrece una descripción general de la resolución del DNS, incluidas las consultas al DNS más cercano, al DNS de nivel superior y a los servidores DNS ubicados en el extranjero:

- Cuando escribes un nombre de dominio (por ejemplo, www.apc.org) en tu navegador web o en cualquier aplicación conectada a internet, tu dispositivo necesita conocer la dirección IP correspondiente a ese servidor o recurso.
- Si la dirección IP del dominio no está almacenada en la memoria caché local, tu dispositivo envía una consulta al servidor DNS especificado en su configuración o establecido por su proveedor de servicios de internet (ISP). Este servidor DNS suele ser el más cercano a su ubicación en términos de topología de red.
- El servidor DNS más cercano comprueba su propia caché. Si tiene la dirección IP del dominio solicitado, responde a tu dispositivo con la dirección IP.
- Si el servidor DNS más cercano no tiene la dirección IP en su caché, inicia una consulta recursiva para encontrar la información. Esta consulta puede involucrar a varios servidores DNS a lo largo del proceso.

- Consulta al DNS de nivel superior:
    - Si el servidor DNS más cercano no tiene la dirección IP, necesita averiguar qué servidor DNS es responsable del dominio de nivel superior (TLD) del dominio al que está intentando acceder. Por ejemplo, en el caso de www.apc.org, el TLD es «.org».
    - El servidor DNS más cercano envía una consulta al servidor DNS del TLD, solicitando información sobre el servidor DNS autoritativo para el dominio «apc.org».
    - El servidor DNS del TLD responde con la dirección del servidor DNS autoritativo para «apc.org».
- En algunos casos, especialmente cuando se accede a sitios web alojados en el extranjero, es posible que la consulta traspase las fronteras de tu país. Es posible que el servidor DNS más cercano no tenga información sobre el servidor DNS autoritativo para el dominio al que intentas acceder, y que el servidor DNS tenga que enviar una consulta a un servidor DNS ubicado en el extranjero que se especialice en gestionar consultas DNS internacionales. El servidor DNS en el extranjero puede entonces proporcionar información sobre el servidor DNS autoritativo para el dominio solicitado.

Utiliza el mapa para trazar la ruta de un par de ejemplos de solicitudes DNS.

Estos componentes y descripciones del mapa sirven como conocimiento básico para ayudar a la gente presente a comprender los conceptos básicos de la infraestructura de internet, la conectividad y los escenarios de juego posteriores.

La explicación del mapa y las actividades relacionadas con él deberían llevar entre 20 y 30 minutos.

CÓMO LLEVAR A CABO EL JUEGO

EJECUCIÓN DEL JUEGO EN PERSONA

La ejecución del juego en persona implica varios pasos y una facilitación cuidadosa para garantizar una experiencia fluida y atractiva para la gente. A continuación se detalla cómo llevar a cabo el juego:

1. Compartir el mapa del juego y explicar las reglas:

- Comienza compartiendo el mapa completo del juego con quienes participan y proporcionando una breve descripción general de las reglas del juego.
- Explica las cartas que tienen a su disposición para sortear los bloqueos.
- Aclara el sistema de puntos utilizado para puntuar a lo largo del juego.

2. Asignar los equipos:

- Asigna los equipos.
- Pídeles que designen a una persona de cada equipo para comunicar, compartiendo la carta que su equipo ha seleccionado para cada ronda.

Opcional: indícales que se reúnan brevemente y elijan un nombre para su equipo.

3. Preparar el marcador de puntos:

- Prepara el marcador utilizando los nombres de los equipos si se han seleccionado.

4. Presentar las tarjetas de elusión:

- Familiariza a los equipos con las tarjetas de elusión, haciendo hincapié en que solo pueden jugar una tarjeta por escenario. Las tarjetas se encuentran en el anexo 1.
- Explica la funcionalidad de cada carta y el impacto que tienen en el escenario del juego. Aclara cómo se cuentan los puntos.
- Destaca que la tarjeta «satélite» solo se puede utilizar una vez y que la tarjeta «comodín» puede representar cualquier escenario técnicamente viable y realista (excepto el satélite).
- Entrega un juego de tarjetas de elusión a cada equipo.

5. Comenzar con un escenario:

- Presenta el primer escenario bloqueando un componente específico en el mapa. Utiliza tarjetas transparentes con una «X» para bloquear los componentes pertinentes.

- Explica los detalles de lo que se bloquea, por qué se bloquea y el nivel de control gubernamental sobre ese componente de la infraestructura.

6. Debatir en equipo:

- Envía a los equipos a un espacio privado cercano (por ejemplo, una mesa) donde también puedan ver el mapa si es necesario.

- Dales 10 minutos para analizar el escenario, debatir posibles soluciones y seleccionar la tarjeta que quieren jugar.

7. Compartir, comparar soluciones y debatir:

- Cuando los equipos regresen, pide a cada uno de ellos que coloque la tarjeta seleccionada boca abajo sobre la superficie del mapa.

- Una vez que todos los equipos hayan regresado, muestra las cartas seleccionadas. Pide a cada equipo que explique los motivos por los que ha elegido la carta concreta que ha utilizado para sortear el bloqueo.

- Participa en el debate con los equipos, evalúa sus soluciones, explica por qué funcionaron o no funcionaron, asegúrate de que las soluciones comodín (si se han utilizado) sean técnicamente viables y precisas, y anota los puntos en función de las decisiones tomadas.

8. Repetir con otros escenarios:

- Repite el proceso con entre tres y seis escenarios, según lo permita el tiempo y ajustándose al nivel de participación de los equipos. Explora varios escenarios de bloqueo para poner a prueba las habilidades de resolución de problemas y creatividad de quienes participan.

9. Reflexión final:

- Concluye el juego facilitando una sesión de reflexión. Anima a debatir lo que han aprendido del juego, haciendo hincapié en las conclusiones clave, como los retos que plantea demostrar que efectivamente existen bloqueos y la eficacia de las herramientas de elusión.

- Anima a la gente presente a reflexionar sobre las implicaciones de estos conceptos en el mundo real.

Adaptaciones del juego:

- Los escenarios del juego se pueden encontrar en el anexo 2. Lo ideal es jugar tres o cuatro escenarios para que las personas involucradas comprendan claramente los diferentes modelos de bloqueo. Comienza siempre con uno fácil, para que la gente pueda entender la dinámica y no se sienta frustrada.

- En el caso de grupos pequeños y tímidos, y si dispones de tiempo adicional, dales cinco minutos al principio para que elijan un nombre para su equipo, ya que esto ayuda a crear una buena dinámica de equipo.

- La carta comodín se puede utilizar en caso de que los equipos respondan muy rápido o de que el público tenga muchos conocimientos técnicos. Se pueden ofrecer más puntos por utilizar esta carta de forma creativa (por ejemplo, +2 puntos).

- Si los equipos tienen dificultades para llegar a un consenso, puedes considerar, después de pasar por varios escenarios, analizarlos todos juntos en el espacio o sala principal, y olvidarse de los puntos o incluso de los espacios separados.

Si sigues los pasos anteriores, te aseguramos que podrás crear una experiencia de juego interactiva e informativa que profundice la comprensión de las personas participantes sobre los apagones de internet y de las estrategias que podemos usar para contrarrestarlos.

Envíanos tus comentarios, ideas de mejora y nuevos escenarios a: shutdown-game@apc.org .

CÓMO JUGAR EN LÍNEA

Para ejecutar el juego en línea hay que seguir varios pasos que garantizan una experiencia fluida y atractiva para quienes participan. Asegúrate de haber preparado los espacios en línea con antelación y de haber asignado funciones claras a cada persona facilitadora. A continuación te ofrecemos una descripción detallada de cómo sugerimos llevar a cabo el juego:

1. Comparte el mapa del juego y explica las reglas:

- Comienza compartiendo el mapa completo del juego con las personas participantes y proporcionando una breve descripción general de las reglas del juego.
- Explica las cartas que tienen a su disposición para sortear los bloqueos.
- Aclara el sistema de puntos que se utilizará para puntuar a lo largo del juego.

2. Asigna equipos:

- Asigna las personas a los equipos. Opcional: indícales que se trasladen a salas separadas para elegir un nombre para su equipo.
- Pídeles que designen a una persona de cada equipo como vocera responsable de compartir la carta que su equipo tiene intención de jugar.
- Anima a los equipos a comunicar el nombre elegido a través del chat privado para practicar, de modo que estén preparados cuando tengan que compartir la carta que quieren jugar.

3. Prepara el marcador de puntos:

- Prepara el marcador utilizando los nombres de los equipos si se han elegido.

4. Presenta las cartas de elusión:

- Familiariza a las personas participantes con las cartas de elusión, haciendo hincapié en que solo pueden jugar una carta por escenario.
- Explica la funcionalidad de cada carta y el impacto que tienen en el juego. Aclara cómo se cuentan los puntos.
- Destaca que la tarjeta «satélite» solo puede usarse una vez y que la tarjeta «comodín» puede representar cualquier escenario técnicamente viable y realista (excepto el satélite).

5. Comienza con un escenario:

- Presenta el primer escenario bloqueando un componente específico en el mapa.

- Explica los detalles de lo que está bloqueado, por qué está bloqueado y el nivel de control gubernamental sobre ese componente de la infraestructura.

6. Debates en salas grupales:

- Envía a los equipos a sus respectivas salas grupales con acceso al mapa del escenario y a las cartas que pueden jugar.
- Otórgales 10 minutos para analizar el escenario, debatir posibles soluciones y seleccionar la tarjeta que quieren jugar.
- Recuérdales que comuniquen a quien facilita cuál es la tarjeta que han seleccionado utilizando el canal secreto predefinido y diles que regresen a la sala principal una vez que hayan tomado una decisión.
- No dudes en visitar las salas virtuales para aclarar dudas u orientar el debate. Llama a todos los equipos de regreso a la sala principal una vez que haya terminado el tiempo asignado.

7. Comparte, compara soluciones y debate:

- Una vez que todos los equipos estén de regreso en la sala principal, comparte las diferentes cartas que cada equipo ha jugado. Pide a los equipos que presenten sus razones para elegir la carta concreta que han utilizado para sortear el bloqueo.
- Participa en el debate con los equipos, explica por qué la tarjeta funcionó o no funcionó, evalúa sus soluciones, incluyendo la viabilidad técnica y la precisión de las soluciones comodín, y anota los puntos en base a las decisiones tomadas.

8. Repite con otros escenarios:

- Repite el proceso con entre tres y seis escenarios, según lo permita el tiempo, y ajústalo en función del nivel de participación. Explora varios escenarios de bloqueo para poner a prueba las habilidades de resolución de problemas y la creatividad de la gente presente.

9. Reflexión final:

Concluye el juego facilitando una sesión de reflexión con la gente.

- Anímales a debatir lo que han aprendido del juego, haciendo hincapié en las conclusiones clave, como los retos que plantea demostrar los cierres y la eficacia de las herramientas de elusión.
- Anima a reflexionar sobre las implicaciones de estas ideas en el mundo real.

Adaptaciones del juego

- La realización del juego en línea requiere una planificación cuidadosa adicional:

    - Configura los espacios en línea con anticipación.
    - Explica cuidadosamente cómo funcionan las salas grupales y cómo entrar y salir de ellas.
    - Permite a la gente convocada a descargar una copia de los escenarios y las cartas que pueden jugar.
    - Asegúrate de que los equipos tengan claro cómo informar al grupo de facilitación de la carta que han seleccionado.

- Los escenarios del juego se encuentran en el anexo 2. Lo ideal es jugar tres o cuatro escenarios para que quienes participan comprendan claramente los diferentes modelos de bloqueo. Selecciona escenarios que sean más fáciles para empezar y añade complejidad según sea necesario, dependiendo del grupo participante, el nivel de energía y la competitividad.
- En el caso de grupos pequeños y tímidos, y si dispones de tiempo adicional, dales cinco minutos al principio para que elijan un nombre para su equipo, ya que esto ayuda a crear una buena dinámica de equipo.
- Si los/as jugadores/as tardan en seleccionar una respuesta o tienen muchas dudas técnicas, juega menos escenarios y dedica más tiempo a los conceptos básicos técnicos, explicando con más detalle los mecanismos de bloqueo y las técnicas de elusión.
- Si las personas jugadoras son muy rápidas, dedica más tiempo a debatir diferentes soluciones alternativas a los escenarios. ¡Incluso puedes ofrecer más puntos a cualquier equipo que utilice una solución comodín válida!
- Si los equipos tienen dificultades para llegar a un consenso, puedes considerar, después de pasar por algunos escenarios, analizar nuevos escenarios todos juntos en el espacio o sala principal, y olvidarse de los puntos o incluso de los espacios separados.

Realizar el juego en línea para un gran número de participantes: en ocasiones, es posible que desees realizar el juego en línea para 30 personas o más. En este caso, trabajar en grupos no será productivo. Una variante sugerida es que, después de presentar cada escenario, cada participante seleccione la tarjeta que desee utilizando una encuesta o método de votación en línea, y luego se debatan las elecciones (tanto las correctas como las incorrectas) con todos los/as participantes.

Siguiendo estos pasos, puedes crear una experiencia de juego en línea interactiva e informativa que profundice la comprensión de la gente sobre los apagones de internet y las estrategias para contrarrestarlos.

Envíanos tus comentarios, ideas de mejora y nuevos escenarios a: shutdown-game@apc.org .

ANEXO 1: TARJETAS DE ELUSIÓN

Las tarjetas de elusión son la forma en que los equipos participantes eligen una solución para “saltar” un escenario de bloqueo específico.

Los equipos solo pueden jugar una carta por escenario. La carta «acceso por satélite» solo se puede jugar una vez por partida (de lo contrario, podrían jugarla en todos los escenarios y siempre funcionaría).

Las cartas jugadas correctas suman +1 punto, y las incorrectas restan -1 punto.

La carta comodín se puede utilizar para representar cualquier otra solución creativa pero viable. Las cartas comodín ofrecen espacio para debatir muchas buenas ideas, especialmente con participantes más expertos/as en tecnología.

Conexión a internet de respaldo

Una conexión alternativa (secundaria) a internet, basada en una tecnología de acceso diferente y con un proveedor de servicios de internet diferente. Por ejemplo, si tu conexión principal es de banda ancha, la conexión de respaldo podría ser una conexión celular 4G.

VPN

Al presentar esta carta, primero explica cómo funciona una VPN: muestra en el mapa la ubicación del servidor VPN en el extranjero.

Explica cómo viajan los datos sin una VPN y luego utilizando una VPN. Comenta que esto es bueno pero también más lento.

Conexión por satélite

Una conexión directa a una constelación de satélites de órbita baja (LEO) que elude toda la infraestructura nacional y se conecta a una estación terrestre en otro territorio. Ejemplos: Starlink, Proyecto Kuiper, IRIS (UE)

Dado que esta tarjeta elude toda la infraestructura del país, sorteará cualquier bloqueo. Sin embargo, puede ser costosa (aunque cada vez más barata) y lenta, y si no es legal, también existe el riesgo de que se localice el emisor de la antena.

Esta carta solo puede jugarse una vez en el juego. Anima a los/as jugadores/as a utilizarla solo en situaciones en las que ninguna otra carta funcione.

Cambia la configuración del DNS

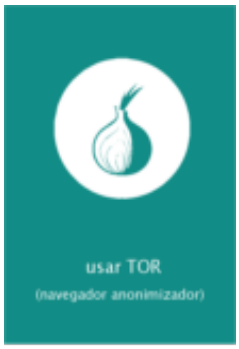
Cambia el DNS (servicio de nombres de dominio) predeterminado por un servidor DNS público (normalmente en el extranjero), en lugar del DNS predeterminado proporcionado por tu proveedor de servicios de internet.

Se recomienda refrescar cómo funciona la resolución DNS.

Utilizar Wi-Fi público

Explica que todos los usuarios que utilizan un punto de acceso público comparten la misma dirección IP, por lo que no es posible la identificación individual.

Además, el punto de acceso público podría utilizar otro proveedor de servicios de internet diferente al de otra ubicación.



Utilizar Tor

Explica cómo esto proporciona una navegación web anónima utilizando tres servidores anónimos ubicados en cualquier lugar. Explica cómo las capas de cebolla cifran el contenido y el destino. Explica por qué esto ralentiza la conexión pero también por qué puede ser muy difícil de bloquear.

La red Tor se puede utilizar con otros servicios, por ejemplo, utilizando Tor como proxy SOCKS, pero puede resultar demasiado complejo para este juego.

Utilizar una tarjeta SIM extranjera

Para países en los que cada tarjeta telefónica debe estar asociada a un documento de identidad nacional. Utiliza acuerdos de *roaming* y la infraestructura nacional de telefonía móvil, pero es posible que se bloquee menos porque tiene un número de teléfono extranjero.

En algunos casos, cuando las personas viven cerca de las fronteras del país, lo utilizan para conectarse a la infraestructura del país vecino.

Comodín

Cualquier otra solución: pensar fuera de lo establecido.

Tiene que ser creativa, pero también técnicamente viable, y no una duplicación de otras tarjetas.

ANEXO 2: ESCENARIOS

A continuación, ofrecemos 13 ejemplos de escenarios que puedes seleccionar para utilizar con tus participantes.
Dadas las limitaciones de tiempo, podrás jugar entre cuatro y seis escenarios durante una partida de dos horas. Puedes seleccionar cuáles jugar de antemano, o elegir a medida que avanza el juego y si las personas participantes encuentran los escenarios demasiado difíciles o demasiado fáciles. Las personas participantes de un país o región específicos pueden beneficiarse de escenarios que se ajusten a los obstáculos reales que han experimentado.

Te sugerimos que empieces siempre con uno fácil para que ganen confianza a medida que aprenden y comienzan a comprender las reglas del juego.
Para mayor claridad, es importante marcar en el mapa del juego (ya sea jugando en forma presencial o en línea) las partes de la infraestructura que están bloqueadas.

Esperamos añadir más escenarios a medida que el juego evolucione con los comentarios recibidos. Si tienes ideas para más escenarios, escribe a shutdowngame@apc.org.

ESCENARIO 1: TOQUE DE QUEDA (TAMBIÉN LLAMADO CIERRE PARCIAL/DE LA RED)

Dificultad: Fácil.

Descripción del escenario: Es época de exámenes y el gobierno ha impuesto un toque de queda para la banda ancha. Tienes banda ancha en casa y tu conexión a internet no funciona.

Qué bloquear: Todas las redes de banda ancha en el punto en el que se conectan a cada proveedor de servicios de internet (véase el ejemplo).

Cartas que se pueden jugar

Comodín:

– Trasladarse a otra ubicación

– Utilizar otro proveedor de servicios de internet (que no sea de banda ancha).

Cosas que hay que explicar

Este es un buen escenario para empezar: la mayoría de la gente se dará cuenta de que solo necesitan utilizar una red de acceso y un proveedor de servicios de internet distinto.

Es una buena oportunidad para destacar la importancia de tener siempre prevista una conexión de respaldo.

Ejemplos del mundo real

Utilizado por muchos países durante elecciones, exámenes y festivales.
Normalmente bloquean la banda ancha y dejan activas las redes de telefonía celular, pero algunos han bloqueado las redes de telefonía celular.

ESCENARIO 2: BLOQUEO DE CONTENIDOS

Dificultad: Fácil.

Descripción del escenario: Para sofocar las protestas, el gobierno ha bloqueado el acceso a Facebook, X y WhatsApp durante unas elecciones.

Qué bloquear: Filtros en todos los proveedores de servicios de internet.

Cartas que se pueden jugar

Comodín:

– Conectarse a una conexión de respaldo (tal vez)

– Utilizar otra herramienta de redes sociales (menos común).

Cosas que hay que explicar

Este tipo de bloqueo puede lograrse utilizando aplicaciones de filtrado comerciales y dispositivos proxy transparentes (que interceptan una solicitud https y hacen que parezca que ha sido respondida por el sitio original).

Las soluciones que utilizan Tor o VPN http tienen que acceder a las plataformas a través del navegador y no de la aplicación.

Ejemplos del mundo real

Se utilizan habitualmente durante protestas y elecciones. Normalmente se dirigen a las herramientas de redes sociales convencionales y no a las alternativas.

ESCENARIO 3: PUERTAS DE ENLACE INTERNACIONALES (*GATEWAYS*) CERRADAS

Dificultad: Fácil.

Descripción del escenario: Intentas acceder a un sitio web en el extranjero y recibes un mensaje de error. Te das cuenta de que esto ocurre con todos los sitios ubicados en el extranjero. Llegas a la conclusión de que el gobierno ha bloqueado los puntos de conexión internacional a internet.

Qué bloquear: Puertas de enlace internacionales.

Cartas que se pueden jugar

Comodín:

– Si se encuentra cerca de otro país, utilizar la red de datos móviles de ese país.

Cosas que hay que explicar

Las conexiones con constelaciones de satélites en órbita baja pueden ser caras, lentas y potencialmente vulnerables, ya que es fácil localizar quién las utiliza, pero evitan eficazmente toda la infraestructura nacional de internet. Por supuesto, la solución debe instalarse de antemano, ya que la configuración lleva un tiempo.

Ejemplos del mundo real

Este bloqueo solo es posible en países con pocas puertas de enlace internacionales que pueden desactivarse y que están todas bajo control gubernamental. En general, se trata de una medida temporal.

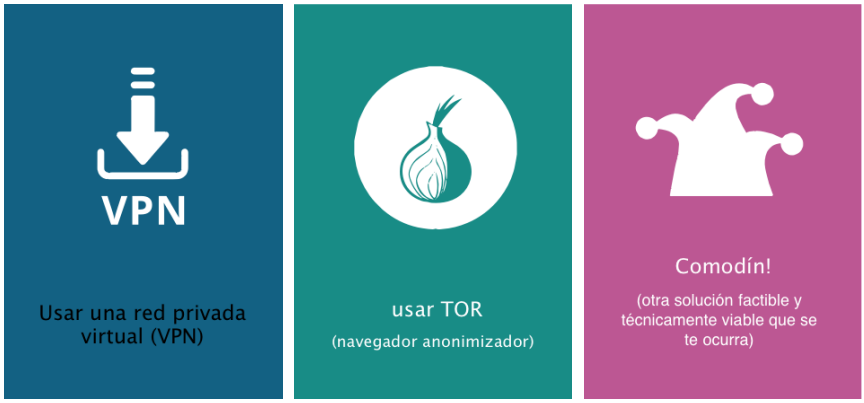
ESCENARIO 4: BLOQUEO DEL TRÁFICO

Dificultad: Fácil.

Descripción del escenario: El gobierno no quiere que accedas a un sitio web extranjero con cierta información. Ha ordenado a todos los proveedores de servicios de internet (ISP) de tu país que eliminen el tráfico destinado a la dirección IP de este sitio.

Qué bloquear: Todos los íconos de los ISP nacionales, para representar los enrutadores.

Cartas que se pueden jugar



Comodín:

– Duplicar el contenido del sitio a nivel local utilizando otra dirección IP

– Utilizar un ISP más pequeño que no obedezca las órdenes del gobierno

– Utilizar un proxy web.

Cosas que hay que explicar

Revisa cómo viajan los datos si se utiliza una VPN o el navegador Tor. Recuerda a los/as participantes que es recomendable tener uno o varios instalados de antemano.

Las tarjetas SIM extranjeras no funcionarán porque seguirán utilizando el enrutamiento a nivel nacional (acuerdos de *roaming* de las compañías de telefonía celular).

Cuando se utiliza el filtrado de paquetes, solo las personas que se encuentran dentro de la red afectada pueden detectar el cierre (utilizando una técnica llamada “sondeo activo”).

Ejemplos del mundo real

Se utiliza para bloquear sitios web sobre el aborto, sitios web de apuestas en línea, contenidos relacionados con la religión, sustancias prohibidas o ilegales, etc.

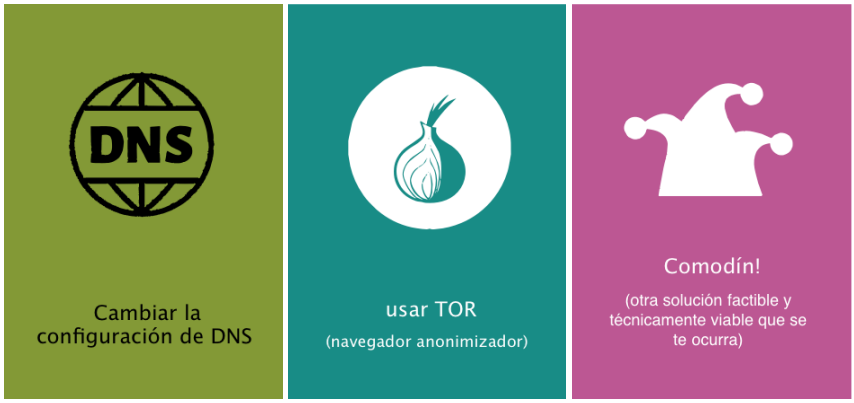
ESCENARIO 5: FILTRADO DE DNS (TAMBIÉN LLAMADO SECUESTRO, ENVENENAMIENTO O SUPLANTACIÓN DE DNS)

Dificultad: Media.

Descripción del escenario: El gobierno ha ordenado a todos los proveedores de servicios de internet nacionales que cambien la resolución DNS de un dominio desde el que se podría haber accedido a un sitio web de protesta. Cuando se intenta acceder al sitio, se redirige a un sitio falso gestionado por el gobierno.

Qué bloquear: Todos los iconos DNS nacionales.

Cartas que se pueden jugar



Comodín:

– Obtener la dirección IP del sitio preguntando a un/a amigo/a en el extranjero o utilizar una herramienta en línea para resolverlo; a continuación, utilizar directamente la dirección IP.

Cosas que hay que explicar

Repasa cómo funciona un DNS.

Ten en cuenta que, al utilizar una VPN, la mayoría utiliza el DNS configurado en los dispositivos, que suele ser el del proveedor de servicios de internet, por lo que aún puede verse afectado por el filtrado.

Ejemplos del mundo real

Solo es eficaz cuando el gobierno controla completamente la infraestructura de la red. Es bastante fácil de demostrar y eludir. Se ha utilizado para bloquear el acceso a motores de búsqueda, sitios específicos y redes sociales y sitios web de videos concretos.

ESCENARIO 6: VPN PROHIBIDA

Dificultad: Alta.

Descripción del escenario: El gobierno ha dicho que castigará a cualquiera que pueda demostrar que utiliza una VPN... pero quieres utilizar una VPN para conectarte a un sitio web específico.

¿Cómo te aseguras de que no te descubran?

Qué bloquear: No se representa

Cartas que se pueden jugar

Quizás

Comodín:

- Tor puede utilizarse con *bridges* (puentes) como alternativa a la VPN o para acceder a la VPN.

Cosas que hay que explicar

Explica cómo un punto de acceso Wi-Fi público comparte la dirección IP y no es posible identificar dispositivos/personas.

Las tarjetas SIM extranjeras pueden funcionar, dependiendo de si el país tiene o no la posibilidad de relacionar un número de teléfono móvil con un dispositivo físico o un ciudadano.

Ejemplos del mundo real

Bielorrusia, China, Egipto, Irán, Irak, Corea del Norte, Omán, Rusia, Siria, Turquía, Turkmenistán, Uganda, Emiratos Árabes Unidos.

ESCENARIO 7: GEOLOCALIZACIÓN

Dificultad: Fácil.

Descripción del escenario: En tu región, el gobierno te impide descargar ciertas aplicaciones (como plataformas de redes sociales o Telegram) y bloquea direcciones IP específicas asociadas con VPN conocidas.

¿Cómo puedes descargar y utilizar estas aplicaciones de todos modos?

Qué bloquear: No se representa

Cartas que se pueden jugar

Comodín:

- Otro servicio VPN
- Herramientas de descarga de otros sitios (proxies)
- Cambiar su ubicación física.

Ejemplos del mundo real

Varios países han bloqueado el acceso a aplicaciones específicas, como las de redes sociales y comunicación, para que no se puedan descargar e instalar desde fuentes normales.

ESCENARIO 8: INTERFERENCIA EN TELÉFONOS CELULARES (*JAMMING*)

Dificultad: Alta.

Descripción del escenario: Estás en una protesta junto con tus amigos/as. Estás utilizando la red de telefonía celular (móvil). Tienes buena recepción en tu teléfono celular pero no puedes enviar ni recibir mensajes. Sospechas que la red está bloqueada. ¿Qué puedes utilizar para mantenerte conectado/a con tus compañeros/as manifestantes?

Qué bloquear: Las antenas de telefonía celular.

Cartas que se pueden jugar

(en la zona, no en el teléfono celular)

(si no estás conectado a la red de telefonía celular)

Comodín:

- Cambiar de ubicación: los dispositivos de interferencia cubren un área limitada
- Si utilizas Wi-Fi, cambiar la frecuencia Wi-Fi, por ejemplo, a la banda de 5 GHz
- Configurar soluciones alternativas entre pares.

Cosas que hay que explicar

El bloqueo podría afectar a la conexión Wi-Fi, Bluetooth, GPS, comunicaciones por radio o servicio celular (bloquea las llamadas telefónicas, los SMS y el acceso a datos móviles) de todas las personas usuarias.

Explica las limitaciones de la solución.

Ejemplos del mundo real

Suele aplicarse en grandes concentraciones de personas, como festivales o protestas. Los dispositivos de interferencia cubren un área muy limitada.

ESCENARIO 9: APAGÓN LOCALIZADO

Dificultad: Media.

Descripción del escenario: Debido a las protestas, el gobierno no quiere que la ciudadanía de su región se conecte a internet. Se dice que cuando los paquetes de datos con sus direcciones IP llegan a los IXP gestionados por el gobierno, los paquetes se descartan. ¿Qué puedes hacer?

Qué bloquear: IXP.

Cartas que se pueden jugar

(en la zona, no en el celular) *(si no estás conectado a la red de celular)*

Comodín:

– ¿

Cosas que hay que explicar

La forma de implementar estos cierres localizados de la conectividad móvil o fija es mediante cambios/filtros en la configuración de la red de telecomunicaciones. Estos cambios pueden desactivar eficazmente los servicios de telecomunicaciones sin tener que apagar o dañar físicamente la infraestructura subyacente y pueden impedir el enrutamiento del tráfico de internet hacia o desde un cierto proveedor de red local.

Ejemplos del mundo real

Se utiliza para bloquear el acceso desde determinadas regiones y comunidades, especialmente territorios controlados, campos de personas refugiadas o zonas de guerra.

ESCENARIO 10: SOLO LOS VIP PUEDEN CONECTARSE

Dificultad: Fácil.

Descripción del escenario: Cuando envías información a través de internet, parece que se bloquea ¡no puedes acceder a ningún servidor! Sin embargo, tu vecina y mejor amiga, que trabaja en el gobierno, te dice que ella puede acceder a todos los recursos sin problemas. Ambas personas tienen conexión al mismo proveedor de servicios de internet.

Qué bloquear: Localizar a la persona jugadora en una determinada red de banda ancha y bloquear todas las conexiones excepto una.

Cartas que se pueden jugar

(puede funcionar si el filtrado lo realizan solo algunos proveedores de servicios de internet)

Comodín:

- Conectarse a la red Wi-Fi de tus vecinos
- Conectarse a otro proveedor de servicios de internet
- Cambiar de ubicación.

Cosas que hay que explicar

Este tipo de filtrado se consigue cambiando las rutas BGP (*Border Gateway Protocol*) o las reglas de enrutamiento interno del proveedor de servicios de internet. Son poco frecuentes, ya que las rutas BGP pueden consultarse públicamente, por lo que estos bloqueos son fáciles de detectar y rastrear hasta los proveedores de servicios individuales (y también es fácil atacar las direcciones VIP).

La diferencia con otros escenarios de filtrado es que este tipo de filtrado comprueba las direcciones IP del origen (remitente) del paquete de datos.

Ejemplos del mundo real

Requiere un amplio control de la infraestructura por parte del gobierno. Algunos lo utilizan para permitir que solo los/as funcionarios/as del gobierno se conecten, mientras que el resto de la población no puede hacer nada.

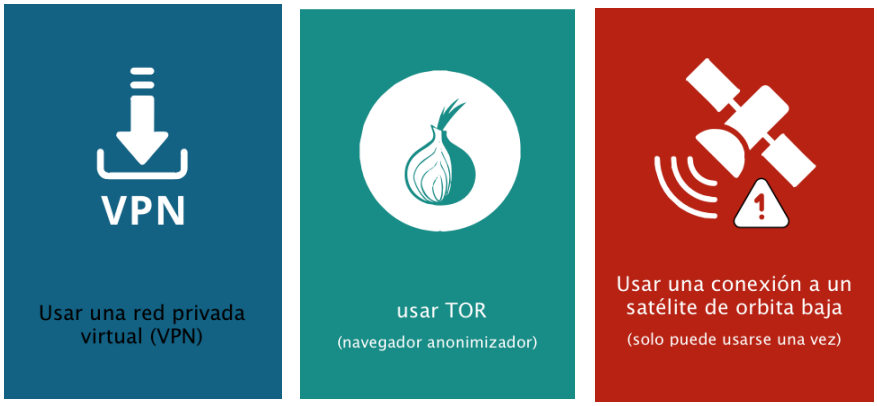
ESCENARIO 11: LIMITACIÓN DE INTERNET (*THROTTLING*)

Dificultad: Alta.

Descripción del escenario: La limitación se define como «restringir artificialmente, pero sin detener, el flujo de datos a través de una red de comunicaciones». En este escenario, tu acceso a internet puede parecer disponible pero es extremadamente lento y, en la práctica, inutilizable para el uso y el intercambio de información.

Qué bloquear: Un punto en el que podamos decir que se encuentra la gente involucrada.

Cartas que se pueden jugar



Cualquier carta (puede funcionar, dependiendo de cómo se implemente la limitación).

Comodín:

-¿

Cosas que hay que explicar

La limitación en las redes móviles se puede realizar reduciendo las conexiones 3G y 4G a 2G.

La limitación en redes fijas y a nivel de aplicación se puede lograr mediante el uso de sistemas de gestión del tráfico instalados en la infraestructura de un proveedor de red.

Ejemplos del mundo real

La limitación es difícil de detectar. Estas medidas suelen ser temporales y están relacionadas con acontecimientos como exámenes nacionales o elecciones, protestas, festivales y otras grandes concentraciones de personas.

ESCENARIO 12: ATAQUE CON INFRAESTRUCTURA MALICIOSA

Dificultad: Alta.

Descripción del escenario: Estás en una protesta. Puedes ver «nuevos» puntos de acceso Wi-Fi (o acceso a teléfonos celulares) que el gobierno promueve como un acceso a internet más rápido y con una señal mucho más fuerte. Los puntos de conexión son sospechosos y parecen conducir a sitios controlados por el gobierno.

Cómo mostrarlo en el mapa: Coloca un nuevo punto de acceso Wi-Fi en otro color.

Cartas que se pueden jugar

(no controlada)

Comodín:

- Si se intercepta la conexión Wi-Fi, una conexión por cable (Ethernet) es una alternativa
- En los teléfonos celulares, seleccionar manualmente la red de acceso.

Ejemplos del mundo real

Es costoso de instalar y normalmente se limita a un evento (por ejemplo, una gran reunión) o una zona (por ejemplo, un campo de personas refugiadas).

ESCENARIO 13: INSPECCIÓN PROFUNDA DE PAQUETES (DPI, TAMBIÉN CONOCIDA COMO *SNIFFING*)

Dificultad: Alta.

Descripción del escenario: Realizas una búsqueda de ciertas palabras clave políticamente controvertidas en tu motor de búsqueda favorito y la búsqueda falla. Pero estás seguro/a de que debería arrojar resultados válidos. ¡Es un tema tan importante!

También estás seguro/a de que la conectividad a internet se ha vuelto más lenta en promedio durante los últimos meses…

Qué bloquear: Símbolos de filtrado en todos los ISP.

Cartas que se pueden jugar

Comodín:

- ¡Cifrar el tráfico!
- Las VPN comunes probablemente serán bien conocidas y, por lo tanto, bloqueadas. Utilizar VPN menos conocidas
- El tráfico https podría abrirse (filtrado SNI) y descifrarse. Existen herramientas para evitarlo, como GoodbyeDPI DPITunnel, Zapret y Geneva

Cosas que hay que explicar

Esta es la forma más sofisticada de control del tráfico de datos, utilizada actualmente por algunos gobiernos. Requiere la capacidad de imponer la instalación de hardware y software en todos los ISP.

Para permitir que los datos viajen a través de su red, los dispositivos de enrutamiento inspeccionan la información del encabezado del paquete, como la dirección de destino, la dirección de origen y el número de puerto. El DPI examina una gama más amplia de metadatos, incluyendo el encabezado y los datos en si que transporta el paquete.

Cuando se implementa el DPI, un dispositivo examina el contenido de todos los paquetes de datos utilizando reglas predefinidas que incluyen qué hacer con el contenido específico que pueda encontrar. Por lo tanto, puede utilizarse para ejercer una variedad de bloqueos, dependiendo de cómo se configure. Por lo tanto, las herramientas de elusión deben adaptarse a las políticas de DPI que se implementen.

Ejemplos del mundo real

Se utiliza en el Gran Cortafuegos de China, conocido oficialmente como Escudo Dorado, a nivel de la puerta de enlace nacional.

ANEXO 3: ENLACES Y RECURSOS COMENTADOS

- **Cortes de internet y derechos humanos** (2024) por APC y Derechos Digitales https://www.apc.org/en/pubs/internet-shutdowns-and-human-rights ofrece una muy buena introducción al uso de los cortes y sus repercusiones en los derechos humanos, así como ejemplos de bloqueos en todo el mundo, muchos de los cuales han inspirado nuestros escenarios.

- Una exploración interdisciplinaria de los cortes de Internet (2022) por Open Technology Fund https://www.opentech.fund/news/an-interdisciplinary-exploration-of-internet-shutdowns/ (seleccionar el idioma) clasifica los diferentes tipos de cierre. Solía tener un buen panel de control de cierres que ahora parece estar fuera de línea.

- **Resumen de políticas: Interrupciones de Internet** (2019) por ISOC https://www.internetsociety.org/es/policybriefs/internet-shutdowns/ ofrece una buena introducción general al tema.

- En 2016, Access Now encabezó la creación de la **coalición #KeepItOn** https://www.accessnow.org/keepiton/, una alianza de más de 300 grupos que recopilan y comparten información sobre los cierres y prestan asistencia a las personas afectadas por ellos. El sitio web de la campaña #KeepItOn de Access Now contiene estadísticas, datos útiles y recursos relevantes, incluida una **taxonomía de los cierres** https://www.accessnow.org/publication/internet-shutdown-types/ que explica las estrategias de mitigación y otros **recursos de la campaña** https://www.accessnow.org/keepiton/#resources

- **The Real Impact of Internet Shutdowns** (2023) de ISOC https://www.internetsociety.org/blog/2023/06/the-real-impact-of-internet-shutdowns/ mide el impacto económico de los bloqueos.

- **OONI** https://ooni.org/ Observatorio Abierto de Interferencias en la Red, una comunidad global que mide la censura en internet desde 2012.

- **Technical multi-stakeholder report on Internet shutdowns: The case of Iran amid autumn 2022 protests** (2022) por OONI e ISOC https://ooni.org/post/2022-iran-technical-multistakeholder-report/

- **Cortes de internet en Paraguay** (2023) por TEDIC https://www.tedic.org/wp-content/uploads/2023/07/Internet-Shutdowns-Report-2023.pdf

- **Anatomy of virtual curfews** (2017) por Digital Empowerment Foundation https://www.apc.org/sites/default/files/Anatomy_of_Virtual_Curfews.pdf se centra en ejemplos de la India y otros países del sur de Asia.

- Sobre constelaciones de satélites y sostenibilidad. https://manypossibilities.net/2023/11/star-link-and-inequality/

- Sobre los satélites de órbita baja para el acceso a internet. https://www.internetsociety.org/resources/doc/2022/perspectives-on-leo-satellites/

ANEXO 4: HERRAMIENTAS Y ENLACES PARA ELUDIR RESTRICCIONES

Quienes han participado nos han pedido que compartamos enlaces que les ayuden a implementar algunas de las técnicas de elusión que se utilizan en el juego. A continuación, se incluyen algunos recursos útiles.

- Cambia tu configuración de DNS para utilizar DNS públicos (instrucciones para Windows, Mac, Linux y Android): https://proprivacy.com/guides/how-to-change-your-dns-settings-a-complete-guide
- Navegador Ceno: https://censorship.no/en/about.html Un navegador móvil para eludir la censura.
- Hermes: https://www.rhizomatica.org/hermes/ Un sistema de telecomunicaciones digitales asequible a través de radio de onda corta/HF.
- Proyecto Briar: https://briarproject.org/ Una herramienta para mensajería cifrada entre pares y foros.
- Bridgefly https://bridgefy.me/ Un sistema de mensajería sin conexión para teléfonos Android.
- Tipos de VPN y cómo instalar una VPN:
    - Por qué podría interesarle una VPN: Guía de Riseup: https://riseup.net/en/vpn/why-is-needed
    - Obtenga la VPN de Riseup: https://riseup.net/en/vpn
    - Una guía detallada y técnica de Freedom of Press Foundation: https://freedom.press/training/choosing-a-vpn/
- Sitio web del proyecto Tor: https://www.torproject.org/
- Oui sync: Intercambio de archivos seguro, de código abierto y entre pares. https://ouisync.net/
- Aidrop: https://en.wikipedia.org/wiki/AirDrop Software propietario para conectar dispositivos Apple directamente.
- GoodByeDPI: Cuenta con varios mecanismos para eludir los bloqueos DPI. https://github.com/ValdikSS/GoodbyeDPI
- Aunque (todavía) no se utiliza para el juego, Tor Bridges son repetidores que ayudan a eludir la censura. Para más información, visita https://bridges.torproject.org/

CRÉDITOS Y AGRADECIMIENTOS

En el diseño de este juego y sus materiales asociados se han utilizado varios íconos e ilustraciones creados por terceros, todos ellos distribuidos bajo una licencia CC-BY-3.0-DEED. A continuación se incluye la lista de créditos:

Satellite por Creative Stall
shut down por P Thanga Vignesh
wifi por Richa
Radio tower por iconcheese
Satellite por SAADI ALA
Cable por IconMark
Building por iconsphere
Router por vectorstall
Laptop por Vectors Market
Cloud por cakslankers
water water by Manohara
server por Dika Neto
internet por RROOK
distributed network por Bruno Castro
Satellite dish por Meko
Satellite dish por AbtoCreative

Gracias al staff, los miembros y socios de APC que aportaron sus comentarios a este proyecto, así como a todos los/as participantes en línea y presenciales, y a Gaba y Jim (Proyecto Tor).


APC
ASOCIACIÓN PARA
EL PROGRESO DE
LAS COMUNICACIONES