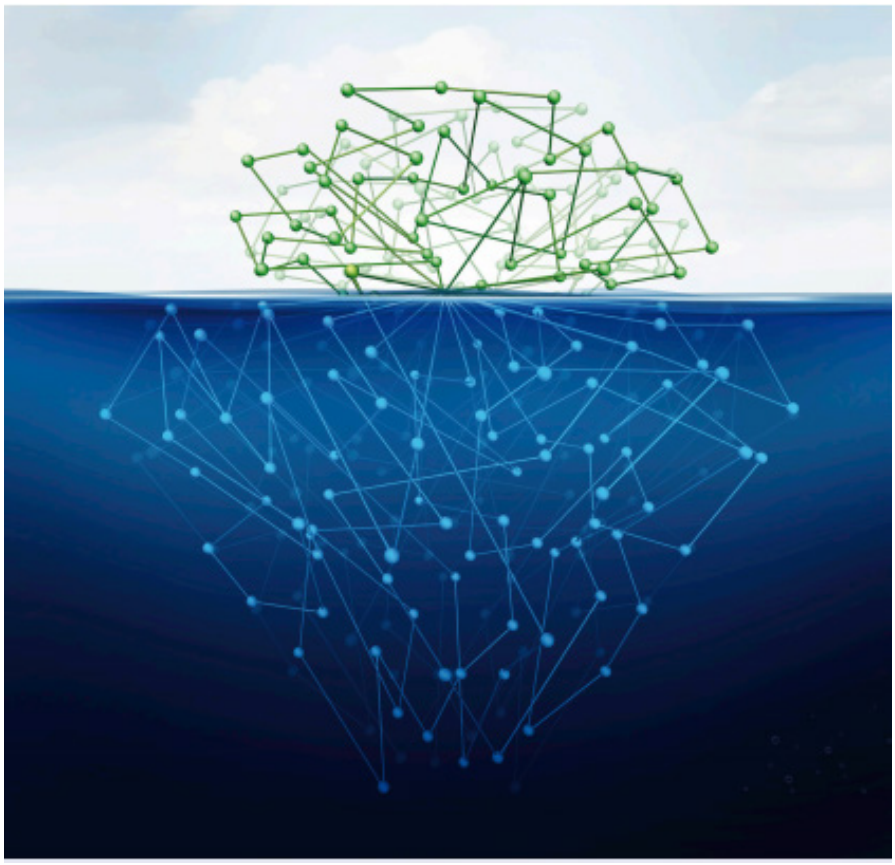
# *Deep Web*: El lado oscuro de la Internet

**Luis Antony Hurtado**
Estudiante del Programa de Ingeniería de Sistemas
Universidad Mariana

**Nancy Cristina Legarda López**
Docente del Programa de Ingeniería de Sistemas
Universidad Mariana



**Resumen**

Antes de abordar el tema de la *Deep Web* o internet profunda, es necesario saber que las páginas visitadas cada día en la Internet, por diversos usuarios, pertenecen a la surface web "web superficial", entre ellas se encuentran Google, eBay, Facebook, YouTube, y otros tantos miles de sitios de la Internet. La otra cara oculta de la red es la *Deep Web*, desconocida por muchos de los usuarios, es visitada por *hackers,* quienes de manera fraudulenta utilizan la Internet para robar información e introducir virus para destruir los datos personales de los usuarios en los ordenadores. También es empleada por los agentes del gobierno para obtener información de delincuentes y de procesos delictivos. En los últimos años ha sido utilizado por personas de altos cargos militares para la obtención de información y posterior captura de ciberdelincuentes.

De igual manera, la *Deep Web* es empleada por varios usuarios en la publicación o búsqueda de información ilegal o parcialmente ilegal. La Internet profunda también es empleada para otras actividades ilícitas, como la creación de páginas *web* para la venta o subasta de órganos humanos, drogas, armas, elementos robados, asesinatos, trata de personas, secretos corporativos, información clasificada de los gobiernos, etc.

**Palabras clave***: Deep Web,* ilegalidad, información, Internet, peligros.

## Introducción

La Internet fue creada para compartir información, pero muchos usuarios desconocen o ignoran el lado oscuro que está posee, en la zona llamada *Deep Web* o Internet profunda se realizan un sinfín de prácticas ilícitas, donde se comercializa desde personas hasta información corporativa o gubernamental, pasando por la compra y venta de drogas, armas, animales en vía de extinción, órganos humanos, entre otros elementos ilegales (Murillo y Diaz, 2018).

La *Deep Web* se originó en Estados Unidos, e irónicamente fue creada por la Fuerza Armada de este país, como un elemento de prueba para el rastreo de las operaciones realizadas por los delincuentes, pero sus fines originales fueron distorsionados; ya que esta sección de la Internet fue aprovechada por los delincuentes como un medio para difundir sus actividades ilícitas (Vitola, Mendoza, Rosero y Romero, 2020).

Actualmente, en la *Deep Web* se puede encontrar todo tipo de información ilegal o parcialmente legal, constituyéndose en el sitio de preferencia por parte de los *hackers*, asesinos, traficantes de personas y órganos, así como de quienes comercializan con drogas, armas, elementos robados, secretos corporativos, documentos gubernamentales, terrorismo mundial (Murillo y Diaz, 2018).

## Niveles de la internet

La Internet es considerada como la "Red de Redes", porque es una red que conecta a varios ordenadores entre si, a tal punto que la gran mayoría de hogares, instituciones educativas, fabricas, bancos, sedes gubernamentales y empresas en el mundo poseen uno o varios dispositivos electrónicos conectados a la misma. La Internet se emplea para compartir información con otros usuarios, pero existe la otra cara de la moneda, donde la red de redes ha sido utilizada por algunos usuarios para compartir información sobre diversos tipos de actividades ilícitas.

Además, al ser la internet un medio para intercambiar información, ha sido denominada por muchos como la "Autopista de la Información", aunque es difícil establecer el alcance al cual ha llegado, se estima que su crecimiento ha sido constante y de forma exponencial, en el año 2005 existían 11.500 millones de páginas web y en el año 2008 ascendieron a 63.000 millones (Pinto y Gonzáles, 2016). La cuestión es que no todos estos nuevos sitios de la internet son legítimos.

Por otro lado, cuando un usuario ingresa a la Internet a consultar cualquier tipo de información, lo hace a través de un buscador, el cual emplea motores de búsqueda denominados arañas, pero las mismas no llegan a cierto tipo de páginas, por encontrarse en la sección denominada Internet profunda, que es la zona oscura de la Internet.

En otras palabras, en las secciones de Internet, donde los usuarios pueden ingresar con libertad y sin limitaciones de búsqueda, se le ha dado el nombre de *web* superficial, porque hace referencia a que las personas navegan o surfean en la sección superficial de la Internet. Por el contrario, el termino correcto en la *Deep Web* no es navegar sino bucear, porque los usuarios que ingresan a esta zona de la Internet se mueven en un submundo más oscuro e ilegal, por tanto, requieren de la dirección exacta del sitio al cual desean acceder, que, por lo general, suelen estar encriptadas (Toro, 2019).

Pero no todo es blanco y negro, incluso en la Internet existe niveles de legitimidad en la *web* superficial, hasta llegar a las páginas más encriptadas y ocultas de la Web, los niveles que se encuentran entre estos dos extremos se conocen como:

**Nivel 1, Surface Web:** Es la parte superficial de la Internet, donde se encuentran los buscadores más empleados y conocidos como Google, Facebook, You Tube, entre otras, muchas páginas.

**Nivel 2, Bergie Web**: En este nivel se puede encontrar todo tipo de páginas con un menor grado de legitimidad, por ejemplo, páginas pornográficas, la comunidad 4chan, que inicialmente fue creada como un foro para los aficionados del anime y la cultura japonesa, servidores FTP y comercialización de drogas licitas.

**Nivel 3, *Deep Web*:** Este nivel se caracteriza por su contenido sexual y violento, encontrando pornografía infantil, películas y material Gore o Splatter conformado por elementos de terror sangriento y violento. En este nivel también se mueven todo tipo de *Hackers,* militares, creadores de virus y troyanos. Para acceder a esta zona de la Internet es necesario contar con un proxy, además los diseñadores de estas páginas web suelen encriptarlas.

**Nivel 4, Charter Web:** Este nivel hace parte de lo más profundo y oscuro de la *Deep Web*, y es conocido como el mercado negro de la Internet, porque los usuarios pueden comprar y vender drogas, sexo, armas, órganos humanos, libros o videos prohibidos y elementos robados. Además, es en esta zona de la web que se encuentran los asesinos asueldo y el tráfico de personas. Cabe aclarar que es el nivel más profundo al cuál no puede llegar un usuario común.

**Nivel 5, Marianas Web:** El nombre de este lugar hace referencia a la Fosa de las Marianas, un sitio en lo profundo del océano al cuál no se ha podido llegar, y es exactamen-te lo que el nivel 5 representa. Se cree que es contralado por el gobierno y, por tanto, en la zona Marianas se puede encontrar todo tipo de armas, incluyendo las nucleares, información de Ovnis, secretos gubernamentales y económicos, esta es una zona en la que nadie debe ingresar (Toro, 2019).

**Características y Funcionamiento de la *Deep Web***

No es fácil ingresar a la *Deep Web*, porque en la misma existen múltiples niveles de seguridad por medio de en criptaciones, como las siguientes:

**URL en la *Deep Web***: Las URL en esta zona de la Web son archivos denominados "no textuales", compuestos por elementos de multimedia, gráficos, imágenes y/o software portable; por ejemplo, una URL tradicional debe com-ponerse por las siglas WWW (Word Wide Web) seguidas por el nombre de la página y la terminación .com, de esta manera: www.nombre de la pagina web.com; pero en la *Deep Web* el formato de las direcciones de las paginas son así: bdf68sd-fy235nusdfguorrtbjo45u9.onion (Valen-cia y Hoyos, 2019).

**Dominio de la URL en la Deep Web:** La zona oscura de la Internet es aquel mercado negro donde se comercializa todo tipo de artículos ilícitos, por lógica no maneja un comercio abierto, por lo cual no emplea la terminación .com sino la extensión .onion.

**Bases de datos:** Los programadores de la Deep Web emplean programas como Oracle, SQL, Access, MySql., entre otros, que solicitan el permiso del creador de la página para que el usuario pueda acceder a la misma, este pase de ingreso puede ser gratis o pagado, pero el fin del mismo es limitar el acceso de los usuarios a las páginas.

**Navegadores**: Los navegadores convencionales como Google Chrome, Internet Explorer o Firefox no están diseñados para hacer búsqueda de páginas en la *Deep Web*, porque las URL son diferentes, ello implica que los usua-rios deben recurrir a buscadores especializados.

¿Se puede tener un perfil anónimo en Deep Web?

Aunque la red de *Deep Web* permite tener un nivel de anonimato este no es total, porque la presencia de hacker en esta zona de la Internet son especialistas en el tema y pueden eliminar cualquier nivel de seguridad o encriptación utilizada por el navegador. Para mantener su anonimato, los usuarios que ingresan a la *Deep Web* suelen utilizar el software TOR, que es un proxy empleado para cambiar la dirección IP, incluso algunos usuarios emplean un portable del mismo en una memoria USB, con el fin de mejorar la seguridad y anonimato del equipo y del usuario (Valencia y Hoyos, 2019).

¿Cómo se puede lograr el acceso a la Deep Web?

La *Deep Web* es utilizada para hacer actividades ilícitas, pero aun así solo una parte de su gran contenido está conformado por páginas que requieren que el usuario ingrese de forma anónima, porque incluso en la zona oscura de la Internet existe una parte "inocente", donde solo es de tipo informativo, para las que no lo son, los usuarios emplean motores de búsqueda temático que son especializado en determinados temas.

Por otro lado, si el usuario desea entrar a la zona más profunda de la *Deep Web* es conveniente que utilice programas que oculten su identidad, por ejemplo, el programa Tor que permite bucear en la *Deep Web* manteniendo siempre el anonimato.

**Recomendaciones**

Si alguien desea bucear en la *Deep Web* es necesario que tenga en cuenta las siguientes recomendaciones:

***Ilegalidad***: En muchos países es ilegal ingresar a la zona de *Deep Web*, por tanto, el usuario debe conocer primero si está actividad es penalizada por las leyes de su país. De todas formas, es siempre recomendable que el usuario tome precauciones para no ser rastreado.

***Evitar ciertas páginas***: En la *Deep Web* existen sitios en los que se comercializa con pornografía infantil y si las au-

toridades rastrean a los visitantes de las mismas ello implicará muchos años de prisión, para evitar esta situación es recomendable no ingresar a las páginas que tengan la referencia pedoBear.onion, hardCandy.onion o pr0n.onion, infantil.onion.

***No hacer descargas***: Al descargar información de la *Deep Web* se corre dos riesgos: el primero, que se rastree al usuario que lo está haciendo y el segundo, que también se descargue un troyano o virus con el archivo descargado, lo que conlleva a la pérdida o robo de la información personal del usuario contenido en su ordenador. Evitar los markets, a menos que se busquen drogas, órganos, trata de personas, etc.

***No tener amistades***: En la *Deep Web* hacer amigos es algo peligroso, por ello, siempre se debe tener un perfil bajo, siendo inadvertido.

***Cuenta Personal***: No es recomendable utilizar la cuenta del correo electrónico, porque es una forma de rastrear a los usuarios, así mismo, no se debe registrar en ningún sitio de la *Deep Web*, ni tampoco activar plugins (Valencia y Hoyos, 2019).

## Conclusiones

Los usuarios que navegan en la Internet suelen desconocer que hay una zona oculta en la misma, en la cual existe un sinfín de páginas enfocadas en actividades ilícitas e ilegales y aquellas personas que saben de su existencia no suelen ingresar, porque piensan que las mismas son de carácter inmoral. Es justamente por estas referencias que se la nombra como la Internet profunda, oscura o *Deep Web*.

Además, en la *Deep Web* se sabe que se comercializa todo tipo de elementos, todos ilegales, porque se compra y vende desde información hasta personas, pasando por armas, drogas, elementos robados, información gubernamental y empresarial.

La cuestión es que en esta zona de la Internet también se encuentran los hackers, acosadores, asesinos, traficantes de órganos y de personas, militares, pedófilos, acosadores; en pocas palabras, la lacra de la sociedad; por tanto, si un usuario desea bucear en la *Deep Web*, debe estar consciente de que puede ser rastreado por cualquiera de los delincuentes mencionados anteriormente y, por ende, puede correr un gran peligro.

## Referencias


Murillo, F. y Díaz, D. (2018). Internet profundo. *Ciencias de la Ingeniería y aplicadas, 2*(19), 16-28.

Pinto de la Fuente, M. y Gonzáles, B. (2016). Séptima encuesta de acceso, usos y usuarios de internet. Informe Final. Recuperado de https://www.subtel.gob.cl/wp-content/uploads/2015/04/Informe-VII-Encuesta-de-Acceso-Usos-y-Usuarios-de-Internet_VF.pdf

Toro, A. (2019). La web profunda, un sitio entre sombras y realidades. *Ventana Informática, 39*, 53-84. Doi: https://doi.org/10.30554/ventanainform.39.3311.2018

Valencia, A. y Hoyos, A. (2019). Una mirada a las profundidades de la DEEP WEB FreeNet. *Tecnología en Sistemas de Información*, 1-13

Vitola, M., Mendoza, C., Rosero, A. y Romero, J. (2020). Conociendo la *Deep W*eb: un acercamiento inicial para minimizar riesgos informáticos en entornos académicos. *Anfibios, 3*(1), 68-77. https://doi.org/10.37979/afb.2020v3n1.64