¿Qué es la Dark Web?, ¿Para qué sirve?, ¿Es seguro entrar a la Dark Web? Y sobre todo, ¿Cómo entrar a la Dark Web?

Este es uno de los artículos que llevaba tiempo queriendo escribir, ya que creo que es un tema muy interesante y muy poco conocido todavía. Además lleváis tiempo pidiéndomelo a través de nuestro canal de YouTube y de nuestras redes sociales. Se trata de la Dark Web. En este artículo, vamos a ir viendo y resolviendo estas otras dudas acerca de la Dark Web.

Iremos resolviendo todas estas dudas y mucho más en este artículo, además de compartir unos consejos de seguridad para protegernos en la Dark Web, así como recomendaciones para poder navegar y encontrar lo que buscamos cuándo entremos a la Dark Web.



Como ya es costumbre en nuestra comunidad, debemos hacer un pequeño disclaimer para eludir toda responsabilidad. Evidentemente, os vamos a compartir mucha información que dependiendo de las manos en las que caiga, puede ser utilizada para realizar prácticas poco recomendables o incluso ilegales. Por lo tanto, no nos hacemos responsables del uso que cada uno pueda realizar con esta información, ya que el fin exclusivo de esta publicación es únicamente con propósitos educativos.

Dicho esto, comenzamos con unos conceptos básicos para entender cómo entrar a la Dark Web …

**Conceptos básicos**

Antes de continuar, debemos tener claros algunos conceptos que nos van a ayudar a entender mejor qué es y cómo entrar a la Dark Web. Estos conceptos son:

* Surface Web
* Deep Web
* Dark Web
* Dark Net



**¿Qué es la Surface Web?**

También conocida como Clear Web. La Surface Web se trata de Internet, tal y como lo conocemos. Concretamente, es la parte indexada de Internet, es decir, que se puede buscar a través de buscadores, como pueden ser Google, Bing, etc. Por tanto, se puede acceder a esta Surface Web a través de los navegadore convencionales, como pueden ser Microsoft Edge, Google Chrome, Firefox, etc.

En la Surface Web, somos muy fácilmente rastreables, ya que nuestra dirección IP con la que navegamos a través de ella, puede ser fácilmente capturada y rastreada. De esta forma, se puede obtener fácilmente nuestra dirección física, y obtener información acerca de nuestra actividad en Internet, como el historial de navegación. ¿Esto que quiere decir?

Pues que todo aquello que realicemos en la Surface Web, quedará en cierta forma “escrito” o registrado en algún servidor o servidores para que se pueda utilizar por un tercero. Esto puede ser positivo para las fuerzas y cuerpos de seguridad, ya que de esta forma se ha capturado a infinidad de delincuentes y ciberdelincuentes. No obstante, no es tan positivo para nosotros, las personas de a pie, ya que sería muy complicado obtener un anonimato completo de todo aquello que estemos realizando en la Surface Web o en Internet tal y como la conocemos.

En el siguiente enlace podéis encontrar más información, [Surface Web](https://es.wikipedia.org/wiki/Internet_superficial).

**¿Qué es la Deep Web?**

La Deep Web es la parte de Internet que no es indexable por los buscadores como Google o Bing, entre otros. ¿Esto que quiere decir? Pues básicamente, que no vamos a poder encontrar estas páginas web, URLs, dominios o lo que sea, a través de estos buscadores, por lo que si no conocemos la URL exacta, o la dirección IP exacta, no vamos a poder acceder a esta Deep Web.

La Deep Web supone aproximadamente el 90% del contenido de Internet. ¿Pero que hay en la Deep Web? Se trata de servicios no indexados, como pueden ser páginas de login a servicios, que para garantizar su seguridad no se indexan en Internet. O sitios web con métodos de pago, como pueden ser Netflix, HBO, etc, donde no encontraréis nunca las URLs de pago a través de los buscadores tradicionales. También pueden ser accesos a bases de datos, sistemas de correo electrónico, etc.

En determinadas ocasiones, por error humano o error de la aplicación o servicio en concreto, se permite la indexación de estos servicios, por lo que supone un grave riesgo a la seguridad del propio servicio, ya que estamos publicando en Internet, para que todo el mundo pueda verlo, un sistema de login con información muy importante para los ciberdelincuentes.

En el siguiente enlace podéis encontrar más información, [Deep Web](https://es.wikipedia.org/wiki/Internet_profunda).

**¿Qué es la Dark Web? ¿Cómo entrar a la Dark Web?**

La Dark Web es un pequeño fragmento de la Deep Web. Es decir se trata de un contenido no indexable, o al menos no indexable a través de nuestros navegadores y buscadores tradicionales. Se dice que la Dark Web puede ser aproximadamente un 0,1% del contenido de la Deep Web.

El contenido en la Dark Web es un contenido que está intencionalmente oculto a los motores de búsqueda y que además utilizan direccionamiento IP enmascaradas, es decir, no se está utilizando la dirección IP real.

Pero, ¿Cómo entrar a la Dark Web? Para poder entrar a la Dark Web, es necesario disponer de un navegador especial, ya que mediante nuestros navegadores tradicionales, como se ha indicado anteriormente, no sería posible acceder. Uno de los navegadores más famosos para entrar a la Dark Web es el navegador “TOR Browser”, que vamos a ver más adelante en el artículo.

Los sitios web alojados en la Dark Web, suelen tener dominios con nombres formados por un conjunto de letras y número, aparentemente sin sentido, y terminados en “.onion” o “.i2p”. Aunque existen otros tipos, estos son los más comunes.

En el siguiente enlace podéis encontrar más información, [Dark Web](https://es.wikipedia.org/wiki/Dark_web).

**¿Qué es la Dark Net?**

La Dark Net se trata de una agrupación de redes y tecnologías. Cuando hablamos de estas Dark Net, estaríamos hablando de la Dark Web, que ya hemos comentador anteriormente. Existen diferentes tipos de Dark Net, pero las más comunes son las siguientes:

**Red TOR**

Esta es la Dark Net más popular del mundo. Para acceder a ella, se necesita el navegador “TOR Browser”, como se ha comentado anteriormente, y aquí es donde se responde a la gran pregunta ¿Cómo entrar a la Dark Web? Pues a través del navegador TOR Browser. Para poder descargar el navegador e instalarlo en nuestros equipos, podéis realizarlo a través del siguiente enlace.

<https://www.torproject.org/download>

La instalación de este navegador es muy sencilla. Lo vamos a ver a continuación un poco más adelante en este artículo. Me gustaría indicar que a través del navegador TOR Browser, podéis navegar en la Surface Web, pero también podréis entrtar a la Dark Web, en concreto a la Dark Net, Red TOR.

Dentro de la red TOR existen buscadores propios, ya que es necesario indexar los dominios .onion como comentábamos antes o no seríamos capaces de encontrar nada, a no ser que tengamos la URL exacta. Un ejemplo de estos buscadores, puede ser “DuckDuckGO”. Otro de los buscadores muy utilizados es “The Hidden Wiki”, donde se mostrarán resultados de URLs dentro de la red TOR, ordenadas por categorías o temáticas.



**Freenet**

Este es otro tipo de Dark Net, y en concreto del tipo P2P. Utiliza un sistema similar a herramientas de descarga masiva, como Torrent.

Para poder acceder a Freenet, también es necesario utilizar una aplicación específica. Para ello, debemos descargar la aplicación alojada en el siguiente enlace.

[https://freenetproject.org](https://freenetproject.org/)



**I2P**

Este es otro de los tipos de Dark Net. También es necesario utilizar una aplicación específica para poder acceder. Podéis realizar la descarga a través del siguiente enlace.

[https://geti2p.net](https://geti2p.net/)



**ZeroNet**

Otro tipo de Dark Net, que además funciona también a través del sistema P2P. Para acceder a esta Dark Net, también es necesario utilizar una aplicación específica. Os podéis descargar la aplicación a través del siguiente enlace.

<https://zeronet.io/es>

En este caso, cuando realicemos la instalación de ZeroNet, encontraremos ZeroList, que básicamente se trata de un índice o listado para poder hacernos una idea de lo que nos podemos encontrar en esta Dark Net.



**¿Qué es la Red TOR y cómo acceder?**

El inicio de la red TOR, aunque no está 100% claro, se dice que la creó el ejército de Estados Unidos. El propósito con el que se creó esta red fue el de permitir a personas que se encuentran fuera de Estados Unidos y que no tienen acceso a una red segura o que la libertad de expresión está muy coaccionada, puedan comunicarse con el resto del mundo sin que nadie pueda interferir estas comunicaciones.

Un ejemplo de ello, pueden ser periodistas que se encuentran en países controvertidos o en guerra, donde tienen que ir informando de lo que allí sucede sin que ni los países donde se encuentran o los proveedores de internet de los mismos, puedan interferir o filtrar estas comunicaciones por el bien o beneficio propio del país donde se encuentran. Mediante esta red TOR, los periodistas pueden comunicarse de forma anónima, segura y sin filtros con el resto del mundo.

Pero ¿qué es esto de ser anónimos en Internet? Ya lo hemos nombrado varias veces, pero no hemos dejado claro que esto de ser anónimo en Internet. Para entenderlo mejor, primero debemos tener claro que todo aquello que realizamos a través de Internet, desde busca información sobre algún tema, enviar un correo electrónico o leer este mismo artículo, está relacionado con nuestra dirección IP pública.

Todo, repito, todo lo que hacemos en Internet está siendo relacionado, y por tanto puede ser registrado y asociado a una dirección IP pública que el propio proveedor de Internet que tengamos contratado nos va a facilitar, para poder navegar por Internet. Esto quiere decir, evidentemente que todo lo que hagamos, puede ser rastreado hacia nosotros. Es como si fuésemos navegando por Internet diciendo quienes somos en cada página o servicio que utilicemos en Internet.

Sin embargo, cuando nos conectamos a Internet a través del navegador TOR Browser, la dirección IP pública que aparece, ya no es la nuestra, sino que es la dirección de uno de los servidores de salto de la red TOR. Esto hace muy difícil el rastreo de lo que hagamos en Internet cuando estemos utilizando este navegador.

Cuando accedemos a la red TOR a través de su navegador, se realizan diferentes saltos entre servidores para poder conectarnos a la red. Cada uno de estos saltos está utilizando una dirección IP diferente, además de estar cifrado todo el flujo de conectividad y navegación. En el último salto es donde nos “quedamos” con la dirección IP del último salto, que en realidad no es la nuestra, por lo que no se podría asociar nuestra navegación a nuestros.

El problema es que esto es ya por todos sabido, y determinados cuerpos y fuerzas de seguridad o incluso países o estados, colocan sus servidores para realizar alguno de estos saltos, por lo que la información que llega a estos servidores podría ser investigada y en última instancia, asociada a nosotros. No es muy sencillo, pero es posible. No obstante, existen diferentes formas de agregar más dificultad a esto que sea prácticamente imposible el asociarnos. Por estos motivos la red TOR es muy utilizada por delincuentes y ciberdelincuentes, para compartir, comunicarse, etc.



La red TOR, está basada en criptografía simétrica. No voy a entrar en el detalle técnico, ya que haría este artículo muy largo. Os dejo un link donde podéis ver mucha información acerca de este tipo de criptografía, [criptografía simétrica](https://es.wikipedia.org/wiki/Criptograf%C3%ADa_sim%C3%A9trica). Como podéis leer en el artículo, básicamente y explicado con pocas palabras, se trata de un método criptográfico en el cual se usa una misma clave para cifrar y descifrar mensajes entre el emisor y el receptor.

Llegados a este punto, debemos indicar que la red TOR es una red de baja latencia, es decir, es una red muy lenta. Pero, ¿Por qué la red TOR es una red de baja latencia? Pues básicamente, porque tiene que cifrar y descifrar varias veces, una por cada nodo utilizado, para que podamos acceder a donde queremos.

La red TOR se basa en un sistema de nodos o capas, es por ello que se le reconoce con una cebolla o modelo por capas. Por este motivo es tan lenta. Existen nodos de entrada, nodos intermedios y nodos de salida. Cuantos más nodos se utilicen, más seguridad tendrá la comunicación, pero más lenta será la navegación.



**Instalación del navegador TOR Browser para entrar a la Dark Web**

Lo primero que debemos realizar para instalar el navegador TOR es al sitio web oficial y descargarlo. Yo os recomiendo que solo os lo descarguéis del sitio web oficial, ya que de esta forma os aseguráis de no tener sorpresas desagradables al descargaros algo que no es lo que parece.

<https://torproject.org/download>

Debemos elegir la plataforma sobre la que vamos a instalar el navegador TOR, Windows, OS, Linux o Android. Cuando lo hayamos seleccionado, tan solo deberemos esperar a que termine la descarga. En este ejemplo, voy a realizar la instalación en una máquina virtual basada en Windows. Veréis que es muy sencillo realizar la instalación.



Una vez descargado el instalador del navegador Tor Browser, tan solo deberemos hacer doble clic en el ejecutable. Se abrirá el asistente de instalación y deberemos elegir el idioma en el que queremos instalar el navegador.



Después, debemos elegir la ruta de instalación. Es indiferente donde lo instaléis, así que elegid una ruta que recordéis para que sepáis donde se ha realizado la instalación.



Hecho esto, hay que hacer clic en el botón “Install” para que comience la instalación. Este proceso de instalación es bastante rápido.

Una vez terminada la instalación, debemos abrir el navegador TOR Browser para poder llevar a cabo una pequeña personalización para que nos vaya todo bien. Cuando se abra por primera vez el navegador, se nos abrirá el asistente de configuración para ver cómo queremos conectarnos a TOR. Para entrar, tan solo deberemos elegir la opción “Connect”, ya que la otra opción es entrar en la configuración del navegador y elegir nuestra personalización. Esta sería la opción más recomendable, pero será el objeto de otro artículo, ya que si lo detallamos en este, al final se convertirá en la biblia por la cantidad de contenido que contendría el artículo.



Una vez que le damos al botón “Connect”, comenzará el proceso de negociación con los nodos de la red TOR, que nos puede llevar unos segundos o incluso unos minutos, dependiendo de la conexión, de vuestro equipo, etc. Aquí es donde iremos saltando entre las capas de la cebolla que hemos comentado antes, que en realidad se trata de saltos entre el servido de entrada, el o los intermedios y el servidor de salida. De hecho si analizamos el nombre del navegador, TOR es el acrónimo de “The Onion Router”. Cada capa irá cifrando y descifrando hasta que se nos abra el navegador TOR directamente.



A partir de aquí, y si personalizamos mejor nuestra conexión y el propio navegador, nuestra conexión, navegación y todo lo que realicemos en la red TOR puede considerarse cifrada y anónima. Aunque debemos tener cuidado con esto, ya que puede dar una falsa sensación de seguridad y anonimato que como hemos visto anteriormente, puede que no sea así del todo.



Ahora os recomiendo que hagáis una pequeña prueba. Abrir vuestro navegador tradicional y navegar hasta la URL [https://cualesmiip.com](https://www.cualesmiip.com/). Anotad la dirección IP que os muestra en el navegador. Esta, es vuestra dirección IP real, sobre la que realizáis vuestra navegación, y puede estar registrando todo lo que estáis haciendo en Internet. Ahora a través del navegador TOR Browser, abrir la misma URL, es decir, [https://cualesmiip.com](https://cualesmiip.com/).

Como comprobaréis, la dirección IP es diferente. Esta es la dirección IP con la que se registrará todo lo que realizáis a través del navegador TOR Browser, que como no es la vuestra, “supuestamente” estaréis siendo anónimos.

Como hemos comentado anteriormente, a través del navegador TOR, podremos navegar como lo hacemos con nuestros navegadores tradicionales en la Surface Web, por ejemplo, para hacer una búsqueda en Google, o para acceder a un determinado servicio. Si hacéis esto, veréis que la navegación es extremadamente lenta. Esto es normal, como ya hemos comentado anteriormente.

Cuando abrimos el navegador TOR Browser, veremos cómo se nos abre por defecto el buscador “DuckDuckGo”. El problema es que si realizamos cualquier tipo de búsqueda ahora mismo, no hará la búsqueda sobre la Surface Web, como si lo estuviésemos haciendo a través de nuestros navegadores tradicionales, pero de forma “anónima”.

Para que nos haga una búsqueda a través de la red TOR, debemos ir a las tres rayitas que aparecen arriba a la derecha, y hacer clic en “Options”. Cuando se nos abra el panel de opciones, debemos irnos a la sección “Search”, y especificaremos en el “Default Search Engine” o motor de búsqueda por defecto, del menú desplegable, la opción DuckDuckGoOnion. De esta forma, configuraremos nuestro navegador para buscar en la red TOR por defecto



Aquí os tengo que recomendar que ya que estáis en las opciones de configuración, que le echéis un vistazo a las opciones de seguridad. Cuando instalamos el navegador TOR, por defecto se selecciona la opción de seguridad “Standard” y evidentemente es la opción menos segura, dentro de la seguridad extra que nos aporta este navegador frente a otros.

Bien, ahora podemos utilizar este buscador, o podemos entrar en otros como puede ser “The Hidden Wiki”, que es muy, muy utilizado para hacer búsquedas en la red TOR. Aquí podréis encontrar diferentes enlaces, divididos por temática.





Algo que tenemos que tener en cuenta también, además de la velocidad tan extremadamente lenta, son los efectos visuales de las web dentro de esta red. Todos los sitios web parecen de hace 20 años, sin efectos visuales, sin dinamismo, etc. Esto es porque como es una red tan lenta, si se meten en el código efectos visuales, imágenes, etc., su carga sería más lenta todavía y haría imposible la visualización del contenido.

A partir de aquí, ya sabéis cómo entrar a la Dark Web y es vuestra responsabilidad lo que hagáis dentro de la red TOR. Espero que lo empleéis para la búsqueda de información, material que podáis utilizar en vuestros trabajos, y sobre todo para poder ayudar a personas o empresas a mejorar su seguridad.

Déjame un comentario si te ha quedado dudas o si quieres ver algo más de detalle sobre alguna de las partes que hemos explicado en este artículo.