

2. SECURIZACIÓN DEL ENTORNO ANTE LAS INVESTIGACIONES

Uno de los aspectos imprescindibles en una investigación es la securización del entorno de trabajo junto con las operaciones en curso. La importancia de esto radica en que debemos proteger todos los recursos y activos que vayamos a utilizar en la investigación para no dar pistas a nuestro objetivo de que le estamos investigando. A lo largo del presente tema veremos cómo podemos generar unas buenas prácticas aplicando OPSEC, anonimizando las conexiones hacia el exterior y protegiendo nuestra privacidad y huella digital entre otras cosas.

2.1. OPSEC

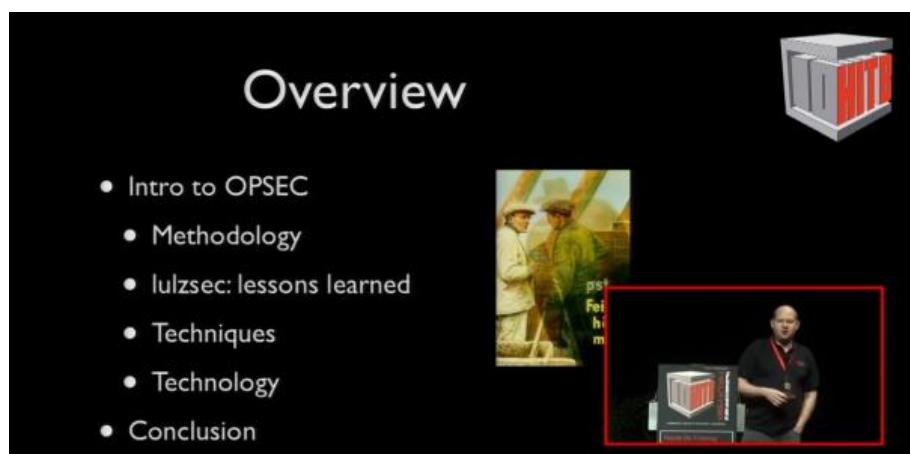
La abreviatura de OPSEC proviene de **OPerations SECurity** o lo que es lo mismo securización de las operaciones. OPSEC es un proceso que trata de identificar la información crítica (en este caso nuestra y/o de nuestra empresa) que se posee para poder tomar las medidas necesarias para eliminar o reducir el riesgo asociado.

Este término proviene del ámbito militar teniendo como objetivo asegurar que las operaciones en curso no se vean comprometidas por fallos de seguridad, sean estos humanos y/o digitales, y protegerse frente a posibles ataques que un adversario pueda realizar para obtener información confidencial y utilizarla en su beneficio. En la actualidad, tal concepto es empleado tanto por empresas como por individuos.

Al final OPSEC no deja de ser una metodología que puede ser empleada para negar al adversario el conocimiento de nuestras capacidades e intenciones con el único fin de identificar, controlar y proteger la información crítica asociada a la planificación y ejecución de nuestras operaciones.

Si interesa este tema enfocándolo desde una perspectiva práctica tenéis una ponencia de **GRUQQ** en la edición del 2012 del **congreso Hack In The Box Security** donde bajo el

título “**OPSEC: Because Jail is for wuftpd**” explica diferentes técnicas OPSEC con el objetivo de ganar anonimato en las investigaciones. Es cierto que la ponencia va dirigida a potenciar y dar las herramientas necesarias para que los hacktivistas puedan protegerse pero las podemos extrapolar al lado del bien ya que nos encontramos ante las mismas técnicas. En el Vídeo 2 puede visualizarse la ponencia.



Video 2. Ponencia de GRUQQ sobre [OPSEC: Because Jail is for wuftpd](#)

2.1.1. CICLO OPSEC

OPSEC dispone de una metodología que sigue de manera secuencial una serie de fases, donde como primer punto de partida será identificar la información crítica y como resultado final será necesario aplicarle una serie de contramedidas para reducir el posible riesgo asociado. Está compuesto de 5 fases siendo las que pueden apreciarse en la Imagen 8.



Imagen 8. Ciclo OPSEC

A continuación, se resume cada una de las fases:

- **Fase 1 - Identificar información crítica.** Detectar que información pudiera ser de importancia para protegerla frente a cibercriminales. Hay que pensar como un adversario y determinar qué información se necesitaría para atacar a una persona u organización. Hay que plantearse una serie de preguntas a responder, relacionadas con la obtención de información crítica. Estas preguntas se conocen como elementos esenciales de información, donde las respuestas a dichas preguntas serán la lista de información crítica.

Sobre un individuo podríamos plantearnos la siguiente lista de preguntas:

- ¿Cuál es el nombre completo de la persona?
- ¿Existen fotos que permitan identificar al objetivo o a su entorno?
- ¿Conocemos en qué empresa trabaja el objetivo? ¿Sabemos qué rutas suele utilizar para ir a trabajar?
- ¿Cuál es la dirección habitual del objetivo?
- ¿Sabemos la fecha de nacimiento del objetivo?

- ¿Disponemos del número de cuenta bancaria y/o tarjeta de crédito del objetivo? ¿Con qué banco tiene una cuenta?
 - ¿Qué números de teléfonos tiene registrado a su nombre el objetivo?
 - ¿Qué conocimientos tiene sobre ciberseguridad?
 - ¿El objetivo tiene alguna afiliación política?
 - ¿Qué hobbies y gustos tiene el objetivo?
-
- **Fase 2 - Análisis de amenazas.** La amenaza, en términos de OPSEC, es aquella debilidad que el adversario puede llegar a explotar para obtener información crítica. Esta fase utiliza la Inteligencia y Contrainteligencia para responder a una serie de preguntas clave sobre el adversario:
 - ¿Quién es? (competidores, criminales, mafia, terroristas, hacktivistas, etc)
 - ¿Qué motivaciones tiene? (Hacktivismo, ciberespionaje, política, cibercrimen, ciberterrorismo, diversión, etc)
 - ¿Qué objetivos persigue?
 - ¿Cuál es la línea de acción utilizada? (OCOA – Opponent Course of Action)
 - ¿Qué información dispone?
 - ¿Qué capacidades tiene?
 - **Fase 3 - Análisis de vulnerabilidades.** Se buscan los puntos débiles del objetivo, ya sea una organización o un individuo. Para identificar las vulnerabilidades hay que plantearse las siguientes preguntas asociadas a las amenazas detectadas en la fase anterior:
 - ¿Qué indicadores están asociados a la información crítica?
 - ¿Qué indicadores puede obtener el adversario?
 - ¿Qué indicadores puede llegar a usar el adversario?

Las principales vulnerabilidades de las organizaciones suelen ser:

- Formación inadecuada de los empleados.
- Falta de seguridad en las comunicaciones.
- Sistemas y productos creados sin prestar atención a la seguridad.

- **Fase 4 - Evaluación del riesgo.** En términos OPSEC consiste en determinar el grado de protección deseable y que daño potencial se considera aceptable. Por ello, únicamente se gestionará el riesgo en aquellos activos que podrían afectar a la organización, en caso de verse comprometidos. Para estimar el riesgo puede emplearse la ecuación vista en el [apartado 1.2](#).
- **Fase 5 - Aplicar contramedidas.** Son aquellas acciones que reducen la capacidad de un adversario con el objetivo de explotar vulnerabilidades y procesar información crítica. Las contramedidas son implementadas, en orden de prioridad, con el fin de proteger a la organización o el individuo de esas vulnerabilidades; de este modo, se disminuye el impacto de la amenaza hasta un nivel de umbral aceptable o eliminándola por completo.

Finalmente, las contramedidas tienen por objeto influir o manipular la percepción de los adversarios.

Dentro de OPSEC es recomendable disponer de una serie de medidas o procedimiento de buenas prácticas como podría ser el siguiente:

- **Actitud de seguridad**
 - Ser paranoico y cauteloso de forma proactiva.
 - No confiar en nadie.
 - No contar planes ni detalles de operaciones (tanto en curso como futuribles) con compañeros ajenos a estas.
 - No hablar sobre investigaciones u operaciones en lugares públicos.
- **Gestión de las operaciones**
 - Planificar todas las operaciones e investigaciones con las medidas de seguridad pertinentes.
 - Definir palabras clave para referirnos al objetivo. Dichas palabras no deben tener relación alguna con el propio objetivo. (Por ejemplo pueden usarse nombres de ciudades, animales, ríos, vinos, quesos, etc).

- **Seguridad digital.**

- Protección y almacenamiento seguro de la información. No dejar evidencias que pudieran ser utilizadas en nuestra contra.
- Utilizar entornos controlados y aislados.
- Creación de diferentes avatares para cada investigación.
- Anonimizar las comunicaciones, por medio de VPNs y/o Tor, para ganar privacidad.
- Cifrado de la información.

2.1.2. FALLOS DE OPSEC CONOCIDOS

Hasta ahora hemos visto cómo protegernos, pero tenemos que conocer también cuales son los principales errores o fallos debido a una mala implementación de OPSEC en las investigaciones o por carecer de ella.

A lo largo del tiempo se han producido diferentes tipos de fallos relacionados con OPSEC siendo alguno de ellos los siguientes:

- Exposición de las operaciones de ITG18, un actor criminal iraní, dentro de un servidor con un total de 40 GB de datos analizados por la unidad de Inteligencia de IBM. Por medio de la investigación se descubrieron por un lado videos que mostraban como uno de los operadores de ITG18 administraba cuentas y realizaba comprobaciones de acceso y extracción de información de las cuentas comprometidas. Por otro lado, los investigadores detectaron datos relacionados con personas y números de teléfono iranies asociados a operadores de ITG18, entre otros datos. Lo mencionado lo podéis ver en el artículo escrito en el blog (Security Intelligence) de IBM bajo el título "[New Research Exposes Iranian Threat Group Operations](#)".

- Exposición de credenciales de la policía de Los Ángeles presentes en una entrevista con el CNN. Techdirt lo publica en su blog bajo el título "[LAPD Exposes Login To Data Harvesting Software During Interview With CNN](#)"

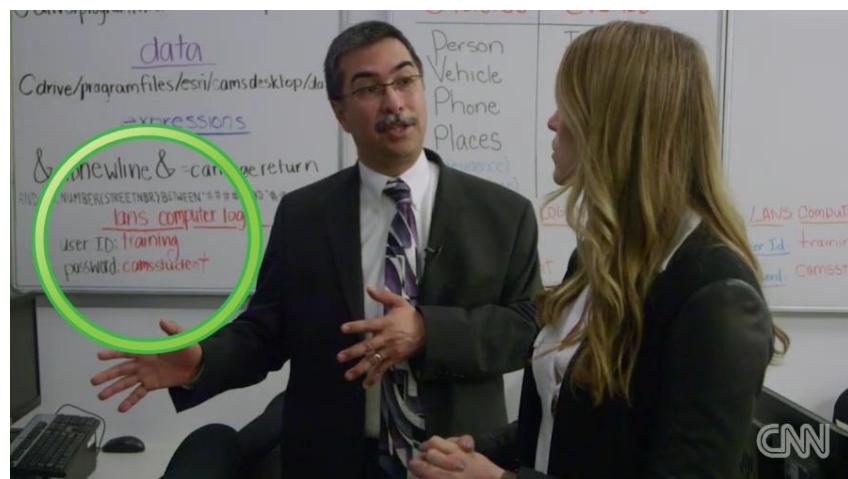


Imagen 9. Credenciales de la policía de Los Ángeles expuestas

- Desanonimización de un traficante de marihuana debido a la huella dactilar presente en una foto compartida en la Dark Web. La información puede consultarse en el blog de Xataka bajo el título "[Un traficante vendía marihuana en la Dark Web de forma anónima: lo identificaron gracias a una foto de sus dedos](#)".

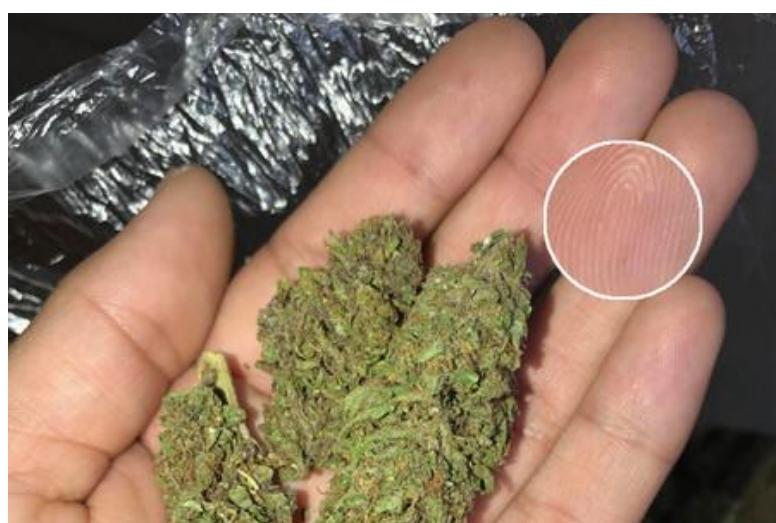


Imagen 10. Desanonimización de un traficante por medio de la huella dactilar extraída de una foto

- Geolocalización de un peligroso delincuente debido a los metadatos de la imagen compartida por su novia. La noticia puede visualizarse en infobae bajo el título "[El FBI atrapó a un peligroso hacker gracias a foto de su novia](#)".

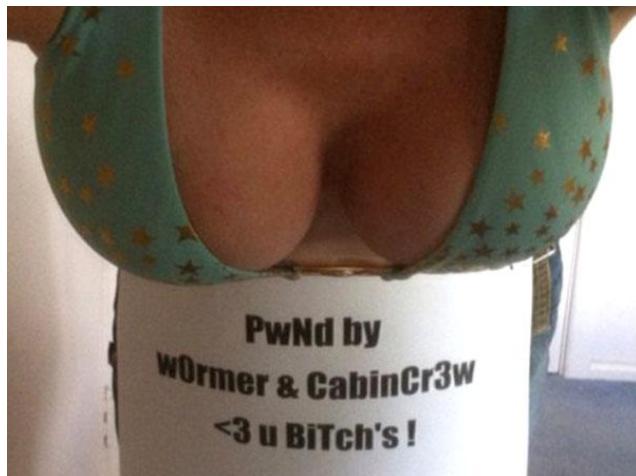


Imagen 11. El FBI atrapo a un delincuente por medio de los metadatos de una foto compartida por su novia

- Geolocalización de los alborotadores que irrumpieron ilegalmente en el Capitolio debido a un ataque a la aplicación de la red social de ultraderecha Parler, red donde los asaltantes compartían los videos grabados en directo durante el asalto. El ataque derivó posteriormente en una exfiltración de estos en diferentes foros de la Dark Web, donde se consiguió extraer coordenadas GPS asociados a los posts de los usuarios. Dicha noticia está disponible en **dailymail** bajo el título "[Where Capitol rioters were when they posted gloating Parler siege videos: Hack of banned right-wing app geo-locates](#)".

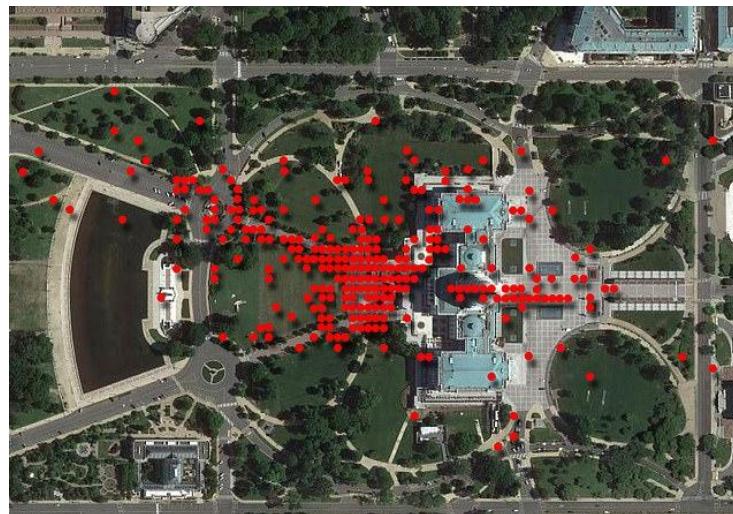


Imagen 12. Mapa de datos GPS de un usuario de Parler superpuesto con el Capitolio

- Geolocalización del lugar donde se realizaron múltiples asesinatos en Etiopía por medio del análisis de verificación de los fotogramas asociados a unos videos compartidos por los asesinos vía Telegram. En dicho análisis efectuaron diferentes triangulaciones por medio de plataformas satelitales y topográficas tomando como referencia diferentes puntos de la zona como por ejemplo la forma que tienen las montañas, la vegetación y puntos similares. La investigación fue desarrollada por analistas de **bellingcat** y puede visualizarse a través del siguiente enlace bajo el título "[Mahbere Dego: Clues to a Clifftop Massacre in Ethiopia](#)".

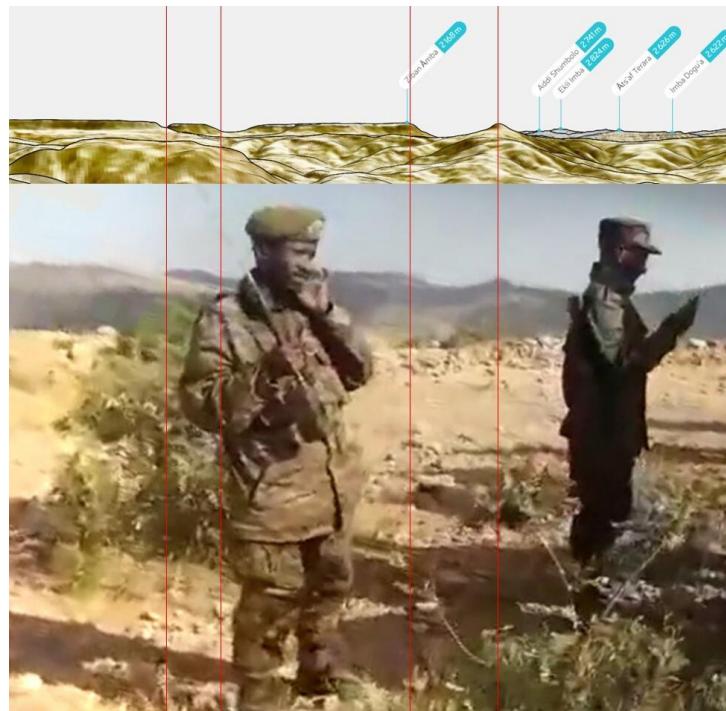


Imagen 13. Coincidencia del análisis de verificación de fotogramas realizado por bellingcat

2.2. ANONIMIZACIÓN Y PRIVACIDAD EN LAS INVESTIGACIONES

La anonimización en las investigaciones es uno de los puntos más importantes de la misma debido a que todo el trabajo que se haga deberá estar protegido en todo momento sin levantar sospechas al objetivo de que está siendo investigado.

Un producto de Inteligencia no servirá de nada si no hemos tenido las precauciones necesarias para proteger las comunicaciones de manera eficiente con un alto grado de anonimato y de privacidad en las propias investigaciones, ya que cualquier descuido o desliz puede tirar por tierra el brillante trabajo que hayamos podido realizar.

Por este motivo es imprescindible contar con un procedimiento que ayude a tener claras cuales son los pasos para blindarnos en la ejecución de las investigaciones. Dichos pasos pueden ser los siguientes:

- Uso de entornos aislados y controlados
- Identificar en todo momento que dirección IP estamos utilizando dentro de las investigaciones
- Utilizar VPNs para proteger los datos con el fin de ganar privacidad en las conexiones establecidas
- Utilizar Tor para proteger al investigador con objetivo de ganar anonimato en las conexiones establecidas
- Securizar los navegadores para bloquear cualquier intento de tracking, malas configuraciones de privacidad de las cuentas o la huella digital que pueda estar compartiendo el navegador sin nuestro conocimiento

2.2.1. ENTORNOS CONTROLADOS

El disponer de un entorno controlado es un punto muy importante cuando nos enfrentarnos a una investigación, ya que es necesario tener una máquina virtual totalmente libre y fuertemente fortificada y protegida frente a posibles fugas de

información durante la investigación de diferentes tipos de recursos online que consultemos. Por este motivo es deseable contar con máquinas virtuales que nos garanticen un nivel de anonimato y privacidad adaptadas a nuestras necesidades operativas.



Imagen 14. Categorización de tipos de entornos controlados para la investigación

En la Imagen 14 pueden verse tres grandes bloques de máquinas virtuales pensadas para realizar investigaciones de cualquier índole, siendo las siguientes:

- **Orientadas a la seguridad.** Este tipo de máquinas virtuales están orientadas a garantizar ese anonimato y privacidad por encima de cualquier otra necesidad. Algunas de las máquinas virtuales a destacar son las siguientes:

- **QUBES OS.** Se trata de un sistema operativo gratuito y open-source orientado a la seguridad en el que mediante el uso de una virtualización basada en Xen² permite la creación y gestión de diferentes compartimentos aislados llamados qubes.

Entre sus principales características destacan:

- Conjunto predefinido de una o varias aplicaciones aisladas (para proyectos personales y/o profesionales).

² **Xen Hipervisor:** Es un proyecto open source que permite ejecutar múltiples instancias de un sistema operativo en paralelo en un único host. Se trata de un hipervisor de tipo 1 o bare-metal que se ejecuta directamente en el hardware del host.

- Disponibilidad de plantillas para la ejecución de múltiples VM (Linux y Windows).
- Diferentes niveles de confianza para la ejecución de cada aplicación en entornos aislados, en función de su nivel de seguridad.

En la Imagen 15 puede verse a nivel general las tres características mencionadas de manera más gráfica. Se dispone de más información en su sitio web: <https://www.qubes-os.org>. Además, cuenta con una guía explicando paso a paso su instalación: <https://www.qubes-os.org/doc/installation-guide/>.

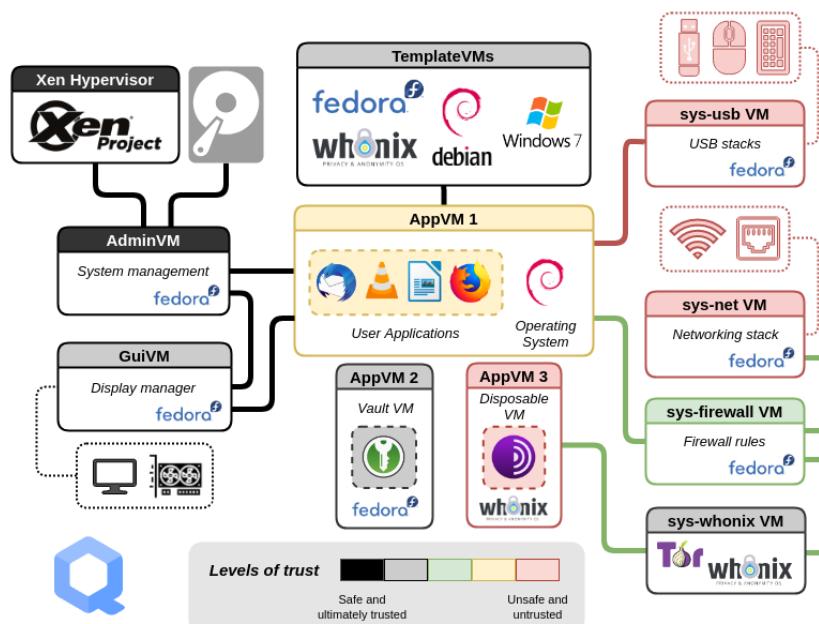


Imagen 15. Principales características de QUBES OS

- **Whonix**. Es un sistema operativo gratuito y open-source pensado en ofrecer una seguridad y privacidad avanzada.

Entre sus principales características destacan:

- Protección Anti-Tracking con el objetivo de proteger la dirección IP real y el tráfico web generado mediante su ocultación a través de

Tor, utilización de Tor Browser para evitar el tracking de la huella digital creada por el navegador web, uso de kloak³ para ganar anonimato con respecto a las pulsaciones de teclas con el teclado y securización de la sincronización de la fecha y hora del equipo mediante sdwdate⁴ y Boot Clock Randomization⁵.

- Basado en Kicksecure. Se trata de una distribución Linux basado en Debian teniendo como objetivo proporcionar un entorno altamente seguro y con diferentes capas de protección frente a posibles ataques. Se dispone de más información en su sitio web: <https://www.kicksecure.com>.
- Principios de seguridad basado en el aislamiento y segmentación de redes
- Dispone de una arquitectura que garantiza una anonimización de conexiones vía Tor. En la imagen 16 puede verse que permite utilizar un Gateway y un Workstation con una red totalmente protegida y aislada que permite realizar peticiones anónimas mediante la red Tor utilizando el sistema Whonix.

³ **Kloak:** Herramienta de anonimización de pulsaciones de teclas. Más información en el sitio web de Whonix: https://www.whonix.org/wiki/Keystroke_Deanonymization#Kloak

⁴ **Sdwdate:** Funcionalidad de Kicksecure. Más información en el sitio web de Kicksecure: <https://www.kicksecure.com/wiki/Sdwdate>.

⁵ **Boot Clock Randomization:** Funcionalidad de Kicksecure. Más información en el sitio web de Kicksecure: https://www.kicksecure.com/wiki/Boot_Clock_Randomization.

Whonix Anonymity Architecture

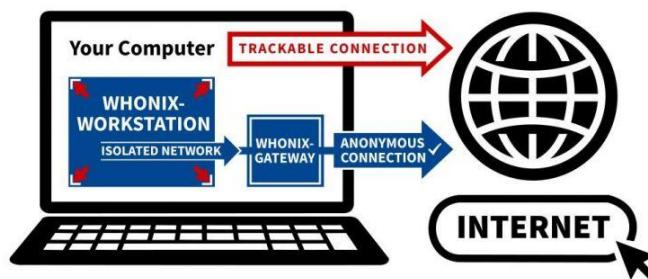


Imagen 16. Arquitectura de anonimato utilizada por Whonix

Se dispone de más información en su sitio web: <https://www.whonix.org>

- **Tails.** Al igual que los otros dos sistemas operativos anteriores, Tails (The Amnesic Incognito Live System) es gratuito y open-source basado en Debian, diseñado para preservar la privacidad y el anonimato. La única diferencia con los anteriores sistemas es que está preparado para ejecutarlo desde un Live CD, o lo que es lo mismo, cargar al vuelo el sistema operativo desde un USB o cualquier otro dispositivo similar sin dejar rastro en el equipo anfitrión.

Entre sus principales características destacan:

- Ejecución del sistema operativo desde memoria y arrancando el mismo siempre desde un Live CD sin dejar rastros de ningún tipo en el equipo.
- Permite disponer de un almacenamiento persistente cifrado de algunos archivos y configuraciones a elegir por el usuario de manera opcional.
- Todas las peticiones que realiza a Internet las anonimiza mediante la red Tor.

Se dispone de más información en su sitio web: <https://tails.boum.org>.

- **Orientadas a OSINT.**

- **Trace Labs.** El equipo de Trace Labs ha creado una máquina virtual específica para OSINT bajo un Kali Linux con un conjunto de herramientas enfocadas a esta disciplina con el objetivo de que facilite las tareas de investigación dentro del [CTF de Search Party](#). Este CTF fue creado en colaboración con la policía de Canadá para encontrar pistas sobre personas desaparecidas en dicho país empleando para ello técnicas OSINT. Se dispone de más información en su sitio web: <https://www.tracelabs.org/initiatives/osint-vm>.

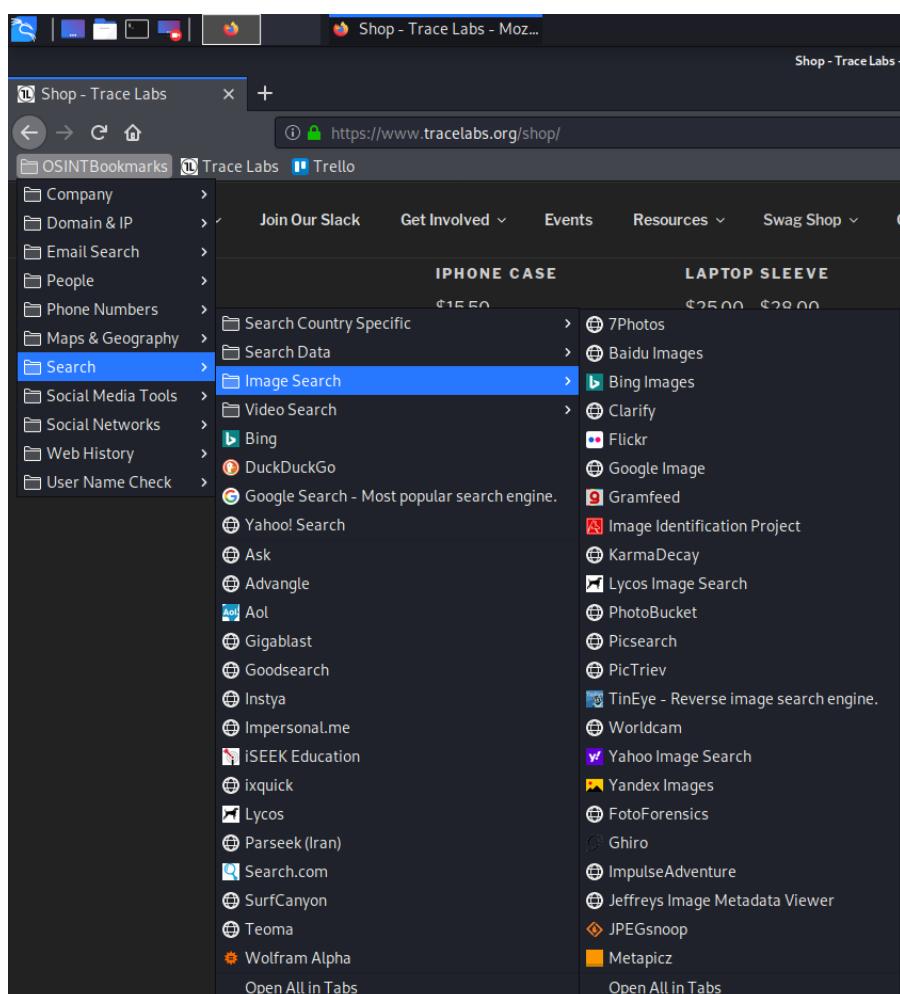


Imagen 17. Máquina virtual de Trace Labs

- **HURON.** Es un sistema operativo bajo Linux preparado con un kit de herramientas destinadas a realizar investigaciones en fuentes abiertas. La máquina virtual fue desarrollada como proyecto final de master y compartida en abierto para su uso.

Alguna de las herramientas que nos podemos encontrar son: Tor Browser, DataSploit, Infoga, Recon-NG, Maltego, Creepy, TheHarvester, TinfoLeak, etc. Se dispone de más información en su sitio web:
<https://huronosint.wordpress.com>.

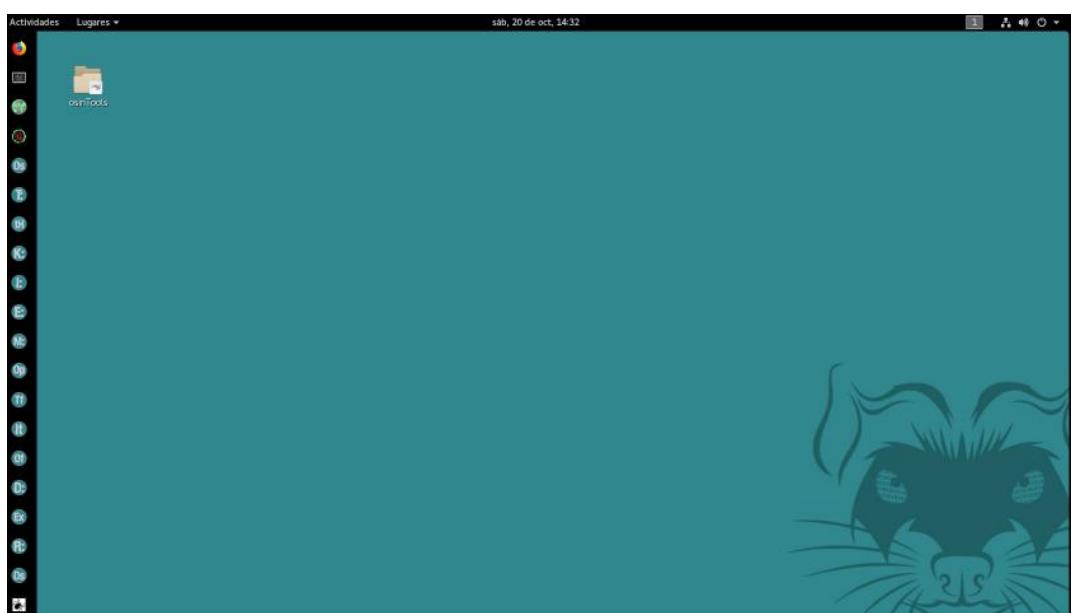


Imagen 18. Escritorio de Huron

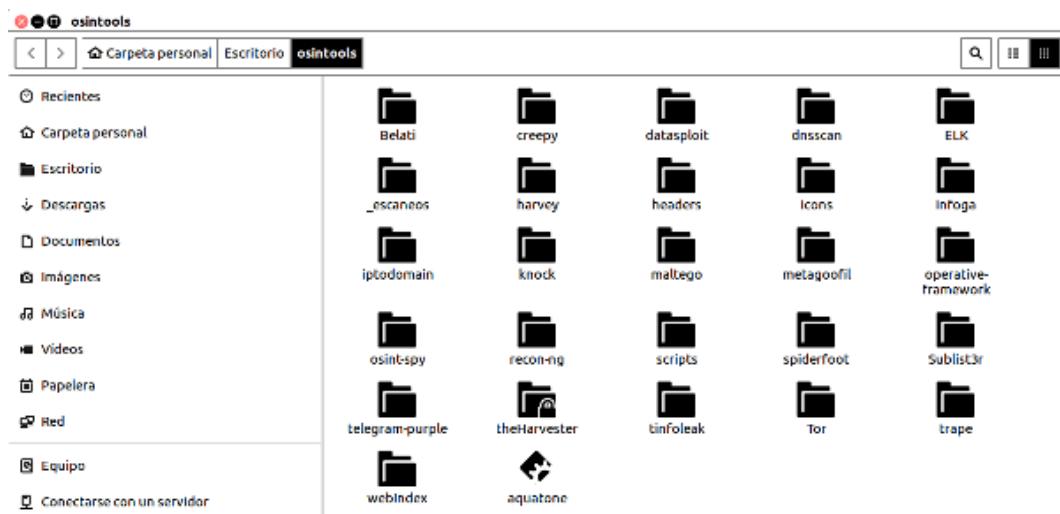


Imagen 19. Listado de herramientas disponibles en Huron

- **OSINTUX.** Al igual que ocurre con Huron se trata de un sistema operativo basado en Linux y orientado a OSINT. Dispone de un inventario de herramientas con una guía de ejecución de cada una de ellas situada en el Escritorio.

Alguna de las herramientas que nos podemos encontrar son: DataSploit, Infoga, Recon-NG, Maltego, Creepy, TheHarvester, Tinfoleak, etc. Se dispone de más información en su sitio web (actualmente en tareas de mantenimiento): <https://www.osintux.org>.



Imagen 20. Escritorio de OSINTUX

- **Sistema Operativo Linux personalizado.** En este caso podemos realizar una instalación limpia de cualquier distribución Linux adecuada a las necesidades que tengamos e instalar en ella nuestro kit de herramientas para la obtención de información y su tratamiento. En el momento que tengamos ya nuestra máquina virtual ya preparada con todo nuestro arsenal, lo ideal sería exportar la misma en una OVA e importarla rápido ante cualquier investigación a la que nos enfrentemos. De esta forma siempre mantendríamos una instalación limpia y sin contaminar con ningún tipo de dato de otras investigaciones.

2.2.2. USO DE VPNs PARA GANAR PRIVACIDAD

La dirección IP pública es un identificador único e irrepetible, con el que nuestro dispositivo accede a Internet. Esta dirección puede ser estática (no varía) o dinámica (cambia cada cierto tiempo).

Usando una analogía con las normas de tráfico, para comprender bien tal concepto, viene a ser la matrícula que ha de llevar nuestro vehículo para que este pueda ser identificado al circular con él por la vía pública.

Al usar una Virtual Private Network (**VPN**) como intermediario entre nuestro equipo y el servidor al que nos conectamos vamos a conseguir que todo el tráfico saliente de nuestro equipo vaya por un túnel cifrado de extremo a extremo hasta llegar al servidor VPN.

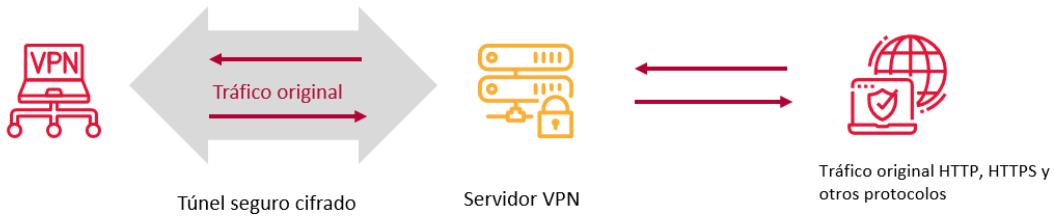


Imagen 21. Funcionamiento de una VPN

Tal como se puede ver en la Imagen 22, el uso de VPN tiene asociado una serie de beneficios, los principales son los siguientes:

- Conseguir una mayor privacidad añadiendo una capa extra de protección sobre la comunicación.
- Disponer de una seguridad adicional que ayude a enmascarar y cifrar la comunicación con el objetivo de que el ISP y el administrador de la red no sepa qué tipo de acciones está realizando por la red ni qué contenido consulta.
- Hacer un bypass de posibles restricciones debido a filtros geográficos que pudiera tener algún país con un régimen férreo sobre el control de las comunicaciones de sus ciudadanos como por ejemplo China, Corea del Norte, etc.

Por contra el uso de VPN también tiene una serie de desventajas, las cuales pueden ser las siguientes:

- Se reduce la velocidad de conexión.
- Tiene un coste en cuanto a precio se refiere, ya que para disfrutar de todas las prestaciones que puede ofrecer su uso, es necesario contratar un servicio de pago. Existen proveedores de servicios gratuitos, pero suelen carecer de cierta fiabilidad o bien que están muy limitada en cuanto a funcionalidades.
- La usabilidad en algunos aspectos puede ser tediosa en el caso de que el usuario no tenga un conocimiento técnico, aunque es cierto que los diferentes proveedores de servicio de este corte van destinando fondos para ir mejorando la propia usabilidad de sus aplicaciones con el objetivo de hacer más intuitivas las mismas.



Imagen 22. Beneficios y desventajas en la utilización de VPNs

De igual modo, hay que tener en cuenta la existencia de alianzas de vigilancia internacional, que promueven el intercambio de información entre agencias de Inteligencia de Señales (SIGINT) de diferentes países. Este es el caso de los **Five Eyes** (5 ojos) en el que cinco países (Estados Unidos, Canadá, Reino Unido, Australia y Nueva Zelanda) crearon una alianza tras la Segunda Guerra Mundial con el objetivo de poder compartir Inteligencia y colaborar entre los países miembros para poder monitorizar y

recopilar datos de sus países en busca de posibles amenazas terroristas u otra índole similar.

Dicha alianza entre los 5 países se oficializó por medio del Acuerdo UKUSA, donde se formalizó la cooperación para la compartición de información referente a Inteligencia de Señales entre los países miembros mencionados anteriormente.

Según ciertos términos del acuerdo, cada uno de los países miembros está obligado a la colaboración y al intercambio de información de todas las comunicaciones asociadas a un interés mutuo y la prohibición expresa de que ninguno de los países pueda utilizar las capacidades de monitorización para eludir las leyes nacionales que rigen la vigilancia.

Muchos años después fueron integrándose nuevos países miembros generando así lo que se conoce como 9 Eyes y 14 Eyes.



Imagen 23. Países miembros de los 5 Eyes, 9 Eyes y 14 Eyes

Por este motivo es bastante importante saber en qué país opera legalmente cada empresa que ofrece este tipo de servicios y si existe alguna alianza entre dicho país y nuestro objetivo. En la [web vpnoveryview](#) ofrecen más información sobre los 14 Eyes y una comparativa de los servicios VPN disponibles en la actualidad que operan fuera del radar

de dichos 14 Eyes (ver Imagen 24) y un listado con el país de origen de todos los servicios VPN conocidos (se puede ver una muestra en la Imagen 25).

En el artículo de dicho sitio web bajo el título “**Best VPN Outside 14 Eyes Countries**” puede consultarse lo comentado: <https://vpnoverview.com/best-vpn/vpn-outside-14-eyes/>.

Feature	NordVPN	ExpressVPN	Surfshark	CyberGhost	Proton VPN
Number of servers	5,000+	3,000+	3,200+	7,900+	1,700+
Number of countries	59	94	100	91	64
Location	Panama	British Virgin Islands	British Virgin Islands	Romania	Switzerland
Protocols	OpenVPN, IKEv2, WireGuard, NordLynx	OpenVPN, IKEv2, WireGuard, Lightway	OpenVPN, IKEv2, WireGuard	OpenVPN, IKEv2, WireGuard	OpenVPN, IKEv2, WireGuard
Price	\$2.99/month	\$6.67/month	\$2.05/month	\$2.03/month	\$3.99/month

Imagen 24. Comparativa de servicios VPN que operan fuera de países pertenecientes a los 14 Eyes

VPN Provider	Country Based	Jurisdiction (Intelligence Alliance)
AirVPN	Italy	14 eyes
Atlas VPN	United States	5 eyes
BolehVPN	Italy	14 eyes
CactusVPN	Canada	5 eyes
Encrypt.me	United States	5 eyes
GOOSE VPN	the Netherlands	9 eyes
HMA VPN	United Kingdom	5 eyes
Hotspot Shield	United States	5 eyes
IPVanish	United States	5 eyes
Mullvad	Sweden	14 eyes
Opera VPN	Norway	9 eyes
Private Internet Access	United States	5 eyes

Imagen 25. Listado de proveedores de VPN con su país de origen y jurisdicción sobre 14 Eyes

Dos de los proveedores de servicios de VPN más utilizados en la actualidad y que están fuera de la jurisdicción de los 14 Eyes son NordVPN y ProtonVPN.

Tal como se puede ver en la Imagen 24, **NordVPN** tiene su sede en **Panamá**, dispone de **59 países de conexión**, tiene más de **5.000 servidores repartidos por el mundo** y utiliza por debajo los protocolos **OpenVPN, IKEv2, WireGuard y NordLynx**. Es compatible con diferentes sistemas operativos y plataformas. **Se trata de una VPN de pago.**

NordVPN cuenta con un plugin para el navegador Firefox para establecer conexiones rápidas sin necesidad de disponer de la aplicación de Escritorio de NordVPN. El plugin se puede instalar desde el siguiente enlace:

<https://addons.mozilla.org/es/firefox/addon/nordvpn-proxy-extension/>.

En la Imagen 26 puede verse el aspecto que tiene la aplicación de Escritorio de NordVPN.
El sitio web oficial de NordVPN es <https://nordvpn.com>.

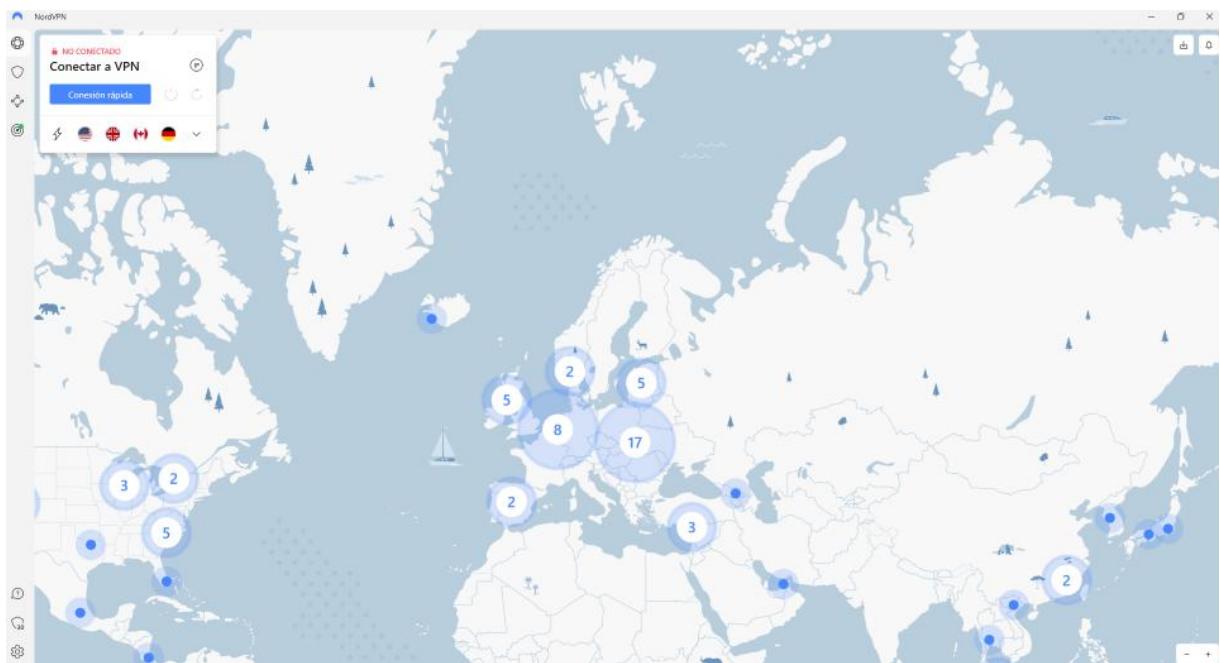


Imagen 26. Aplicación de Escritorio de NordVPN

El otro proveedor de VPN es ProtonVPN, el cual tiene su sede en **Suiza**, dispone de **64 países de conexión**, tiene más de **1.700 servidores repartidos por el mundo** y utiliza por debajo los protocolos **OpenVPN, IKEv2 y WireGuard**. Es compatible con diferentes sistemas operativos y plataformas. Este proveedor VPN es ampliamente conocido debido a su servicio de correo que garantiza una mayor privacidad y seguridad que el resto de los servicios de correo existentes, el cual es ProtonMail.

ProtonVPN dispone de dos modalidades, una gratuita bastante limitada y otra de pago con las máximas prestaciones.

En la Imagen 27 puede verse el aspecto que tiene la aplicación de Escritorio de ProtonVPN.
El sitio web oficial de ProtonVPN es <https://protonvpn.com>.

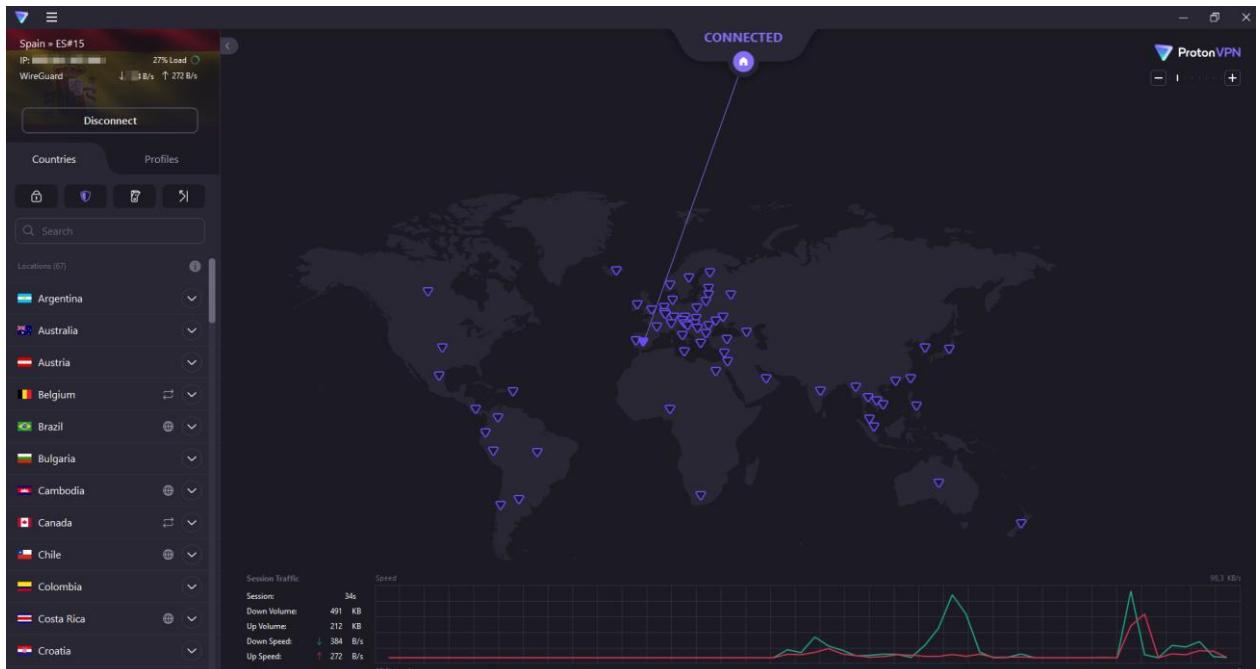


Imagen 27. Aplicación de Escritorio de ProtonVPN

Otro de los proveedores de VPN ampliamente conocido en el mundo de la investigación es Mullvad VPN. Este proveedor se caracteriza debido a que no necesita un correo electrónico para registrarse y solo será necesario contar con un identificador único que ellos mismos te ofrecen de manera automática.

Mullvad VPN tiene su sede en **Suecia** (bajo la jurisdicción de los 14 Eyes), dispone de **39 países de conexión**, tiene más de **410 servidores repartidos por el mundo** y utiliza por debajo los protocolos **OpenVPN** y **WireGuard**.

En la Imagen 28 puede visualizarse el proceso de creación del número de cuenta (como comentaba anteriormente lo genera Mullvad automáticamente), realizar el pago del tiempo deseado para conectarse a la VPN y descarga de la aplicación. Mullvad permite el pago mediante efectivo, bono, criptomonedas (Monero, Bitcoin o Bitcoin Cash), tarjeta de crédito, PayPal, entre otros, tal como puede verse en la Imagen 29.



Imagen 28. Primeros pasos con Mullvad VPN

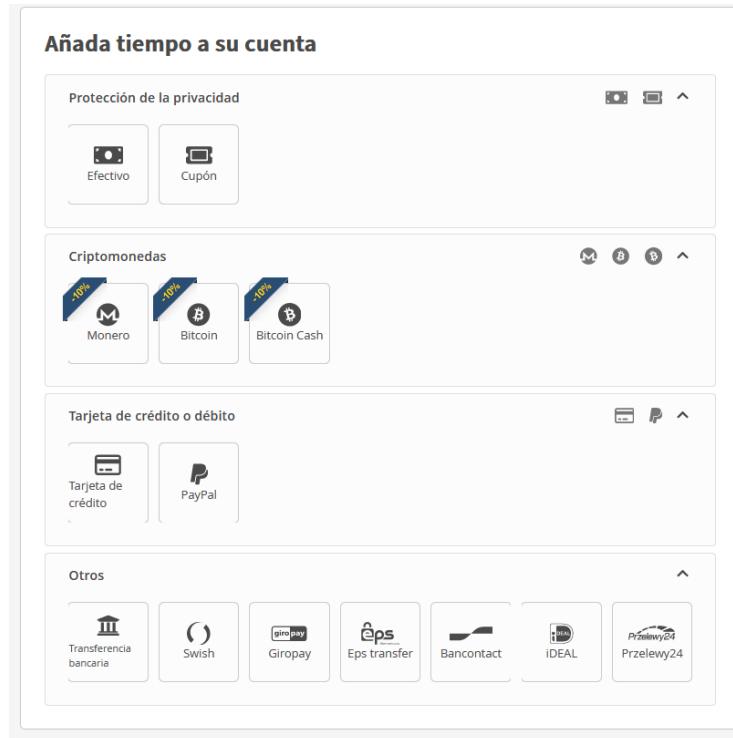


Imagen 29. Métodos de pago de Mullvad VPN

En la Imagen 29 puede verse el sitio web oficial de Mullvad VPN: <https://www.mullvad.net>.



Imagen 30. Sitio web de Mullvad VPN

2.2.3. USO DE TOR PARA GANAR ANONIMATO

The Onion Router (Tor) es una red anónima vinculada al equipo de **Tor Project**, liderado por Roger Dingledine, que se lanzó en el año **2003** con el objetivo de que las personas pudieran ejercer su **derecho a la privacidad** y **navegar libremente por Internet**, sin censura ni restricción alguna.



Tor está formada como una red centralizada compuesta de un conjunto de servidores llamados autoridades de directorio que son los encargados de gestionar la red, su configuración y la creación de un fichero de consenso con toda la información de todos

los nodos de la red. Además, estas autoridades de directorio van creando estadísticas sobre su uso.

En la comunicación se utilizan una serie de nodos aleatorios, conocidos en su conjunto como **circuito virtual**, que generan **distintas capas de cifrado** sobre los paquetes que viajan a través de ellos; de este modo, se enmascara el origen de la petición cuando esta llega al correspondiente destino.

El único protocolo soportado por Tor sin perder el anonimato es **TCP**; en cambio sí son utilizados otros protocolos, la propia comunicación no circulará dentro del circuito virtual, al no soportarlo, produciéndose en este caso una conexión entre el cliente del usuario y el destino de manera directa perdiendo anonimato por el camino.

En la Imagen 31 puede observarse un ejemplo de creación de circuito virtual, el cual generalmente va mutando cada 10 minutos aproximadamente en un circuito nuevo. Este circuito siempre va a contar con tres tipos de nodos siendo los siguientes:

- **Nodo de entrada.** Es el punto de entrada a la red Tor mediante una comunicación cifrada. Con este nodo hay que tener especial cuidado cuando nos conectamos porque conocerá desde qué dirección IP nos estamos conectando.
- **Nodo intermedio.** Su objetivo es recibir el tráfico del nodo de entrada y retransmitirlo al nodo de salida mediante una comunicación cifrada.
- **Nodo de salida.** Es el último nodo del circuito y el encargado de transmitir toda la comunicación al destino. Con este nodo deberemos tener especial cuidado porque el tráfico entre el nodo de salida y el destino a donde queremos acceder no estará cifrado.

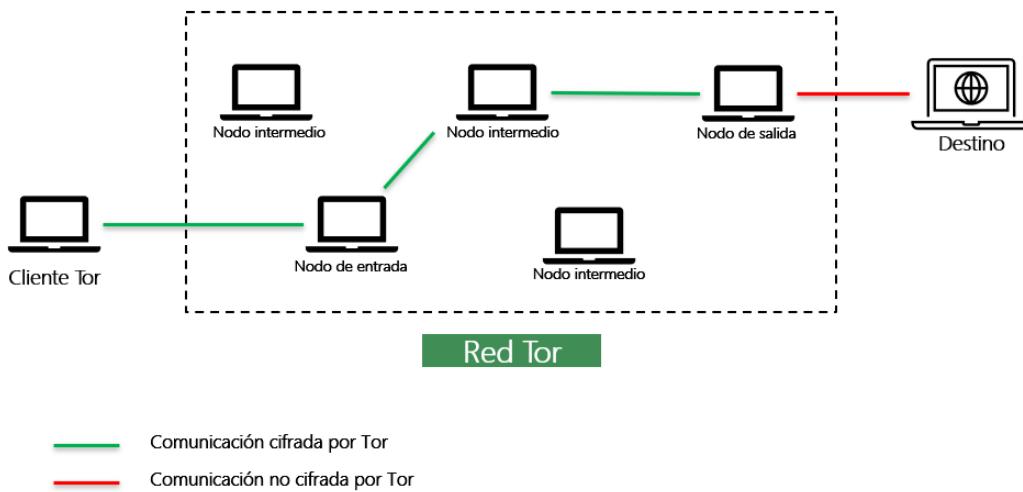


Imagen 31. Creación del circuito virtual desde el cliente hasta el destino

Tenemos disponible un sitio web donde podemos consultar información referente a los nodos mencionados anteriormente, además de descargar el contenido en formato CSV para un mejor análisis. Dicho sitio web se llama Tor Status (<https://torstatus.rueckgr.at>).

En la Imagen 32 se puede ver el tipo de datos que podemos obtener sobre cada nodo: nombre, ancho de banda, días activo, dirección IP, puerto, etc. Además, disponemos de estadísticas a nivel general de todos los nodos que forman parte de la red Tor.

Router Name	Bandwidth	Uptime	Hostname	ORPort	DirPort
00000f00x	4077	14 d 11 h	88.218.226.91 [88.218.226.91]	9001	None
0001	6972	6 d 6 h	91.92.109.43 [91.92.109.43]	443	None
017700000001	12598	7 d 20 h	82.77.176.77 [82.77.176.77]	443	None
084f9fa25relay	23990	16 d 14 h	105.125.169.177 [105.125.169.177]	443	None
084f9fa25relay2	26005	63 d 12 h	v202022171787821916.powerserv.de [105.232.70.209]	443	None
0x0	3913	84 d 11 h	tor.0x0.in [105.133.210.207]	9001	None
0x1e57deadbeef	10182	60 d 21 h	tor-exit-node.Test7deadbeef.de [108.68.45.180]	9001	None
0xd3d01	14731	1 d 0 h	mn.0x3d.lu [145.239.206.31]	9001	None
0xd3d02	14731	1 d 0 h	mn.0x3d.lu [145.239.206.31]	8001	None
0x42FF	6069	28 d 18 h	ghostshell.substack.gr.org [188.40.166.29]	9001	None
0x67726579	12108	26 d 0 h	netcup.grey.pe [89.58.60.200]	9001	None
0x766c6164	9802	1 d 23 h	5.12.75-240.residential.ridernet.rs [5.12.75.240]	9162	None
0x766c6164	16772	1 d 20 h	5.12.75-240.residential.ridernet.rs [5.12.75.240]	9161	None
0x90	184916	64 d 2 h	static.108.98.9.176.clients.your-server.de [176.9.98.108]	9001	None
0xcccc	24698	64 d 12 h	nobody.yourserver.net [105.181.159.40]	9001	None
0xdeadbeef	21277	1 d 16 h	vps-0f62c2fc.vpn.ovh.net [151.80.148.159]	443	None
0xdeadbeef	184575	15 d 7 h	static.20.72.216.95.clients.your-server.de [96.216.72.20]	9001	None
0xdeadbeef	1207	1 d 16 h	v76282.tku.de [178.254.40.9]	9001	None
0xdeadbeef	42372	64 d 3 h	mail.my-mst.rocks [45.136.31.178]	9001	None
0xdeadbeef	4498	87 d 0 h	mail.0xdeadbeef.club [37.187.96.183]	443	None

Imagen 32. Sitio web de Tor Status

En la Imagen 33 puede verse el total de nodos disponibles, número de nodos de entrada y de salida, nodos más rápidos, etc.

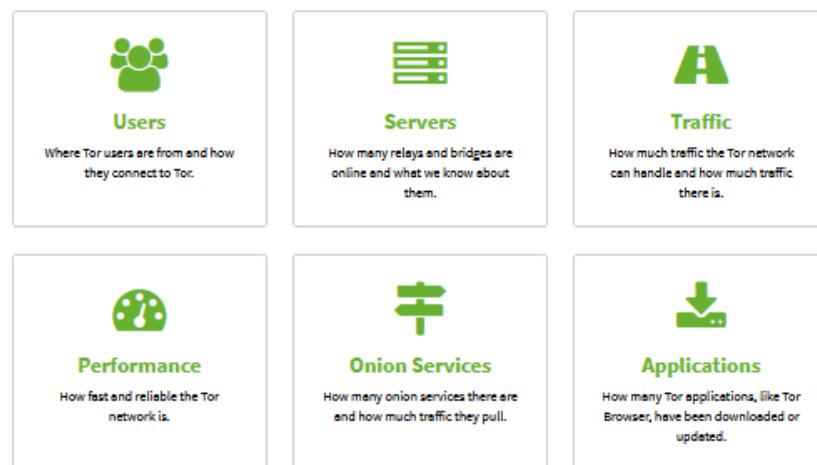
Aggregate Network Statistic Summary Graphs / Details		
Total Number of Routers:	6537	100%
Routers in Current Query Result Set:	6537	100%
Total Number of 'Authority' Routers:	9	0.14%
Total Number of 'Bad Directory' Routers:	0	0%
Total Number of 'Bad Exit' Routers:	57	0.87%
Total Number of 'Exit' Routers:	1767	27.03%
Total Number of 'Fast' Routers:	6097	93.27%
Total Number of 'Guard' Routers:	3602	55.1%
Total Number of 'Hibernating' Routers:	0	0%
Total Number of 'Named' Routers:	0	0%
Total Number of 'Stable' Routers:	5820	89.03%
Total Number of 'Running' Routers:	6537	100%
Total Number of 'Valid' Routers:	6537	100%
Total Number of 'V2Dir' Routers:	5608	85.79%
Total Number of 'HSDir' Routers:	3776	57.76%
Total Number of 'Directory Mirror' Routers:	325	4.97%

Imagen 33. Tabla de estadísticas de los nodos de la red Tor

Dentro del sitio web de Tor Project tenemos una sección de métricas oficiales desde la infraestructura del propio proyecto, siendo el siguiente: <https://metrics.torproject.org/>. Tal como se puede ver en la Imagen 34 podemos visualizar diferentes bloques de datos con los que podemos aplicar diferentes tipos de filtrados, como por ejemplo obtención del número de usuarios que se conectan desde España a Tor (ver Imagen 35).

Analysis

View visualizations of statistics collected from the public Tor network and from Tor Project infrastructure.



Services

Perform interactive queries for more detailed information relating to relays or bridges in the public Tor network.

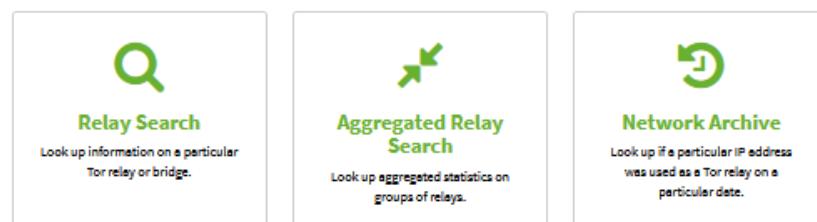


Imagen 34. Opciones de filtrado por diferentes métricas oficiales de Tor Project

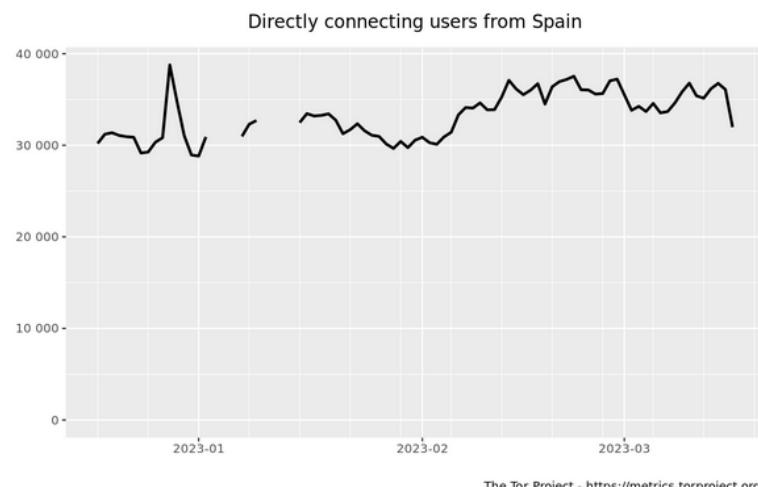


Imagen 35. Conexiones desde España a Tor

2.2.3.1. TOR2WEB

Tor2Web es un proyecto de software libre que permite acceder a los Hidden Services⁶ de la red Tor sin necesidad de utilizar Tor Browser. El sitio web oficial puede consultarse en el siguiente enlace: <https://www.tor2web.org>.

Permite acceder a dichos Hidden Services por medio de navegadores convencionales, como Firefox, Chrome u otros, añadiendo detrás del .onion de la url una serie de terminaciones que permiten esta conversión (.to, .ly, .link, .city, .sh, .pet, .dog o .w).

Tor2web: Browse the Tor Onion Services

What's Tor2web

[Tor](#) is a software project that lets you anonymously browse the Internet. Tor2web is a project to let Internet users access Tor Onion Services without using [Tor Browser](#).

Getting started

Whenever you see a URL like <http://duskgytldkxiuqc6.onion/>, that's a Tor Onion service. Just replace .onion with .onion.to or .onion.city or .onion.cab or .onion.direct or any other domain made available by volunteers Tor2web operators Example:

<https://duskgytldkxiuqc6.onion.to/>

This connects you with Tor2web, which then talks to the onion service via Tor and relays the response back to you.

WARNING: Tor2web only protects publishers, *not readers*. As a reader [installing Tor Browser](#) will give you much greater anonymity, confidentiality, and authentication than using Tor2web. Using Tor2web trades off security for convenience and usability.

Imagen 36. Sitio web oficial de Tor2Web

La utilización de este tipo de servicios puede provocar la perdida de privacidad y el anonimato, ya que el servicio Tor2Web no deja de ser un intermediario operando en la Surface Web, por lo tanto, puede recopilar información como por ejemplo la dirección IP desde donde se conecta y el contenido buscado por el usuario.

⁶ **Hidden Service:** Son los servicios ocultos que podemos crear en Tor, los cuales son muy similares a los que tenemos disponibles en la Surface Web pero en este caso no estarán indexados por los buscadores.

Desde un buscador como Google podemos localizar diferentes tipos de direcciones .onion seguido del TLD correspondiente al Tor2Web, tal como se puede comprobar en la Imagen 37.

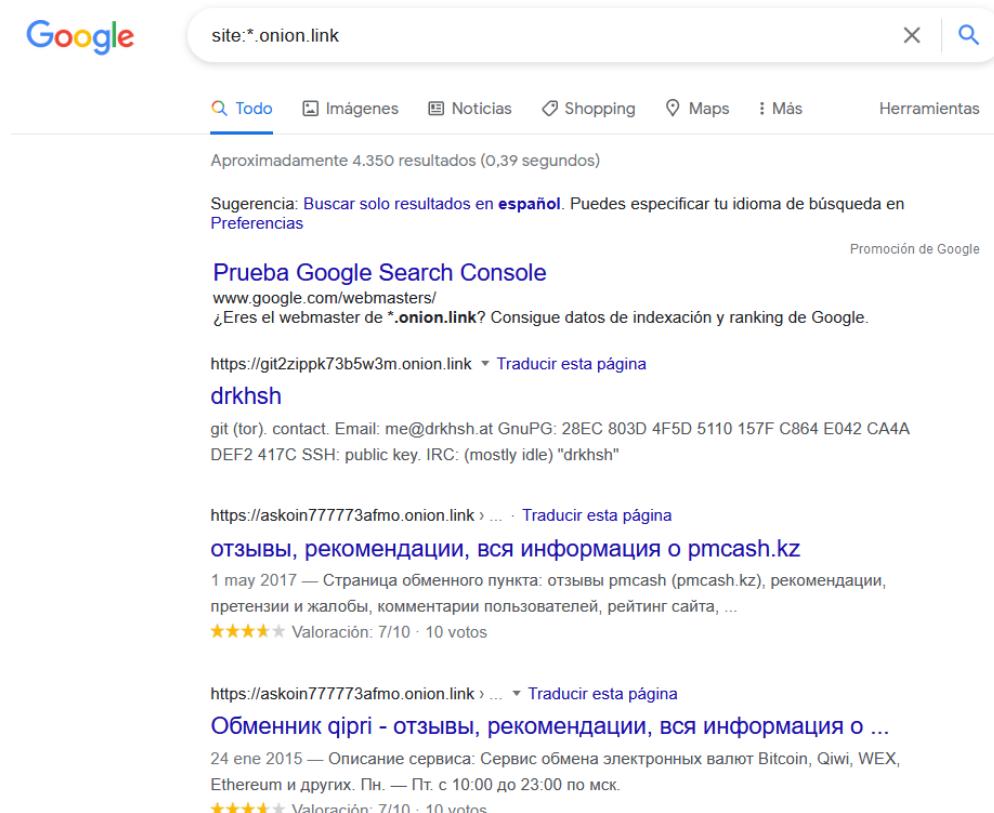


Imagen 37. Búsqueda de dominios .onion con el TLD del Tor2Web .link

2.2.3.2. INSTALACIÓN DE TOR BROWSER

Tor Browser es un navegador web de código abierto basado en Firefox que nos va a permitir navegar por Internet de manera anónima y dandonos acceso a la red Tor.

Las principales ventajas que tiene Tor Browser es que es bastante efectivo ocultando nuestra ubicación real y que el propio tráfico que generemos sea rastreado. Además, en este caso es bastante recomendable no instalar ningún plugin en el propio navegador de Tor Browser ya que podría derivar en la pérdida del anonimato y privacidad.

Tor Browser también tiene desventajas, como por ejemplo la disminución de la velocidad debido a que tenemos que conectarnos a diferentes nodos hasta llegar al destino.

Para descargar la última versión de Tor Browser será necesario acceder al sitio web oficial de Tor Project y elegir el sistema operativo donde lo queremos instalar. Tal como puede verse en la Imagen 38.

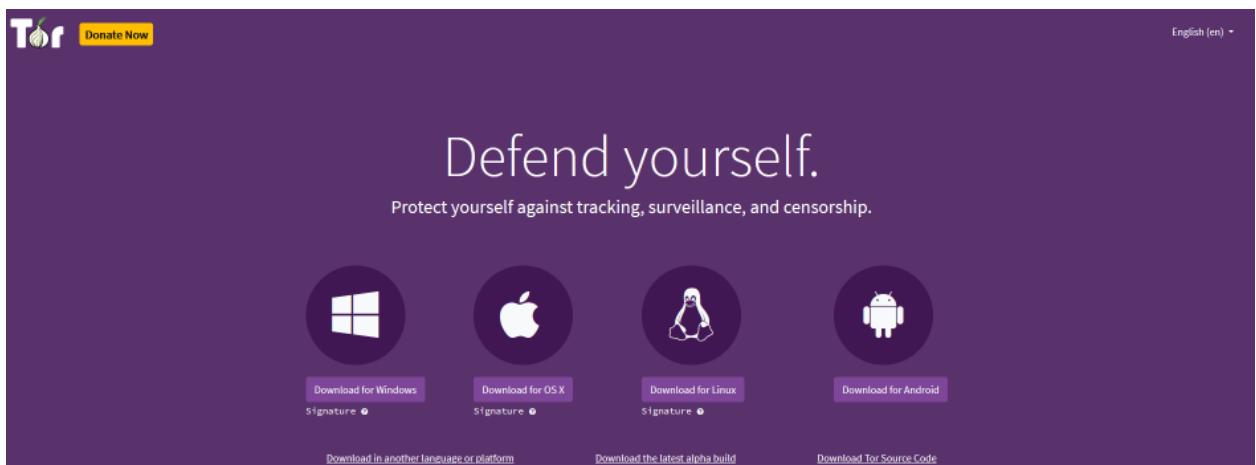


Imagen 38. Sitio web oficial de Tor Project para [descargar Tor Browser](#)

En este caso elegimos la versión para Linux, descargándola vía wget desde la Terminal, tal como se puede ver en la instrucción de abajo.

```
wget https://www.torproject.org/dist/torbrowser/16.0a1/tor-browser-linux-x86_64-16.0a1.tar.xz
```

Lo siguiente a realizar será descomprimir el fichero en formato xz recién descargado mediante la instrucción inferior:

```
tar -xvf tor-browser-linux-x86_64-16.0a1.tar.xz
```

En este momento accedemos al directorio recién creado de “tor-browser” y lanzamos el script start-tor-browser.desktop tal como se puede ver en la instrucción inferior.

```
cd tor-browser  
. ./start-tor-browser.desktop
```

Acto seguido arrancará Tor Browser y podremos elegir la opción de configurar primero la configuración o conectarnos a Tor, tal como puede verse en la Imagen 39.



Imagen 39. Arranque de Tor Browser

Antes de conectarnos a Tor vamos a configurar el Nivel de Seguridad de Tor Browser, para ello elegimos la opción de “Configurar la conexión” de la Imagen 39 y en la pestaña de “Privacidad & Seguridad” marcamos como “Nivel de Seguridad” la opción “El más seguro de todos” (Ver Imagen 40)

General

Inicio

Buscar

Privacidad & Seguridad

Conexión

Advertirle cuando los sitios web intenten instalar complementos

[Excepciones...](#)

Seguridad

Nivel de seguridad

Deshabilita ciertas funciones web que se pueden usar para atacar tu seguridad y anonimato. [Aprende más](#)

Estándar
Están habilitadas todas las características del navegador y los sitios web.

Más seguro
Deshabilita características del sitio web que a menudo son peligrosas, lo que causa que algunos sitios pierdan funcionalidad.

El más seguro de todos
Sólo permite las características de sitio web requeridas para sitios estáticos y servicios básicos. Estos cambios afectan a imágenes, medios, y scripts.

- JavaScript está deshabilitado por defecto en todos los sitios.
- Algunas fuentes, iconos, símbolos matemáticos, e imágenes están deshabilitados.
- Audio y vídeo (HTML5 media), y WebGL son click-to-play.

Imagen 40. Elección del Nivel de Seguridad para Tor Browser.

En el momento que ya tengamos toda la configuración de Tor Browser preparada, le indicamos que procedemos a conectarnos para poder navegar por la red Tor.

Desde el propio navegador podemos conocer el circuito virtual por el que pasa la comunicación tanto si accedemos a la Surface Web como a la Dark Web. Vamos a realizar dos peticiones con lo indicado:

- Primero accedemos al sitio web de marca.com en la Surface Web, pudiendo comprobar en la Imagen 41 que crea un circuito pasando por tres nodos. El nodo de entrada en Alemania, el nodo intermedio en Holanda y el nodo de salida en Estados Unidos.

Información del sitio para www.marca.com

Conexión segura (actualizado a HTTPS) >

Modo solo HTTPS

Activado ▾

Si el sitio no funciona correctamente, es posible que quiera desactivar el modo solo HTTPS para volver a cargarlo usando una conexión HTTP insegura.

🕒 Circuito Tor

- Este navegador
- Alemania 212.227.206.135, 2001:8d8:1800:1f1::1 **Protección**
- Holanda (Países Bajos) 188.166.31.252
- Estados Unidos 38.97.116.244
- marca.com

Tu nodo de protección no puede cambiar. [Conocer más](#)

[Nuevo Circuito para este Sitio](#)

Imagen 41. Circuito hacia marca.com mediante Tor Browser

- Ahora procedemos a conectarnos a un Hidden Service, al The Hidden Wiki en concreto. En la Imagen 42 se puede ver el circuito creado pasando por 6 nodos. El nodo de entrada en Finlandia y los nodos intermedios en Luxemburgo y Holanda, pero no conocemos los 3 últimos nodos, únicamente que se conectan a un repetidor.



Imagen 42. Circuito hacia The Hidden Wiki en la Dark Web

2.2.3.3. CONFIGURACION DE BRIDGES EN TOR BROWSER

Los bridge o puentes son nodos no públicos que no están presentes en los listados mencionados anteriormente con el resto de los nodos de la red Tor. Su función radica en eludir la censura y ofuscar las conexiones de la propia red Tor para evitar el bloqueo y acceso de los usuarios a la misma, independientemente del país desde el que se conecten.

Tor Browser permite la configuración de dichos puentes por medio del servicio BridgeDB para obtener la información necesaria para poder navegar por Tor utilizando dichos puentes. Desde el propio [sitio web de Tor Project](#) se pueden conseguir, tal como se puede observar en la Imagen 43.



BridgeDb can provide bridges with several types of Pluggable Transports, which can help obfuscate your connections to the Tor Network, making it more difficult for anyone watching your internet traffic to determine that you are using Tor.

Imagen 43. Sitio web de los bridges de Tor

Para poder obtener los puentes debemos solicitarlos por medio del Step 2 y hacer clic en "Get Bridges" (ver Imagen 43). El siguiente paso trata de elegir el tipo de transporte del puente que en nuestro caso será obfs4 (ver Imagen 44).

Get Bridges!

BridgeDB can provide bridges with several types of [Pluggable Transports](#), which can help obfuscate your connections to the Tor Network, making it more difficult for anyone watching your internet traffic to determine that you are using Tor.

Some bridges with IPv6 addresses are also available, though some Pluggable Transports aren't IPv6 compatible.

Additionally, BridgeDB has plenty of plain-old-vanilla bridges — without any Pluggable Transports — which maybe doesn't sound as cool, but they can still help to circumvent internet censorship in many cases.

[Just give me bridges!](#)

Advanced Options

Please select options for this bridge type:

Do you need a pluggable transport?

obfs4

Do you need IPv6 addresses?

Yes!

[Get Bridges](#)

Imagen 44. Elección del tipo de Bridge para Tor

En la Imagen 45 se puede observar la creación de tres nodos de tipo puente, las cuales serán añadidas en Tor Browser.

Here are your bridge lines:



Imagen 45. Generación de Bridges para Tor

En este momento es necesario añadir los puentes recién creados dentro de Tor Browser, para ello accedemos a la sección de puentes dentro de la pestaña de “Conexión” de la configuración del navegador e indicamos que queremos añadir un puente manualmente (ver Imagen 46). Lo siguiente a realizar será introducir los puentes creados en la Imagen 45 dentro de la pantalla que aparece en la Imagen 47.

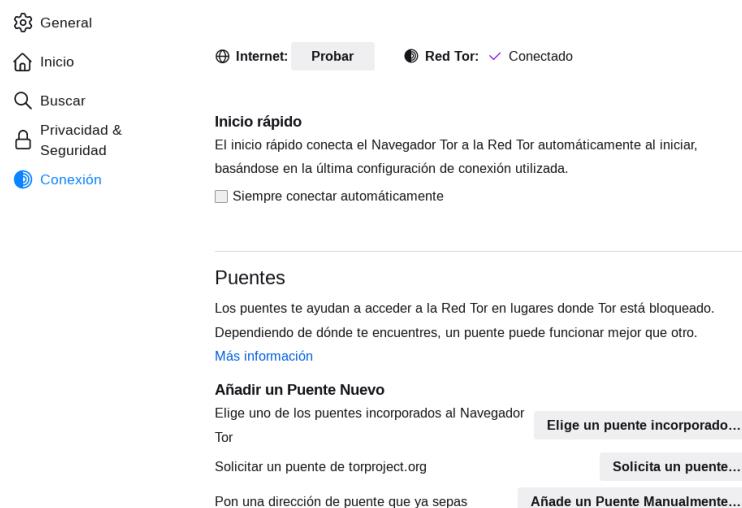


Imagen 46. Pestaña Conexión de las opciones de configuración para añadir los bridges de manera manual

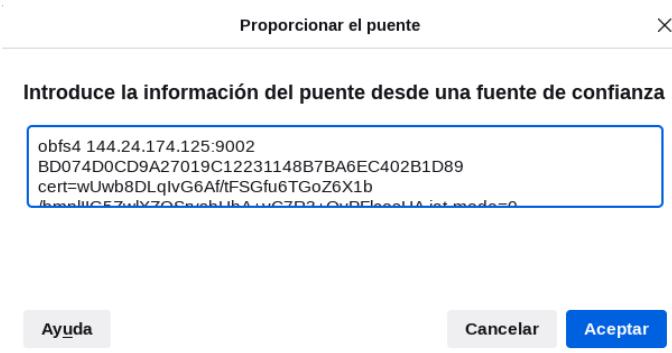


Imagen 47. Añadir los puentes manualmente

En el momento de pulsar el botón “Aceptar” se añadirán los puentes en la configuración de Tor Browser tal como puede verse en la Imagen 48.

Puentes

Los puentes te ayudan a acceder a la Red Tor en lugares donde Tor está bloqueado. Dependiendo de dónde te encuentres, un puente puede funcionar mejor que otro.

[Más información](#)

Tus puentes actuales

Puedes dejar guardados uno o varios puentes y Tor elegirá cuál usar cuando te conectas.

Tor cambiará de forma automática a otro cuando sea necesario.

Puente obfs4:  obfs4 144.24.174.125:9002 BD074D0CD9A2... 

Puente obfs4:  obfs4 37.228.129.30:2056 F2AFF91007766B... 

Puente obfs4:  obfs4 130.61.178.131:9091 7AEE925458E8... 

[Eliminar todos los puentes](#)

Imagen 48. Puentes configurados en Tor Browser

Ahora si accedemos de nuevo al sitio web de The Hidden Wiki podemos observar (ver Imagen 49) como el nodo de entrada dentro del circuito virtual está utilizando el puente recién creado (obfs4 con la dirección IP 37.228.129.30) y que será el punto de partida para acceder a la red Tor.

Información del sitio para
zqktlwiuavvvqqt4ybgvi7tyo4hjl5xgfvupdf6otjiycgwqbym2qad.onion

Conexión segura >

Círculo Tor

- Este navegador
- Repetidor puente (bridge): obfs4 37.228.129.30
- Suiza 85.195.230.249, 2a02:168:ae0d:99::1111
- Estados Unidos 173.232.194.19, 2a07:442:1:3::4
- Repetidor
- Repetidor
- Repetidor
- zqktlwi...ym2qad.onion

Nuevo Circuito para este Sitio

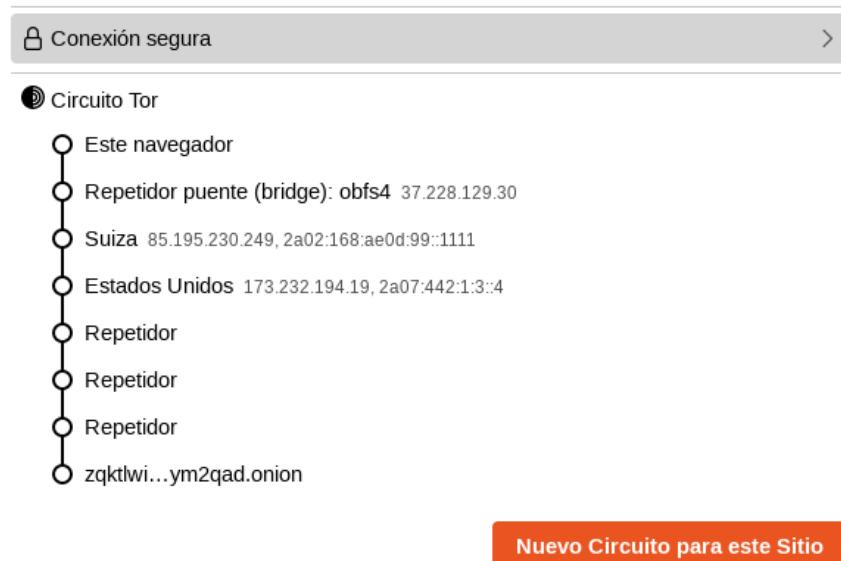


Imagen 49. Circuito virtual de Tor utilizando el puente

2.2.4. SECURIZACIÓN DE LOS NAVEGADORES

El navegador web puede dejar una huella digital única por usuario, lo que implica que mediante un análisis de la configuración de este es posible rastrear la actividad que realice un usuario en Internet.

Dicha huella digital es creada por medio de la combinación de diferentes aspectos de la configuración del navegador y del equipo o dispositivo que se esté utilizando, como por ejemplo: la versión del navegador, tipo de dispositivo, sistema operativo, información de la tarjeta gráfica, resolución de la pantalla, idioma del navegador.

Existen una serie de herramientas que pueden ayudar a comprobar que tipo de información estamos ofreciendo de nuestro navegador. Dichas herramientas son las siguientes:

- **Cover Your Tracks by EFF.** Es una herramienta que realizar una prueba del navegador teniendo en cuenta una serie de elementos para determinar si dispone un riesgo para la privacidad del usuario. El sitio web de la herramienta es

<https://coveryourtracks.eff.org>. En la Imagen 50 puede verse un ejemplo de prueba con el navegador en el que se indica que el navegador tiene una huella única, lo que supondría un riesgo de privacidad.

The screenshot shows the homepage of Cover Your Tracks. At the top, there's a logo with the text 'COVER YOUR TRACKS' and a green circular graphic. Below the logo, there are links for 'See how trackers view your browser', 'Learn', and 'About'. A main heading says 'Our tests indicate that you have **strong protection** against Web tracking.' Below this, there's a section titled 'IS YOUR BROWSER:' with a table showing results for blocking ads, invisible trackers, and fingerprinting. A note at the bottom states that the browser has a unique fingerprint. A 'LEARN MORE' button is also present.

Imagen 50. Prueba de privacidad del navegador con Cover Your Tracks

- **Browser Leaks.** Esta herramienta realiza una serie de pruebas del navegador como la anterior, pero en este caso separa en categorías los elementos y rastreadores detectados. Su sitio web es <https://browserleaks.com>.



Imagen 51. Sitio web de Browser Leaks

En el siguiente enlace (https://victorhck.gitlab.io/privacytools-es/#about_config) hay disponible una guía de configuraciones que podemos establecer y personalizar en Firefox para ganar mayor privacidad y anonimato. En la Imagen 52 puede visualizarse el recurso online.

Servicios Navegador Software Sistemas operativos Participa Acerca de Comparte Dona Código fuente

Preparación:

1. Escribe "about:config" (sin comillas) en la barra de direcciones de Firefox y presiona la tecla Enter.
2. Presiona el botón "Tendré cuidado, lo prometo"
3. Sigue las instrucciones que se detallan a continuación...

Empezando:

1. **privacy.firstparty.isolate = true**
 - o Un resultado del esfuerzo de [Tor Uplift](#), esta preferencia aisla todas las fuentes de identificación (por ejemplo cookies) al primer dominio, con el objetivo de prevenir el rastreo a través de dominios diferentes.
2. **privacy.resistFingerprinting = true**
 - o Como resultado del esfuerzo de [Tor Uplift](#), esta preferencia hace a Firefox más resistente a la identificación del navegador.
2. **privacy.trackingprotection.enabled = true**
 - o Esta es la nueva oferta de Mozilla como protección del rastreo. Utiliza el listado de filtros de Disconnect.me, que es redundante si ya estás utilizando los filtros uBlock Origin 3rd party, además deberías ajustarlo a "false" si estás utilizando las funcionalidades del complemento.
2. **browser.cache.offline.enable = false**
 - o Inhabilita la cache "offline".
2. **browser.safebrowsing.malware.enabled = false**
 - o Inhabilita las comprobaciones de malware de la navegación segura de Google. Tiene riesgos de seguridad pero mejora la privacidad.
2. **browser.safebrowsing.phishing.enabled = false**
 - o Inhabilita la protección de la navegación segura de Google y la protección de "phishing". Tiene riesgos de seguridad pero mejora la privacidad.
2. **browser.send_pings = false**
 - o El atributo debería ser útil para permitir a los sitios web rastrear los clics de los visitantes.
2. **browser.sessionstore.max_tabs_undo = 0**
 - o Incluso con Firefox ajustado para no recordar el historial, tus pestañas cerradas se almacenan temporalmente en Menú -> Historial -> Pestañas cerradas recientemente.
2. **browser.urlbar.speculativeConnect.enabled = false**
 - o Inhabilita la carga anticipada de direcciones autocompletadas. Firefox anticipa la carga de "URLs" que son autocompletadas cuando un usuario escribe en su barra de direcciones, lo cual es una preocupación si se sugieren URLs a las que el usuario no desea conectarse. [Fuente](#)
2. **dom.battery.enabled = false**
 - o Los propietarios de sitios web pueden rastrear el estado de la batería de tu dispositivo. [Fuente](#)

Imagen 52. Guía de configuración para ganar privacidad y anonimato en Firefox

A continuación, cito algunos plugins para Firefox muy útiles para privacidad y anonimato y no exponer la huella digital del navegador:

- **Firefox Multi-Account Containers.** Se trata de un plugin que ayuda a ganar privacidad realizando una gestión de contenedores con el objetivo de separar y aislar las cookies entre los mismos. Muy útil cuando estamos realizando varias investigaciones en paralelo y no queremos que se mezclen las cookies de sesión de diferentes cuentas. Enlace: <https://addons.mozilla.org/en-US/firefox/addon/multi-account-containers/>.
- **User-Agent Switcher and Manager.** Plugin que permite modificar el User-Agent que utilizamos en el navegador web. Enlace: <https://addons.mozilla.org/en-US/firefox/addon/user-agent-string-switcher/>.
- **HTTPS Everywhere.** Plugin que permite cifrar las comunicaciones de manera segura. En la actualidad la mayoría de navegadores ya vienen con el soporte nativo de HTTPS. Enlace: <https://www.eff.org/https-everywhere>.

- **IP Address and Domain Information.** Plugin que permite saber qué información exponemos de nuestra dirección IP y para recolectar información sobre el dominio y la dirección IP del objetivo. Enlace: <https://addons.mozilla.org/en-US/firefox/addon/ip-address-and-domain-info/>.
- **FoxyTab.** Permite tener un control y una copia de seguridad de las pestañas abiertas en el navegador. Muy útil frente a posibles “crasheos” del navegador. Enlace: <https://addons.mozilla.org/en-US/firefox/addon/foxytab/>.
- **NoScript Security Suite.** Plugin que permite bloquear cualquier tipo de JavaScript no deseado. Enlace: <https://addons.mozilla.org/en-GB/firefox/addon/noscript/>.
- **uBlock Origin.** Bloqueador de anuncios bastante popular. Enlace: <https://addons.mozilla.org/en-GB/firefox/addon/ublock-origin/>.
- **Privacy Badger.** Plugin que permite bloquear rastreadores basados en diferentes comportamientos. Enlace: <https://addons.mozilla.org/en-GB/firefox/addon/privacy-badger17/>

2.3. LA GESTIÓN DE AVATARES EN LAS INVESTIGACIONES

Antes de comenzar a explicar cómo poder crear un avatar, hay que destacar la gran diferencia existente entre un **nombre de usuario, username o nickname** (empleado normalmente para darse de alta en un servicio online/red social) y **la identidad real de la persona** que lleva a cabo tal proceso (vinculada esta con una persona física que tiene un nombre y apellidos).



Por ello, siempre hay que tener en cuenta que una **identidad real** puede llegar a **gestionar múltiples identidades digitales**, así como que un **mismo perfil digital** puede llegar a ser gestionado por **varias personas a la vez**.

Es bastante recomendable disponer de una identidad digital distinta para cada operación, adaptándolas a las necesidades particulares, evitando la reutilización de identidades previas. Las identidades digitales generadas van a permitir **preservar la privacidad** y el **anonimato** de la persona que este detrás de la misma, a la par que pueden aportan verosimilitud a las propias acciones que se lleven a cabo.

A estas identidades digitales se les suelen conocer también como avatar o sock puppet.

2.3.1. CREACIÓN DE UN AVATAR

Antes de crear el avatar es recomendable tener una guía de buenas prácticas para su creación y su uso en las operaciones, siendo las siguientes:

- Tanto para crear la cuenta como para acceder a ella es imprescindible utilizar siempre VPN o Tor para no perder ese anonimato que buscamos y no dar pistas de cuál es nuestra dirección IP real.
- Para aquellas redes sociales y diferentes plataformas que no permitan el uso de VPN será recomendable conectarse a ellas desde una WiFi pública.
- Crear un correo electrónico de manera anónima antes de asociarlo al avatar
- Disponer de un número de teléfono únicamente para realizar investigaciones, ya sea contratando otra línea totalmente separada de tu línea personal o bien mediante números de teléfono virtuales. Es recomendable disponer de un teléfono físico y asociarle ese número de teléfono.
- No reutilizar nunca las mismas cuentas de correo electrónicos ni las contraseñas en la creación de nuevos avatares en diferentes plataformas.

- Disponer de un gestor de contraseñas para tener un control de todos los avatares disponibles con sus respectivas contraseñas.
- En la medida de lo posible utilizar herramientas para generar avatares ficticios sino se tiene la suficiente imaginación para crearlo desde cero.
- No usar nunca datos relacionados con la vida personal del investigador como por ejemplo el nombre y apellidos (o variación de estos), nombre de familiares, fechas de nacimiento reales, etc.
- Añadir en los avatares fotos de perfil siempre, ya sea con un logo o imagen de un personaje de televisión y/o cine o bien generarlos con alguna herramienta de Inteligencia Artificial.

Como se ha comentado en las buenas prácticas, podemos utilizar diferentes herramientas para crear nuestro avatar de manera automática. Las herramientas más interesantes y utilizadas para ello son las dos siguientes:

- **Fake Name Generator.** Es el generador de nombres más conocido en la actualidad. Permite crear un avatar desde cero basándose en diferentes aspectos relacionados con 31 países y 37 idiomas, donde va generando distintos datos ficticios asociados a una identidad digital como pueden ser nombre y apellidos, numero de seguridad social, número de teléfono, fecha de nacimiento, dirección de correo, número de tarjeta de crédito, empresa donde trabaja, características físicas (altura, peso, tipo sanguíneo) y modelo de coche, entre otros datos. En la Imagen 53 puede verse la creación de un avatar con dicha herramienta. El sitio web es el siguiente: <https://es.fakenamegenerator.com.>



Imagen 53. Avatar creado con Fake Name Generation

- **Random Name Generator.** Herramienta muy similar a la anterior. Permite crear avatares partiendo del nombre de un país y generando una identidad con datos como por ejemplo el nombre y apellidos, dirección postal, número de teléfono, correo electrónico, username, contraseña, dirección IP, número de tarjeta bancaria, IBAN y nombre de empresa donde trabaja. Además, esta herramienta ya permite crear un rostro en forma de imagen asociado al avatar. En la Imagen 54 puede verse una generación de avatar con dicha herramienta. El sitio web es el siguiente: <https://www.random-name-generator.com>.

Generated Fake Data:



María Mar Gutierrez (Female)
Random Address: Camiño Montemayor, 2, 5º E, 87125, A Apodaca Alta
Phone Number: +34 996-23-8524

Fake online data:

Email: esther.mata@velez.com
IP: 156.108.179.63
Username: mariamez
Password: 6281c3ee

Payments

Credit Card No.: 4716 0644 7889 0232
Expiration Date: 11/24
IBAN: ES523045050453032420471
Swift Bic Number: MNAXSEKEIVC

Job

Company: Solorio-Guerra

Imagen 54. Creación de avatar con Random Name Generator

En el momento que ya tengamos creado nuestro avatar, deberíamos crear una imagen asociada al mismo (en el caso de que no se haya creado ya con la herramienta Random Name Generator) pero siempre utilizando imágenes ficticias y no existentes en la vida real ya que estaríamos cometiendo un delito de suplantación de identidad.

Existen diferentes herramientas que permiten crear imágenes de rostros, algunas de ellas son las siguientes:

- **This Person Does Not Exist.** Herramienta que permite generar rostros ficticios utilizando un algoritmo de aprendizaje automático mediante Inteligencia Artificial. El sitio web es el siguiente: <https://www.thispersondoesnotexist.com>. En la Imagen 55 pueden observarse rostros generados mediante esta herramienta.

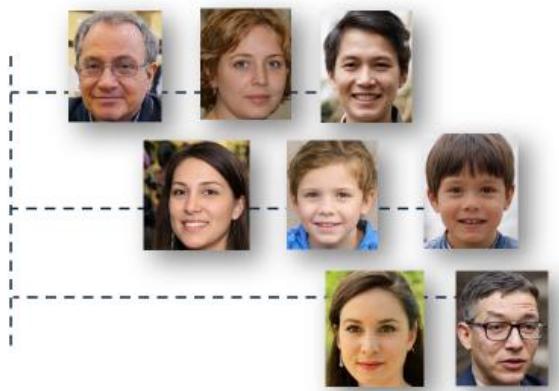


Imagen 55. Rostros generados por This Person Does Not Exist

- **Generated Photos.** Herramienta de pago que permite generar rostros ficticios utilizando Inteligencia Artificial, donde es posible ir seleccionando diferentes filtros para personalizar el rostro. En la Imagen 56 puede verse el repositorio de rostros creados, con un total de 2 millones. El sitio web es el siguiente: <https://generated.photos/faces>.

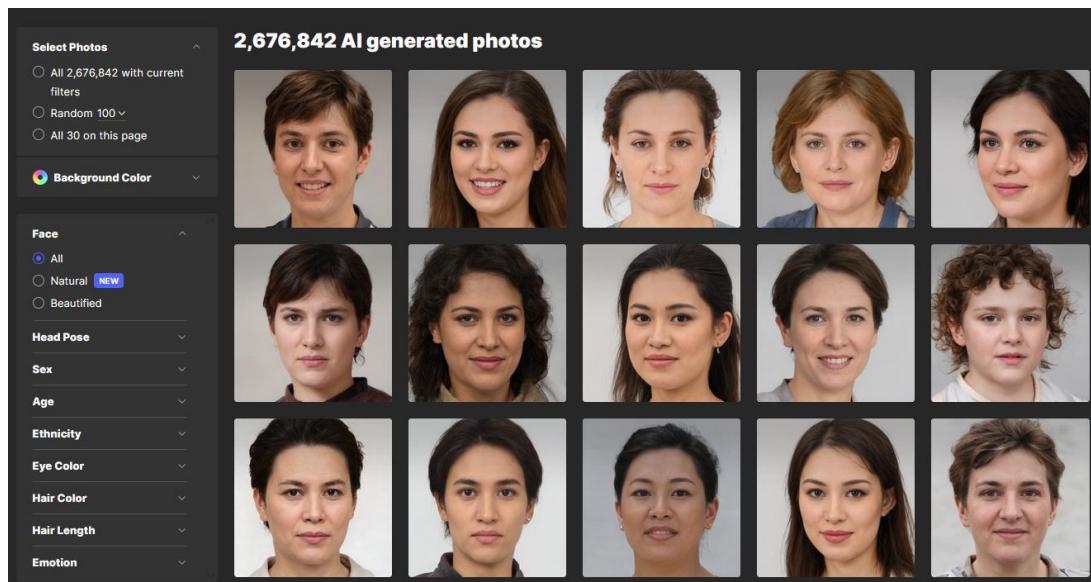


Imagen 56. Sitio web de Generated Photos

2.3.2. CREACIÓN DE CORREOS ELECTRÓNICOS

Uno de los puntos importantes a tener en cuenta a la hora de crear nuestro avatar es el correo electrónico que le asociaremos. Tenemos varias opciones que podemos elegir sobre el tipo de correo electrónico a utilizar:

- **Proveedores de correo electrónico genéricos.** Podemos emplear proveedores ampliamente conocidos como pueden ser Gmail, Hotmail, Yahoo!, etc. Este tipo de correos electrónicos son los más recomendables, ya que no levantarían sospechas en las diferentes plataformas donde nos registremos.

Una técnica que podemos emplear con Gmail es el de añadir al final del username del correo el carácter "+" con el objetivo de indicarle a Google que vamos a utilizar una etiqueta en el correo electrónico. En este sentido, podríamos utilizar diferentes tipos de palabras clave después del carácter "+" para catalogar las fuentes donde nos registremos y tener un control de estas.

A continuación, se facilitan unos ejemplos de lo mencionado:

juan.suarez+shodan@gmail.com
juan.suarez+twitter@gmail.com
juan.suarez+twitch@gmail.com

Todos los correos que recibamos en ese correo con etiqueta, lo iremos recibiendo también en el "correo principal" sin la etiqueta. De esta forma unificaremos en el mismo buzón de correo todos los correos usados en las distintas plataformas sociales o fuentes donde nos registremos y en caso de fugas de información o similares, sabremos desde qué plataforma ha tenido lugar la propia brecha.

- **Proveedores de correo electrónico pensados para ganar privacidad y anonimato.** Este tipo de proveedores están enfocados en garantizar la privacidad y el anonimato del usuario. Tienen una desventaja clara, siendo la desconfianza que genera en las diferentes plataformas de redes sociales y por este hecho es

más recomendable utilizar avatares con proveedores de correo electrónico genéricos. A continuación, se citan los más destacados:

- **ProtonMail.** Proveedor ampliamente conocido por garantizar la privacidad. Enlace del sitio web: <https://proton.me>.
 - **Tutanota.** Proveedor basado en que los usuarios dispongan de la privacidad necesaria en todo momento. Enlace del sitio web: <https://tutanota.com/es/>
 - **Mail2Tor.** Proveedor de correo electrónico anónimo y alojado en un Hidden Service de Tor. Enlace del sitio web: <http://mail2tor.cc/>
 - **Cock.** Permite el registro anónimo y el uso desde la red Tor. Es necesario disponer de una invitación para el registro. Enlace del sitio web: <https://cock.li>.
-
- **Proveedores de correos temporales.** Este tipo de proveedores permiten disponer de correos desechables sin la necesidad de registro y generados al vuelo. Estos correos temporales tienen una clara desventaja frente a los otros proveedores: las diferentes plataformas y fuentes la tienen categorizada con mala reputación, lo que implica que no podrá utilizarse correctamente en alguna de ellas. Además, cualquiera que tenga la dirección de correo electrónico temporal podrá visualizar todos los mensajes recibidos. Algunos de los proveedores de correos temporales son los siguientes:
 - **GuerrillaMail.** Enlace del sitio web: <https://www.guerrillamail.com>
 - **Email Temporal Gratis.** Enlace del sitio web: <http://www.emailtemporalgratis.com/>
 - **TEMPAIL.** Enlace del sitio web: <https://temp-mail.org/es>
 - **TEMPAIL.** Enlace del sitio web: <https://tempail.com/es>



Imagen 57. Sitio web de GuerrillaMail

2.3.3. USO DE NÚMERO DE TELÉFONO VIRTUAL

Tal como se ha podido ver en las buenas prácticas relacionadas con la creación de avatares, es muy importante disponer de un número de teléfono exclusivamente para las investigaciones y separado de la vida personal.

Para ello tenemos la posibilidad de utilizar números de teléfono virtuales, siendo [Hushed](#) la empresa más conocida y utilizada que ofrece este tipo de servicios de manera segura.

Hushed permite adquirir números de teléfono privados con la capacidad de enviar y recibir mensajes SMS y realizar llamadas telefónicas. En la Imagen 58 pueden verse los países que son seleccionables desde Hushed para elegir un número de teléfono virtual (**Estados Unidos, Canadá, Reino Unido y Puerto Rico**). Tal como puede verse en la Imagen 59, Hushed cuenta con varios **planes prepago (7, 30, 90 o 365 días)** o subscripciones para una o tres líneas. Los **métodos de pago** soportados son mediante **tarjeta de crédito** o por **criptomonedas**.

1 2 3

Select a Number

Get local numbers from over 300 area codes!

Select a Country

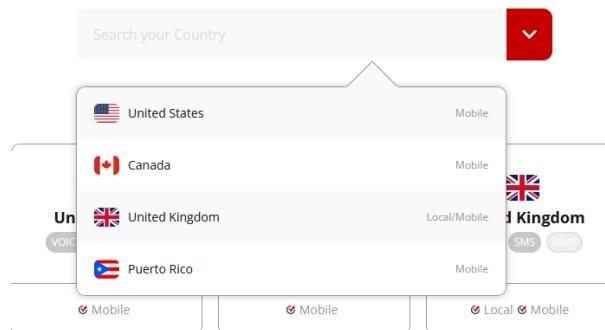


Imagen 58. Países seleccionables como números virtuales desde Hushed

PREPAID PLANS

Our most flexible plans bundled with local minutes and SMS usage.

7 DAY 20Min/60SMS	30 DAY 50Min/150SMS
US\$2.00	US\$3.99
90 DAY 100Min/250SMS	365 DAY 500Min/1100SMS
US\$9.99	US\$29.99

Bundled minutes/SMS for local calling and texting

7, 30, 90, and 365 Day expiry plans available - extend your number at any time!

One-time payment. Perfect for any short term or long term use case

UNLIMITED SUBSCRIPTIONS

UNLIMITED talk & text, auto-renewing subscription plans available on US, Canada, and UK mobile numbers.

3 Line SUBSCRIPTION <small>YEARLY</small>	1 Line SUBSCRIPTION <small>YEARLY</small>
US\$139.99/year	US\$47.99/year

UNLIMITED local talk & text.* Auto-renewing subscription, no expiry date!

Available in 1 or 3 Line bundles. Choose one line now, add two more numbers later

Choose from monthly or yearly plans. Sign up yearly and save up to 20%

PAY-AS-YOU-GO INTERNATIONAL PLANS

For international calling capabilities with your Hushed number.

30 Day WORLDWIDE <small>(Includes \$1.00 Credits)</small>
US\$4.99

Call internationally anywhere in the world at great rates!

Uses Hushed Credits directly from your account balance

International texting capabilities available with US/CAN numbers

Imagen 59. Planes y suscripciones de Hushed

2.3.4. GESTIÓN DE CREDENCIALES DE AVATARES CON KEEPASS

Uno de los temas más importantes con los avatares es su propia gestión, tener a buen recaudo toda la información referente a los avatares creados en las distintas fuentes y plataformas sociales.

Por este motivo es imprescindible disponer de una herramienta que nos permita tener un inventario de todo lo relacionado a los avatares, como por ejemplo tener una serie de carpetas categorizadas por tipos de operaciones y temáticas, donde en cada una de ellas dispondremos de ítems asociados a cada identidad creada en las diferentes plataformas con información relacionada (credenciales, username, url de acceso, 2FA, nombre y apellidos si se diera el caso, correo relacionado, etc).

Dos de las herramientas más conocidas para ello son las siguientes:

- **Keepass.** Es un gestor de contraseñas gratuito que nos permite disponer de todas las credenciales de diversos recursos bien categorizadas por carpetas. Su instalación es en local.

En la Imagen 60 puede verse el aspecto gráfico de la herramienta. El enlace del sitio web es el siguiente: <https://keepass.info>.

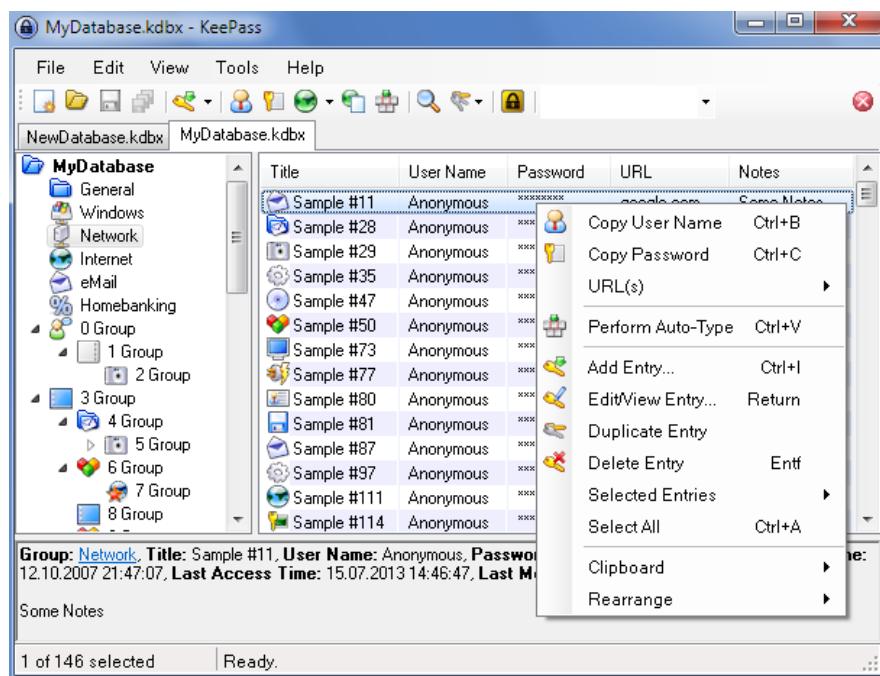


Imagen 60. Herramienta Keepass

- **Bitwarden.** Es otro gestor de contraseñas similar a Keepass, donde su punto diferencial radica en que ofrece (a parte de su versión en local) una versión en la nube con dos modalidades: una gratuita y otra de pago con distintos planes.

En la Imagen 61 puede verse el aspecto gráfico de la herramienta. El enlace del sitio web es el siguiente: <https://bitwarden.com>.

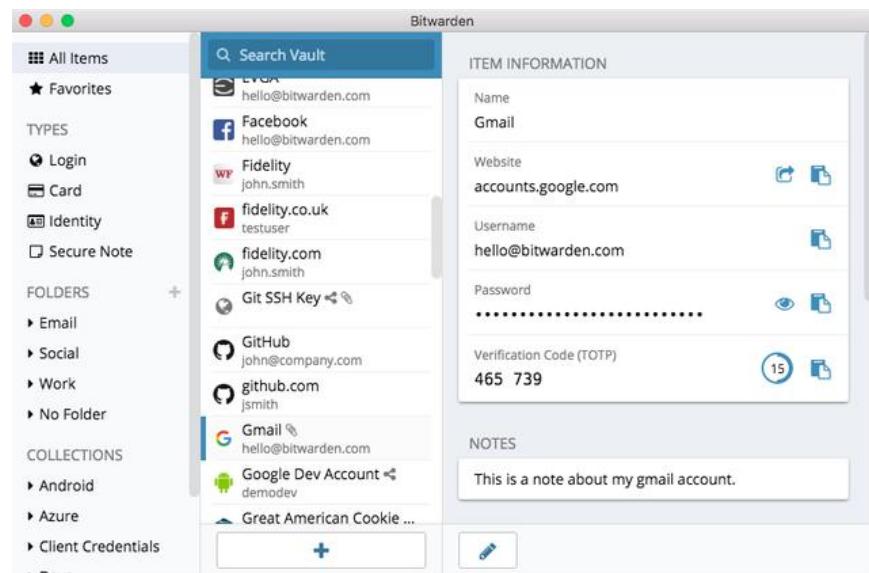


Imagen 61. Herramienta Bitwarden