PONTIFICIA UNIVERSIDAD CATÓLICA DEL ECUADOR
FACULTAD DE INGENIERÍA
ESCUELA DE SISTEMAS

DISERTACIÓN DE GRADO PREVIA A
LA OBTENCIÓN DEL TÍTULO DE INGENIERO EN
SISTEMAS Y COMPUTACIÓN

"GUÍA METODOLÓGICA DE USO SEGURO DE INTERNET PARA PERSONAS Y EMPRESAS UTILIZANDO LA RED TOR"

NOMBRES:

Javier Andrés Vicente Alarcón

Verónica Cristina Guillén Guillén

DIRECTOR:

Msc. Luis Alberto Pazmiño Proaño

QUITO, 2015

TABLA DE CONTENIDO

RESUMEN

La palabra internet es un anglicismo que se forma de la abreviación del término en inglés International Network of Computers, en español se traduce como Red. Se trata de una composición de redes conectadas entre sí, mediante distintos medios. El internet es una red que nos permite tener una conexión a través de protocolos como el TCP/IP.

Con la llegada del internet, se abren las posibilidades al mundo entero, pero esto también abre la posibilidad a la vulnerabilidad de información. Los ciberataques es toda acción ilegal que tiene como meta causar daño en la información de las personas o empresas.

Como existen ataques, también hay formas de protegerse de estos actos. La ciberseguridad, es el conjunto de conceptos de seguridad, buenas prácticas, directrices, métodos para proteger la información de una organización o de un usuario. Otra definición, puede ser que la ciberseguridad es la ausencia de amenazas por medio de tecnologías de la información.

Las buenas prácticas al momento de navegar en el internet, permiten que se mantenga de manera segura. También depende mucho del usuario para que tenga una cultura de navegación segura.

La mayoría de usuarios que navegan diariamente por Internet, desconocen que existe un mundo virtual paralelo, ya que lo hacen mediante páginas habituales o utilizan buscadores estándar como Google, Yahoo!, etc., obteniendo aquello que los interese, ya sea información, productos, servicios o redes sociales. Llegando a decir hasta incluso que "Si no existe en Google, no existe en ningún lado". Detrás de todo esto, existe un mundo virtual oculto, donde se debe mantener una mente muy abierta asimilando el contenido que uno se puede topar dentro del mundo oscuro, a esto se lo conoce como Deep Web.

La Deep Web (Internet Profunda) o Invisible Web (Internet Invisible), se define como contenido web no indexado por motores de búsqueda, donde se puede encontrar todo lo que se pueda imaginar, es una porción sumamente grande de la internet, contiene páginas,

información, documentos, etc. que se encuentran desarrollados de tal forma que es imposible descifrar. Su estructura hace que su rastreo se dificulte. Mucho de la Deep Web es temporal: al consultar una base de datos se genera páginas dinámicas. Lo que se realice dentro de la Deep Web se lo hace mediante anonimato, no puede asociarse con la identidad del usuario que navegue por la web profunda.

Dentro de la Deep Web la información que se encuentra es privada, confidencial y en muchos casos llega a ser ilegal, ya que llega a ser usada mayormente por pederastas, amparados por el anonimato, llegan a hacer un mal uso dentro de este mundo oscuro. El pago de las compras que se deseen realizar dentro de la Deep Web se realiza mediante “bitcoins (moneda electrónica anónima, independiente e inconfiscable)”, son monedas simbólicas que no están registrados por ningún instituto económico de emisión central.

Para adentrarse al lugar más oscuro e invisible de Deep Web se lo hace a través del Onionland (también denominada Darknet.). Aquí se encuentran páginas bajo dominios “.onion”, estos dominios se encargan de no divulgar las URL, ni revelar el título del contenido en la dirección web. Para acceder a la Deep Web existen redes anónimas, motores de búsqueda que nos permiten navegar con facilidad.

La red Tor llamada así por sus siglas "The Onion Router" o dicho en español El Encaminamiento/Enrutamiento de Cebolla. Es un proyecto cuyo objetivo principal es el tener una comunicación privada a través de una red pública. Hablaremos de su uso, funcionalidad, velocidad y los proyectos realizados con la red Tor.

La investigación de una empresa residente en Ecuador que hace uso de la red Tor para fines netamente empresariales.

El principal objetivo del uso de la red Tor es que cualquier persona pueda utilizar esta herramienta y tenga acceso a toda la red. Para lograr este objetivo, TOR desarrollo un software que funciona de forma sencilla y agradable al usuario: “Tor Browser”.

Una guía metodológica dará a conocer los debidos pasos que se deben realizar para el uso de la red Tor, instalación del “Tor Browser”, herramientas, ventajas y desventajas que representó al usar “Tor Browser” y sus aplicaciones.

INTRODUCCIÓN

El uso de internet por parte de los usuarios se ha masificado en los últimos años, la gran demanda que ahora se ha generado, ha hecho que la tecnología evolucione para que podamos conectarnos al internet en cualquier parte del mundo.

La mayoría de usuarios están acostumbrados a navegar por la web a través de buscadores estándar como son Google, Yahoo!, Bing, etc., realizan consultas, manejan cuentas, se conectan y contactan con personas o clientes, realizan intercambios, compras, ventas, acuerdos que en mayores casos son legales como ilegales, tienen la oportunidad de denunciar casos fraudulentos o estafas realizadas, utilizar redes sociales o páginas que conllevan a tener mucha seguridad, pero a pesar de su seguridad corren un alto riesgo de que se comentan ataques, robo de información, suplantación de identidad, hackeos, etc.. Existe una serie de consecuencias negativas al momento de navegar por la red. Los usuarios no toman en cuenta la importancia de proteger su información frente a cualquier debilidad al momento de navegar, teniendo una vulnerabilidad de información considerada como privada. La inseguridad del internet es visto como una oportunidad de extraer información, haciendo que la información sea usada de manera mal intencionada para atacar la integridad, disponibilidad y confidencialidad de la información de las empresas y personas.

Para tener en cuenta de todo lo que abarca el internet, llegaremos a conocer que solo el 4% del total usuarios que navegan diariamente alrededor del mundo hacen uso del internet con buscadores tradicionales; pero qué hay del 96% restante? Pues la respuesta es, que el navegar por el internet va más allá de lo que el mundo está acostumbrado a ver, existe un mundo paralelo llamado “Deep Web”, este mundo está esperando que sea descubierto. La navegación anónima nos permite evitar que sepan quienes somos. Pero como funciona la red Tor? La red usa un diseño con puntos de introducción y de encuentro. En vez de ir de un punto A hacia B, usa una red de nodos, una especie de túnel formado por varios nodos.

Para poder descubrir el mundo de la Deep Web, nos hemos planteado realizar una guía metodológica utilizando la red “TOR (The Onion Router)”. El objetivo de esta guía es aprender a usar la herramienta del proyecto de Tor para poder navegar por la Deep Web.

En la guía se hará mención a la instalación de la herramienta “Tor Browser”, que nos servirá para conectarnos a la Deep Web. Cabe recalcar que la identidad de los usuarios va a ser protegida ya que el navegador usa la red Tor para navegar por la Deep Web.

Para realizar todo esto existen links con dominios “.onion”, que tienen como fin ser un medio para el uso de: emails, mensajería, redes sociales, hosting de archivos, hosting de imágenes, hosting de texto, etc.; que se encargan de mantener la confidencialidad del usuario y su anonimato.

No se puede considerar que todo lo que se realice dentro de la red Tor es segura y anónima. Como en el internet, se corre riesgos de que se llegue a cometer un delito o perdida de información debido a que se ingresa a páginas que no deberían ser consultadas por personas o empresas que buscan un fin adecuado. O por el desconocimiento de la información que se está accediendo, se debe tener en mente que el uso de esta información es responsabilidad de quien la usa.

0. ANTECEDENTES

0.1. Internet

0.1.1. Definición

La palabra internet es un anglicismo que se forma de la abreviación del término en inglés International Network of Computers, en español se traduce como Red

Internacional de Computadoras. Se trata de una composición de redes conectadas entre sí, mediante distintos medios. El internet es una red que nos permite tener una conexión a través de protocolos como el TCP/IP.

Figura 0.1 Red de Computadores (TKM, 2015)

Esta red de computadores es el resultado de un experimento del Departamento de Defensa de los Estados Unidos, en el año de 1969. El objetivo de este experimento era poner tener un intercambio entre datos de la nación. Consecutivamente se unieron países de Europa Asia y el resto del Mundo. Este intercambio de información tuvo el nombre de ARPAnet.

El ARPAnet (Advanced Research Projects Agency Network por sus siglas en inglés) tenía como fin interconectar cada computadora para uso como medio de comunicación entre los diferentes organismos nacionales estadounidenses. En la Universidad de California en Los Ángeles se creó el primer nodo de esta red. Y dio como resultado a la espina dorsal de Internet hasta 1990, tras finalizar la transición al protocolo TCP/IP, iniciada en 1983.

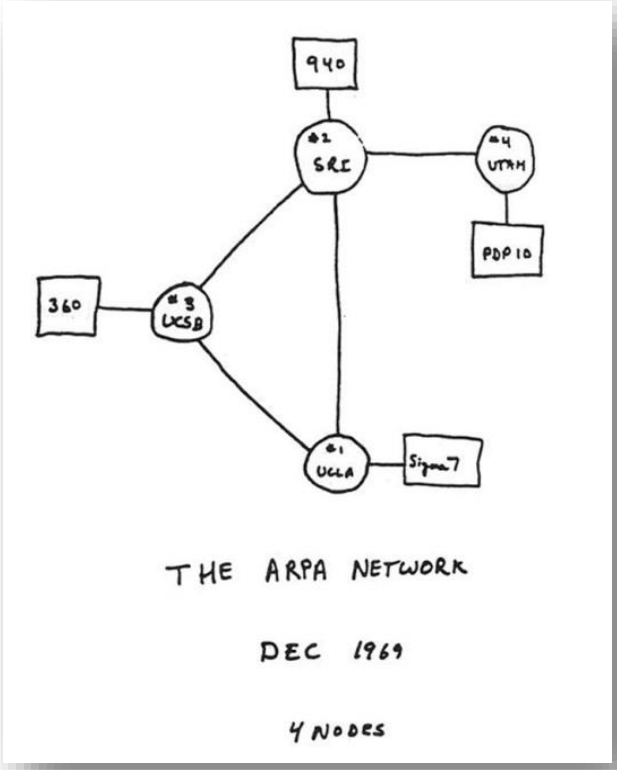

Figura 0.2 Esquema básico de la red Arpa en 1969 (Sánchez, 2015)

El internet se ha convertido en una herramienta importante en nuestra sociedad debido al gran potencial que se tiene. Con el internet nos podemos comunicarnos, nos permite búsqueda y transferencia de información a tiempo real.

0.1.2. Historia

La historia del internet se da temprano en el desarrollo de las redes de comunicación. La idea que se tuvo es que se tenga una red de ordenadores diseñara para permitir la iteración genera entre varios usuarios de computadores.

Los inicios de las primeras iteraciones hechas por una red de computadores se dan en agosto de 1962. Estos acontecimientos están registradas en escritos realizados por J.C.R Licklider, en los cuales analiza sobre la red Galáctica.

> “El proyecto de Licklider en el fondo era muy similar a la Internet de hoy en día. Licklider era el director del programa de investigación informática de DARPA, que comenzó en octubre de 1962. Mientras estaba en DARPA convenció a sus sucesores en dicha agencia (Ivan Sutherland, Bob Taylor y Lawrence G. Roberts, investigador del MIT), de la importancia de su concepto de red. Uno de los objetivos más objetivos del proyecto fue que las maquinas interacción entre sí. Para esto, en 1995, se trabajó con Thomas Merril. Roberts conectó el TX-2 con el Q-32, mediante una línea de telefónica conmutada de baja velocidad, creando la primera red de área amplia del mundo.” **(Leiner, 2012)**.

Este experimento dio el inicio a lo que ahora llamamos como internet.

> “A finales de 1966, Roberts entro a DARPA para implementar y desarrollar redes informáticas. Con el pasar del tiempo creó su plan para “ARPAnet”. En la conferencia en la que presentó el artículo había otra ponencia sobre el concepto de redes de paquetes, que venía del Reino Unido, de la mano de Donald Davies y Roger Scantlebury, del NPL. Scantlebury le comentó a Roberts el trabajo del NPL y el de Paul Baran y otras personas de RAND. El grupo RAND había escrito un artículo sobre redes de conmutación de paquetes para cifrar comunicaciones de voz en el ejército en 1964. La labor del MIT (1961-1967), de RAND (1962-1965) y del NPL (1964-1967) se había llevado a cabo en paralelo sin que los investigadores conociesen el trabajo de los demás. Se adoptó el término “paquete” del trabajo del NPL, y la velocidad de línea propuesta en el diseño de ARPANET pasó de 2,4 kbps a 50 kbps.
>
> En agosto de 1968, DARPA solicitó presupuesto para el desarrollo de un elemento clave: los procesadores de mensajes de interfaz (IMP). La solicitud fue

otorgada en 1968 a Frank Heart, de Bolt, Beranek y Newman (BBN). Mientras el equipo de BNN trabajaba en los IMP con Bob Kahn desempeñando un importante papel en el diseño arquitectónico general de ARPANET, Roberts, junto con Howard Frank y su equipo de Network Analysis Corporation, diseñaron la topología y la economía de la red. El sistema de medición de la red lo preparó el equipo de Kleinrock en UCLA.

Gracias a los logros conseguidos por Kleinrock en la teoría de conmutación de paquetes y a su trabajo en el análisis, el diseño y la medición, su Network Measurement Center de UCLA fue seleccionado como el primer nodo de ARPANET. Se recogió el fruto de estos esfuerzos en septiembre de 1969, cuando BBN instaló el primer IMP en UCLA y se conectó el primer host. Un mes más tarde, se realizó el primer envío de un paquete de datos desde un host a otro. Se añadieron dos nodos más que incorporaron proyectos de visualización de aplicaciones. De esta forma, un total de 4 nodos estaban conectados en el ARPANET.

En los años posteriores, se trabajó para conseguir un protocolo para que funcione por completo desde un host a otro host, y se trabajó en un protocolo para software de red. En diciembre de 1970, el Network Working Group (NWG), bajo el liderazgo de S. Crocker, terminó el protocolo de host a host inicial de ARPANET, llamado Network Control Protocol (NCP).

En 1972, Kahn hizo la primera presentación exitosa de ARPANET frente a la International Computer Communication Conference (ICCC). En este año también se introdujo la aplicación inicial, el correo electrónico. En marzo, Ray Tomlinson, de BBN, escribió el software básico de envío y lectura de mensajes de correo electrónico, motivado por la necesidad de los desarrolladores de ARPANET de un mecanismo sencillo de coordinación. En julio, Roberts amplió su utilidad escribiendo la primera utilidad de correo electrónico para hacer listas de mensajes, leerlos selectivamente, archivarlos, reenviarlos y responder a los mismos. A partir

de ese momento, el correo electrónico se convirtió en la aplicación de red más importante durante más de una década." **(Leiner, 2012)**

0.1.3. Evolución

El protocolo IP es la forma de enrutar paquetes entre distintas redes. Para garantizar un correcto enrutamiento, la IP genera su propio encabezado a los paquetes. El proceso se actualiza en las tablas permanentemente.

En las redes no está orientado a la conexión y no es completamente seguro en la transmisión de los datos, para eso se usa el protocolo TCP.

La versión que se está ocupando de este protocolo es la 4, donde se tiene conectividad, pero también ciertas restricciones de espacio. Es por eso que las grandes empresas proveedoras del servicio de internet migraran a la versión IPv6.

La web ha tenido una evolución en diferentes frentes y de manera rápida. Gracias a eso se ha podido ver:

- Velocidad de acceso frente a número de dispositivos conectados.

- El uso de las aplicaciones para conectarse con el internet ha ido aumentando desde su creación.

- Mientras el internet se va desarrollando, la iteración con el usuario se hace necesaria.

En la evolución con la iteración con el usuario se conocen 3 etapas:

- **Web 1.0:** son páginas estáticas, con usos de marcos. Debido a que son creados de forma fija, las páginas pocas veces se pueden actualizar.

- **Web 2.0:** con la esta nueva versión, las paginas facilitan la interoperabilidad y hace que el usuario tenga más participación en la producción de contenidos. Entre los sitios que usan la Web 2.0 están: redes sociales, blogs y contenidos multimedia.

- **Web 3.0:** es la siguiente generación de la red de Internet. El objetivo de esta nueva extensión es hacer uso de un lenguaje el cual pueda ser entendido e interpretado. Además que pueda ser usado por agentes de software, con la finalidad de integrar y compartir datos.

Figura 0.3 Esquema de la evolución de Internet (Marrocostudio)

0.2. Ciberataque

0.2.1. Definición

En términos generales consiste en actos en los cuales personas ponen en duda la seguridad de una red de computadoras utilizando diferentes métodos y herramientas.

Los hackers usan diferentes armas para realizar un ciberataque, entre las más usadas son los virus informáticos. Los actos que comenten los atacantes obligan a las organizaciones a desarrollar estrategias de defensa para atajar cualquier riesgo de ciberguerra.

Figura 0.4 Imagen referencial del Ciberataque (etcétera, 2015)

Los ciberataques son actos en el cual los hackers cometen daños en contra de personas por medio de computadoras. Estos pueden ser sociales, sofisticados o sigilosos.

Estos ataques suelen estar dirigidos a sistemas de computación que se encuentran operando en la red a nivel mundial. Cuando los ataques son dirigidos a equipos y sistemas buscan alguna debilidad en la seguridad para anular el servicio que prestan.

Un ataque muy común es la redirección de pequeñas fracciones de centavos en transacciones bancarias.

0.2.2. Historia

Hay diferentes casos que se ha dado de ataques entre los más sonados se dieron los siguientes:

- **Primera Guerrilla Informática Global:** en 2010 la defensa de Wikileaks como respuesta de filtración de documentos del gobierno de Estados Unidos. Diversas autoridades tratan de boicotear los canales de financiación y su presencia en la red. El 6 de diciembre en defensa de WikiLeaks, el grupo de Internet Anonymous lanza un ciberataque contra PostFinance y PayPal por el bloqueo de las cuentas de WikiLeaks. Ante este ataque, WikiLeaks se ha pronunciado y ha manifestado que tiene una postura neutral ante estos ataques.

  El 10 de diciembre de 2010, Anonymous decide cambiar de rumbo la estrategia de su ataque. El resultado de este cambio es menos ataques hacia DoS y mayor publicación de la información filtrada por Wikileaks.

- **La Primera Guerra Informática Mundial:** Ley SOPA (Stop Online Piracy Act), el objetivo principal de SOPA, es proteger la propiedad intelectual en internet y combatir el tráfico de contenidos protegidos por derechos de autor y propiedad intelectual. Esta ley provoco movimientos entre usuarios y compañías. El 19 de enero de 2012 el FBI cerró oficialmente Megaupload, provocando comentarios y respuestas en todo el mundo. Como resultado, Annonymus inició la "Operación Blackout", en la cual declararon oficialmente la Primera Guerra Informática Mundial, motivados por muchos intentos de censura en todo el mundo.

Figura 0.5 Ley SOPA (Planeta GEA, 2012)

- **Ataque a Sony Pictures:** el ciberataque contra Sony en 2014 fue considerado para mucho como el mayor ataque a una empresa multimillonaria. Los hackers produjeron un daño de más de 100 millones de dólares y comprometieron alrededor de 100 Terabytes de información de usuarios.

- **Celebgate:** en 2014 muchas celebridades famosas que alojaban fotos íntimas en la nube fueron víctimas de filtración de información. En un inicio, toda la culpa recaía sobre iCloud, pero después de investigación se llegó a la conclusión de que hackers lograron entrar a la base de contraseñas y sustraerlas.

- **Ataque a Hacking Team:** Hacking Team es una controvertida firma de software italiana popular por suministrar de forma legal herramientas de espionaje e intrusión remota como spyware y malware. Entre sus clientes figuran agencias de inteligencia y gobiernos. La compañía sufrió un ataque donde se han filtrado a la red 500 Gb de datos confidenciales.

- **Ataque al gobierno de Estados Unidos:** se trata de uno de los ataques más importantes que se ha dado en la historia del internet. Hackers violaron la seguridad de la oficina de Administración de Personal de Estados Unidos. Esto dejo al descubierto datos de más de 20 millones de personas. El ataque se produjo en China y tenía como objetivo obtener información de chinos residentes en Estados Unidos.

0.2.3. Tipos de Ataques

Existen diferentes tipos de softwares o ataque que pretenden arremeter la información de usuarios o de grande compañías:

- **Trashing**: esto es cuando un usuario anota sus credenciales o claves de algún sitio en específico en un papel, o cuaderno. Y cuando lo recuerda totalmente bota en la basura. Esto aunque es un acto inconsciente puede usar un atacante para husmear en la basura y conseguir conocer sus claves personales

- **Denial of Service (DoS):** el objetivo de este ataque es saturar los recursos del dispositivo o servidor de la víctima, dando como resultado colapsar los servicios brindados por la misma

- **Ataque de Autenticación:** este ataca engaña al sistema para ingresar al mismo. Generalmente el atacante toma las sesiones ya ingresadas por la víctima.

- **Virus:** estos son los tipos más conocidos de ataques, y se distinguen de la manera que se propaga. Para este tipo de ataque, es necesario de la participación del usuario para que se pueda expandir automáticamente.

- **Drive-by Downloads:** son sitios que instalan pequeños códigos que extraen datos de los dispositivos. Generalmente se lo hace de manera automática a través de soluciones que buscan sitios web con debilidad en su seguridad e instalan un código malicioso dentro del código HTLM de la página

- **Hijackers:** son pequeños porciones de códigos que cambian la configuración del navegador web, haciendo que las páginas de inicio del navegador tenga publicidad, o las re direccionen con anuncios de pago. Esta técnica es comúnmente utilizada para obtener claves o datos personales.

- **Botnets:** son computadoras infectadas que son usadas para el envío de spam masivo.

- **Rogue software:** este tipo de ataque hace creer al usuario que su computadora esta con alguna clase de virus. Esto induce al usuario a instalar un software de solución para estos problemas, lo que ocasionas que puedan infectarse o que se puedan sustraer los datos de la computadora.

0.3. Ciberseguridad

0.3.1. Definición

La ciberseguridad es el conjunto de conceptos de seguridad, buenas prácticas, directrices, métodos para proteger la información de una organización o de un usuario. Otra definición, puede ser que la ciberseguridad es la ausencia de amenazas por medio de tecnologías de la información.

Figura 0.6 Ciberseguridad (abcis, 2015)

La ciberseguridad, entonces consiste en proteger toda la estructura de una organización respondiendo a ataques que se tenga en la red. Todo esto es a nivel de software.

Las amenazas cibernéticas son difíciles de identificar. Entre estas amenazas se tienen los virus, intrusos del sistema. Hay una gran variedad de riesgos cibernéticos, y su gama es ilimitada. La fragilidad de las seguridades permite la perdida de información. Estos casos aumentan si toda la estructura de la red es expuesta. Todos los dispositivos que se conectan al internet tienen un potencial riesgo.

0.3.2. Historia

Existe un sin número de herramientas que usan los hackers para burlar las seguridades que existe. Una de estas herramientas es Kali Linux, la distribución especializada para crackers y profesionales de la seguridad informática. Los usuarios que tienen acceso a esta herramienta, cuentan con posibilidades necesarias para realizar un ataque a diferentes bases de datos, web y servidores a gran escala.

Gran cantidad de ataques a la seguridad pueden ser mencionados en una lista donde se presentan los ataques más relevantes de la historia:

- **Ataque Carbanak:** es una banda delictiva que se dedicó atacar cajeros automáticos. La banda recaudo más de mil billones de dólares. La cifra más grande violando la seguridad de los bancos fue de 10 millones de dólares

- **Home Depot:** los sistemas de pago informáticos del proveedor de equipos para la construcción, fueron atacados por piratas en una filtración de datos que afectó a millones de clientes. La empresa confirmó que su sistema de pagos había sido violado, lo que afectó a clientes que usaron las tarjetas de pago en tiendas canadienses y estadounidenses.

- **Target:** el ataque a esta gran empresa de supermercados represento que más de 40 millones de personas fueran hackeadas sus números de tarjetas bancarias y claves. Sin contar los 30 millones que fueron sustraídos sus información personal.

Figura 0.7 Ataque a puntos de Venta de Target (Pagnotta)

- **Sony PlayStation Network:** hackers sustrajeron información de más de 77 millones de cuentas en todo el mundo. Lo sorprenderte de este caso es que la empresa se dio cuenta una semana después del hecho.

- **eBay:** los delincuentes informáticos rompieron la seguridad de la base de datos de la página de comercio online, obligó el año pasado a que 145 millones de personas cambiaran sus contraseñas debido a que no se pudo calcular el volumen exacto de la información que fue robada.

0.3.3. Buenas prácticas de Ciberseguridad

- Mantener siempre actualizados el software de la máquina, un programa desactualizado es una debilidad y puede ser usado por un atacante para infiltrarse en la información.

- Crear una contraseña segura. Tratar de crear una contraseña lo bastantemente fuerte como para que no sea adivinado por un hacker. Para eso podemos usar el Método Salt, que consiste en reemplazar letras en caracteres especiales.

- Tener una copia de seguridad.

- Proteger el acceso al sitio web, para esto cambiar las credenciales por defecto de "admin"

- Instalar software de seguridad y mantenerlos actualizados.

0.4. Consejos para una navegación segura

Las buenas prácticas al momento de navegar en el internet, sirven para elevar la protección que se tiene a un equipo o dispositivo. También depende mucho del usuario para que tenga una cultura de navegación segura.

Se debe tener en cuenta estos consejos para poder navegar en el internet de una forma segura:

- **Evitar los enlaces sospechosos:** evitar hacer clic en los enlaces que son sospechosos. Algunos enlaces vienen en mails, en páginas, etc.

- **No acceder a sitios web de dudosa reputación**: el usuario debe estar atento a mensajes de jugosos descuentos, o de ganar plata de manera plata y evite acceder a páginas web con estas características. Ya que estos anuncios suelen contener links que pueden redirigir a un sitio infectado.

- **Tener actualizado todos los complementos de la maquina**: una práctica sana es tener los componentes de la maquina con las últimas actualizaciones.

- **Descargar aplicaciones desde sitios web oficiales:** muchos sitios ofrecen software para descargar y la mayoría de veces estas páginas descargan código que pueden afectar al funcionamiento de la máquina.

Figura 0.8 Navegación a través de sitios https:// (Noticias SEO, 2014)

- **Evitar el ingreso de información personal en formularios dudosos**: al momento de que el usuario esté al frente de una página en la cual le solicite su

información personal, es recomendable verificar la legitimidad del sitio. Una buena práctica para confirmar si se encuentra en una página segura es el uso del protocolo HTTPS.

- **Evitar la apertura de documentos o archivos de dudosa procedencia**: la expansión de virus pueden ser por medio de archivos ejecutables. Se recomiendo rechazar el pedido de ejecución de los archivos que se desconozca por seguridad propia ya que su procedencia no es de fuente fiable.

- **Utilizar contraseñas fuertes**: Se recomienda el uso de contraseñas de por lo menos 8 caracteres, usar mayúsculas, caracteres especiales y nunca usar nombre de familiares, fechas personales, etc.

Figura 0.9 Contraseña de al menos 8 caracteres (Rizzo, 2015)

- **Elije un navegador seguro:** la mayor parte de las actividades que desarrollamos por Internet se centran en nuestro navegador, por lo que hacer una elección adecuada es importante. Además de elegir uno que nos permita navegar de forma rápida, sea ligero y no nos de problemas tenemos que ver también el nivel de seguridad que nos puede proporcionar.

- **Cuida la protección de tu equipo:** de igual forma que los dos anteriores puntos, salvo que extrapolado a todo nuestro equipo. De nada sirve que tengamos mucho cuidado con el resto de cosas si de buenas a primeras metemos un CD o un pendrive que puede estar infectado y nos *contagia* nuestro equipo.

A pesar de todos los consejos el más es tener sentido común, sin el sentido común las posibilidades de que tengamos problemas aumentan considerablemente. Es importante que antes de hacer click en un enlace pensemos bien en que página estamos y a cual nos puede llevar. Tenemos herramientas que nos bloquean posibles amenazas, pero no son efectivas al cien por cien, por lo que no hay mejor herramienta que uno mismo, que vigilar en que páginas entramos y que datos dejamos en estas.

Siguiendo un poco todos estos consejos nos encontraremos con que nuestro equipo será más seguro y por lo tanto nuestros datos, mejorando la privacidad de estos.

1. DEEP WEB

1.1. Definición

La mayoría de usuarios que navegan diariamente por Internet, no saben de lo que se trata, o desconocen que existe un mundo virtual más allá de lo que se puede encontrar, ya que lo hacen mediante sus páginas habituales o utilizan buscadores estándar donde se puede encontrar por así decirlo "de todo" gracias a Google, Yahoo!, etc., obteniendo aquello que los interese, ya sea información, productos, servicios o redes sociales. Llegando a decir hasta incluso que "Si no existe en Google, no existe en ningún lado". Detrás de todo esto, existe un mundo virtual oculto, más grande del que podemos pensar, más allá de su visión o conocimiento, donde más usuarios navegan por el lado oscuro y oculto del Internet, que para acceder no se necesita una habilidad o conocimiento de sistemas informáticos, se trata de buscar las herramientas necesarias, manteniendo una mente muy abierta, y asimilando con el contenido que uno se pueda topar dentro de un mundo oscuro, a esto se lo conoce como Deep Web, donde se puede ver, encontrar, escuchar, comprar, ofrecer, contratar y "lavar" de todo por así decirlo.

> “Jill Ellsworth utilizó el término "la Web Invisible" en 1994 para referirse a los sitios web que no están registrados por algún motor de búsqueda. Otro uso temprano del término Web Invisible o Web Profunda fue por Bruce Monte y Mateo B. Koll de Personal Library Software, en una descripción de la herramienta @ 1 de Web Profunda, en un comunicado de prensa de diciembre de 1996.” **(Wikia)**

Lo que todos sabemos de la navegación web es solo el 4% de lo que en realidad se encuentra en el internet, el 96% que falta resulta de información que se encuentra privada, en confidencial y en muchos casos llega a ser ilegal, ya que llega a ser usada mayormente por pederastas, amparados por el anonimato, llegan a hacer un mal uso dentro de este mundo oscuro, es posible encontrar todo esto dentro de la Deep Web.

> “Se estima que el Internet superficial contiene sólo 19 terabytes de contenido y un billón de documentos. Por su parte, el lado oscuro de la web ocupa 7.500 terabytes, lo que equivale a 550 billones de documentos individuales.” **(Frutos, 2015)**

Figura 1.1 Porcentaje del internet visible y la Deep Web (Ranchal, 2014)

La Deep Web (Internet Profunda) o Invisible Web (Internet Invisible), se define como contenido web no indexado por motores de búsqueda, donde se puede encontrar todo lo que se pueda imaginar, es una porción sumamente grande de la internet, contiene páginas, información, documentos, etc. que se encuentran desarrollados de tal forma que es imposible descifrar, su contenido puede estar realizado en flash, sin ningún código HTML, etc. Su estructura hace que su rastreo se dificulte por parte de los bots. Mucho de la Deep Web es temporal: al consultar una base de datos se genera páginas dinámicas.

> “La Deep Web es un “Internet paralelo” protegido por sistemas de protección del tráfico que están ideadas para maximizar la privacidad y el anonimato.” **(Gónzales, 2015)**

Lo que se realice dentro de la Deep Web se lo hace mediante anonimato, no puede asociarse con la identidad del usuario que navegue por la web profunda. Se puede encontrar por el lado bueno al navegar por la Deep Web con contenido como AIW.

El termino de Web Invisible, no es bien visto, ya que muchos usuarios llegan a la conclusión de que para acceder a la web se debe realizar mediante un buscador; su información puede ser hallada de manera más rápida que otra, pero no se encuentra del todo invisible; contiene información variada que puede ser almacenada y a la vez obtenida con facilidad de distintas formas; el contenido que se encuentra indexado está almacenado en bases de datos y mediante la administración del usuario, por lo tanto, se puede decir que la información almacenada en sus bases de datos no está invisible.

1.2. Uso de la Deep Web

Muchos organismos gubernamentales han clasificado a la Deep Web como refugio de delincuentes, con mucho material ilegal, como:

- Estafas
- Jailbait
- Blanqueo de bitcoins
- Snuff
- Crush fetish
- Compra de narcóticos
- Contratación de hackers
- Mercado negro de sicarios
- Documentos clasificados: wikileaks.
- Phishers, spammers, botnet agents que buscan víctimas
- Compra o fabricación de armas en la DNM
- Etc.

Existen páginas falsas del FBI, donde puedes ser sorprendido por cometer alguna actividad ilegal, al ser atrapado recibirás una "Love Letter" sin vuelta atrás.

No todo hace que la Deep Web sea del todo calificada como un acceso a páginas con contenido desagradable, existen:

- Bibliotecas digitales
- Bases de datos que representan un gran porcentaje muy importante de información
- Material educativo o científico
- Contenido almacenado por gobiernos de varios países
- Organizaciones con información confidencial, como; la NASA y su información sobre sus investigaciones científicas; datos meteorológicos, financieros, información de personas, etc.
- Foros con diversas temáticas

El debido uso de la Deep Web se encuentra más en el sentido común del usuario que está adentrándose a la búsqueda dentro de la Deep Web, una gran fuerza de voluntad, gran sentido de ética y formación.

1.2.1. Moneda electrónica en la Deep Web

Figura 1.3. Moneda electrónica anónima Bitcoin dentro de la Deep Web (Ranchal, 2014)

Bitcoins (moneda electrónica anónima, independiente e inconfiscable), son monedas simbólicas que no están registrados por ningún instituto económico de emisión central, por lo que los pagos de las compras que se realice dentro de la DNM serán con bitcoins y son directas de usuario a usuario. Los usuarios lo utilizan como medio de pago preferencial y sirve para el pago de cualquier cosa que se ofrece dentro de la Deep Web,

sea buena o mala. Los BTC se transforma en dinero de uso corriente a través de páginas que al hacer la transformación cobran comisión.

Esta moneda virtual sigue siendo cotizada para su alza, a pesar de que existen usuarios que se abstienen de su uso por su falta de seguridad o su rastreo que en muchos casos llegan a ser fácil de encontrar. La dirección donde el usuario recibe su pago de BTC es completamente anónima pero sus transacciones son públicas, por eso en páginas de compra-venta existen servicios que se encargan de mezclador de bitcoins o blanqueo de bitcoins, dificultando la unión de sus BTC con los de otra persona.

Existen graves problemas de seguridad al utilizar BTC, como ciberataques masivos e incluso robos, por su conexión con la forma de pago relacionado con actividades turbias.

Si los usuarios quieren realizar compras ilícitas dentro de la Deep Web, su pago lo realizan con BTC, como clientes al recibir un buen trato, el arma está en buen estado o la droga es buena, puede puntuar al vendedor y el siguiente comprador puede ver la calidad del producto, que suele mostrarse con fotografías adjuntas. A pesar de que exista una gran cantidad de anuncios, la mayoría de veces son estafas, especialmente en anuncios sobre tráfico de órganos. Para realizar estos pagos con BTC se debe tener una cuenta considerable de la moneda.

Se ha considerado esta moneda virtual como medio de pago para: hoteles de Las Vegas, EE.UU., por servicios de almacenamiento MEGA, juegos virtuales de Zynga o compras en Overstock.

1.2.2. Escrow y Multisig Escrow

- **Escrow:** permite protegerse de las estafas que existen al realizar compras en los mercados de la Deep Web. Escrow ofrece un servicio que consiste en que los administradores de la tienda se encargan de asegurar el dinero depositado del comprador durante el proceso compra-venta, evitando que el vendedor obtenga el dinero hasta que el producto llegue a manos del comprador. Dependiendo de la

tienda, escrow cobra un porcentaje del 0,5% de la venta incluye un sistema de desacuerdos por si existe algún problema.

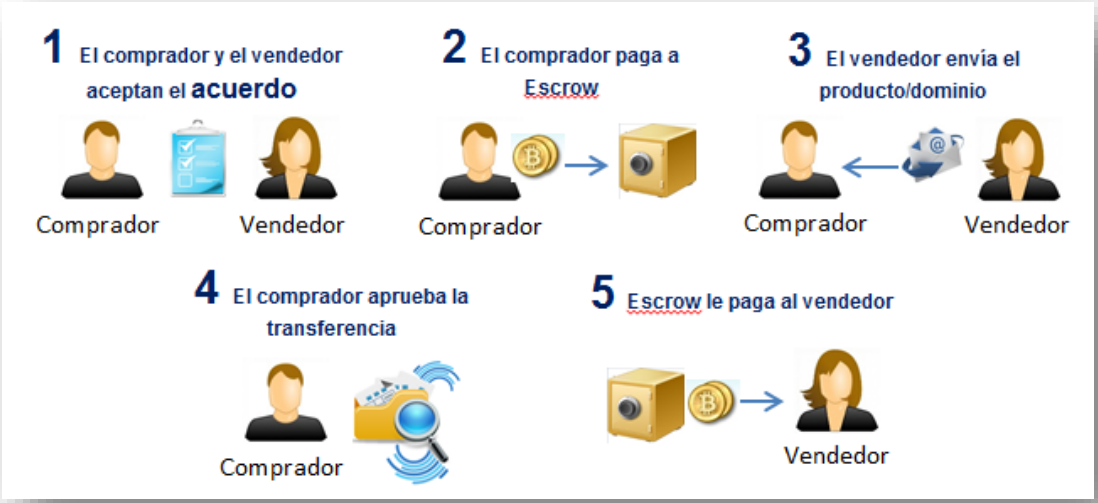

Figura 1.2 Como funciona Escrow (Guillén & Vicente, 2015)

- **Multi-Signature Escrow (o Multisig Escrow):** al utilizar Multisig Escrow, tanto el vendedor como el comprador deben firmar un acuerdo en una dirección de BTC, donde el dinero del comprador se mantendrá guardado hasta que el producto llegue a sus manos. De esta manera, tanto el comprador como el vendedor serán intermediarios del dinero.

En muchos casos los usuarios F.E., al realizar una compra dentro del mercado negro, corriendo el riesgo de ser estafado con facilidad.

Figura 1.3 Representación Multisig Escrow (alexwyn, 2014)

1.2.3. Dominios .onion

Para adentrarse al lugar más oscuro e invisible de Deep Web se lo hace a través del Onionland (también denominada Darknet.). Aquí se encuentran páginas bajo dominios ".onion", estos dominios se encargan de no divulgar las URL, ni revelar el título del contenido en la dirección web (por ejemplo: amazon.com). Las URL son de tipo: "w363zoq3ylux5rf5.onion" que contiene 16 caracteres alfa numéricos, estos se encargan de mostrar los sitios manteniendo su anonimato. Si se quiere hacer uso de estos URL se debe conocer su IP o introducirlo en un motor de búsqueda.

1.3. Funcionamiento

Al nosotros saber ya la definición de Internet, tenemos en cuenta que es una red de ordenadores y dispositivos que se encuentran conectados, estos ordenadores hacen también de servidores, como su nombre lo indica, cumplen con servir información. Estos servidores almacenan información de páginas web que permiten ser extraídos por robots de indexación. La Deep Web contiene información que se encuentra en páginas web que no están apuntando o no está permitido su acceso a sus URL, a robots de indexación de buscadores estándar como Bing, Google, Yahoo!, etc., ya que estos exploran un gran fichero, lo revisan, interpretan y generan su índice de contenido.

Sin embargo, para el acceso a una página web, por medio de buscadores estándar, se requiere de dominios (www.xxxx.com), que apunte a sus servidores. Al escribir el dominio proporcionado, nos dan una puerta abierta para tener acceso a su información y son interpretados por buscadores estándar, dando lugar a una navegación en la que todos estamos relacionados. Para este caso la Deep Web no puede buscar mediante motores de búsqueda estándar información de páginas web que se encuentran invisibles. Todo material que este en la Deep Web no es accesible fácilmente, siendo necesario desviar el tráfico con servidores proxy o VPN que actúan como protector y evita ser capturado.

Aun así, si estos buscadores estándar pudieran apuntar al contenido web, no existiría más la Deep Web.

El contenido de la información encontrada dentro de la Deep Web está en sitios generados dinámicamente. Los dominios cambian con frecuencia y terminan en ".onion", también pueden ser combinaciones alfanuméricas aleatorias.

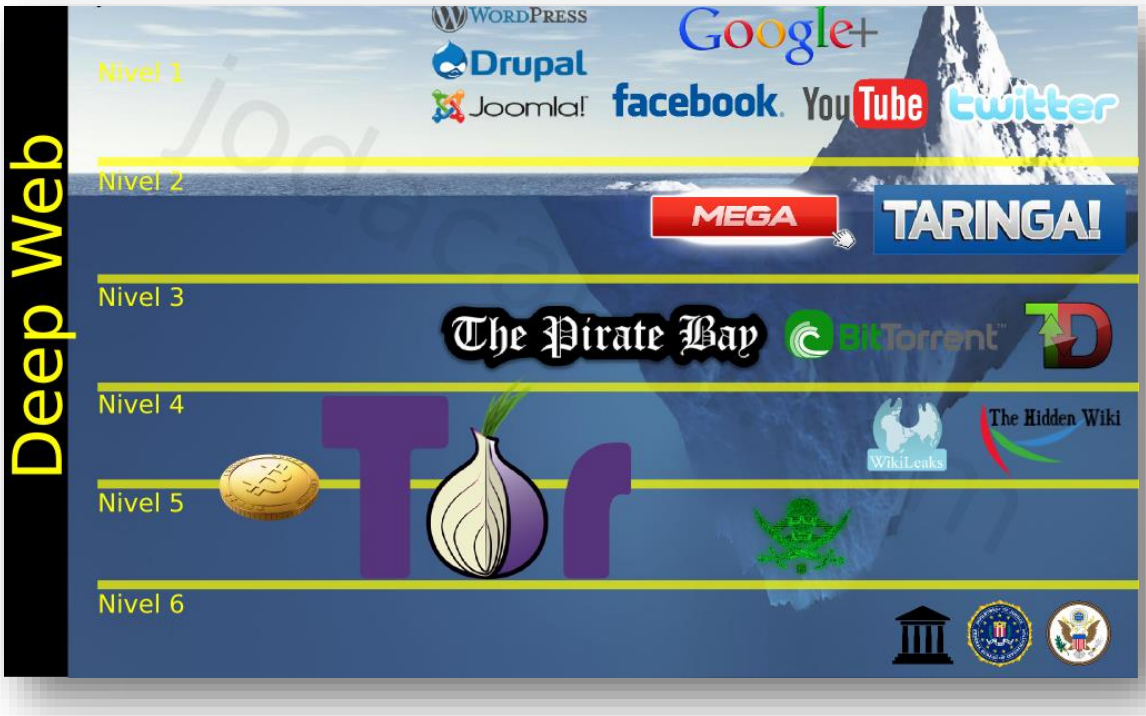

Figura 1.4 Niveles de la Deep Web (Ranchal, 2014)

1.4. Redes anónimas para acceder a la Deep Web

Para acceder a la Deep Web, se necesita acceder a una red que es anónima, entre estas redes están: TOR, I2P y Freenet. Nos permiten navegar por páginas web y servicios que están escondidos detrás de un pseudo-dominio.

- **TOR (The Onion Router):** El más común, fue creado en el Laboratorio de Investigación Naval de EE.UU. como una forma segura de comunicación para militares. Tor está estructurado en nodos o capas, de forma que el usuario va saltando de capa en capa, protegido por una capa de cifrado que no permite que el servidor destino conozca su IP, contiene la una gran cantidad de servicios y a su propio navegador que facilita la búsqueda en el The Hidden Weeky; sin embargo al funcionar a través de un enrutado complejo, es muy fácil tener acceso a la Red TOR, es una buena opción para navegar de forma anónima y segura.

  Más adelante hablaremos sobre la red Tor.

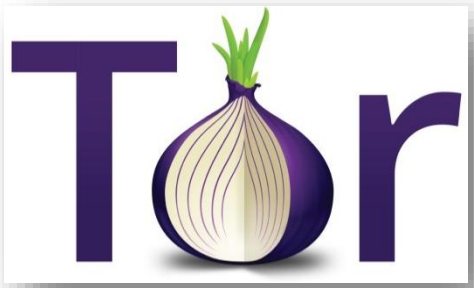

Figura 1.5 Logo Tor (Amaya, 2015)

- **I2P:** Surgió en 2003, es parecida a Tor, usa comunicaciones cifradas, haciendo que el usuario salte entre varios nodos de la red, ocultando su identidad. Sin embargo con respecto a Tor, por dentro del I2P las cosas cambian.

  En Tor, al conectar un ordenador a otro nodo, se elige un conjunto de nodos intermedios (un circuito) entre ambos ordenadores y se envían las comunicaciones. I2P es diferente: se hace uso de túneles de entrada y salida

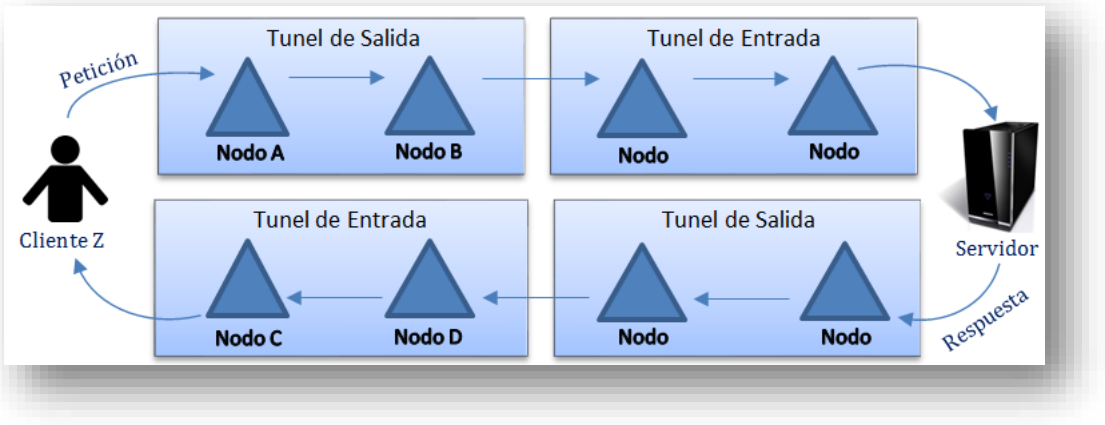

Figura 1.6 Modelo sencillo de los túneles en I2P. (Guillén & Vicente, 2015)

Cuando un usuario ingresa, su computador en este caso Z, al conectarse a I2P crea un túnel de salida con dos nodos, A y B. La creación del túnel de entrada es mediante la elección de dos nodos extras, C y D. Por medio de B, se enviará una solicitud de A. que conducirá a C (siendo C la finalización del túnel) el cual enviará a su destino que es el nodo de entrada del computador al que se realice la solicitud. El cual enviará a un nodo cualquiera de la red, enviará nuevamente a un nodo intermedio que hará llegar la solicitud al servidor destino.

Lo mejor de utilizar túneles es que dentro de una red se puede conectar mediante varios ordenadores, se tiene privacidad. Los túneles son unidireccionales, por lo tanto si se requiere un análisis de tráfico, se necesitará el doble de nodos que los que utiliza Tor.

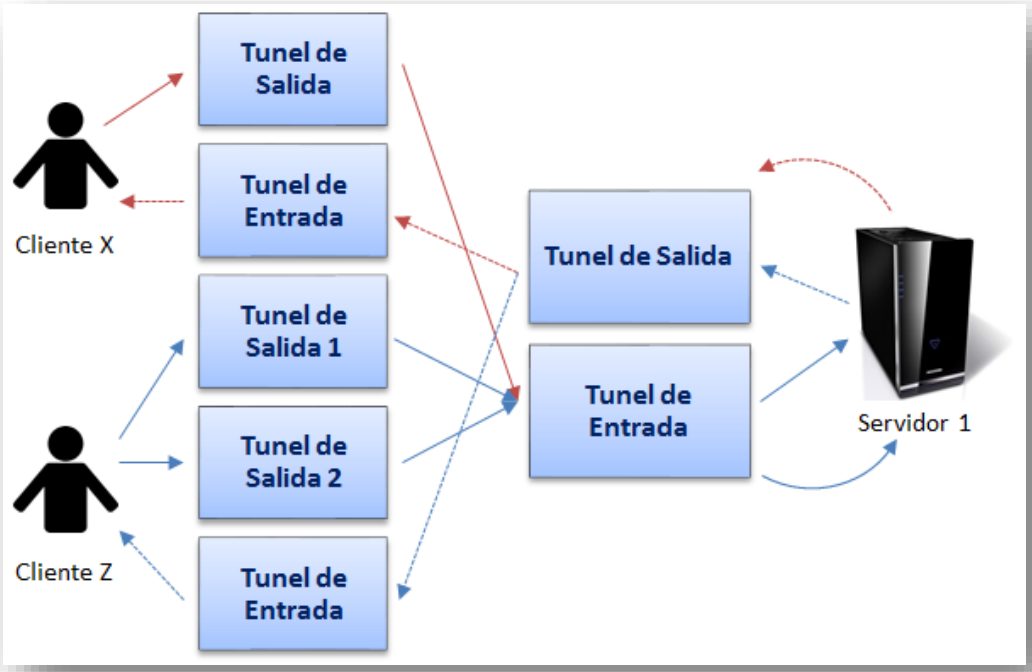

Figura 1.7 Grafico de clientes en túneles paralelos y servidores (Guillén & Vicente, 2015)

En Tor, para que el ordenador se conecte se lo hace a través de un circuito. Para I2P es lo contrario, el túnel de salida sirve para enviar respuestas a varios ordenadores. En cierto modo, se podría obtener un número de túneles de salida en paralelo.

Haciendo que en I2P las conexiones sean de mayor velocidad en transacciones ocultas, que Tor ya que al establecer conexiones se tiene una estructura más complicada.

I2P es poco conocido, tiene menor ancho de banda conjunto, pocos desarrolladores, con poca experiencia. I2P ha sido estudiado, atacado y corregido pocas veces, a modo de proxy Tor se encuentra más desarrollado para su uso. Por ende menos usuarios, el cual I2P lo hace más privado que Tor.

- **Freenet:** es una red P2P, que comparte archivos como plataforma de intercambio de información. Freenet es una especie de caché enorme y su contenido de Freenet se encuentra distribuido entre todos los nodos al momento de su carga, al realizar

un pedido, se obtiene una parte de cada nodo. No existen conexiones directas, ni reconocimiento de nodos, dando un alto nivel de anonimato. Freenet tiene un gran número de niveles de seguridad, como los tipos de conexión: Opennet y Darknet. Opennet da a Freenet una conexión más adecuada a todos los usuarios que se encuentran conectados entre sí.

- **Hornet (High-speed Onion Routing at the NETwork layer):** o Avispón, una opción de Tor, programado en Python haciendo uso de software de enrutamiento que pertenece a Intel. nueva red anónima que está siendo desarrollada por investigadores de varias universidades, prescinde de VPN al momento de navegar por las redes Onion, promete una navegación web mucho más rápida y con mayor protección a su privacidad dentro de la Dark Web. Avispón podrá procesar el tráfico a una velocidad de hasta 93 gigabytes por segundo.

1.5. Motores de búsqueda dentro de la Deep Web

Existen varios motores de búsqueda dentro de la Deep Web, los más conocidos y utilizados por usuarios son:

The Hidden Wiki

The Hidden Wiki, actúa como motor de búsqueda que tiene acceso directo a páginas web dentro de la Dark net. Contiene un índice de algunas páginas web alojadas dentro de la Deep Web. The Hidden Wiki es un túnel de salida de la Deep Web, teniendo una lista de un grupo de páginas ocultas donde los usuarios de encargan de revisar y actualizar a diario. Las páginas cambian de dominio innumerables veces y Tor navega con enlaces que son actualizados a mano.

Figura 1.8 Logo The Hidden Wiki, motor de búsqueda dentro de la Deep Web (Genbeta, 2015)

Al ingresar a The Hidden Wiki se podrá visualizar que clase de servicios y páginas webs se ocultan en la Deep Web, entre ellos están:

- **Servicios financieros:** lavado de bitcoins, cuentas de PayPal que han sido robadas, tarjetas de crédito que se han clonado, billetes falsos, etc...

- **Servicios comerciales:** explotación sexual y mercado negro: gadgets hurtados, armas y municiones a la venta, documentación ilícita y drogas.

- **Anonimato y seguridad:** información de cómo en Tor se puede aumentar el anonimato, esencialmente al usar bitcoins en ventas o transacciones.

- **Servicios de hosting:** privacidad de imágenes almacenadas y alojamiento web. Algunas páginas prohíben el almacenamiento de archivos falsos sin impedimentos.

- **Blogs, foros y tablones de imágenes:** existen dos categorías de este tipo como son el hacking y cambio de imágenes entre usuarios, con relación a los servicios de que se ofrecen.

- **Servicios de correo y mensajería:** existen direcciones de mail gratis o mediante el cobro del servicio, con SSL y soporte de IMAP. Los servicios de chat hacen uso de IRC o XMPP.

- **Activismo político:** intercambio de información confidencial, hacktivismo, hasta se puede organizar "magnicidios financiados en masa". La ideología que prevalece dentro de la Deep Web es la anarquía.

- **Secretos de Estado y soplones:** existe un espejo de WikiLeaks, páginas donde se publican secretos.

- **Libros:** bibliotecas virtuales con una gran cantidad de ebooks en distintos formatos y con un gran peso en gigas. Muchos se encuentran libres de copyright y otros están distribuidos como descarga directa ilegalmente.

- **Páginas eróticas:** de libre acceso y mediante pago. Se encuentran variadas y sin ninguna restricción.

Torch

Es un motor de búsqueda que hace el papel de Google dentro de la Deep Web. Se puede navegar con solo introducir palabras clave, exactamente a Google, se puede buscar según lo que se desee encontrar.

Figura 1.9 Logo Torch, motor de búsqueda dentro de la Deep Web (Genbeta, 2015)

Grams

Creado por un programador anónimo, motor de búsqueda de mercados negros, trabaja similar a Torch, ingresando palabras clave, debe estar conectado mediante Tor y escribir su dirección. Sus creadores muestran portales que han sido previamente pedido que se los incluya dentro de Grams.

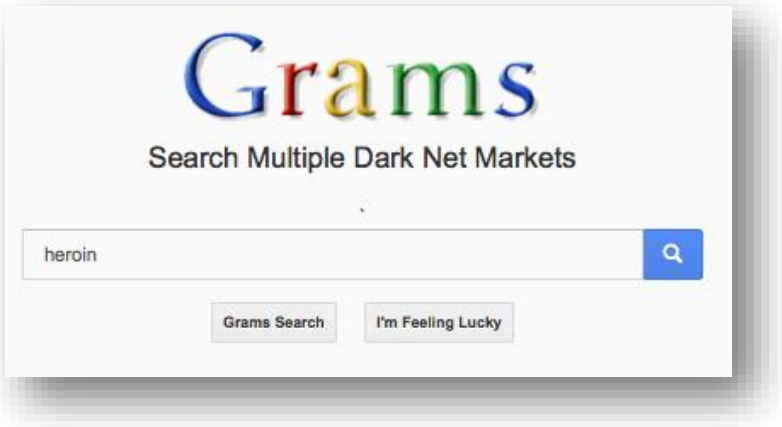

Figura 1.10 Logo Grams, motor de búsqueda dentro de la Deep Web (fayerwayer, 2014)

Memex

Creado por un programador anónimo, motor de búsqueda capaz de indexar páginas ocultas de la Deep Web, que ha sido creado para combatir el crimen. Facilita la lucha contra actividades ilícitas que se encuentran en el lado oculto de la Deep Web. Memex no sólo se encarga de rastrear las millones de páginas web que pasan invisibles para los buscadores estándar, yendo más allá poniendo la lupa en páginas .onion de los servicios ocultos que se encuentran en TOR y ordenando el contenido sobre temas y dominios específicos.

Figura 1.11 Logo Memex, motor de búsqueda dentro de la Deep Web (Frutos, 2015)

Onion City

Es un motor de búsqueda que se encarga de indexar páginas ".onion" de servicios que permanecen ocultos en Tor. Es muy parecido al motor de búsqueda Memex, pero no se encarga de luchar contra el crimen cibernético dentro de la Deep Web. Onioncity no encripta, ni protege a usuarios de los peligros que pueden ocurrir al navegar por la Deep Web. Esta sencilla herramienta tiene acceso a 650.00 páginas que están ocultas bajo dominios ".onion" sin usar el motor de búsqueda Tor.

Figura 1.12 Motor de búsqueda OnionCity de la Deep Web (Genbeta, 2015)

Las búsquedas realizadas en este motor son a través de proxy Tor2web, tiene el papel de cliente navegando por la red Tor y busca dominios de páginas web ".onion.city". Las páginas web que se busquen en Onioncity también se puede encontrar en Google Search, ya que tienen la misma tecnología, esto es posible usando el dominio "site:onion.city" antes de empezar la búsqueda de lo se quiere.

1.6. Recursos de la Deep Web

La Deep Web tiene recursos que se encuentran clasificados en:

- **Contenido de Acceso limitado:** Páginas que limitan su acceso de forma técnica (por ejemplo, los motores de búsqueda suprimen el uso de robots o captcha y duplicados almacenados en caché).

- **Contenido Dinámico:** Páginas dinámicas que contestan a una interrogación o mediante un formulario, sobre todo si se utiliza contenido de entrada como campos de textos que se encuentran en dominios abiertos.

- **Contenido No Vinculado:** Páginas que no se encuentran relacionadas con otras, impidiendo que programas que traten de violar su contenido no tengan acceso. Conocido como páginas web sin enlaces entrantes.

- **Contenido Programado:** Páginas que solo se puede acceder a través de enlaces generados por JavaScript y contenido que ha sido descargado de servidores web de forma dinámica a través de Flash o Ajax.

- **Sin contenido HTML:** Paginas con contenido codificado en archivos o formatos multimedia específicos (imagen, video), que no son manejados por motores de búsqueda.

- **Web privada:** Páginas que requieren del registro de un usuario y su contraseña previa para el inicio de sesión.

- **Web contextual:** Páginas con diferentes contenidos con contextos diferentes al acceder (por ejemplo, rangos de direcciones IP del usuario o su historial de navegación previa).

1.7. Sitios Web dentro de la Deep Web

Existe un listado grande acerca de links que se encuentran dentro de la Deep Web, en este casó publicaremos el listado de links que son de frecuente visita por parte de los usuarios por su seguridad y anonimato que ofrece, este listado ha sido actualizado hasta fines de Noviembre del 2015:

- **WIKIS**

The Hidden Wiki 2015: kpvz7ki2lzvnwve7.onion/index.php/Main_Page
DeepWiki: deepwikizpkrt67e.onion/index.php/Main_Page
The Uncensored Hidden Wiki:
uhwikih256ynt57t.onion/wiki/index.php/Main_Page
Tor Wiki: torwikignoeupfm.onion/index.php?title=Main_Page
WikiTor: wikitor74em2u6rq.onion/Main_Page

- **DIRECTORIOS**

Tor Links: torlinkljcc4uv3y.onion/
Anylink Onion: vizpz65utiopch7t.onion/
OnionDir: dirnxxdraygbifgc.onion/
TorX: pdizimmrq5mwjkun.onion/
New Tor Directory: auutwvpt2zktxwng.onion/
Yet another Tor Directory: bdpuqvsqmphctrcs.onion/
Harry71: skunksworkedp2cg.onion/sites.html

- **BUSCADORES**

Ahmia: msydqstlz2kzerdg.onion/search/
Torch: xmh57jrzrnw6insl.onion/
not Evil: hss3uro2hsxfogfq.onion/
Grams: grams7enufi7jmdl.onion/

- **EMAIL / MENSAJERIA**

Torbox: torbox3uiot6wchz.onion/
Lelantos: lelantoss7bcnwbv.onion/
SIGAINT: sigaintevyh2rzvw.onion/
RuggedInbox: s4bysmmsnraf7eut.onion/
Mail2Tor: mail2tor2zyjdctd.onion/
Mailtor: mailtoralnhyol5v.onion/src/login.php
SMS4TOR: sms4tor3vcr2geip.onion/
OnionChat: chatrapi7fkbzczr.onion/

- **REDES SOCIALES**

Blackbook: blkbook3fxhcsn3u.onion/
Twitter clone: npdaaf3s3f2xrmlo.onion/
Galaxy2: w363zoq3ylux5rf5.onion/
Facebook: facebookcorewwwi.onion/

- **HOSTING DE ARCHIVOS**

Anonfiles: anonfiles.com/
Onion Uploader: nk3k2rsitogzvk2a.onion/
Tarsier Uploader: dke34xlun4xa3w4z.onion/files/index.php

- **HOSTING DE IMAGENES**

Ukaz.cz: r4tylitxaom2zqu5.onion/
Free Image Hosting: imagexutrag65hxl.onion/
Hidden Image Upload: 63dduge2x3xdggc6.onion/hbb/uploader.html
Freedom Image Hosting: freedomsct2bsqtn.onion/
Matrix Image Uploader: matrixtxri745dfw.onion/neo/uploader.php

- **HOSTING DE TEXTO**

Onion-pastebin: pastetorziarobi7.onion/

InserTor: 54ogum7gwxhtgiya.onion/insertor/

Post It!: postits4tga4cqts.onion/

2. RED TOR

2.1. Definición de la Red Tor

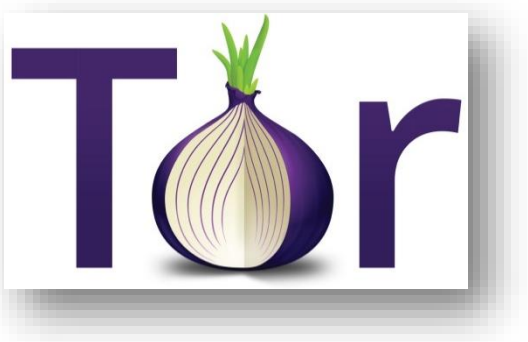

Figura 2.1 Logo Tor (Amaya, 2015)

La red Tor llamada así por sus siglas "The Onion Router" o dicho en español El Encaminamiento/Enrutamiento de Cebolla. Es un proyecto cuyo objetivo principal es el tener una comunicación privada a través de una red pública. En palabras técnicas tendríamos una red de comunicaciones de baja latencia superpuesta sobre internet (esto puede variar en el concepto ya que en si podría funcionar en cualquier otra red pública que no sea internet, ejemplo una intranet de una empresa), esto es debido al enrutamiento de los mensajes intercambiados entre los usuarios (llamemos mensajes a cualquier tipo de intercambio de paquetes, podría ser hasta realizar un ping a otro servidor en la misma red Tor) no revela su identidad (dirección ip) y además mantiene el contenido del mensaje integro. Esta es la razón principal de que la red Tor sea usada en la Deep web o web profunda.

Debemos entender que no es una red de punto a punto (peer to peer) ya que existen enrutadores especiales (onion routers) que encaminan los mensajes, y otros que hacen el trabajo de directorio (a donde se debe entregar el mensaje).

Se puede decir que la red Tor es conformada por gente que dona su infraestructura, es decir provee de equipos routers, ancho de banda, enlaces, etc. De manera voluntaria para que otras personas puedan navegar de manera privada.

2.2. Historia de la Red Tor

Para conocer un poco de la historia de la red Tor, debemos retroceder el tiempo, ya que la red Tor es una evolución o una segunda versión de Onion Routing.

Onion routing o como se lo dice en español encaminamiento cebolla, es el primer proyecto para la búsqueda de anonimato al navegar o intercambiar paquetes de datos a través de una red, y así preservar la privacidad de forma limpia entre quienes interactúan en ella.

Así se logra el objetivo principal de la red Tor y de onion routing que es el tener una comunicación privada a través de una red pública.

Onion Routing fue expuesto por primera vez por David M. Goldshlag, Michael Reed y Paul Syverson.

Con este antecedente ahora si podemos entender la historia de la red Tor y porqué fue creada.

La red Tor, surgió de manera oficial (paso la etapa alfa y beta) en el 2003, creada por Roger Dingledine, Nick Mathewson y Paul Syverson, (entendemos que Paul Syverson estuvo en el proyecto inicial y en la segunda versión) como un proyecto del laboratorio de investigación naval de los estados unidos, inicialmente financiado por dicho laboratorio y progresivamente pasó en el 2004 a ser financiado por Electronic Frontier

Foundation hasta noviembre del 2005 cuando pasa a ser parte de una organización sin ánimos de lucro llamada Tor Project.

Actualmente la red Tor sigue en constante desarrollo, y es liderado por Roger Dingledine.

Tor ha ganado varios premios entre ellos recibió un premio de la organización Free software foundation por proyectos a beneficio social, como mención en "permitir que aproximadamente 36 millones de personas de todo el mundo, usando software libre, hayan experimentado libertad de acceso y de expresión en Internet manteniendo su privacidad y anonimato." **(Wikipedia, 2015)**.

En sencillas palabras y como se explicó antes la red Tor tiene un objetivo primordial que es el anonimato, no revelar una dirección ip y así no revelar una ubicación exacta de un usuario y además mantener el contenido que viaja a través de la red Tor seguro y privado. Esto puede tener connotaciones buenas y malas. Las buenas ya las mencionamos la privacidad, pero si no existe una regla o un control en una red que mantiene la privacidad del contenido, podríamos enviar cualquier tipo de contenido desde el acceso root a un servidor de la NASA, hasta el planeamiento de un ataque terrorista a una ciudad en medio oriente.

2.3. Usos de la Red Tor

El uso de la red Tor puede ser ilimitado, en si todos queremos que nuestros datos sean privados, a nadie le gusta ser vulnerado o espiado, existen muchos sitios desde los cuales miran tus movimientos, transacciones, que has realizado en el sitio, y luego te bombardean con productos dependiendo de tu navegación, lo cual puede ser molesto.
En si podemos decir que el uso de la red Tor es ilimitado.

Entonces vamos a describir algunos usos comunes:

- **Familia:** Una familia puede usar una red Tor para protegerse, para no ser espiados y para proteger a sus hijos. Para proteger conversaciones privadas, emails con amigos entre otras cosas.

- **Empresas y Compañías:** Muchas empresas y compañías tienen datos privados muy importantes desde una clave de acceso a un email hasta el acceso a la cuenta bancaria. Generalmente los usuarios de una empresa intercambian accesos, documentos, archivos privados para la empresa y a veces lo hacen a través de emails. Con una red Tor estos protocolos serían mucho más seguros ya que no podrían ser espiados al momento de intercambiar información.

  Por otro lado si accedemos a una cuenta bancaria desde una red normal podríamos llegar a ser vulnerados, conociendo desde donde se accede generalmente a dicha web, su ubicación etc. Si manejamos una red Tor esto no pasaría y la seguridad de la empresa se elevaría.

- **Activismo Político:** El espionaje en el activismo político es muy común, todo partido político quiere saber los planes de su contrario, todo régimen quiere saber que planea su oposición.

  La red Tor es una gran herramienta en esta área ya que el cyber espionaje en la misma es muy alto, podemos entender que la red Tor es una herramienta eficaz para no ser espiados al momento de intercambiar información.

- **Medios de comunicación:** Todo medio de comunicación quiere ser el primer en dar la noticia más reciente, además sus investigaciones online pueden ser protegidas a través de una red Tor.

- **Milicia, tácticas militares, etc:** La inteligencia militar es algo muy importante, se debe proteger siempre la información militar ya que esta conlleva evitar ataques terroristas, ataques extranjeros, proteger a civiles entre otras cosas. El intercambio de información online a través de una red segura y privada ayuda mucho a que esto se cumpla.

Podríamos describir muchas más áreas, pero como repetimos el uso es prácticamente ilimitado, se puede usar en donde se quiera proteger la privacidad del cliente y de su información. Y en un mundo en el que todos estamos conectados a través de redes sociales, emails, etc. ¿Quién no quisiera proteger su privacidad e información?

2.4. Funcionamiento de la Red Tor

Para entender la red Tor primero debemos hablar de los componentes que usa para que pueda funcionar.

OR (onion router o enrutador onion): funciona como un encaminador es decir enruta los paquetes al destino con la información proporcionada por el directorio.

OP (onion proxy): El cliente o usuario final sería siempre el encargado de ser el proxy a través de un software específico, el cual obtiene información del directorio, generan circuitos aleatorios en la red y transmite la información a través de la red de OR's.

Las conexiones OR-OP no son permanentes. Un OP debería cerrar una conexión a un OR si no hay circuitos ejecutándose sobre la conexión y ha vencido cierto temporizador.
Directorio: Es una base de datos de OR con información de cada uno de los OR's (descripción del router), esta base de datos la puede acceder cualquier OR y cualquier usuario final y así tener pleno conocimiento de la red.

Si tenemos pocos directorios o servidores de directorios se puede correr el riesgo de que toda la red falle, por lo cual existen varios servidores de backup y cache de servicios de directorio.

El servicio de directorio es en realidad un grupo de OR's confiables, toda la información que entra a los directorios son protegidas criptográficamente con firmas digitales, esto quiere decir que solo las firmas registradas de OR's confiables pueden proporcionar información a la base de datos del directorio. Es así como si aparece un nuevo OR este

debe ser registrado y firmado en los OR’s confiables para que pueda acceder a la base de datos del directorio.

Esto es un método para proteger de ataques agregando nodos OR’s que no son confiables a la red, si añadimos muchos nodos que no están registrados y no existiera este tipo de seguridad, la base de datos del directorio fallaría, sería un hueco de seguridad ya que puede ser que un OR no confiable este agregado en esa base de datos y este OR proporcione información a terceros y rompa el concepto de privacidad de la red Tor.

No hay sistema automático para aprobar OR's; Los administradores del servidor de directorio lo hace manualmente.

Cuando se registra un nuevo nodo OR, en esta base de datos se describe a él, su funcionamiento y sus capacidades.

Entre algunos campos o atributos de la base de datos están:

- Dirección ip
- Nombre amigable al usuario
- Versión de software de Tor
- Sistema Operativo

Ya con los antecedentes de los componentes de la red Tor, podemos ver su funcionamiento en tres pasos sencillos a través de un ejemplo:

Paso 1:

Supongamos que Cliente A ha entrado a utilizar la red Tor, por lo tanto se bajó el cliente Tor y configuro su máquina para poder empezar a utilizar dicha red.

El cliente obtiene una lista de nodos o OR’s del servicio de directorios.

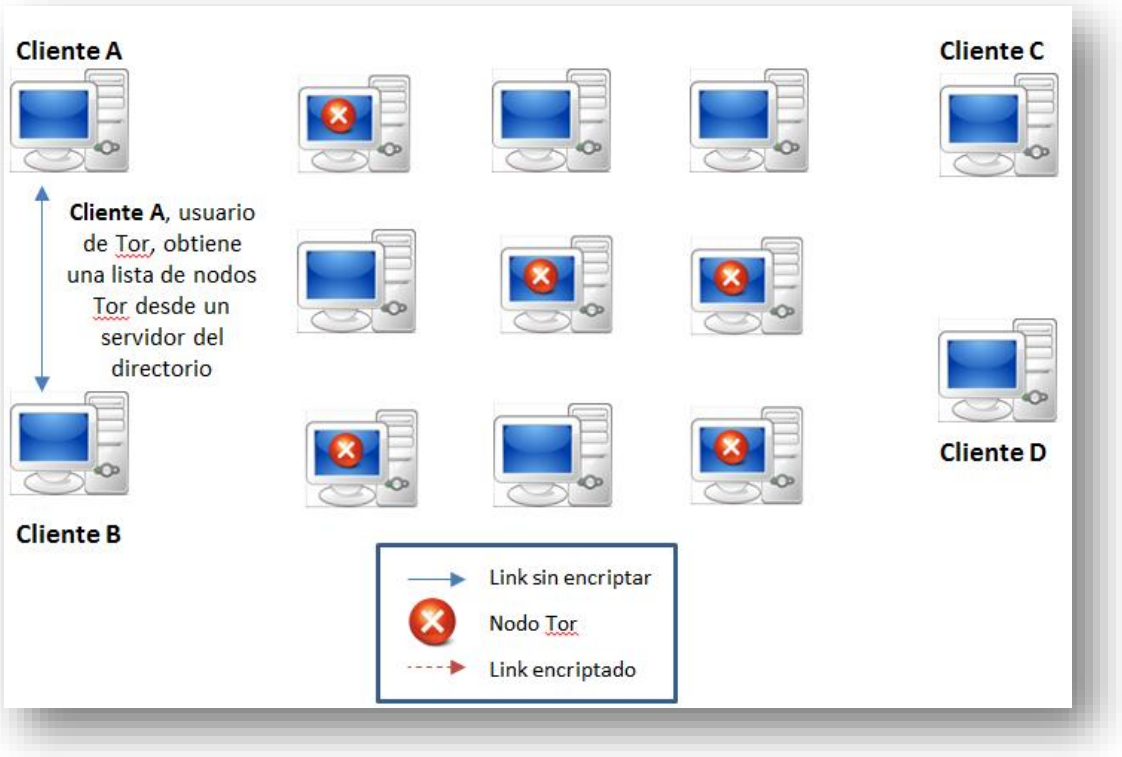

Figura 2.1 Paso 1, como funciona la red Tor (Guillén & Vicente, 2015)

Paso 2:

El cliente de Tor, el cliente A, que es un OP escoge la ruta aleatoria para llegar a su destino a través de conexiones encriptadas, como la ruta es aleatoria a través de los nodos, en ningún punto se puede saber el destino final del paquete.

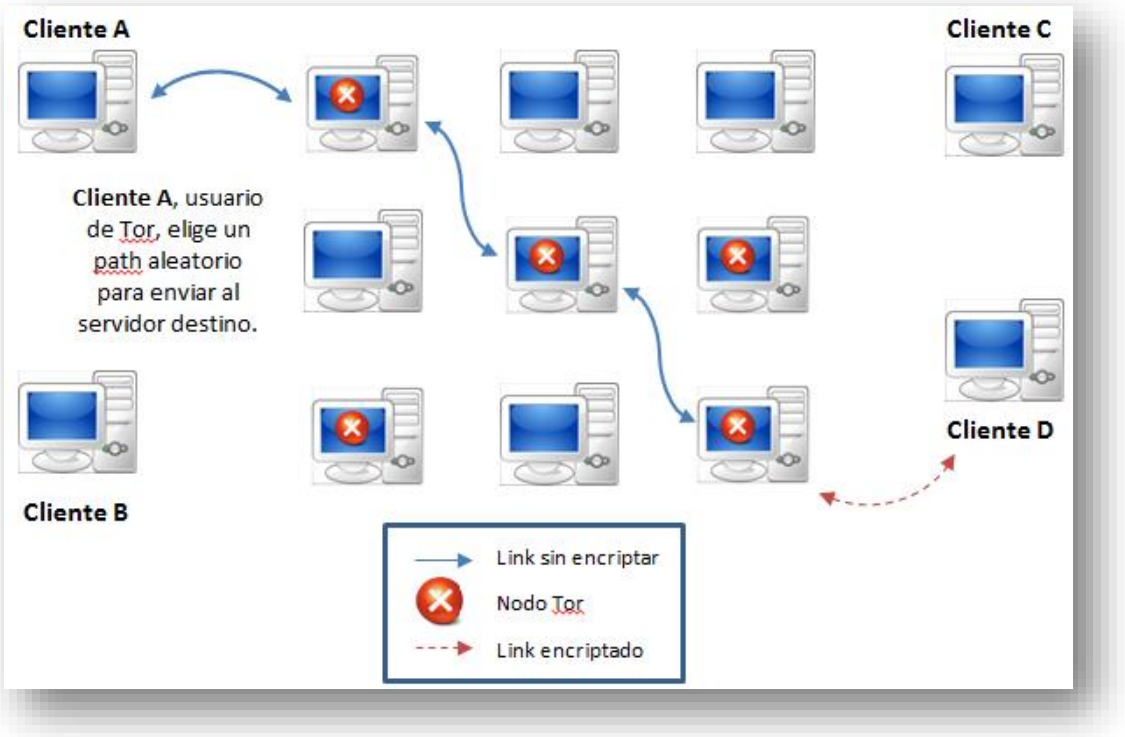

Figura 2.2 Paso 2, como función la red Tor (Guillén & Vicente, 2015)

Paso 3:

Una vez creada la ruta, se pueden enviar y recibir paquetes, a través de diferentes tipos de software, una web, etc. Tor solo trabaja con conexiones TCP, cualquier software que maneje este tipo de conexiones será compatible con la red Tor.

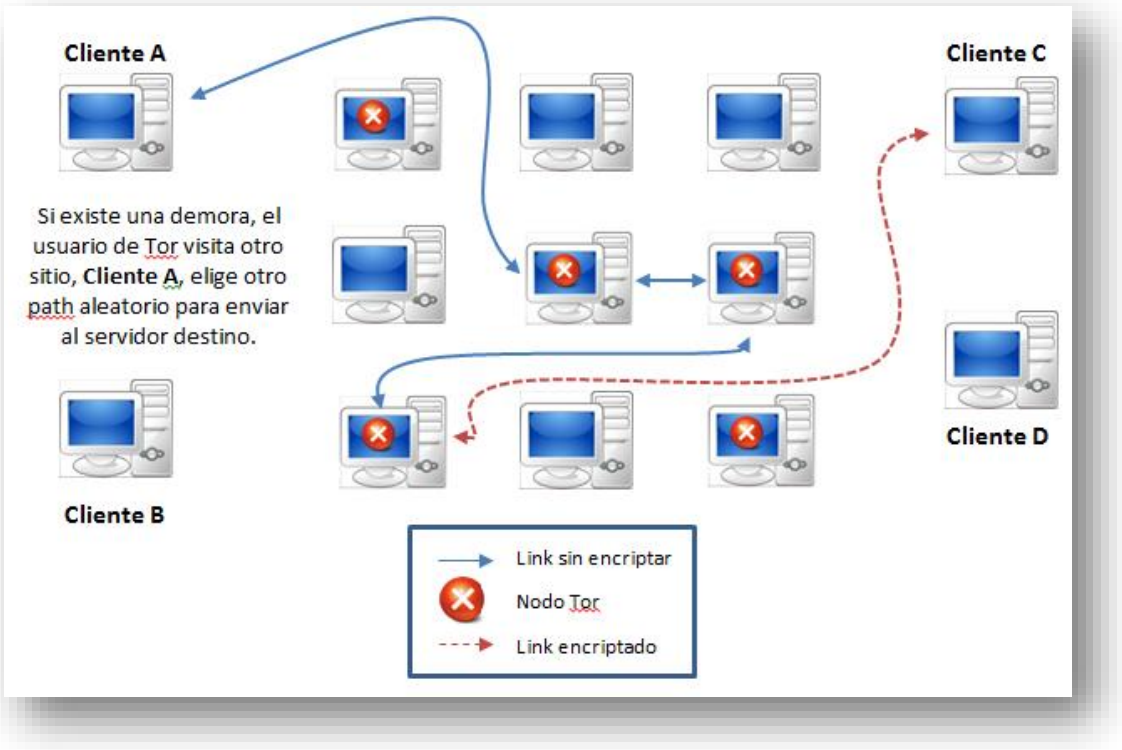

Figura 2.3 Paso 3, como función la red Tor (Guillén & Vicente, 2015)

Después el Cliente A visita otro sitio, así el cliente Tor, genera otra ruta aleatoria que llegue al nuevo destinatario final, y se repite el proceso.

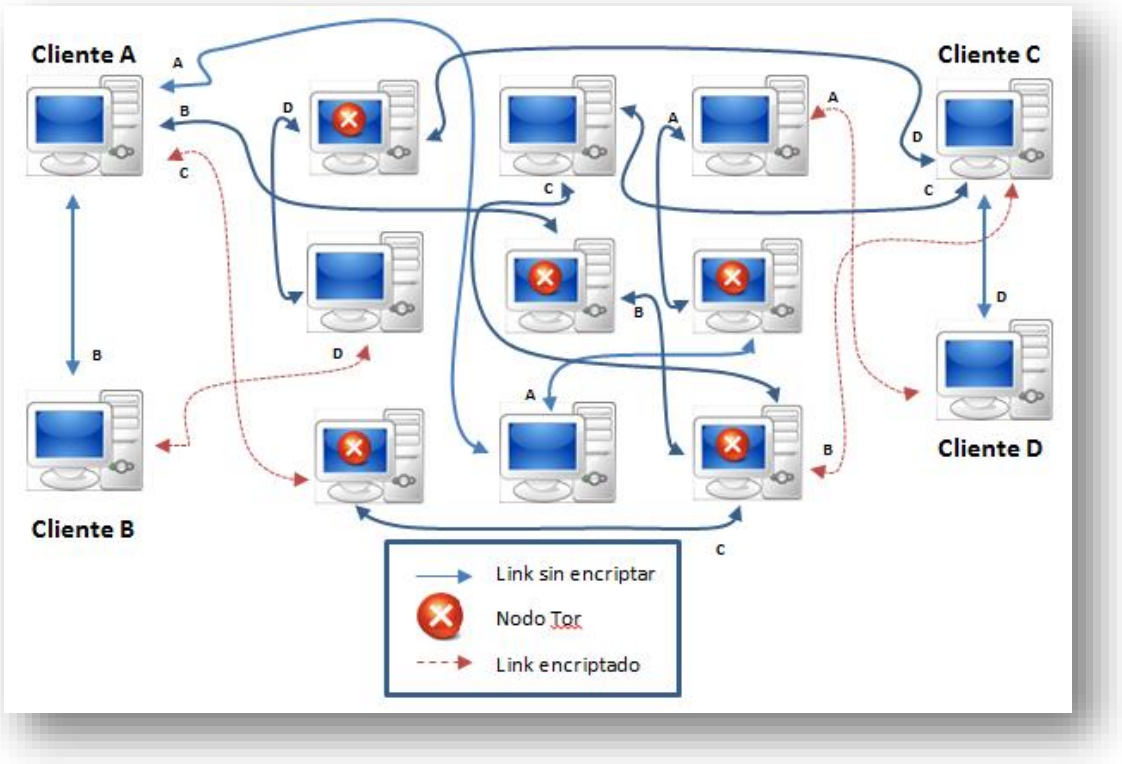

Figura 2.4 Como navegarían 4 usuarios en la red Tor (Guillén & Vicente, 2015)

2.5. ¿Es la Red Tor completamente infalible?

Con todo lo que hemos hablado, podríamos asumir que la red Tor es completamente segura, ni los propios nodos RN conocen el destino final del mensaje a excepción del primero y el último, pero esto no asegura que sea un sistema infalible, ya que sabemos bien que ningún sistema es completamente perfecto.

Como mencionamos antes, ni los propios nodos intermedios conocen el destino final del mensaje, así que si se llega a interceptar uno de estos nodos de igual manera no podríamos obtener mucha información, pero que pasa si analizamos el tiempo de envío de paquetes, si el tiempo se repite de manera constante podemos asumir que un nodo está conectado a otro ya que transmiten la información en el mismo tiempo. Cabe recalcar que aun así se debe des encriptar el mensaje original, por lo que de igual manera sería un trabajo muy difícil.

Existe un caso específico en la que influenciaron todas estas teorías y se rompió el anonimato de los usuarios de la red Tor.

Un exploit instalado en el navegador de la red Tor (Tor browser) rompía el anonimato de los usuarios y enviaba una dirección ip real de los usuarios y su navegación a un servidor remoto.
Pero **¿cuál es la razón de atacar a un proyecto que lo que busca es ayudar al usuario a proteger su información?**

Al ser una red que mantiene el anonimato de la navegación y del usuario, esta es usada para ser un nido de un gran número de webs de mercado negro, por esta razón varias organizaciones han tratado de hackear la red o por lo menos controlarla para así poder conocer los usuarios que trabajan y consumen en este mercado negro.

2.6. Velocidad de la Red Tor

Al conocer su funcionamiento, podemos entender que los datos de navegación pasan por varios nodos, así que no debemos esperar que la red Tor tenga un tiempo de respuesta rápido o similar a la navegación común en internet.

2.7. Red Tor 100% anónimo

La red Tor no te va a garantizar el anonimato al 100%, ya que eso también depende mucho de tus patrones de navegación.

Generalmente las personas tienen un patrón establecido de navegación, acceden a su correo, acceden a sus redes sociales, miran una película, etc. Esto puede generar patrones que pueden identificarte con un nombre y el patrón generado.

Además debemos entender que cualquier script como un Activex, javascript, flash, etc. Podría obtener tus datos de navegación sin que te des cuenta. Es por esta razón que todos estos complementos vienen desactivados por defecto en el navegador Tor a excepción del javascript que siempre es necesario para una experiencia de usuario y navegación completa.

2.8. Proyectos desarrollados con la Red Tor

El principal proyecto realizado con la red Tor es la misma red Tor y su proyecto Anonymity Online el cual busca que las personas en todo el mundo usen la red explicando las bondades de la privacidad, sus ventajas y que puede pasar si no usas una navegación privada.

Entre los proyectos que usan la red Tor tenemos:

- **Tor Browser:** un browser para navegar en la red Tor.
- **Arm:** una terminal al más puro estilo unix, para monitorear conexiones, pings, entrada y salida de paquetes, etc.
- **Metrics Portal:** Un aplicativo para medir métricas tales como uso de ancho de banda, número de usuarios entre otras.
- **Obfsproxy:** Un proxy para evitar censores de los protocolos de la red Tor.
- **ORBOT:** un explorador para sistemas android
- **Shadow:** Un simulador de red que corre toda la red Tor como plugin
- **Stem:** librerías python y scripts que interactúan con la red Tor
- **Tails:** sistema operativo basado en Linux pre configurado con todo lo necesario para usar la red Tor. (puede ser usado como live cd o live usb)
- **Torbirdy:** cliente para envío y recepción de emails a través de la red Tor.
- **Tor2web:** Permite a usuarios de internet, navegar por webs usando la red Tor a través de servicios escondidos.

- **Txtorcon:** control del protocolo de Tor a través del lenguaje python, tiene mucha documentación para entender más acerca de Tor.

- **OONI:** Open Observatory of Network Interference recupera datos de buena y alta calidad utilizando herramientas opensource para compartir observaciones y datos sobre los distintos tipos, métodos, y las cantidades de redes de manipulación en el mundo.

2.9. Empresa en Ecuador que usa Red Tor

Iniciamos la búsqueda de una empresa que haga uso de la red Tor para un sin número de actividades dentro de la empresa. El resultado de la búsqueda nos guió a una empresa que tiene un gran peso dentro y fuera del país. De antemano queremos informarles que por cuestiones de confidencialidad de su información, la empresa nos solicitó que nos reservemos el uso del nombre su entidad, a cambio de contenido que nos permita concluir con la investigación de esta disertación.

La empresa, que por cuestiones mencionadas anteriormente, la llamaremos 'R2 Save Car', esa empresa se dedica al servicio de rastreo, monitoreo, compra y venta de vehículos, lo diferente de esta empresa es que todo lo hace a través del internet.

Un resumen de cómo se surgió esta empresa dentro del Ecuador, la empresa 'R2 Save Car' inició su operaciones en Ecuador hace 13 años, ofrece servicios de avanzada tecnología gracias a la alianza estratégica que mantiene con otros países de la región y con Estados Unidos. Gracias al esfuerzo de las personas que trabajan en la empresa, ha recibido varios premios de calidad y ha logrado expandir su presencia en Perú y Bolivia.

La misión y visión de la empresa es dar servicio rastreo, monitoreo, compra y venta de vehículos, en un futuro tienen en mente liderar el mercado gracias a sus estándares de servicio y de calidad.

La empresa hace uso de la red Tor mediante la aplicación "we.riseup". Nos preguntamos, porqué la aplicación "we.riseup" fue elegida por la empresa?.

Al investigar más a fondo sobre lo que hace “we.riseup”, nos encontramos que se trata de un sitio web que provee distintas herramientas de correo, chats y listas de usuarios, las cuales se caracterizan por tener un nivel de seguridad sobre los parámetros normales. Esto es posible gracias a que no se almacenan direcciones IP. Toda información que es enviada y recibida a través de mails, chats y sus listas de usuarios se mantiene almacenada en servidores “riseup”. Estos servidores salvaguardan la información de manera encriptada. Únicamente el usuario que sea propietario y tenga conocimiento de su contraseña, podrá hacer uso de ellos.

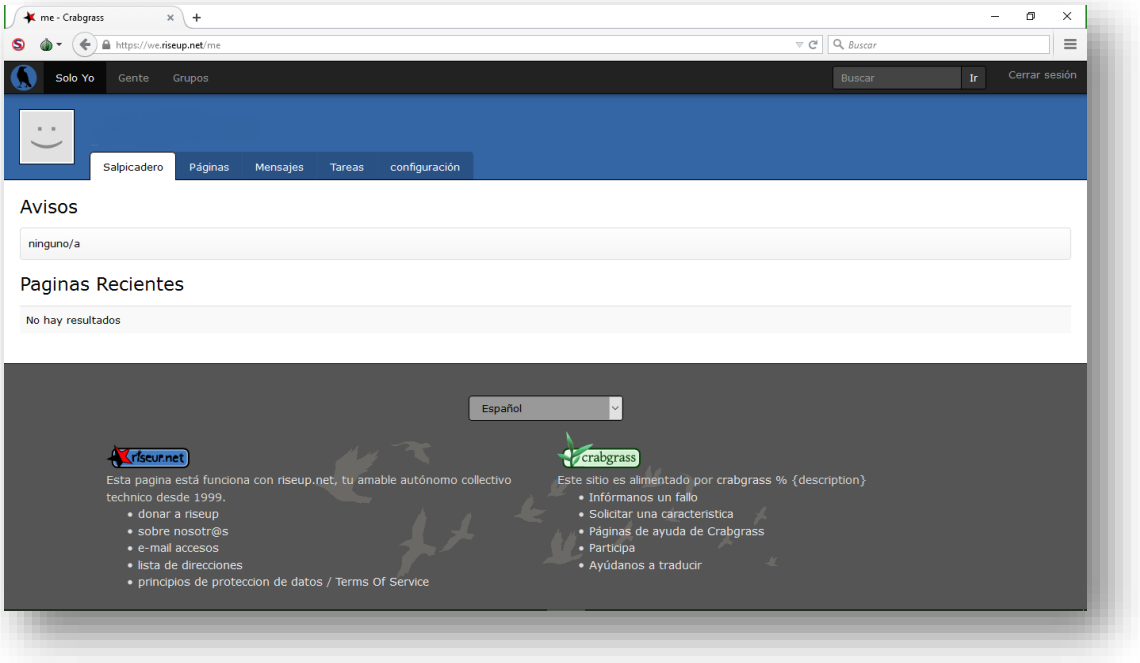

Figura 2.5 Página we.riseup.net (Guillén & Vicente, 2015)

Para continuar con la respuesta a nuestra pregunta, la obtuvimos a través de una de las personas encargadas del manejo de una de sus cuentas en “we.riseup”, que por motivo de anonimato lo llamaremos “Mario”.

Mario nos comentó que las actividades de su trabajo demandan que se envíe información confidencial de compras, ventas, pedidos, solicitudes, encargos, transacciones, maneja bases de datos con información personal de clientes, etc.

También nos contó que consideraron usar un servicio de mail corporativo abierto, pero corrieron un riesgo muy alto, ya que su información era expuesta a gente que no debía llegar a conocer los movimientos que se realizaban al llegar a un acuerdo con la empresa. Es por esto que decidieron hacer uso de la herramienta "we.riseup" utilizando la red Tor. Con la cuenta de mail, se mantiene su información encriptada y tiene la seguridad que nadie puede tratar de interceptar estos datos. La empresa guarda toda la información de manera confidencial, así solo los dueños de esa cartera de clientes van a saber dónde está esa información y el manejo de cada uno de ellos dentro de la Deep web.

Mario nos comenta, que sus clientes se encuentran muy a gusto con la política del manejo confidencial de información y el servicio ofrecido a través de la Deep Web.

También que hubo casos donde algunos de sus clientes querían ocultar tanto su identidad, que trataron de suplantar identidades, llevando a cabo contratos legales de compra y venta de autos. Las transacciones no se llegaron a completar debido a que la empresa se encarga de validar los datos de los clientes antes de cada transacción. El cliente que quiso suplantar la identidad, nunca más se contactó con la empresa.

Esta fue la poca y suficiente información que nos podía proveer la empresa. Les damos gracias a la distancia por su colaboración y su confianza depositada en nosotros.

Esta investigación fue de gran ayuda, con un grado de dificultad alto, al no haber empresas que utilicen la Deep Web para realizar sus negocios, especialmente utilizando la red Tor. Es realmente imposible que una empresa preste información de su material de trabajo utilizando la Deep Web. Muchas empresas si llegaran a utilizar este medio seguramente preferirían que su método de contactarse con el cliente no sea de conocimiento público y prefieren mantener su negocio en anonimato.

3. GUÍA METODOLÓGICA PARA USUARIOS Y EMPRESAS

3.1. Herramientas para uso de la Red Tor

Una de las características más atractivas que tiene el uso de la Red Tor es su gran capacidad de entregarnos un nivel de anonimato a través del Internet sin ningún impedimento ni complicación. El principal objetivo del uso de la red Tor es que cualquier persona pueda utilizar esta herramienta y tenga acceso a toda la red.

Para lograr este objetivo, TOR desarrollo un software que funciona de forma sencilla y agradable al usuario: "Tor Browser" .El software está integrado en un paquete portable, y puede ser empleado en sistemas operativos Windows (versiones de 32bits y 64 bits), Mac OSx y Linux.

Este software protege su información transmitiendo las comunicaciones desde la computadora o dispositivo, hacia una red de repetidores. Esto evita que los sitios descubran la situación física del dispositivo.

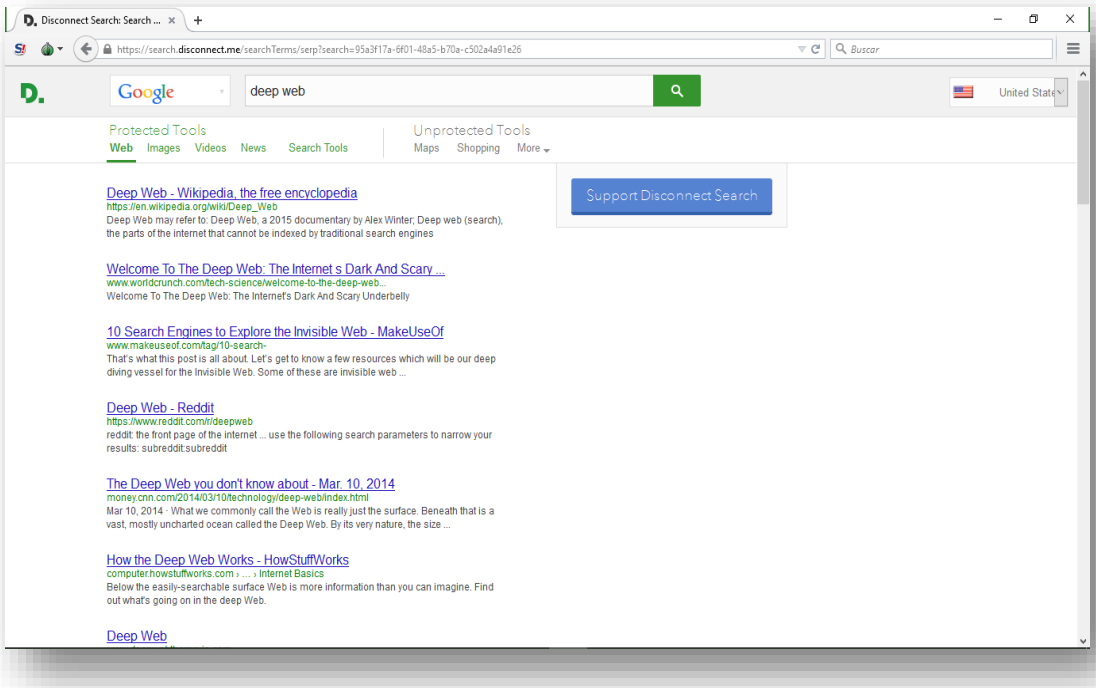

Figura 3.1 Ejemplo de navegación del Tor Browser (Guillén & Vicente, 2015)

3.2. Donde encontrar y como instalar el navegador Tor Browser

En el portal oficial del proyecto de red Tor, se encuentra toda la información referente a esta red. En uno de los links se puede descargar el paquete que contiene el instalador para hacer uso del navegador.

En esta parte del capítulo se explica cómo instalar el navegador y sus complementos para tener una navegación totalmente segura.

Figura 3.2 Página Oficial de Tor Project (Tor Project: Anonymity Online, 2006)

3.2.1. Configuración Automática

Antes de realizar todo el proceso de instalación tenemos que desactivar el Firewall y el Antivirus, ya que algunos de los links o archivos que se van a descargar pueden ser detectados como virus.

Una vez desactivado el firewall y antivirus, comenzamos con la instalación. Para poder descargarnos el instalador, debemos ir a la página principal de red Tor:

“https://www.torproject.org/”. En la página se va a desplegar todo lo que deseamos saber sobre esta red.

Una vez adentro de la página oficial, hacemos click en “Download”, como se muestra en la imagen de abajo, en el recuadro rojo:

Figura 3.3 Descarga del browser de Tor (Guillén & Vicente, 2015)

Después de eso, se despliega una pantalla donde aparece un botón para descargar el paquete.

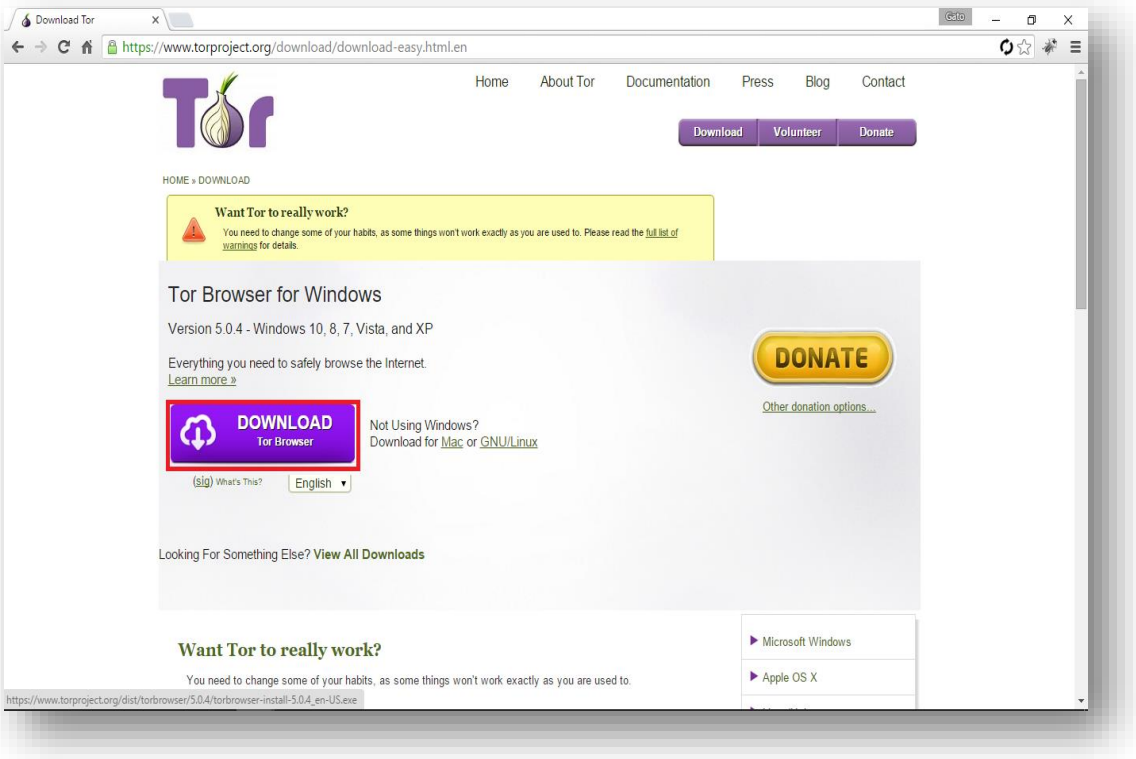

Figura 3.4 Detalles de descarga del Paquete (Guillén & Vicente, 2015)

Si es que no usamos Windows como sistema operativo, también existe un paquete tanto para Linux como para Mac:

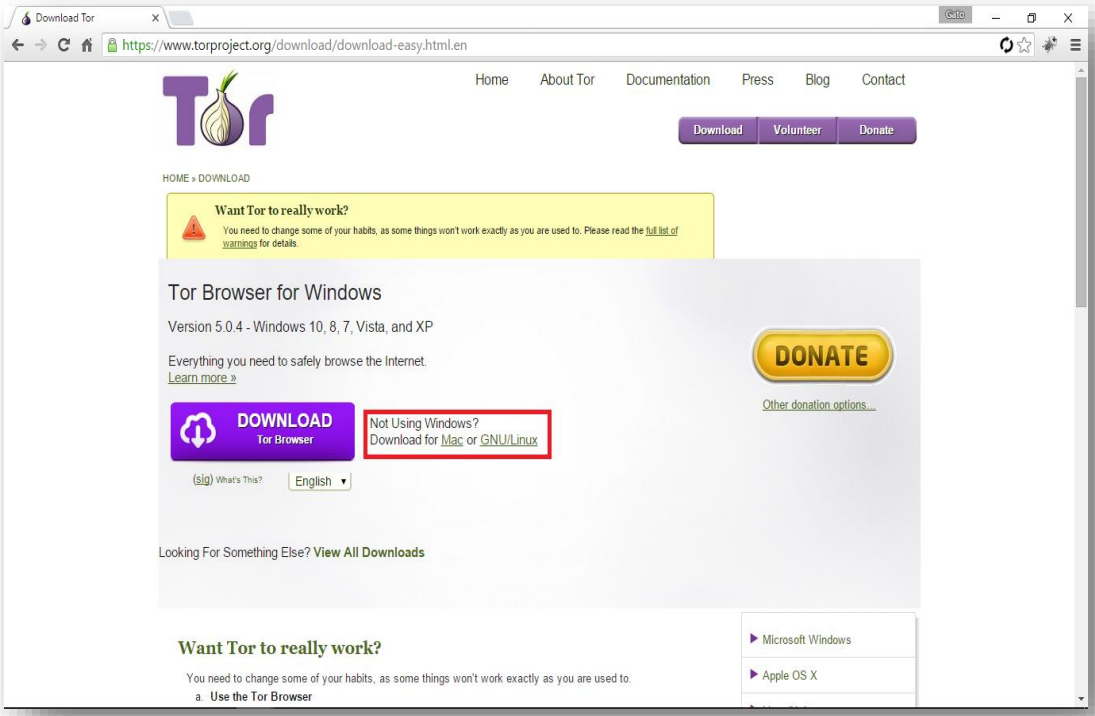

Figura 3.5 Links de descarga para otras plataformas (Guillén & Vicente, 2015)

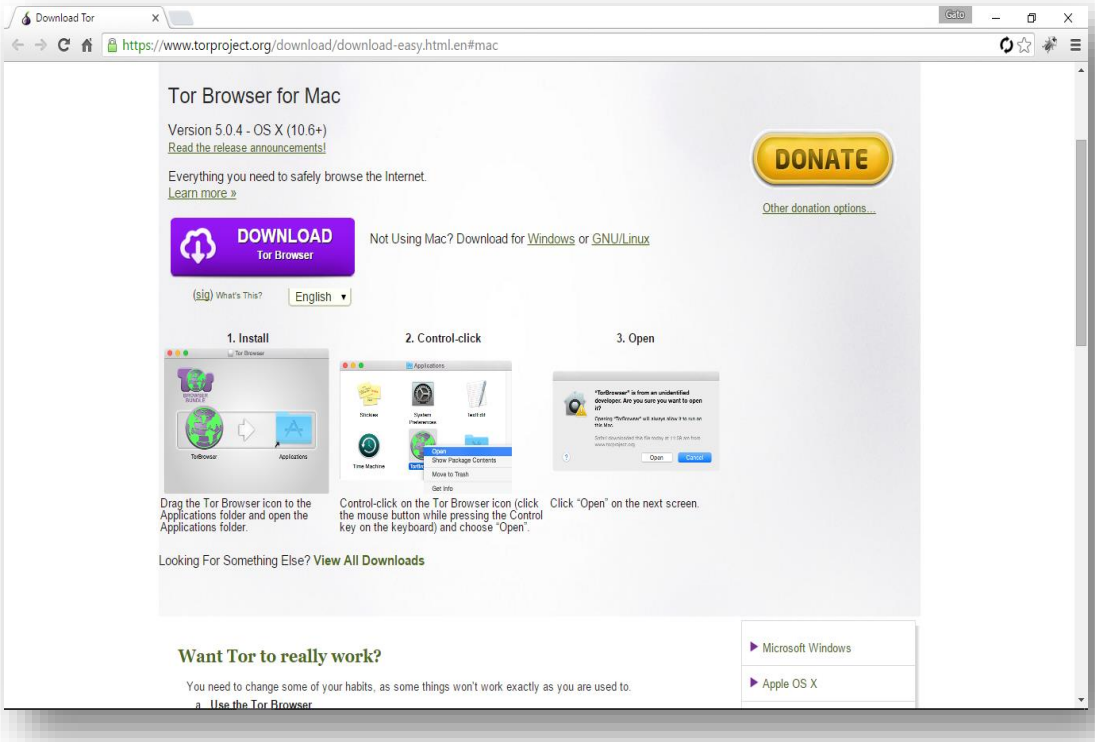

Figura 3.6 Detalles de descarga del Paquete para Mac (Guillén & Vicente, 2015)

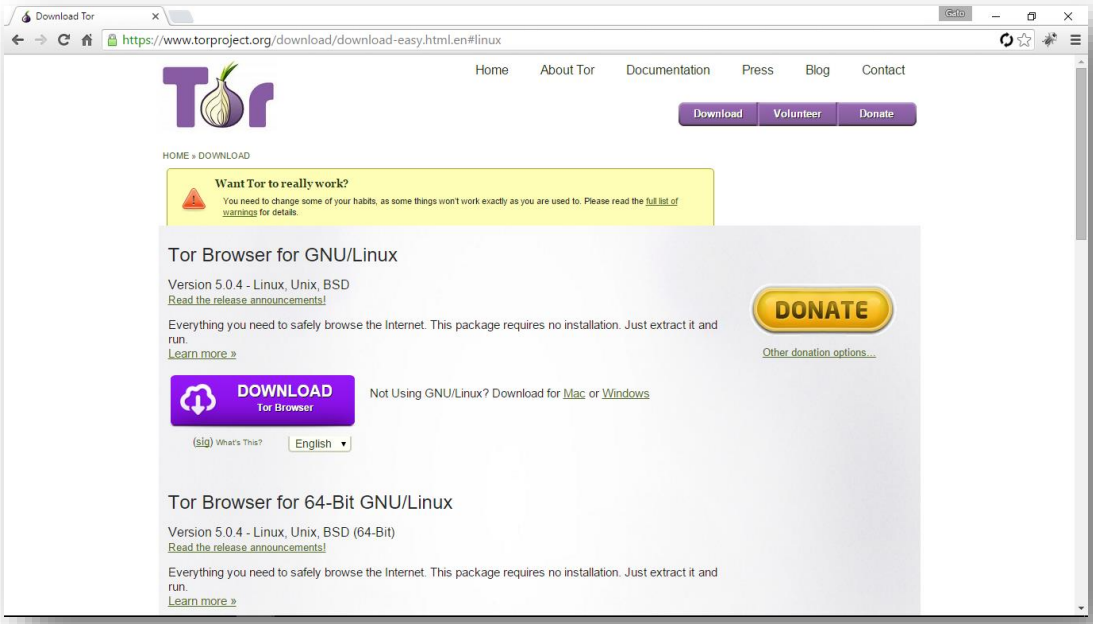

Figura 3.7 Detalles de descarga del Paquete para GNU/Linux (Guillén & Vicente, 2015)

En el siguiente link se puede ver todos los instaladores para las diferentes plataformas que soporta el navegador de Red Tor: “https://www.torproject.org/download/download.html.en”.

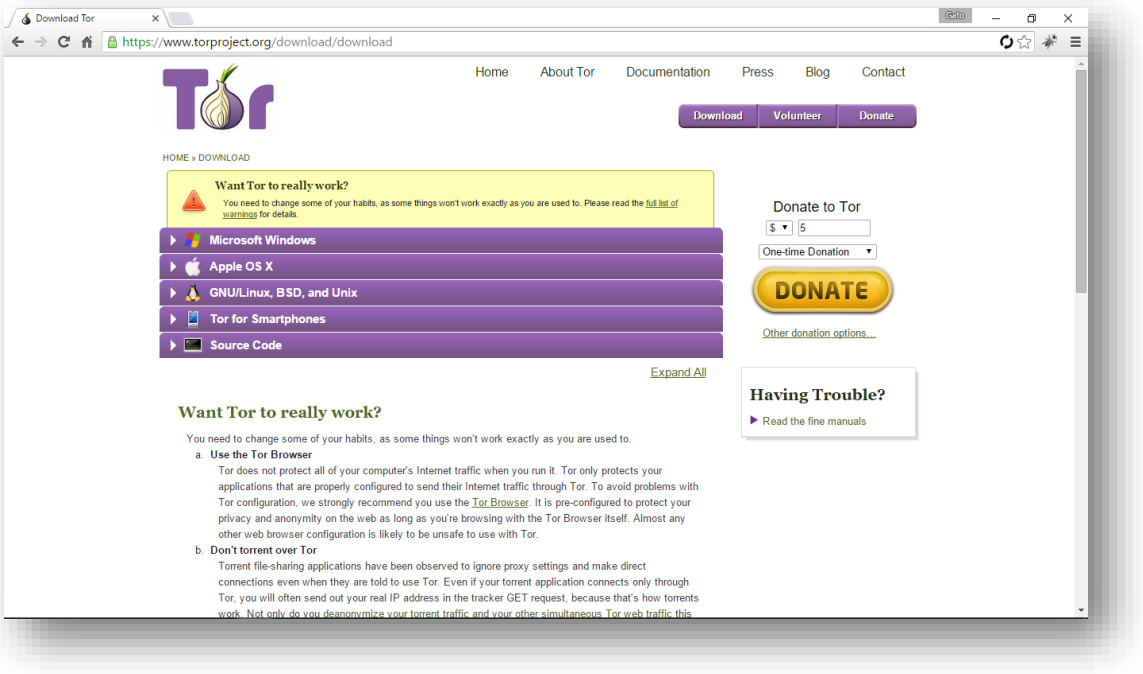

Figura 3.8 Links de descarga para diferentes plataformas (Guillén & Vicente, 2015)

Una vez descargado el paquete de instalación, hacemos doble click en el archivo descargado. Nos va a aparecer una pantalla donde vamos a escoger el idioma para la instalación:

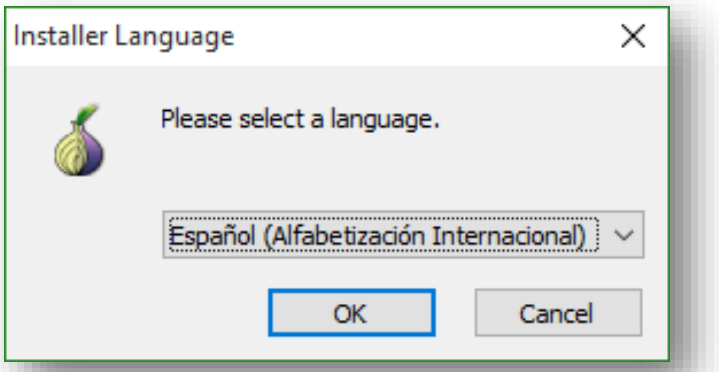

Figura 3.9 Selección de lenguaje para la instalación (Guillén & Vicente, 2015)

Después de escoger el lenguaje, nos pedirá el destino donde va a ser instalado el navegador. Por defecto, se instala en “C://Archivos de Programa/Tor_Browser”, pero nosotros podemos instalar en la carpeta o disco de nuestra preferencia.

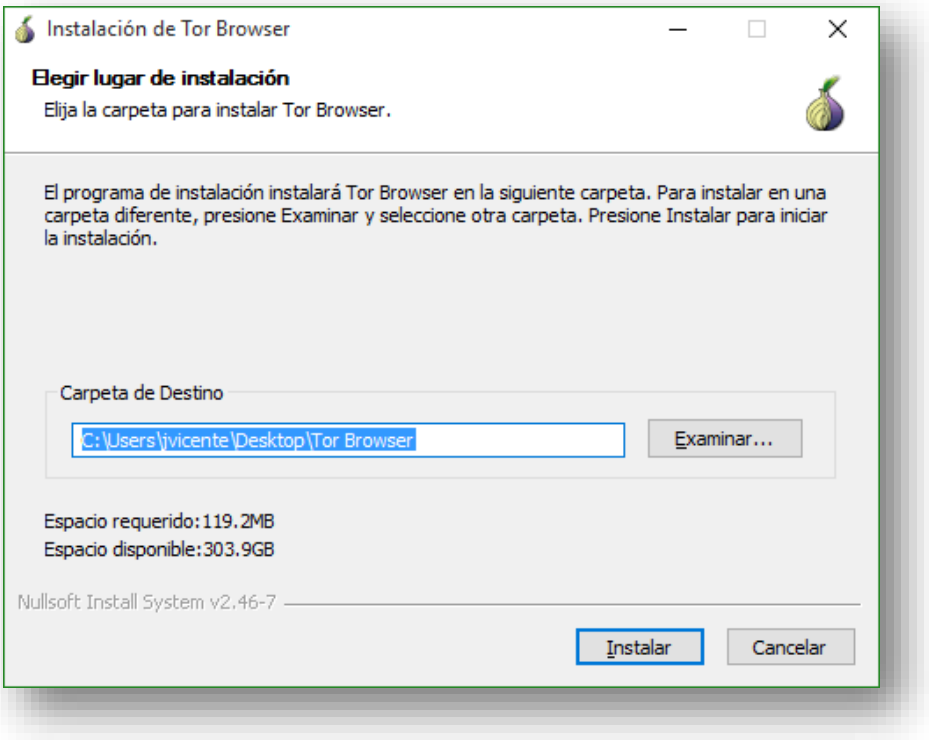

Figura 3.10 Selección del destino de instalación (Guillén & Vicente, 2015)

Una vez seguro del destino de la instalación, damos click en "Instalar". Posteriormente comenzará el proceso de instalación, y si no existen problemas, culminará con éxito.

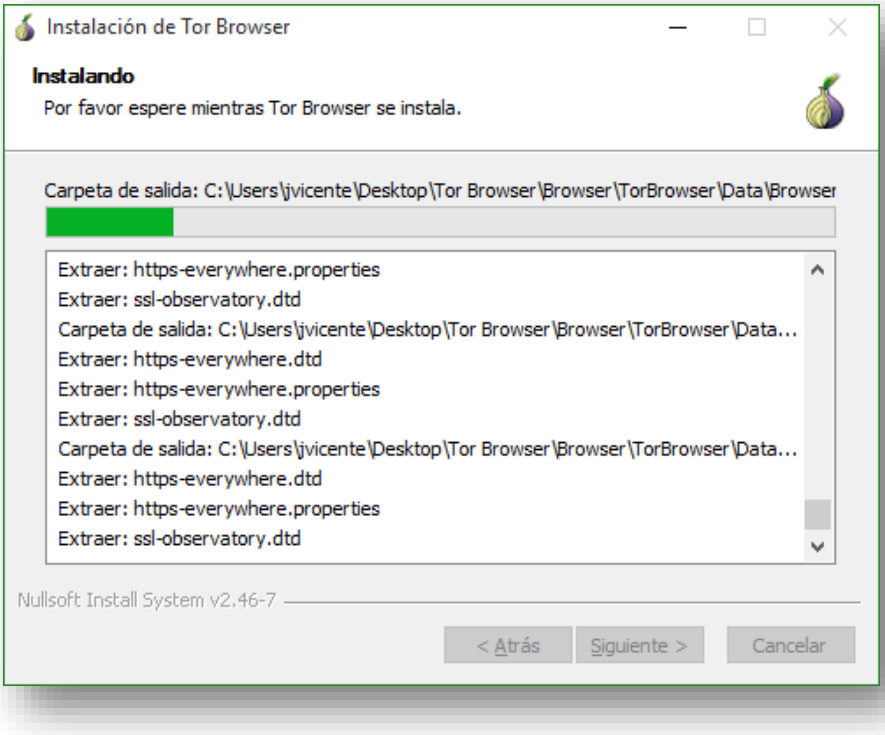

Figura 3.11 Proceso de Instalación del Browser de Tor (Guillén & Vicente, 2015)

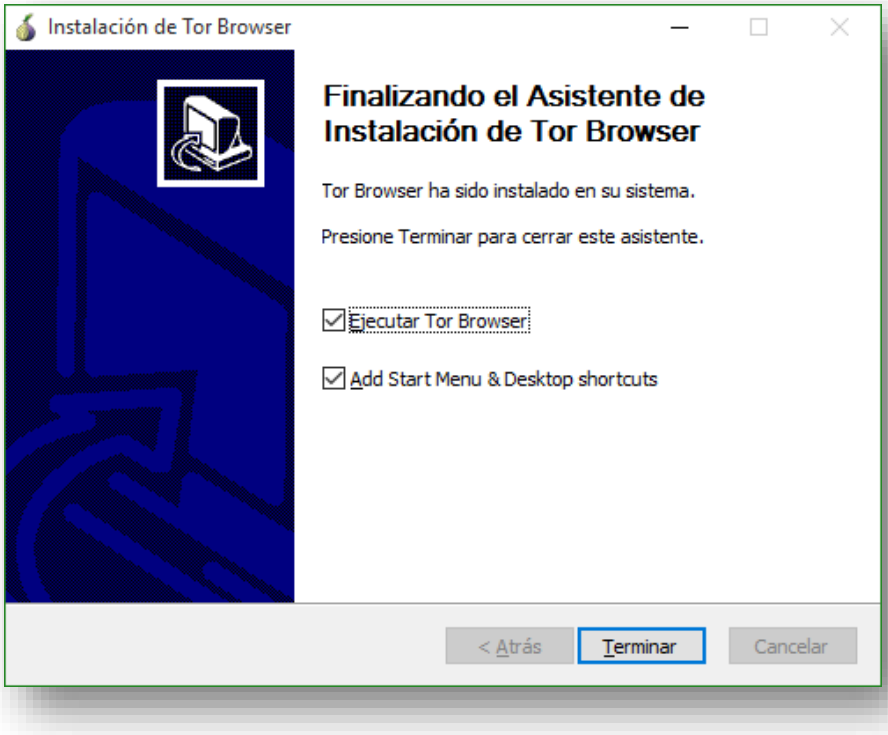

Figura 3.12 Pantalla de Finalización de la Instalación (Guillén & Vicente, 2015)

3.2.2. Configuración Manual

En esta parte se va a mostrar como configurar de forma manual para poder usar el navegador de Red Tor

Lo primero que vamos a instalar es un aplicativo que se llama Privoxy.

Privoxy es un proxy web que usa conocimiento avanzado para la protección y filtrado del contenido de la página web. Este aplicativo es compatible con sistemas mono y multi usuario.

Para instalar el complemento, debemos dirigirnos a la página oficial de Privoxy: "http://www.privoxy.org/". Ya dentro de la página, en la parte de Descarga, nos va a decir que el instalador está en el sitio SourceForge

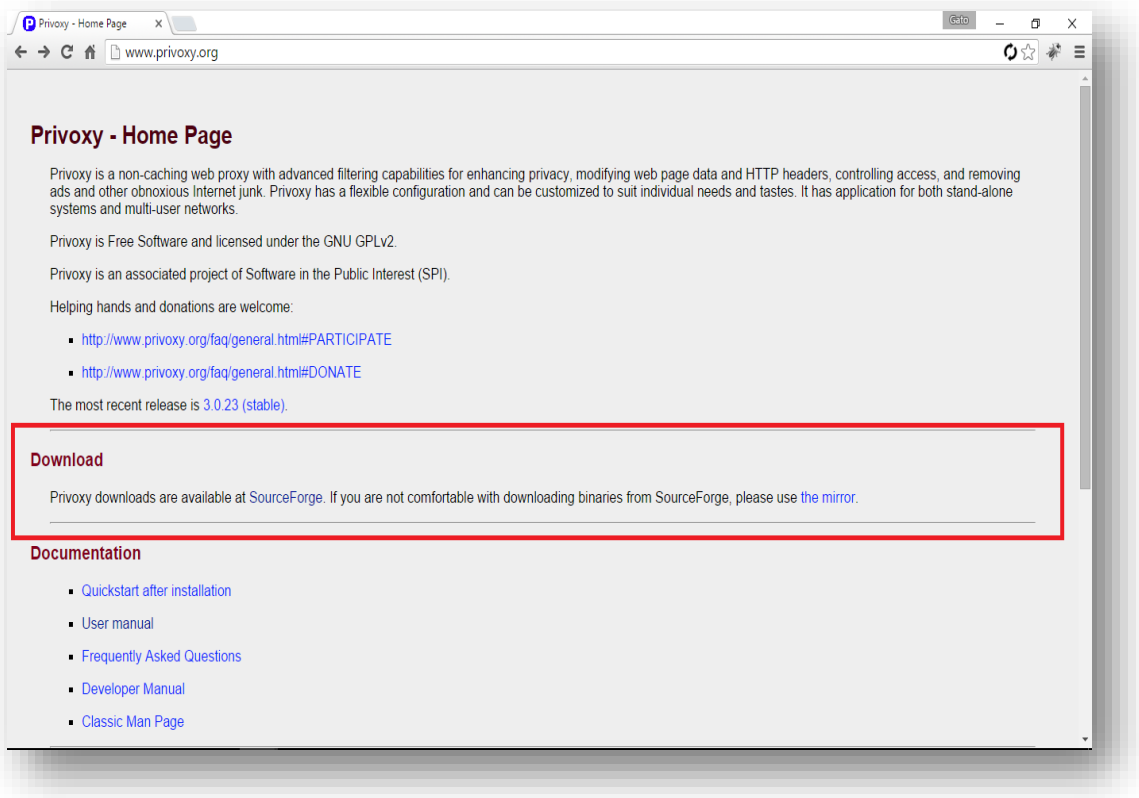

Figura 3.13 Página oficial de Privoxy, descarga. (Guillén & Vicente, 2015)

Al hacer click en SourceForge, nos va a redirigir a la página web de SourceForge donde están alojados los instaladores de las diferentes plataformas:

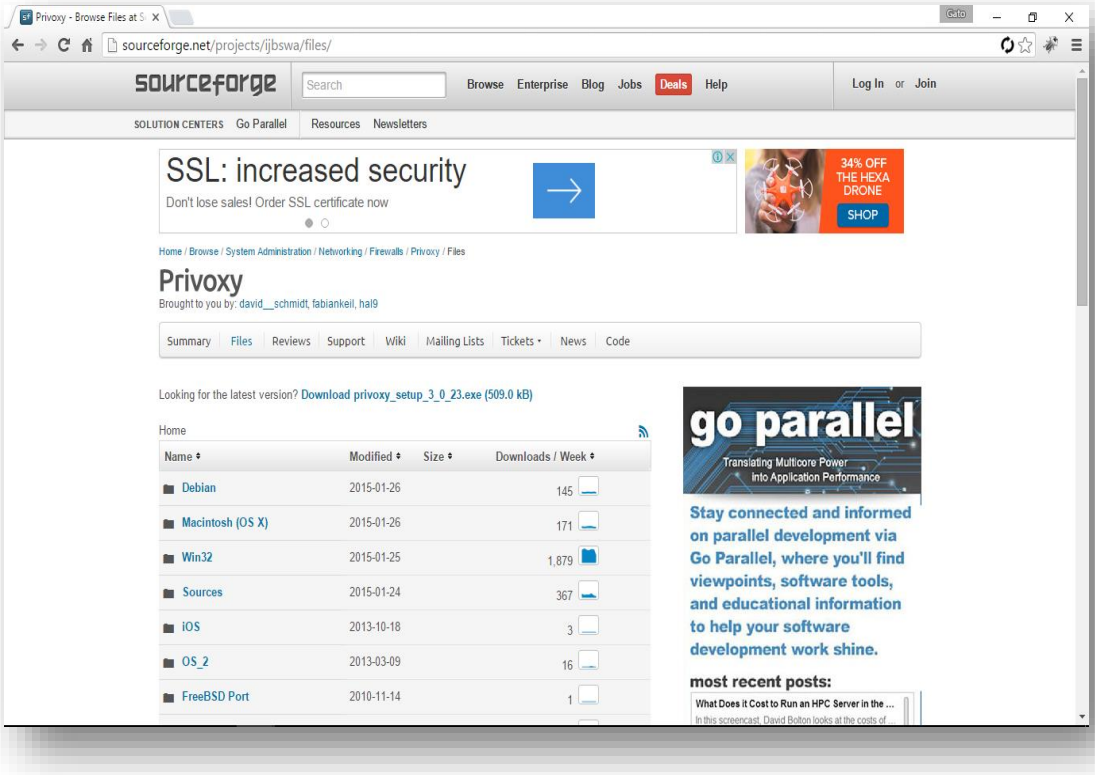

Figura 3.14 Página oficial de SourceForge donde están alojado los instaladores de Privoxy. (Guillén & Vicente, 2015)

Hacemos click en el lugar donde nos indica la última versión, tal como se muestra en la imagen de abajo en el recuadro rojo:

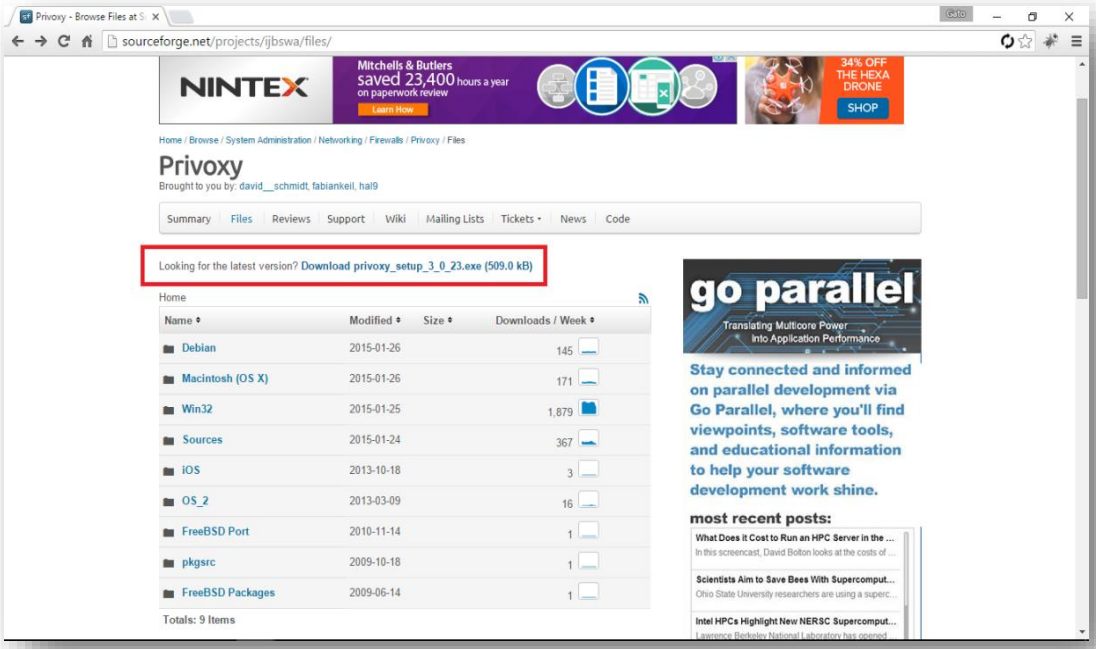

Figura 3.15 Links instalación última versión de Privoxy. (Guillén & Vicente, 2015)

Una vez descargado el archivo, ejecutamos el instalador. Nos va a solicitar los componentes queremos instalar, lo más recomendable es dejarle por defecto, como se enseña en la imagen:

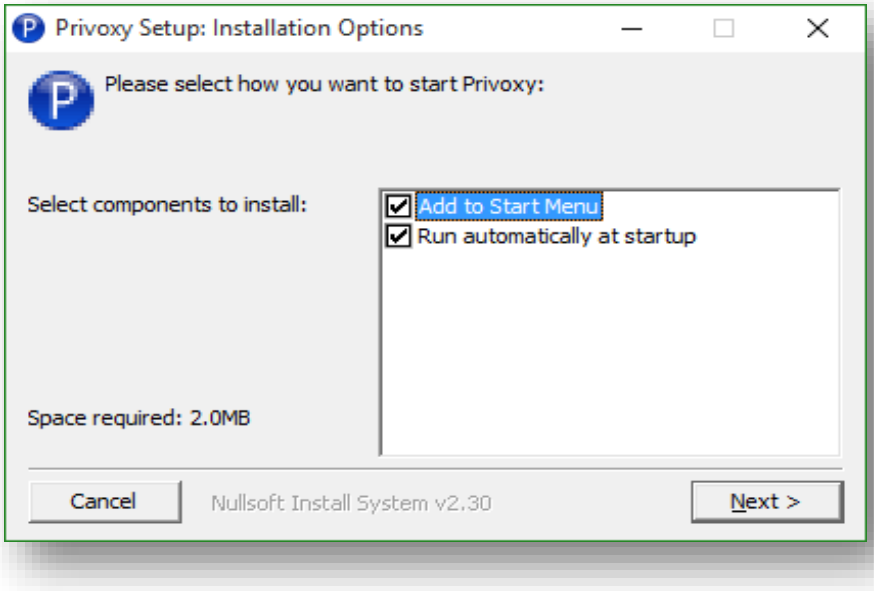

Figura 3.16 Selección por defecto de componentes de Privoxy. (Guillén & Vicente, 2015)

Se selecciona la ubicación del directorio de instalación. Una vez seleccionado se da click en "Install" y se instalará sin problemas:

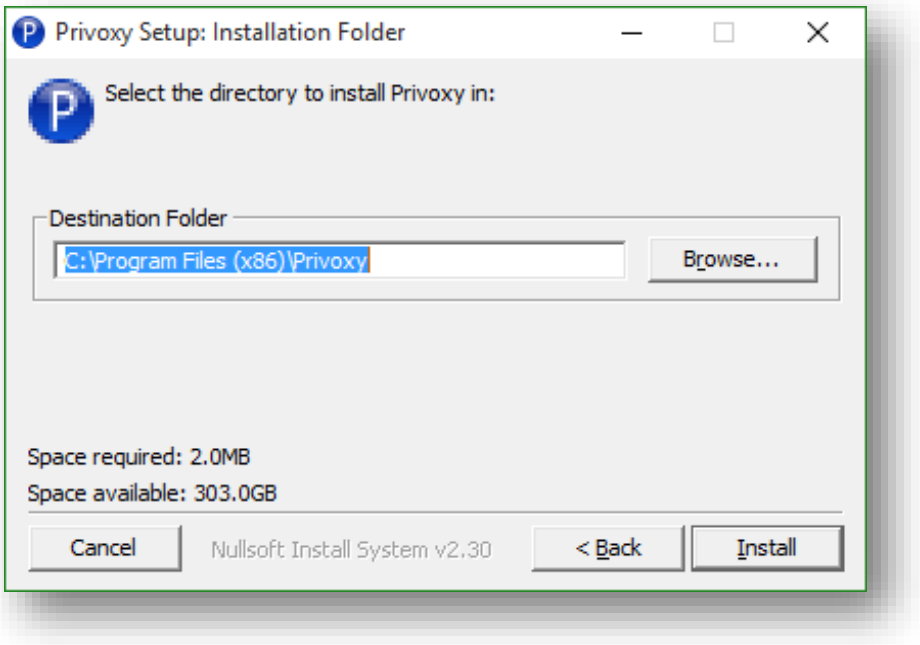

Figura 3.17 Selección del directorio de instalación. (Guillén & Vicente, 2015)

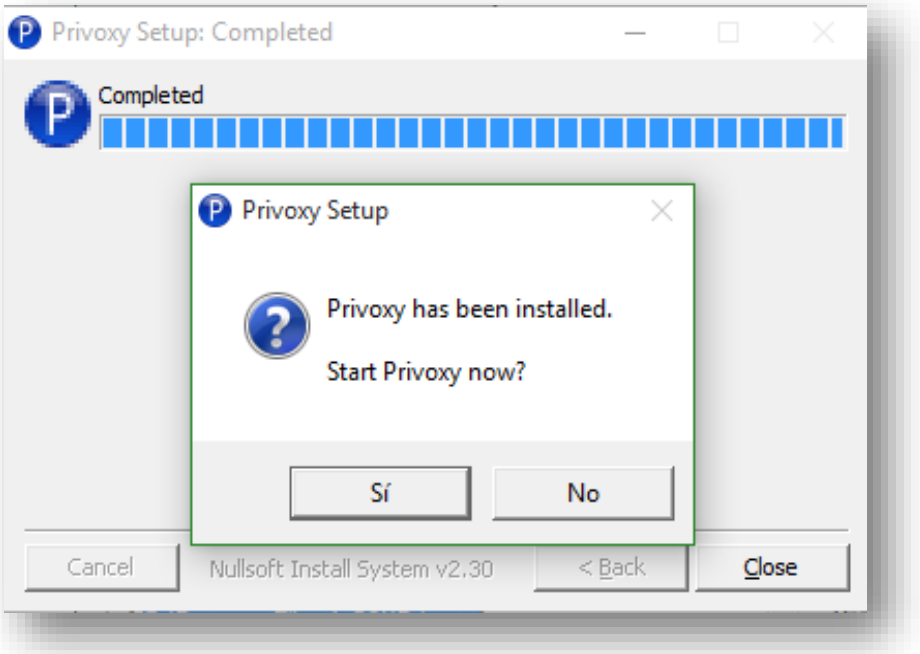

Figura 3.18 Instalación Exitosa (Guillén & Vicente, 2015)

Después de haber instalado Privoxy, se procederá a configurar: Nos dirigimos a "Options" → "Edit Main Configuration"

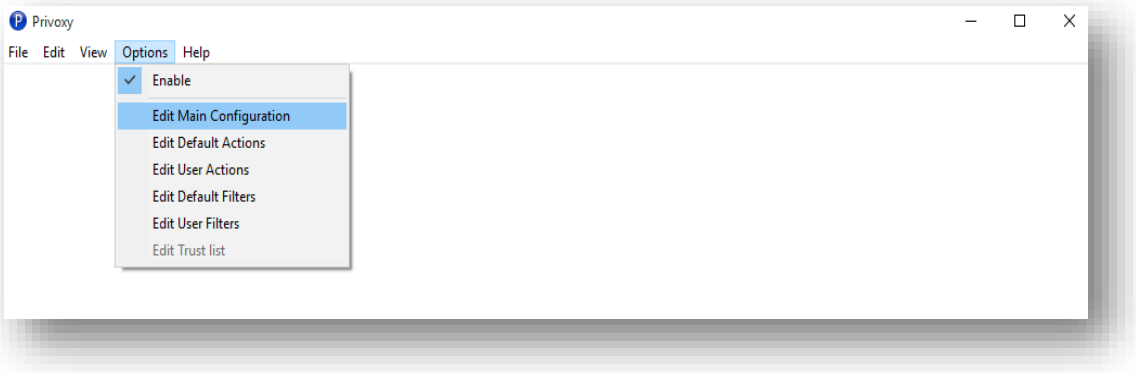

Figura 3.19 Pantalla de Privoxy (Guillén & Vicente, 2015)

Se abrirá el archivo config.txt. En ese archivo debemos incluir la línea "forward-socks4a / localhost:9050", y guardamos.

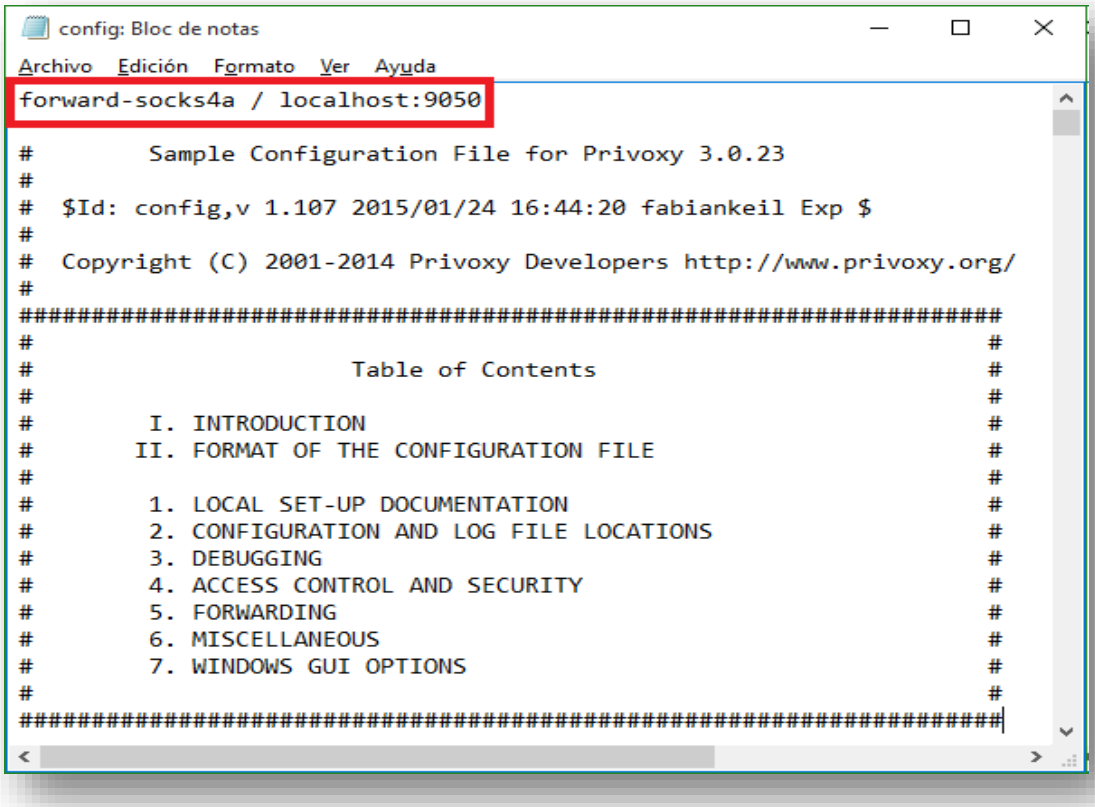

Figura 3.20 Archivo de configuración *config.txt* (Guillén & Vicente, 2015)

Ahora tenemos que configurar un navegador para usar Red Tor. En Mozilla nos dirigimos a Herramientas → Opciones

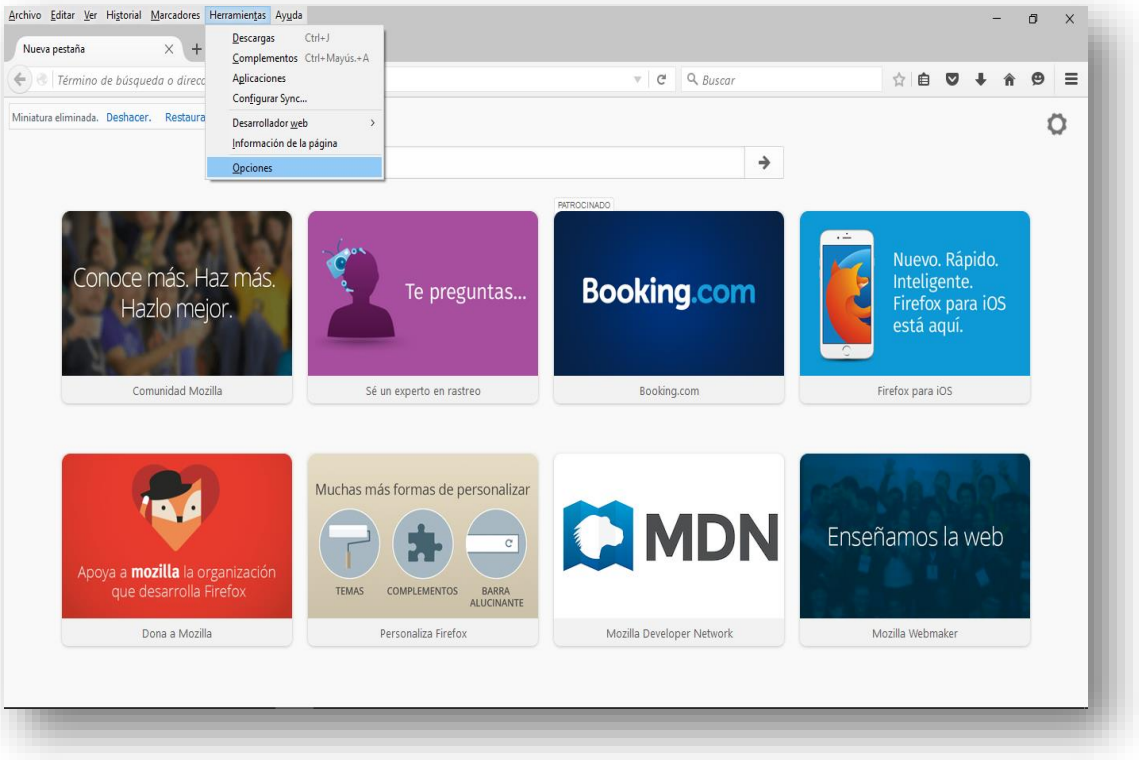

Figura 3.21 Pantalla del Navegador Firefox (Guillén & Vicente, 2015)

Después Avanzado→ Red → Configuración

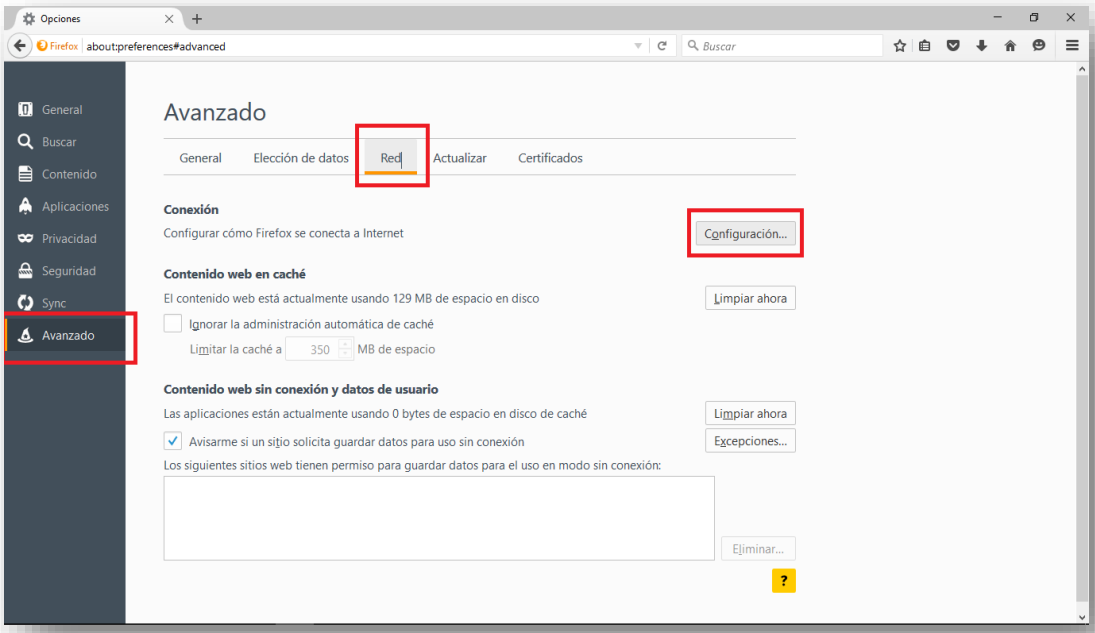

Figura 3.22Configuración avanzada de conexión (Guillén & Vicente, 2015)

Se cambia los parámetros de IP y puertos: se debe poner localhost y puerto8118, tal como se ve en la figura 3.2.2.11:

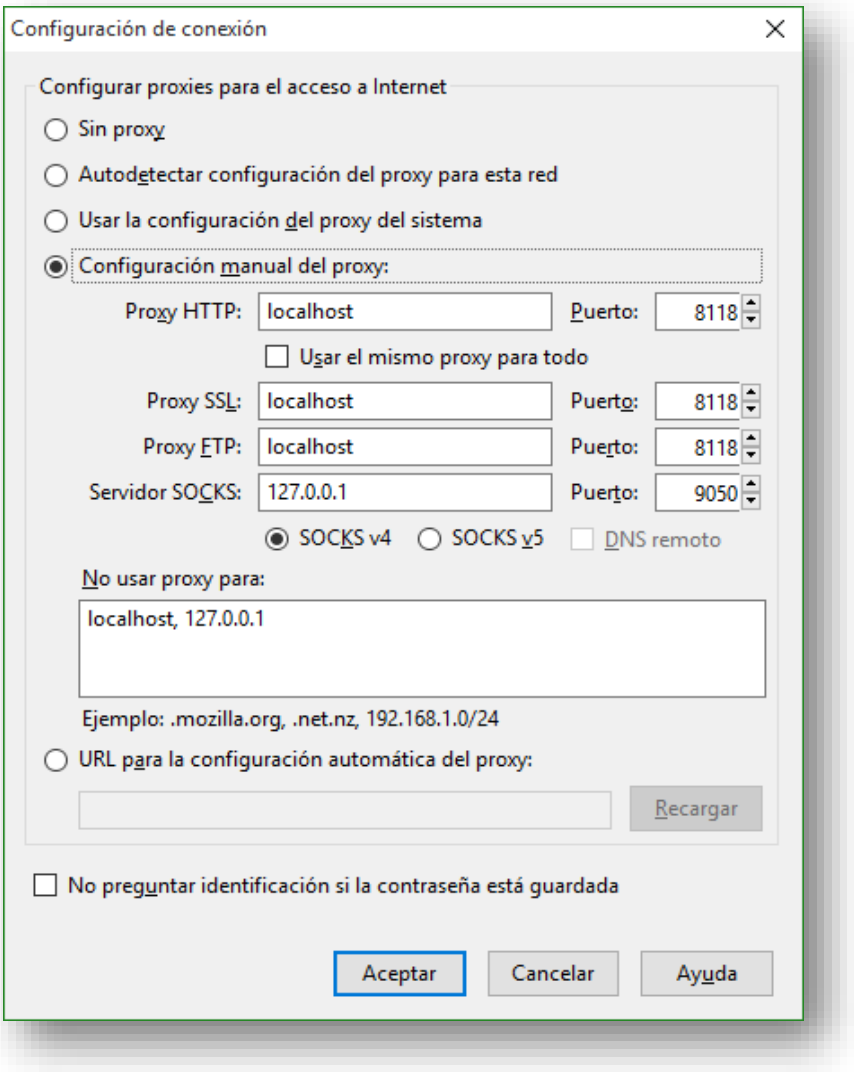

Figura 3.23Cambio de parámetros de IP y puertos (Guillén & Vicente, 2015)

Una vez cambiado los parámetros del proxy, se ejecutar un navegador y se comprobará que se tiene acceso a la red Tor

Cuando hemos acabado de instalar el navegador y los complementos, hacemos doble click en el icono creado en el escritorio del Navegador para el uso de la red Tor:

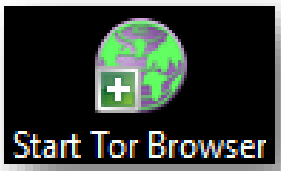

Figura 3.24 Icono de Red Tor (Guillén & Vicente, 2015)

Se desplegará la siguiente pantalla, que es el panel de configuración de la red Tor.

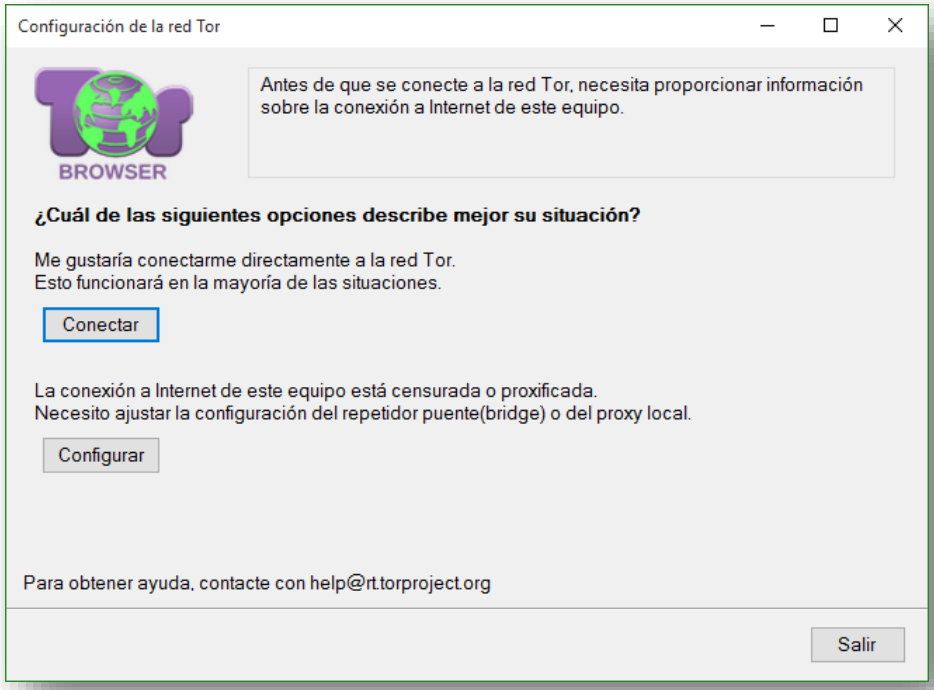

Figura 3.25Configuración de la red Tor (Guillén & Vicente, 2015)

En la pantalla se encuentran 2 botones "Conectar" y "Configurar".

a) Conectar, se hará la configuración predeterminada y se presentará una pantalla con el progreso de la conexión.

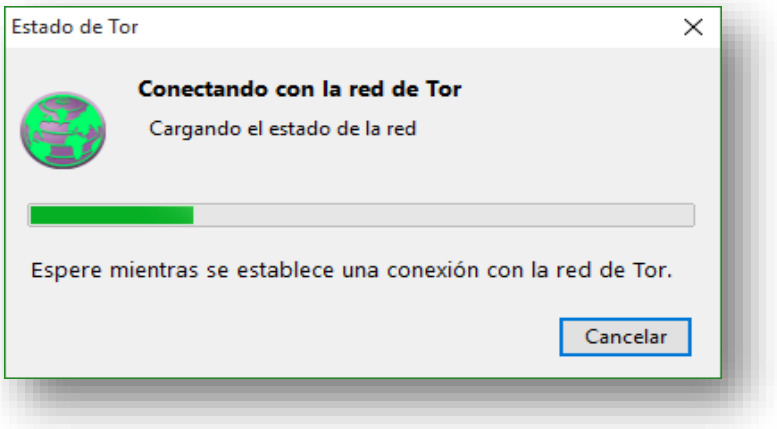

Figura 3.26 Estado de conexión (Guillén & Vicente, 2015)

b) Configurar, esta opción la usan usuarios con un conocimiento más avanzado sobre redes y también cuando la red es monitoreada o está bloqueado. Para esto la red usa "puentes" para no ser detectado.

Aparecerá una pantalla preguntando si el proveedor de servicios de internet bloquea o censura alguna forma de conexiones hacia Tor.

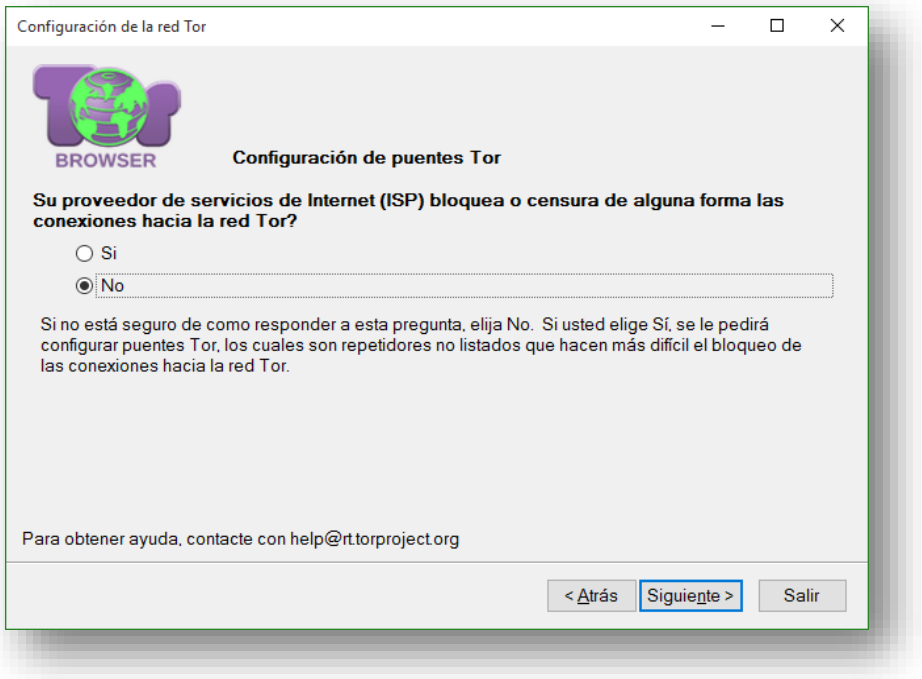

Figura 3.27 Icono de Red Tor (Guillén & Vicente, 2015)

Si uno no está seguro de cómo responder la pregunta debe seleccionar NO.

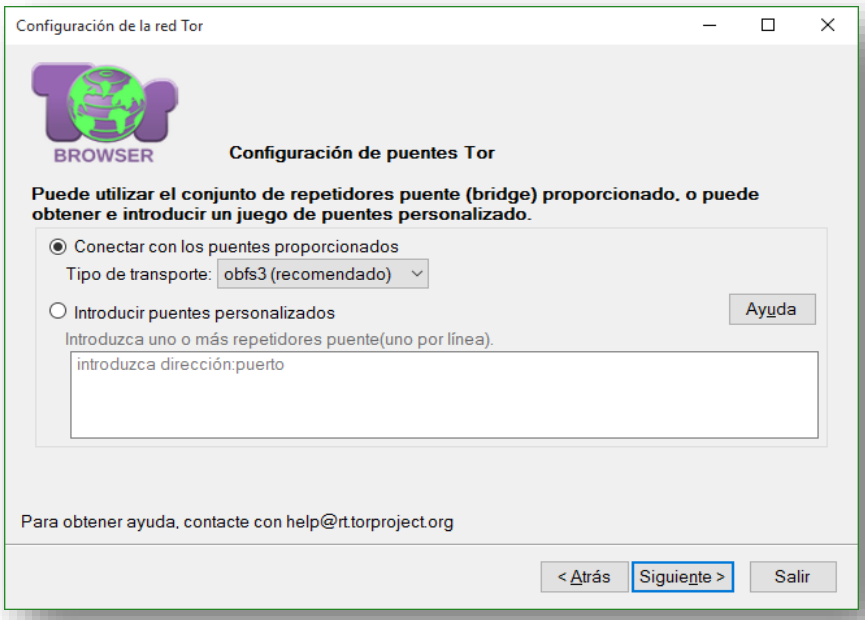

Figura 3.28 Configuración de conexión por puentes proporcionados (Guillén & Vicente, 2015)

Lo recomendado es usar la configuración de puentes por defecto. Una vez configurado los puentes aparecerá una pantalla con el estado de la conexión y posterior finalización.

Figura 3.29 Página principal de la Red Tor (Guillén & Vicente, 2015)

Para comprobar nuestra privacidad, podemos entrar a la siguiente página web “http://whatismyipaddress.com/” y revisar cual es nuestra ubicación y cuál es nuestra IP.

En la imagen de abajo se muestran los datos de nuestra ubicación y datos de nuestra IP con un navegador normal

Figura 3.30 Navegador sin Red Tor (Guillén & Vicente, 2015)

En cambio, en la siguiente imagen se muestra los datos con la red Tor

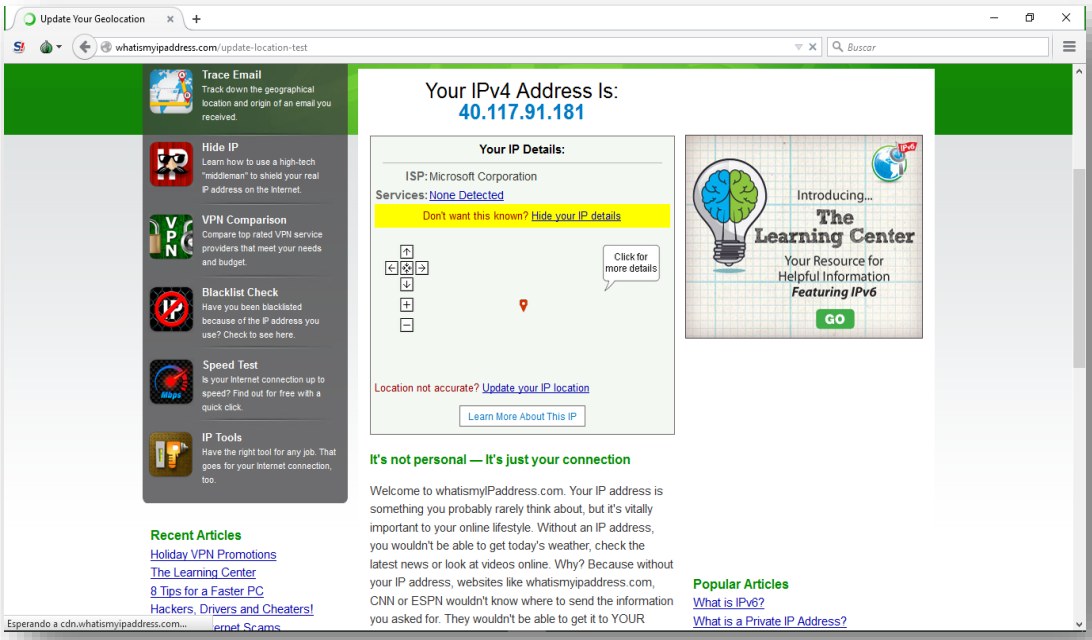

Figura 3.31 Navegador con Red Tor (Guillén & Vicente, 2015)

Otra forma de comprobar si estamos conectados a la Red Tor es entrando en la dirección "https://check.torproject.org".

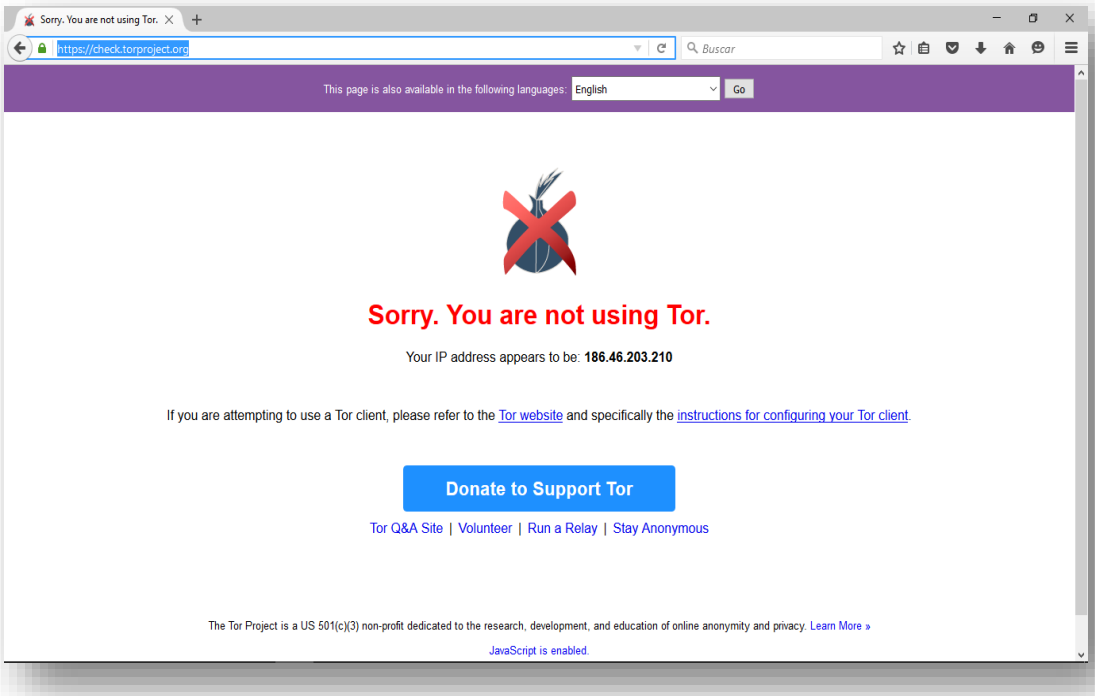

Figura 3.32 Navegador sin Red Tor (Guillén & Vicente, 2015)

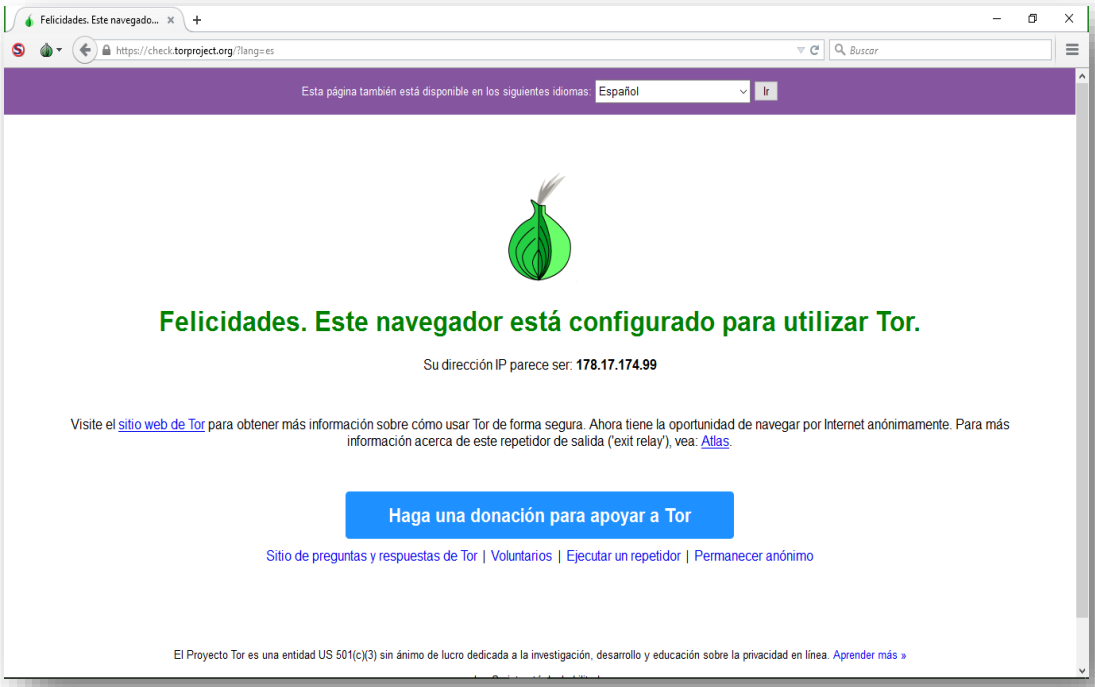

Figura 3.33 Navegador con Red Tor (Guillén & Vicente, 2015)

3.3. Problemas al usar la Red Tor

Cualquier software tiene problemas, y Tor no es la excepción. Entre los problemas más comunes están:

- **Vulnerable a ataques:** Es posible que un usuario pueda examinar el tráfico de entrada y de los destinatarios de una persona que esté usando la red Tor. Con ese análisis es posible que relacione el tiempo de entrada y de salida de cada destinatario y posiblemente acerté a un objetivo para atacarlo.

- **Bloqueos:** En algunas partes del mundo se intenta evitar el uso de Tor mediante bloqueos a gran escala. Estos ataques son posibles ya que las direcciones de los retransmisores son descubiertas mediante un análisis de red. Para evitar esto, Tor desarrollo el uso de "Puentes" que son usados por retransmisores no listados en los directorios.

- **Problemas de escalabilidad:** Este gran problema se da ya que la arquitectura de Tor requiere que cada nodo esté conectado entre los demás.

- **Mala configuración:** Es común el abuso de funcionalidades que se presenta en un navegador, y eso es un punto débil ya que aquí es donde se viola el anonimato de un cliente que usa Tor. Esto se da porque los elementos activos insertados en una página web hacia un servidor de dudosa procedencia no son monitoreados por un usuario.

- **Dificultad de acceso:** Esto debido a la gran cantidad de información y de procedimientos que hay que hacer para acceder a esa información. Esto resulta abrumador e incómodo.

- **Peligrosidad:** Este es uno de los problemas más relevantes ya que la información ni los navegadores no están controlados a niveles estándares de organizaciones de seguridad informática.

3.4. RESULTADOS

3.4.1. Ventajas

- El navegador de Tor, es un software realmente fácil de instalar ya que con el paso de los años se ha desarrollado para que este tenga todos los complementos necesarios para su uso.

- Se puede comprobar el anonimato inmediatamente después de haber instalado el software. Lo mejor de todo es que existe una opción que si se desea se puede re mapear las IPs para cambiar el lugar constantemente.

- Es una herramienta que permite que las actividades que realicemos sean anónimas ya que oculta la identidad y protege las actividades en línea.

- Este software protege su información transmitiendo las comunicaciones desde la computadora o dispositivo, hacia una red de repetidores.

- Se puede usar dos navegadores a la vez, un navegador para internet abierto (Mozilla, Chrome, Explorer, Edge) y un navegador Tor. Se puede navegar en las dos partes a la vez.

3.4.2. Desventajas

- En algunas ocasiones navegar por la red Tor, es realmente lento ya que consume un 20% de nuestro ancho de banda para ser un nodo para otros enlaces.

- Hay algunos casos donde el puerto 9051 o 8118 esta usado por otro programa, y eso no a hacer que se configure correctamente el Privoxy.

- Para hacer la configuración manual, se debe tener un conocimiento medio sobre redes y conexiones.

- El usuario debe tener en mente que en la Deep Web va a encontrar contenido fuera del mundo del Internet, y eso puede llegar a afectar la susceptibilidad del usuario si no está preparado para ello.

- Existen links que por motivo de seguridad no están disponibles siempre, o solo fueron publicados por algunas horas. Esto es debido a que muchas personas usan estos links para atacar a otros usuarios.

4. CONCLUSIONES

- La única información que es se encuentra de manera segura en la Deep Web es aquella información que se puede intercambiar a través del navegador Tor.

- En la red Tor no se va a poder usar redes sociales, ya que estas páginas usan servicios que almacenan información de los usuarios, y si nuestro objetivo es la privacidad de información, estas páginas no son buena idea.

- Evade restricciones electrónicas por lo que es muy comúnmente usado por periodistas para expresar su opinión a través de blogs o reportes de noticia.

- El servidor de Tor está diseñado para que se desconozca tanto los sitios que se visitan como la ubicación de quien visita esos lugares.

- La red Tor puede ser usada para proteger a personas como también para dañarlas, ya que en el mismo canal pueden manejar cosas buenas y cosas malas, no siempre el anonimato es la mejor opción.

- La red Tor envía la información por varios nodos, realizando diferentes caminos que imposibiliten la localización.

- Creer que la red Tor es infalible es un error, ya que entendemos que ha tenido problemas ya hasta ha sido vulnerada en algunas ocasiones.

- Que una web no está indexada por un motor de búsqueda no significa que sea parte de la Deep Web.

- No todas las webs de la Deep Web son ilegales.

- Siempre debemos entender que Deep Web va relacionado con anonimato y por ende va a relacionarse a la red Tor o a cualquier red que cumpla estas características.

- Generalmente vamos a relacionar Deep Web con la palabra ilegal o ilícita, pero también existe contenido bueno que rescatar, bibliotecas e información que no se puede encontrar en una web común.

- No estas rompiendo ninguna norma, regla, etc. Si navegas por la Deep Web, pero dependiendo de las webs que visites si podrías cometer algún tipo de delito.

- La moneda Bitcoin tan popular en este internet profundo, tiene algunos otros usos, no solo en la Deep Web.

- Si realizas una transacción en la Deep Web, no puedes usar métodos tradicionales como pagos en línea con tarjeta de crédito o transacciones bancarias, todo se debe manejar a través. de una moneda virtual o electrónica

5. RECOMENDACIONES

- Debido a que la Deep Web está plagado de vulnerabilidades y fallos de seguridad, es recomendable deshabilitar el Flash en el Navegador Tor.

- Antes de realizar la instalación del navegador de la red Tor, es prudente hacer un punto de restauración.

- Hacer que todos los servicios que usen internet trabajen a través de la red Tor, ya que no todos los servicios van a trabajar bajo esta red y podría ser motivo de vulnerar el anonimato.

- No usar conexiones de punto a punto (peer to peer) ya que estas ignoran configuraciones de proxy y realizan conexiones directas.

- Tener en cuenta que antes de publicar algo en la red Tor, todo lo que se publica puede permanecer al alcance de otros.

- Tener cuidado al momento de manejar una cuenta en la red Tor, ya que muchos mensajes que no se conoce quien lo envía, podrían contener virus o códigos maliciosos.

- Generalmente no solo la buena configuración de un ambiente para la red Tor y el uso de su navegador es suficiente, se recomienda usa varios plugins para siempre mantener la mayor seguridad posible.

- Todo el tráfico de la red Tor es cifrado hasta el punto de salida, por lo tanto el momento del último nodo este solo tiene el cifrado de la propia web, por lo cual se recomienda navegar en webs que posean un certificado SSL y realizar conexiones https.

- Desconectar el ordenador de la red al descargar un archivo, ya que este archivo puede disparar conexiones a terceros y así saltarse la red Tor el momento que se abren o se ejecutan.

- Siempre usar la última versión del navegador Tor, ya que siempre viene con mejores funcionalidades.

- Como las webs tienen el tipo de formato “.onion” se recomienda usar el navegador de Tor que es capaz de interpretar dicho formato.

- Para poder acceder a la Deep Web es necesario estar en la red Tor, recomendamos en primer lugar aprender a usar dicha red antes de adentrarse en la Deep Web.

- El contenido de la Deep Web es sumamente delicado, se recomienda acceder y buscar solo lo que se necesite, puede ser que la curiosidad nos lleve a webs ilegales que pueden ser hasta falsas o creadas por entidades tales como el FBI y llegar a estar presos por simple curiosidad.

- Todo depende de lo que busques, es recomendable solo para usos didácticos o metodológicos.

- Usarlo con responsabilidad, no es un juego el acceder a un sitio “.onion”, ya que generalmente son ilegales y pueden traer consecuencias mucho más graves.

- Se recomienda a la facultad de Ingeniería, escuela de Sistemas, realizar prácticas de cómo se podría configurar una red Tor, o como acceder a ella, es de suma importancia que exista este tipo de clases o charlas para entender que el internet no solo es lo que podemos ver a simple vista.

- Se recomienda a la facultad de Ingeniería, escuela de Sistemas, informar a los estudiantes el debido uso de la Deep Web, los motores de búsqueda que se pueden hacer uso y su debido manejo, para que no tengan problemas tanto con la ley como el vulnerar su información.

6. BIBLIOGRAFÍA

abcis. (30 de mayo de 2015). Obtenido de http://abcis.com.co/2015/05/30/los-10-pasos-para-que-las-empresas-alcancen-el-exito-en-ciberseguridad/

AgendaEmpres. (3 de Agosto de 2015). Obtenido de http://agendaempresa.com/29601/ciberseguridad-origen-y-riesgos/

alexwyn. (2014). Obtenido de http://www.alexwyn.com/company/mission-objectives

Amaya, J. (28 de mayo de 2015). *Reiniciando*. Obtenido de http://www.reiniciado.net/tor-que-es-y-para-que-sirve/19149/

Belt. (18 de Septiembre de 2015). Obtenido de http://www.belt.es/expertos/imagenes/Revista_Ejercito_837_Retos.pdf

Definicion. (18 de Junio de 2015). Obtenido de Definicion: http://definicion.de/internet/#ixzz3fid5ChMT

definicionabc. (2007). Obtenido de http://www.definicionabc.com/tecnologia/internet.php

Ecomerce. (15 de Agosto de 2015). Obtenido de http://ecommerce-news.es/internacional/los-10-mayores-ciber-ataques-a-las-companias-tecnologicas-de-la-historia-infografia-30013.html#

etcétera. (8 de abril de 2015). *Etcétera*. Obtenido de http://www.etcetera.com.mx/articulo/Los-ciberataques-aumentan-en-Latinoamerica,-hay-mayor-riesgo:-OEA/35669

fayerwayer. (18 de abril de 2014). Obtenido de https://www.fayerwayer.com/2014/04/grams-el-buscador-estilo-google-para-la-deep-web/

FM, Y. (27 de julio de 2015). *Genbeta*. Obtenido de http://www.genbeta.com/web/asi-es-hornet-el-candidato-a-suceder-a-tor-que-nos-promete-mayor-velocidad-y-privacidad

Frutos, A. M. (12 de diciembre de 2015). *ComputerHoy*. Obtenido de http://computerhoy.com/noticias/internet/que-es-deep-web-37795

Genbeta. (s.f.). Obtenido de http://www.genbeta.com/seguridad/como-funciona-la-red-tor

Genbeta. (12 de febrero de 2015). Obtenido de http://www.genbeta.com/a-fondo/kit-de-supervivencia-en-la-deep-web

Gitsinformatica. (15 de Agosto de 2015). Obtenido de http://www.gitsinformatica.com/ciberataques.html#ciberataque

Gónzales, C. (14 de Junio de 2015). *ADSL ZONE*. Obtenido de http://www.adslzone.net/2015/06/14/la-deep-web-no-es-lugar-para-impulsivos-morbosos-e-inexpertos/

Guillén, V., & Vicente, A. (2015). Quito.

ITU. (20 de Julio de 2015). Obtenido de https://www.itu.int/net/itunews/issues/2010/09/20-es.aspx

Joan. (23 de marzo de 2013). *geekland*. Obtenido de http://geekland.eu/acceder-a-la-deep-web/

Julián, G. (2015 de febrero de 2015). *Genbeta*. Obtenido de http://www.genbeta.com/actualidad/i2p-la-nueva-generacion-de-la-deep-web

Leiner, B. M. (2012). *Internet Society*. Obtenido de http://www.internetsociety.org/es/breve-historia-de-internet

Maestros del Web. (20 de Junio de 2015). Obtenido de http://www.maestrosdelweb.com/internethis/

Marrocostudio. (s.f.). Obtenido de https://marrocosoft.wordpress.com/2011/06/27/la-evolucion-del-internet-el-internet-de-las-cosas/

norfipc. (2015). Obtenido de http://norfipc.com/trucos/como-navegar-red-tor-proteger-nuestra-identidad-en-internet.php

Noticias SEO. (18 de agosto de 2014). Obtenido de http://noticiasseo.com/noticias-seo/implantes-https-en-tu-web-todavia

Pagnotta, S. (s.f.). *Security Channels Network*. Obtenido de http://securitychannelsnet.com/articulo.php?id=327

Planeta GEA. (16 de enero de 2012). Obtenido de https://planetagea.wordpress.com/2012/01/16/el-pais-el-congreso-de-ee-uu-congela-la-ley-sopa-censura-internet-hasta-encontrar-consenso-y-el-promotor-republicano-de-la-ley-ha-propuesto-retirar-la-posibilidad-de-bloquear-acceso-a-webs-oper/

quees. (2013). Obtenido de http://www.quees.info/que-es-internet.html

Ranchal, J. (24 de enero de 2014). *muycomputer*. Obtenido de http://www.muycomputer.com/2014/01/24/deep-web-introduccion

Ready. (10 de Octubre de 2015). Obtenido de http://www.ready.gov/es/ciberataque

Redes Telematicas. (20 de Julio de 2015). Obtenido de http://redestelematicas.com/historia-de-internet-nacimiento-y-evolucion/

Rizzo, T. (2 de abril de 2015). *Scorpion software*. Obtenido de http://insights.scorpionsoft.com/top-10-signs-your-password-is-weak

Sabermas. (30 de Agosto de 2015). Obtenido de http://www.sabermas.umich.mx/archivo/secciones-anteriores/la-ciencia-en-pocas-palabras/45-numero-5/91-ciberseguridad.html

Sánchez, I. (9 de febrero de 2015). *Walskium*. Obtenido de http://www.walskium.es/magazine/tecnologia/arpanet-el-origen-de-internet/

TKM. (14 de septiembre de 2015). Obtenido de http://www.mundotkm.com/us/destacados/26400/todo-lo-que-internet-sabe-sobre-nosotros

Tor Project. (s.f.). Obtenido de https://www.torproject.org/about/overview.html.en#overview

Tor Project: Anonymity Online. (17 de Octubre de 2006). Recuperado el 07 de Febrero de 2015, de Tor Project: Anonymity Online: https://www.torproject.org/index.html.en

trendmicro. (1989). Obtenido de http://www.trendmicro.es/tecnologia-innovacion/seguridad-cibernetica/

Velasco, R. (5 de agosto de 2013). *Redes Zone*. Obtenido de http://www.redeszone.net/2013/08/05/un-exploit-identifica-a-los-usuarios-de-la-red-tor/

We live Security. (10 de Octubre de 2015). Obtenido de http://www.welivesecurity.com/la-es/2015/06/16/ciberseguridad-seguridad-informacion-diferencia/

Web, D. (26 de noviembre de 2015). *DeepWeb.es*. Obtenido de http://www.deepweb.es/links-para-la-deep-web/

Wikia. (s.f.). Obtenido de http://es.creepypasta.wikia.com/wiki/Deep_Web

Zavia, M. S. (11 de febrero de 2015). *Xacata*. Obtenido de http://www.xataka.com/analisis/una-semana-en-la-deep-web-esto-es-lo-que-me-he-encontrado

7. GLOSARIO

A

Aplicación: programa informático diseñado para facilitar al usuario realizar cualquier tipo de trabajo y actividad, es utilizada como una herramienta de ayuda para las personas, a través de un rápido y fácil acceso.

C

Captcha: son las siglas de Completely Automated Public Turing test to tell Computers and Humans Apart (prueba de Turing completamente automática y pública para diferenciar computadoras de humanos). Test controlado por una máquina, no por un humano como en la prueba de Turing. Considerándolo como prueba de Turing inversa.

Cibernética: es una disciplina que se encarga de desarrollar un lenguaje y técnicas para atacar problemas de control y comunicación, se dedica al estudio de regulación y control de sistemas de comunicación entre personas, máquinas, en especial informáticos.

Crush fetish: Ilegal, fetiche y parafilia; vídeos donde se aplastan alimentos u objetos; golpea, maltratan y matan animales, con su cuerpo y objeto.

E

Exploit: programa o código que se aprovecha de una vulnerabilidad de seguridad de una aplicación o sistema, de forma que un hacker puede hacer uso de este.

Enlace: también conocido como link, es una expresión que sirve para conectar una información con otra ya sea a través de una imagen, palabra, hipertexto, dirección web, línea de programación o referencia. Un usuario al pinchar sobre el mismo tiene acceso a otro documento u otra página web, generalmente se presenta como palabras subrayadas.

J

Jailbait: Ilegal, es pornografía infantil o contenido erótico de adolescentes o

menores de edad, también llamado como "JB". En muchas páginas permiten jailbait pero no contiene contenido erótico infantil.

L

Love Letter: Notificación oficial al realizar una compra ilícita o delito considerado fraudulento, que agentes de la seguridad envían por correo postal, confiscando el producto comprado.

M

Mezclador de bitcoins: Existen empresas como BitMixer, BitBlender, Tor Wallet, etc. Se encargan de mezclar los bitcoins de un usuario con los bitcoins de otros usuarios y reenviar paquetes de direcciones específicas. La comisión que se cobra es un porcentaje fijo del total de bitcoins que se blanquea (por ejemplo: Bitmixer, cobra un porcentaje de 0,5%). Dependiendo de las tiendas dentro de la Deep web, los mezcladores van se encuentran dentro del proceso de compra.

O

Onionland: Describe el contenido de las redes anónimas, servicios ocultos, páginas oscuras de la red Tor.

Ordenador: se denomina ordenador a una computadora o equipo que recibe y procesa datos para transformarlos en información útil, está formado por redes de circuitos y elementos que se relación entre sí.

P

Protocolo TCP: (Protocolo de Control de Transmisión), uno de los principales protocolos de capa de transporte del modelo TCP, permite que se puedan administrar los datos al nivel más bajo del modelo, este protocolo se orienta a la conexión, es decir permite que dos máquinas través de comunicación controlen el estado de la transmisión.

R

Red: sistema de comunicación entre distintos equipos con el fin de realizar una comunicación eficiente, para transmitir datos de un ordenador a otro a través de un intercambio de información, además de recursos disponibles.

S

Sistema operativo: más conocido como software básico de una computadora que presenta una interfaz entre los programas del computador, dispositivos de hardware y el usuario, tiene como

objetivo administrar los recursos de la máquina, coordinar el hardware y organizar el almacenamiento.

Snuff: Ilegal, son vídeos de torturas, violaciones, asesinatos, suicidios, etc. Varios de estos videos son mitos urbanos o falsos, y otros son verídicos.

W

Web: por su definición del inglés, red o malla, se utiliza en el ámbito tecnológico para referirse a una red informática o general Internet, sirve para hacer referencia a una página web o sitio web.

WikiLeaks: es una organización internacional que por medio del internet, pública a través de su sitio web informes anónimos y documentos con contenido de interés público, manteniendo el anonimato de sus fuentes.

7.1. Acrónimos

AIW: su significado es "The Academic Invisible Web", es un conjunto de bases de datos y colecciones que no pueden ser utilizadas por motores de búsqueda estándar, contienen: avances tecnológicos o cientificos, contenido académico, etc.

BTC: su significado es "Bitcoin", moneda utilizada dentro del DNM, para el pago de compras o cambios ilicitos.

DNM: su significado es "Dark Net Market" (Mercado Negro de la Deep Web). Sitios donde se realizan adquisiciones ilícitas.

FE: su significado es "Finalize Early", cuando se toma como opción el evadir el método de Escrow para culminar su transacción antes de tiempo.

IMAP: su significado es "Internet Message Access Protocol" (IMAP, Protocolo de acceso a mensajes de internet), protocolo que permite acceder a correos de varios usuarios que se encuentran en un servidor en línea.

IRC: su significado es “Internet Relay Chat”, protocolo que permite que dos usuarios o más mantengan contacto en tiempo real.

SSL: su significado es: "Secure Sockets Layer", protocolo que permite transmitir información buscando que su comunicación de retorno sea seguro por medio de una red.

XMPP: su significado es “Extensible Messaging and Presence Protocol” es un protocolo que mediante mensajes basados en XML (Extensible Markup Language) se comunica con el middleware.