

Conociendo la deep web: un acercamiento inicial para minimizar riesgos informáticos en entornos académicos

Getting to know the deep web: an initial approach to minimizing IT risks in academic environments

Marena Vitola-Quintero

Escuela Naval de Cadetes “Almirante Padilla” –
Colombia
ORCID iD: <https://orcid.org/0000-0001-5219-3615>
marena.vitola@escuelanaval.edu.co

Jenny Romero-Duarte

Escuela Naval de Cadetes “Almirante Padilla” –
Colombia
ORCID iD: <https://orcid.org/0000-0002-6930-1448>
jenny.romero@armada.mil.co

Cristhian Mendoza-Pérez*

Escuela Naval de Cadetes “Almirante Padilla” –
Colombia
ORCID iD: <https://orcid.org/0000-0002-7885-815X>
poseidon@enap.edu.co

Fecha de recepción: 02/11/2019

Fecha de evaluación: 05/01/2020

Fecha de aceptación: 03/05/2020

Angie Rosero-Castro

Escuela Naval de Cadetes “Almirante Padilla” –
Colombia
ORCID iD: <https://orcid.org/0000-0003-0003-828X>
angie.rosero@armada.mil.co

Cómo citar: *Vitola-Quintero, M., Mendoza-Pérez, C., Rosero-Castro, A., & Romero-Duarte, J. (2020). Conociendo la Deep Web: un acercamiento inicial para minimizar riesgos informáticos en entornos académicos. Revista Científica Anfibia, 3(1), 68-77. <https://doi.org/10.37979/afb.2020v3n1.64>*



[Atribución-NoComercial-CompartirIgual 4.0 Internacional](https://creativecommons.org/licenses/by-nc-sa/4.0/)

* Autor a quien debe ser dirigida la correspondencia

Resumen

El presente trabajo es el resultado de una búsqueda y recopilación de información relacionada con la Deep Web o web profunda, la cual hace referencia a una pequeña parte de la red que contiene material, información y páginas web no indexadas en buscadores como Google, Bing y Yahoo. A partir de la opinión expuesta por Gay (2015) resulta importante resaltar que “La Deep Web es un espacio oculto de internet donde la primera garantía es el anonimato”. Esta garantía sirve para albergar una vasta red de servicios ilegales, como el narcotráfico, la trata de blancas, contratación de sicarios, compra-venta de pasaportes y cuentas bancarias, entre otros delitos, además posibilita que activistas políticos que viven en países dictatoriales puedan compartir información sensible con el resto del mundo y mucha información clasificada por países como Estados Unidos, sin embargo también ofrece la posibilidad de acceder a contenido académico diverso que puede ser útil a la hora de construir un documento de esta naturaleza; en ese orden de ideas el objetivo de la presente investigación fue realizar un estudio descriptivo (Hurtado, 2001) recopilando información documental acerca de los riesgos y amenazas asociados a la Deep Web, para generar un acercamiento inicial al tema por parte de los tripulantes de la Escuela Naval de Cadetes “Almirante Padilla” y demás escuela de formación, evitando futuros posibles riesgos asociados a fugas de información por desconocimiento y uso inadecuado de la internet profunda. Se abordaron las características más importantes del objeto de estudio con respecto a su aparición y comportamiento en el tiempo.

Palabras claves:

Web profunda; Anonimato; Riesgos; Desconocimiento; Riesgos informáticos

Abstract

This work is the result of a search and compilation of information related to the Deep Web or Deep Web, which refers to a small part of the network that contains material, information and web pages not indexed in search engines such as Google, Bing and Yahoo. From the opinion expressed by Gay (2015) it is important to highlight that “The Deep Web is a hidden internet space where the first

guarantee is anonymity”. This guarantee serves to house a vast network of illegal services, such as drug trafficking, white trafficking, hiring of hitmen, passport purchase and bank accounts, among other crimes, also allows political activists living in dictatorial countries to share sensitive information with the rest of the world and a lot of information classified by countries like the United States, however, it also offers the possibility of accessing diverse academic content that can be useful when building a document of this nature; in that order of ideas the objective of the present investigation was to carry out a descriptive study gathering documentary information about the risks and threats associated with the Deep Web, to generate an initial approach to the subject by the crew of the Naval School of Cadets “Admiral Padilla”, avoiding future possible risks associated with information leaks due to ignorance and inappropriate use of the deep internet. The most important characteristics of the object of study with respect to its appearance and behavior over time were addressed.

Keywords

Deep web; Anonymity; Risks; Ignorance; IT risks

Introducción

La web está dividida en distintos niveles de información y seguridad, lo que se traduce en una mayor cantidad de restricciones proporcional a un aumentando de nivel. Los niveles más profundos e inaccesibles corresponden a la Deep Web también conocida como Internet Profunda y la define López-Barbera (2014), como un conjunto de páginas que no se encuentran elaboradas en formato HTML o CSS. Los contenidos alojados en muchas de esas páginas son ilegales debido a que ofrecen servicios o productos fuera de la ley, siendo estos de difícil acceso por estar alojados en páginas protegidas con contraseñas o que requieren un programa específico para poder acceder a ellas; uno de los inconvenientes recurrentes en la internet profunda, es que el usuario principiante no tiene la certeza de acceder a la información que realmente quiere encontrar. Así pues, “puede establecer contacto con usuarios no deseados, foros de temática ilegal, virus y troyanos que con mucha probabilidad pueden acceder a su servidor” (Diario La Opinión de Murcia, 2016).

De otra parte, Becerra (2018) señala que los conceptos de internet profunda, tecnologías de privacidad e incluso mercado negro se entremezclan. Opina que la Deep Web corresponde a una porción de Internet a la que sólo se puede acceder a través de la consulta exacta dentro del contenido de alguna base de datos, por lo tanto para visitar una página no indexada por un navegador, es necesario conocer la dirección o ruta exacta del sitio en particular. Por lo tanto, según su criterio esta se puede comparar con un océano, donde existe información en la superfi-

cie a la que es fácil acceder y otra información que requiere un mayor esfuerzo para adquirirla y procesarla.

En ese orden de ideas, Vélez (2018) hace referencia a los diferentes usos que se le suelen dar a la Deep Web, resaltando que la web profunda no es sinónimo de ilegalidad, sin embargo, dentro de su universo se encuentra la denominada Dark Web (Red Oscura), constituida por páginas web que se han ocultado deliberadamente y que no pueden ser visitadas por navegadores convencionales para acceder a ellas. Además el dicho autor aclara que acceder a Deep Web no significa tener acceso inmediato a redes delincuenciales, simplemente se ingresa a espacios donde el usuario no es monitoreado y puede proteger su privacidad, puesto que el propósito de esta plataforma no es ocultar la venta de productos ilícitos, ni encubrir actos criminales, pero por tener la facultad de conservar el anonimato, muchos individuos o empresas se escudan en ella para dar rienda suelta a la publicación y mercadeo de productos y servicios de dudosa procedencia y origen ilegal.

Hablando de algunos beneficios, la Deep Web ofrece acceso a grandes bibliotecas mundiales, como la del Congreso de Estados Unidos y diverso contenido de carácter académico, información privilegiada sobre política de empresas, gobiernos y mercados financieros, páginas de Wikileaks que no se encuentran en la web global e información Top Secret, entre otros (Bergman, 2001); por esto último puede

representar algunos riesgos y amenazas orientados a la fuga de información afectando a una institución o incluso la seguridad de una nación, sin embargo, cuando se le da un buen uso allí se almacena gran cantidad de información que puede resultar de mucha utilidad al usuario ampliando sus conocimientos en distintos ámbitos incluyendo el naval y militar.

Con base en lo anterior, para el personal que labora y se instruye en la Escuela Naval de Cadetes “Almirantes Padilla” (ENAP) y demás escuelas de formación de la fuerza, resulta importante conocer conceptos básicos y parámetros para la navegación segura en la Deep Web, así como los riesgos a los cuales se pueden enfrentar cuando no se emplean los mecanismos de seguridad informática pertinentes, más aun, teniendo en cuenta que por su naturaleza de universidad los estudiantes y funcionarios de la misma deben hacer usos de equipos informáticos conectados a internet. Por consiguiente, el presente estudio pretende realizar una descripción detallada, sobre lo que significa navegar en la Deep Web, así como los ciber-riesgos y ciber-amenazas a las que los tripulantes de la ENAP se pueden enfrentar, cuando se cruza delgado límite que existe entre la red superficial y la red profunda, resaltando recomendaciones para una navegación segura en caso de ser requerida.

Metodología

En esta sección se describe el procedimiento adelantado para obtener una descripción detallada sobre la navegación en la Deep Web mencionando riesgos, beneficios, y aspectos de seguridad informática a tener en cuenta para evitar ataques cibernéticos o fuga de información, para ello, se empleó el tipo de investigación descriptivo que se centra en describir las maneras o formas en que aparece un fenómeno y evoluciona en el tiempo, aclarando dudas o vacíos en torno al tema (Hurtado, 2001).

Además, para obtener la información relevante y relacionada con el objeto de estudio se empleó la técnica de Revisión y Análisis Documental (Barbosa, Barbosa, & Rodríguez, 2013), de acuerdo a los siguientes pasos:

- Planificación y desarrollos de protocolos de búsqueda y revisión de fuentes de información.
- Extracción de datos haciendo uso de ficha de recolección de datos.
- Lectura, análisis, interpretación y comprensión crítica y objetiva, enmarcada de acuerdo al procedimiento de ordenamiento y manipulación de la información en sus fuentes; resumen de datos; escritura detallada de categorías y relaciones entre estas; refinamiento de la búsqueda de categorías centrales; y texto analítico final.

Posterior a esto se establecieron los siguientes ejes temáticos a desarrollar en los resultados del presente manuscrito:

- Historia de la Deep Web.
- Características de la Deep Web.
- Aspectos a tener en cuenta para navegar en la Deep Web.

Resultados

A continuación, se presenta la información recopilada en cada uno de los ejes temáticos seleccionados y su respectivo análisis:

Historia de la Deep Web

La historia del Internet se remonta al año 1969, cuando en los Estados Unidos se crea una red para uso militar exclusivamente, denominada “Arpanet”, con el objeto de que durante un posible ataque ruso, se tuviera acceso a la información militar desde cualquier lugar del país. Esta red inicial contaba con 4 ordenadores ubicados en distintas universidades del país, que dos años después se amplió a 40 ordenadores conectados entre sí. La red creció a tal punto que con el tiempo quedó obsoleta, lo que llevó a la creación del Protocolo TCP/IP, protocolo estándar de las redes informáticas que se sigue utilizando actualmente. Con el tiempo el “Arpanet” se fue abriendo y cualquier persona podía tener acceso a esta red, con fines académicos o investigativos, lo que obligó a

las fuerzas militares estadounidenses a crear otra red propia, a la cual denominaron “Milnet” (Delgado, 2018). Cabe mencionar que “Arpanet”, tenía como objetivo el intercambio de datos entre científicos y militares, llegando a su final en 1990 debido a que se unieron nodos que son los puntos de corrección para la transmisión de datos entre Europa y del resto del mundo (López, Valenzuela, & Zavala, 2016).

Posterior a esto, inicia en el año 1994 la red conocida como “Hidden Web” hasta 2001, cuando fue denominada con el nombre con el que hoy en día se conoce “Deep web”, la cual se inició como un proyecto militar con el fin de almacenar todo tipo de información sobre las organizaciones mundiales como el FBI, la CIA o la INTERPOL, con el fin de tener conocimiento acerca de qué estrategias militares

utilizaban y la forma en que ocultaban su identidad (Albarracín & Holloway, 2012). Desde un comienzo este proyecto pretendía ser secreto para así poder ser utilizado como una herramienta de espionaje, pero al pasar de los meses y las continuas innovaciones tecnológicas se perdió el control de toda esta información haciéndose pública en casi todo el mundo, sin embargo, las instituciones de autoridad no permitieron que mucha información estuviera al alcance de todos y decidieron ir eliminándola poco a poco de la red común, quedando relegada a la internet profunda (Ramírez, 2004).

Para entender un poco más la historia del origen de la Deep Web a continuación se presentan los hechos históricos más relevantes de la evolución del internet (Tabla 1):

Tabla 1. Historia y evolución del tecnológica de internet a nivel mundial

1967	EE.UU consigue conectar por vía telefónica dos ordenadores ubicados a miles de kilómetros
1969	Internet surge con la aparición de ARPANET (<i>Advanced Research Project Agency Net</i>), un proyecto militar diseñado para que las comunicaciones de los sistemas de defensa no se interrumpiesen, ni tan siquiera en el supuesto de un ataque nuclear.
1971	Se envía el primer mensaje electrónico.
1972	Cerca de 50 universidades se encuentran conectadas a ARPANET.
1974	Vinton Cerf junto con Bob Kahn publican “Protocolo para Intercomunicación de Redes de Paquetes”, donde se especifica el diseño del nuevo protocolo TCP-IP (<i>Transfer Control Protocol-Internet Protocol</i>)
1979	ARPANET crea la primera Comisión de Control de la configuración de la Red.
1981	Culmina el proceso de desarrollo y definición del Protocolo TCP/IP. En 1982 se adopta definitivamente como estándar.
1983	Como consecuencia, nace Internet con la interconexión de las redes ARPANET, MILNET y Csnet.
1985	Finaliza el desarrollo del protocolo para la transmisión de ficheros en Internet (<i>FTP, File Transfer Protocol</i>). Por esta época, también se crea el sistema de denominación de dominios (<i>DNS, Domain Name System</i>).
1989	El Laboratorio Europeo de Física de Partículas (CERN) desarrolla el concepto de World Wide Web (WWW) y el sistema de información hipertextual.
1993	La Universidad de Illinois distribuye gratuitamente Mosaic, el primer navegador que permite navegar por Internet, desarrollado por Marc Andersen. Comienza a funcionar el primer servidor Web en español.
1995	Se produce el gran boom de la Internet comercial.
1998	Nace Internet 2.
2000	Más de 300 millones de usuarios se conectan a Internet.

Fuente: Pérez, Frías, & Urueña (2018)

Teniendo en cuenta lo anterior, el origen de la web profunda se remite a un programa militar con fines específicos de intercambio y almacenamiento de información, el cual fue cambiando de naturaleza a lo largo del tiempo debido a la apertura de dicha plataforma a diversas personas del común; lo que contribuyó a los múltiples usos que se le da hoy día motivados por la preservación del anonimato de los usuarios, lo que se ha convertido en un factor determinante para que pululen actividades ilegales, propias de tratos entre desconocidos que no dejan huella en una transacción. En ese sentido, es posible mencionar que en el tiempo no se percibe un cambio significativo en tendencias para aprovechar las bondades propias de navegar en esta red, tales como acceso a múltiples bibliotecas a nivel mundial, ya que los gobiernos no tienen manera de controlar o regular este punto del ciberespacio que es aprovechado para facilitar la materialización de maniobras fuera de la ley, lo que lo convierte en caldo de cultivo que atrae a criminales más que a personal en búsqueda de información académica o científica.

Finalmente es relevante destacar que la Deep Web es utilizada más que todo en países donde no hay libertad de expresión y las personas se comu-

nican por medio de foros o blogs en la internet, utilizando este medio para realizar denuncias anónimas contra el gobierno o incluso investigaciones encubiertas (López, Valenzuela & Zavala, 2016).

Características de la Deep Web

La Internet se ha dividido en dos ramas: la Internet Superficial y la Internet Profunda. La Internet Superficial se compone de páginas estáticas o fijas, mientras que la Web Profunda está compuesta de páginas dinámicas (Figura 1). Las páginas estáticas no dependen de una base de datos para desplegar su contenido, sino que residen en un servidor a la espera de ser recuperadas y son básicamente archivos HTML, cuyo contenido no cambia, mientras que las páginas dinámicas se crean como resultado de una búsqueda de base de datos y se proporciona solamente cuando lo solicita el usuario. Se estima que la Web superficial representa un 5% de todo el contenido publicado, mientras que la Web profunda tiene un peso aproximado de un 95%. Además, que el tamaño de la web invisible es aproximadamente 500 veces superior a la web visible y consideran que los contenidos de calidad en la Deep Web multiplican entre 1000 a 2000 veces a los encontrados en la Web superficial (Bergman, 2001).

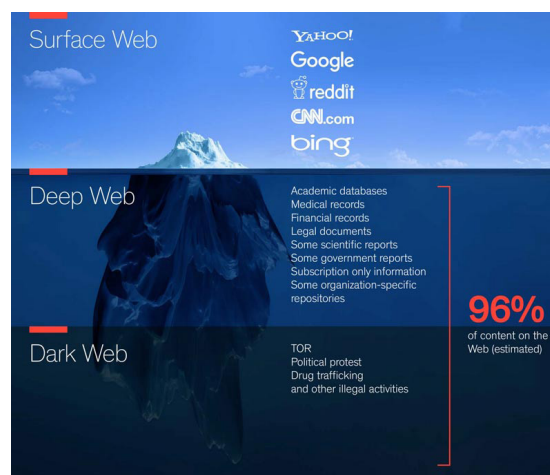


Figura 1. Ilustración de los contenidos de la internet superficial e internet profunda

Fuente: TheDarkWebLinks (2019)

De otro lado cabe anotar, que La web está dividida en niveles de información y seguridad, lo que quiere decir que a medida que se va indagando en su contenido se va haciendo cada vez más difícil avanzar. Los niveles más profundos

e inaccesibles corresponden a la Deep Web. En la Figura 2, se presenta una breve descripción de los niveles en que se divide la Web y lo que se puede encontrar en cada uno de ellos.

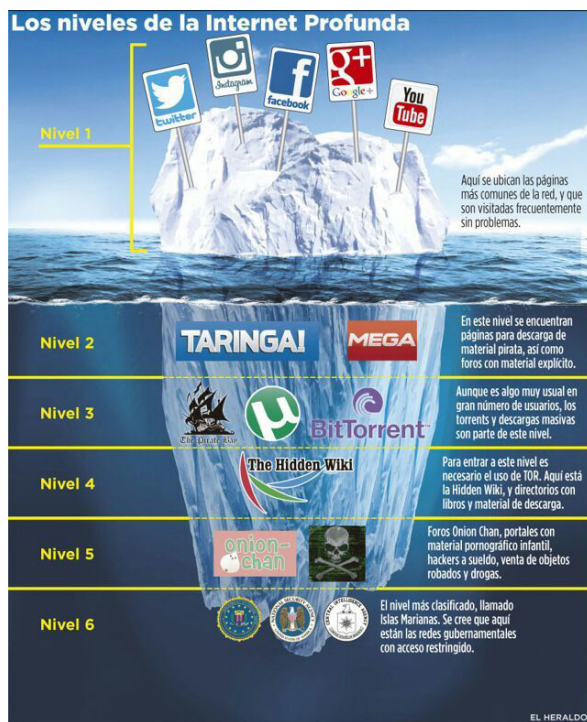


Figura 2. Descripción de los niveles de información de la Deep Web

Fuente: Mundo Secreto (2017)

Es importante resaltar también que el contenido que se puede encontrar en la Deep Web, según Bergman (2001) puede clasificarse en las siguientes categorías:

Contenido Dinámico: Corresponde a las páginas dinámicas que se devuelven en respuesta a una consulta enviada o se accede solo a través de un formulario, especialmente si se utilizan elementos de entrada de dominio abierto (como campos de texto); tales campos son difíciles de navegar sin conocimiento del dominio.

Contenido no enlazado: Son páginas que no están vinculadas a otras páginas, lo que puede impedir que los programas de rastreo Web accedan al contenido. Este contenido se conoce como páginas sin vínculos de retroceso (o enlaces).

Web privada: Son sitios que requieren registro y acceso (recursos protegidos por contraseña).

Web contextual: Páginas con contenido que varía según los diferentes contextos de acceso (por ejemplo, intervalos de direcciones IP de clientes o secuencia de navegación anterior).

Contenido de acceso limitado: Sitios que limitan el acceso a sus páginas de una manera técnica (p. Ej., Utilizando los encabezados HTTP de Pragma de Robots Exclusion Standard, CAPTCHAs o de no cache que prohíben que los motores de búsqueda los exploren y creen copias en caché).

Contenido de secuencias de comandos: Páginas accesibles sólo a través de enlaces producidos por JavaScript, así como contenido descargado dinámicamente desde servidores Web a través de soluciones Flash o Ajax.

Contenido no HTML / texto: Contenido textual codificado en archivos multimedia (imagen o video) o formatos de archivo específicos no manejados por los motores de búsqueda.

Tomando como referencia la investigación de Vilagarut y Carro (2004) con relación al contenido y cantidad de información que se encuentra en la Deep Web (Internet profundo) plantea que abarca el 85 por ciento del total de la red. De la misma manera se refiere a buscadores como Google, Yahoo y Hotmail, que solo pueden indexar 45000 millones de páginas, lo cual resulta poco en comparación de la infor-

mación que se encuentra en el internet oculto, que como se mencionó anteriormente se calcula que es 500 veces mayor. Existe un navegador adicional a los ya citados, que fue diseñado exclusivamente para permitir el acceso al Internet Profundo, el cual se denomina TOR, cuyo objetivo principal es la investigación y desarrollo de herramientas de privacidad en línea.

De otro lado, con el fin de realizar transacciones en la red profunda de forma segura y anónima se utiliza una moneda llamada Bitcoin, que corresponde a una divisa electrónica con características novedosas, destacada por su eficiencia, seguridad y facilidad de intercambio, con la cual se pueden comprar productos y servicios en todo el Internet en general, tanto en la Deep Web como en la Surf Web. El Bitcoin forma parte de una moneda e inclusive se ha introducido en la bolsa de cambio, pues ya está catalogada como una moneda influyente por todo el mundo. Por esta razón, la moneda Bitcoin no solo se usa en la Deep Web, sino que muchos sitios regulares aceptan este tipo de pago hoy en día, equiparándose con monedas como el Euro o el Dólar estadounidense, utilizada para intercambiar bienes y servicios (Batista, 2015).

Aspectos a tener en cuenta para navegar en la Deep Web

Para abordar este ítem es relevante abordar las ventajas y desventajas propias del uso de la Deep Web, en primera instancia en lo concerniente a las ventajas se precisa que hay gran cantidad de servicios que no son ilegales, ni lícitos, son solo sitios web donde las personas, las empresas o las entidades gubernamentales pueden guardar información de manera muy confidencial y restringida, además aquellos que les gusta pasar su tiempo libre recorriendo estos túneles subterráneos del internet, o de páginas para gente que se ve obligada a permanecer ahí porque viven bajo regímenes dictatoriales, debido a que es un lugar donde todo el mundo puede expresarse o acceder a la información de otros países sin temor a la censura o a represalias gubernamentales, lo cual resulta muy útil para periodistas y activistas de derechos humanos (Quisbert, 2014)

Teniendo en cuenta lo anterior para Zeballos (2017) estas son algunas de las ventajas o beneficios del uso de la Deep Web:

Acceso a libros censurados, por autores y páginas de internet regulares, debido a que la web profunda no admite censura.

Es una herramienta útil para el gobierno, debido a que permite monitorear crímenes, actividades ilícitas y terrorismo.

La web profunda contiene millones de documentos individuales, con 40 veces más capacidad de almacenamiento y 200.000 sitios más en comparación con la Web superficial.

Se puede navegar libremente, sin que se guarden los datos de las páginas visitadas y prevalece el anonimato, esto permite mejor el uso de la libre expresión sin riesgos.

Así mismo, como existen una serie de ventajas con el uso de la Deep Web, también se presentan múltiples desventajas en especial porque no se pueden rastrear a los usuarios de esta red, lo que permite que se incremente la mala utilización, adicionalmente, gracias a esta característica de anonimato se organizan y realizan actos ilegales, es por esto que la web profunda se considera un lugar sin fronteras físicas ni legales, donde se puede participar en actividades que serían censuradas y/o castigadas en el internet normal, dentro de las cuales según Garcia & China (2018) se resaltan:

Acceso a conocimiento Bélico, como las instrucciones para fabricar todo tipo de artefactos explosivos o armamento, así mismo procedimiento para armar bombas biológicas o agentes químicos.

Como no se conservan los derechos de autor, información como las patentes, prototipos industriales o secretos empresariales se hacen públicas sin ninguna restricción.

Los buscadores convencionales no pueden indizar su contenido, lo que dificulta la búsqueda de información; se debe instalar un buscador especial como podría ser TOR, o para dispositivos móviles ORBOT.

A través de esta red se comercializa con órganos vitales, personas, armas, todo tipo de drogas, infinidad de sitios que contienen pornografía infantil, contrato a sicarios secuestros, robos o asesinatos.

De otro lado, en lo concerniente al acceso al material que pertenece a la Deep Web no se realiza de forma común, como se accede a los demás contenidos del internet, para ello es necesario la utilización de una herramienta dif-

erente, como lo es la Red Tor (por sus siglas en inglés: The Onion Router) (Figura 3), la cual gestiona desde su propio paquete de software el acceso de forma anónima, debido a que esta oculta el origen y destino del tráfico de Internet, esta red ha estado en desarrollo durante muchos años, y ya es un producto maduro y estable, actualmente es gratuito y fue diseñado por la marina de los Estados Unidos como una red de servidores mundiales que permitían navegar de forma anónima (Chaparro, 2015).

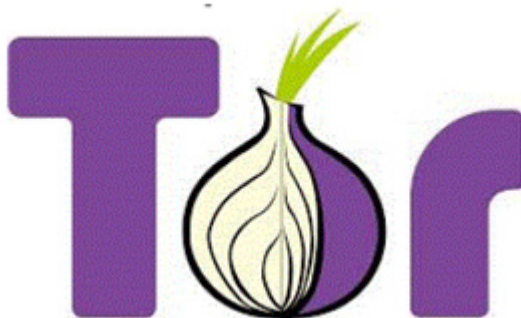


Figura 3. Logo oficial del navegador Tor

Fuente: Chaparro (2015)

Actualmente, la Red no solamente permite la navegación anónima sino que también permite alojar sitios ocultos y consta de más de miles de máquinas repartidas por decenas de países en todo el mundo, en estos se encuentran información de todo tipo, como bases de datos de agencias de inteligencia, disidentes políticos, mercados ilegales y sitios en los cuales se pueden comprar armas, drogas, órganos e incluso contratar asesinos, incluso se encuentran bases de datos de avances tecnológicos, publicaciones científicas y material académico en general. La forma más sencilla de usar Tor es descargar el paquete de navegación Tor Browser Bundle, para ello se debe utilizar el explorador de Firefox y es totalmente gratuita, posteriormente, se debe instalar Tor en el ordenador, es muy sencillo porque ya viene pre configurada y se observará un icono de una cebolla. Una vez descargado el paquete, el sistema lo descomprimirá automáticamente en la ruta donde haya sido descargado y para ejecutarlo únicamente se debe hacer click sobre el icono de la cebolla para que este inicie (Ruano, 2017). Como se describe el procedimiento no requiere ningún conocimiento técnico adicional y la herramienta está pensada para que cualquiera

pueda usarla sin demasiadas complicaciones.

Ya al estar inmerso en la Deep web en vez de Google o Yahoo se puede utilizar un navegador llamado DuckDuckGo; en vez de encontrar libros en Amazon, se encontrarán enciclopedias escaneadas, pero resulta necesario dedicar gran parte del tiempo a conocer usuarios internos los cuales facilitan enlaces, que permitan ir un paso adelante, que muestren y enseñen cómo mejorar la seguridad al momento de navegar. Para finalizar simplemente se cierra la aplicación, se recomienda desinstalar y borrar todo rastro: aplicación, datos del proxy y, en el caso de querer volver a entrar, repetir todo el proceso desde el primer paso.

Además del buscador en mención es posible encontrar diversos motores de búsqueda que cumplen la misma función, por lo tanto a continuación se detallan los más utilizados y conocidos según lo planteado por Vicente & Guillen (2015)

Onion City: Es un sencillo motor de búsqueda capaz de indexar las páginas “.onion” de los servicios ocultos de TOR, este no

encripta información ni protege a los usuarios de los riesgos del uso de esta web, actualmente cuenta con 65.000 páginas.

Memex: La Agencia de Proyectos de Investigación Avanzados de Defensa de Estados Unidos o DARPA desarrolló un motor de búsqueda llamado Memex, el cual es capaz de indexar las páginas más ocultas de la deep web, fue creado para combatir el crimen y las actividades ilícitas de esta parte de internet, este motor permite rastrear millones de páginas invisibles para otros buscadores y organiza la información por temas y dominios, cuenta con mejor capacidad de búsqueda que Onion.

The Hidden Wiki: Este motor es bastante potente permite incluso realizar búsquedas en la Dark Web, también se considera in túnel de salida de la deep web, actualmente cuenta con páginas que se actualizan diariamente y brinda servicios financieros, comerciales, de anonimato y seguridad, de hosting, blogs, foros, correo, mensajería, activismo político, secretos de estado, libros.

Torch: Es un motor que trabaja muy parecido a Google, pero en esta parte de internet, es muy

sencillo de utilizar, solamente se introduce una palabra clave de lo que se desea consultar.

Grams: Es un motor que se utiliza para búsquedas de mercados negros, es igualmente sencillo de utilizar como el anterior.

Como se abordó en el desarrollo de este inciso, son muchos los aspectos a tener en cuenta para llevar a cabo una búsqueda segura en la Deep Web, que van desde el conocimiento de las ventajas y desventajas del proceso, hasta el cuidado que se debe tener a la hora de seleccionar un navegador que permita acceder al contenido de manera segura evitando un hackeo o fuga de información, sin embargo, todas estas recomendaciones son inútiles si el usuario navega de manera irresponsable por este espacio virtual, de allí la relevancia de hacer una apropiación adecuada del conocimiento en relacionado con cada una de las características y usos de web profunda, para de esta manera tener claro a qué información se puede acceder sin estar violando alguna normativa o ley, este es un principio básico que sin duda alguna aplica también para la navegación en la red superficial.

Conclusiones

Durante la fase de recopilación de información fue posible evidenciar que los artículos académicos que abordan el tema de estudio conforman una minoría al realizar búsquedas en bases de datos reconocidas como Scielo, Dialnet, Google Scholar, Pubindex entre otras, por lo tanto la mayor parte de la información acerca de la Deep Web se encuentra centralizada en otro tipo de medios tales como Blogs, Artículos de Periódicos, y trabajos de grados, en ese orden de ideas, el presente trabajo constituye un aporte base para la familiarización con este tipo de tema en las escuela de formación de la Armada.

De otro lado, son muchos los mitos que surgen alrededor del uso de la Deep Web, los cuales tienen origen en el anonimato que ofrece esta red a sus usuarios lo que facilita el planeamiento y ejecución de delitos, sin embargo, hay que anotar que la Web profunda no fue concebida para tal fin, por lo tanto con el uso adecuado puede constituir una herramienta novedosa para el levantamiento de información orientado al desarrollo de trabajos académicos.

Referencias

- Albarracín, P., & Holloway, C. (7 de Noviembre de 2012). *Aetecno*. <https://tecno.americaeconomia.com/articulos/deep-web-las-oscuras-profundidades-de-internet-que-ya-preocupan-gobiernos>
- Barbosa, J. W., Barbosa, J. C., & Rodríguez, M. (2013). Revisión y análisis documental para estado del arte: una propuesta metodológica desde el contexto de la sistematización de experiencias educativas. *Bibliotecológica*, 83-105.

- Batista, D. (2015). Deep Web: Aproximaciones a la ciber irresponsabilidad. *Revista Latinoamericana de Bioética*, 26-37.
- Becerra, J. (2 de 10 de 2018). *Seguridad Cultura de prevención para TI*. <https://revista.seguridad.unam.mx/numero-20/mitos-y-realidades-de-la-internet-profunda>
- Bergman, M. (1 de Agosto de 2001). *the journal of electronic publishing*. <https://quod.lib.umich.edu/jjep/3336451.0007.104?view=text;rgn=main>
- Chaparro, H. (2015). *Universidad de Buenos Aires, Biblioteca Digital*. http://bibliotecadigital.econ.uba.ar/download/tpos/1502-0885_ChaparroZunigaHD.pdf
- Delgado, H. (30 de Noviembre de 2018). *Akus.net*. <https://disenowebakus.net/historia-y-evolucion-de-internet-introduccion.php>
- Diario La Opinión de Murcia. (15 de Marzo de 2016). *Deep Web, el lado oscuro de la Red. Semana Tecnológica*. <http://www.laopiniondemurcia.es/vida-y-estilo/tecnologia/2016/03/15/esconde-deep-web-trafico-organos/721915.html>
- García, V., & China, J. (31 de Diciembre de 2018). *Openaccess*. <http://openaccess.uoc.edu/webapps/o2/bitstream/10609/88545/7/jcotssTFM0119memoria.pdf>
- Gay, J. (2015). *Deposito de investigación Universidad de Sevilla*. <https://idus.us.es/xmlui/handle/11441/29281>
- Hurtado, J. (2001). *Metodología de la investigación holística*. Caracas: SYPAL.
- López, L., Valenzuela, M., & Zavala, E. (26 de Mayo de 2016). *In Slide Share*. <https://www.slideshare.net/leone11a12/doc-deepweb-2>
- López-Barbera, M. (2014). Deep Web o Internet Profundo. *Seguritecnia*, 96.
- Mundo Secreto. (20 de enero de 2017). *Amino*. https://aminoapps.com/c/mundosecretooficial/page/blog/entrar-a-la-deep-web-oscura-explicado/8Bmw_jmrImujREkXIKXXZ7DxrMkbqlbBPxV
- Pérez, J., Frías, Z., & Urueña, A. (2018). *La evolución del internet en España: Del Tesys a la economía digital*. Madrid: Red.es.
- Ramírez, A. (2004). Una visión al mundo de la búsqueda y recuperación de la información electrónica. *Revista Lasallista de Investigación*, 117-122.
- Ruano, M. (2017). La red Tor como elemento de privacidad en nuestras vidas. *Seguridad Cultura de Prevención Para Tí*, 13-17.
- TheDarkWebLinks. (22 de agosto de 2019). *TheDarkWebLinks*. <https://www.thedarkweblinks.com/what-is-the-deep-web/>
- Vélez, C. (5 de 11 de 2018). *Instituto de Ingeniería de la UNAM*. <http://www.iingen.unam.mx/es-mx/Publicaciones/CapsulasdeTI/Docs/CapsulaTI21LaRedProfunda.pdf>
- Vicente, J., & Guillen, V. (2015). *Pontificia Universidad Católica del Ecuador Repositorio de Tesis de Grado y Posgrado*. http://repositorio.puce.edu.ec/bitstream/handle/22000/11982/Disertacion%20de%20grado%20Guillén%20Vicente_Final.pdf?sequence=1&isAllowed=y
- Zeballos, C. (21 de Febrero de 2017). ¿Qué es la Deep Web? Ventajas y desventajas de navegar en la red profunda, *Walac*. <https://walac.pe/que-es-la-deep-web-ventajas-y-desventajas-de-navegar-en-la-red-profunda/>