



UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO

POSGRADO EN BIBLIOTECOLOGÍA Y ESTUDIOS DE LA INFORMACIÓN

FACULTAD DE FILOSOFÍA Y LETRAS

INSTITUTO DE INVESTIGACIONES BIBLIOTECOLÓGICAS Y DE LA INFORMACIÓN

ACCESO A LA WEB PROFUNDA

TESIS

QUE PARA OPTAR POR EL GRADO DE:

MAESTRO EN BIBLIOTECOLOGÍA Y

ESTUDIOS DE LA INFORMACIÓN

PRESENTA:

HUGO ALBERTO GUADARRAMA SÁNCHEZ

ASESOR: DR. EGBERT JOHN SÁNCHEZ VANDERKAST

INSTITUTO DE INVESTIGACIONES BIBLIOTECOLÓGICAS Y DE LA INFORMACIÓN

Ciudad de México, octubre de 2016



Universidad Nacional
Autónoma de México



UNAM – Dirección General de Bibliotecas
Tesis Digitales
Restricciones de uso

DERECHOS RESERVADOS ©
PROHIBIDA SU REPRODUCCIÓN TOTAL O PARCIAL

Todo el material contenido en esta tesis esta protegido por la Ley Federal del Derecho de Autor (LFDA) de los Estados Unidos Mexicanos (México).

El uso de imágenes, fragmentos de videos, y demás material que sea objeto de protección de los derechos de autor, será exclusivamente para fines educativos e informativos y deberá citar la fuente donde la obtuvo mencionando el autor o autores. Cualquier uso distinto como el lucro, reproducción, edición o modificación, será perseguido y sancionado por el respectivo titular de los Derechos de Autor.

AGRADECIMIENTOS

En primera instancia, a la Universidad Nacional Autónoma de México, por permitirme desarrollarme en los aspectos académicos, personales y espirituales.

A mi asesor de tesis, Dr. Egbert John Sánchez Vanderkast, por su confianza, guía y asesoría las cuales permitieron la dirección adecuada para esta investigación.

A mis sínodos, por su ayuda, su tiempo y sus observaciones:

- ❖ Dr. Hugo Alberto Figueroa Alcántara
- ❖ Dr. Juan Voutssás Márquez
- ❖ Dr. Ariel Alejandro Rodríguez García
- ❖ Mtro. Miguel Gama Ramírez

A los profesores que me formaron en la senda del posgrado, con sus enseñanzas y conocimientos:

Dra. Patricia Lucía Rodríguez Vidal, Dr. Jesús Francisco García Pérez, Dr. Miguel Ángel Rendón Rojas, Dra. Georgina Araceli Torres Vargas, Dra. Brenda Cabral Vargas, Dr. Egbert John Sánchez Vanderkast, Dr. Daniel de Lira Luna, Dra. Isabel Galina Russell, Dr. Perla Olivia Rodríguez Reséndiz, Mtra. Norma Aída Manzanera Silva y Dra. Elsa Margarita Ramírez Leyva.



TABLA DE CONTENIDO

Introducción.....	VI
-------------------	----

Capítulo 1

Acceso a la Web

1.1 Introducción.....	2
1.2 Antecedentes.....	3
1.3 Internet y la Web.....	4
1.4 El servicio de Internet.....	6
1.4.1 Conexión.....	7
1.4.2 Conexión a Internet en México 2012 – 2015.....	8
1.5 Acceso y disponibilidad.....	14
1.5.1 Acceso a Internet.....	17
1.5.2 Navegación en la Web.....	18
1.5.3 Recuperación de la información.....	21
1.5.4 Acceso a la información.....	24
1.6 Elementos de accesibilidad.....	31
1.6.1 Restricción.....	31
1.6.2 Control.....	32
1.6.3 Censura.....	33
1.6.4 Poder.....	34
1.7 Elementos de la complejidad en la Web.....	35
1.8 La utilidad de la Web.....	41
1.8.1 Servicios en línea.....	42
1.8.2 Tipos de usuario.....	43
1.8.3 Veracidad de la información.....	49
1.8.4 Información privilegiada.....	52

Capítulo 2

La web profunda

2.1 Introducción	56
2.2 Estratificación de la Web	57
2.2.1 La red oscura y su vínculo con la web profunda.....	64
2.3 Conceptualización social de la web profunda (2012 - 2015)	65
2.3.1 The onion routing network: Tor.....	75
2.3.2 Funcionamiento.....	76
2.3.3 Usuarios.....	77
2.3.4 Niveles de acceso.....	78
2.4 Riesgos de consulta y acceso	80
2.4.1 El arte de la duda.....	80
2.4.2 El marco de la legalidad.....	81
2.5 Servicios, productos y contenidos	83
2.5.1 Consecuencias psicológicas de los servicios, contenidos y productos.....	87
2.6 ¿Quién busca la información privilegiada?	88

Capítulo 3

Acceso a las redes oscuras

3.1 Introducción	93
3.2 Redes oscuras	94
3.3 Recursos para acceder a las redes oscuras	106
3.3.1 Sistema operativo.....	109
3.3.2 Prevención de riesgos informáticos.....	111
3.3.3 Tipo de conexión a Internet.....	112
3.3.4 Alternativas para evitar el monitoreo.....	114
3.4 Caso práctico de navegación en las redes oscuras	115
3.4.1 Instalación y configuración para la navegación.....	119
3.4.2 Bitácora de monitoreo.....	120

3.4.3 Resultados del monitoreo.....	123
3.5 Las redes oscuras después del 2015.....	129
3.6 ¿Se recupera la misma información en la web superficial?.....	132
3.7 Aspectos legales en torno a los servicios y contenidos.....	133
3.7.1 Contexto internacional.....	133
3.7.2 Contexto nacional.....	135
3.8 Las redes oscuras en el quehacer bibliotecario.....	140
3.8.1 Servicio de Internet en la biblioteca.....	141
3.8.2 Políticas de acceso a Internet.....	143
3.8.3 Escenario rígido en el acceso a Internet en la biblioteca.....	144
3.8.4 Escenario flexible en el acceso a Internet en la biblioteca.....	147
3.9 La biblioteca como medio de acceso a la información privilegiada.....	149
3.10 Prospectiva de las redes oscuras.....	150
Conclusiones.....	154
Obras consultadas.....	166
Anexo A Cédulas de la red oscura Tor.....	201
Anexo B Cédulas de la red oscura Freenet.....	216
Anexo C Cédulas de la red oscura I2P.....	228

Tablas

Tabla 1. Mayor rango de edad en los usuarios que realizan la conexión a Internet.....	9
Tabla 2. Medios de conexión más utilizados.....	10
Tabla 3. Servicios de conexión a Internet.....	11
Tabla 4. Estados de donde se realiza la mayor conexión a Internet.....	12
Tabla 5. Clasificación de la información judicial.....	25
Tabla 6. Clasificación de la información gubernamental.....	25
Tabla 7. Clasificación de la información de las empresas privadas.....	26
Tabla 8. Criterios de autoría de la información.....	49
Tabla 9. Criterios de sitios web.....	50
Tabla 10. Precios de productos, servicios y acceso en el mercado negro de la web profunda.....	85
Tabla 11. Características de Tor como red oscura.....	95
Tabla 12. Características de la web profunda.....	96
Tabla 13. Redes oscuras como elementos de oposición a la accesibilidad y en pro de la optimización en la complejidad de la Web.....	104
Tabla 14. Características de la computadora personal y sistema operativo.....	116
Tabla 15. Las mejores marcas y modelos de computadoras portátiles laptop en el contexto internacional y nacional.....	117
Tabla 16. Comparación de los contenidos temáticos de las redes oscuras: Tor, Freenet e I2P.....	125
Tabla 17. Servicios de las redes oscuras: Tor, Freenet e I2P.....	126
Tabla 18. Comparación de los temas frecuentes en las redes oscuras: Tor, Freenet e I2P.....	126
Tabla 19. Idiomas recurrentes de las redes oscuras de acuerdo a su índice de frecuencia.....	127
Tabla 20. Tipo de acceso conceptual.....	128

Tabla 21. Clasificación de la información de acuerdo a la cantidad de sitios detectados con este atributo.....	128
--	-----

Figuras

Figura 1. La anatomía de la dirección URL.....	19
Figura 2. Enfoque general en el acceso a la información.....	30
Figura 3. La Web y sus tipos de usuario.....	48
Figura 4. Esquematización d acceso y visibilidad en la estratificación Web.....	63
Figura 5. Proceso de pago para la adquisición de servicios, productos y contenidos.....	86

Esquemas

Esquema 1. ¿Qué tan profunda es tu Web?.....	70
Esquema 2. ¿Qué es la web profunda?.....	71
Esquema 3. Traducción de esquema de la deep web en sus diferentes niveles.....	72
Esquema 4. La metáfora del iceberg: niveles de acceso y visibilidad.....	74

Introducción

Con base en una indagación preliminar sobre la literatura se detectó que, el concepto de la *web profunda* ha sido estudiado y utilizado en los inicios de la década de los años noventa de forma multidisciplinaria, por lo que surge la inquietud y la expectativa a raíz de estos antecedentes por encontrar las líneas interdisciplinarias que permitan clarificar el concepto de la *web profunda*, además de su acceso. De manera que, es a partir de este interés, el fundamento que da origen al desarrollo de esta investigación, siendo uno de los primeros acercamientos desde la óptica de la Bibliotecología en cuanto al análisis conceptual de la *web profunda* y, las dificultades de acceso a las *redes oscuras*.

La Bibliotecología¹ como disciplina, se conforma a partir del conjunto de conocimientos, teorías y saberes provenientes de distintos estudios clásicos y tradicionales como: la bibliología; el estudio histórico y descriptivo de los documentos. La bibliotécnica; la elaboración, composición, restauración y preservación de los documentos. La biblioteconomía; los procesos técnicos, la organización, la operatividad y la administración de las áreas departamentales referentes a la gestión de la información. La bibliografía; el estudio acerca del origen, trascendencia, relevancia y vínculos entre los distintos textos y contenidos temáticos. Y, la bibliotecografía; el estudio de la historia, desarrollo y tipología de las bibliotecas, además de la apertura en el acceso a la información para la sociedad.

Asimismo, la Bibliotecología requiere de procedimientos, estrategias, técnicas, métodos y medios tecnológicos para elaborar, constituir y obtener la

¹ Véase Rendón Rojas, Miguel Ángel. **Bases teóricas y filosóficas de la bibliotecología**. 2a ed. (México: UNAM, Centro Universitario de Investigaciones Bibliotecológicas, 2005). Pág. 75 y 112. Martínez de Sousa, José. **Diccionario de bibliología y ciencias afines**. 3ra ed. (Gijón, Asturias: Trea, 2004). Pág. 115 y García Ejarque, Luis. **Diccionario del archivero-bibliotecario: terminología de la elaboración, tratamiento y utilización de los materiales propios de los centros documentales**. (Gijón, Asturias: Trea, 2000). Pág. 116

organización de la información. Los estudios de la información² se orientan al quehacer administrativo encaminado a la identificación, selección, adquisición, organización, descripción, almacenamiento, preservación, análisis, interpretación, evaluación, síntesis, diseminación, gestión y recuperación de la información. Los estudios de la información además de administrar los datos y contenidos, se enfocan en el uso de los servicios tecnológicos, que facilitan la gestión documental. Por tanto la teoría bibliotecológica y la práctica referente a los estudios de la información, son los pilares fundamentales para la organización y el acceso a la información.

Es en este sentido, el acceso, la recuperación de la información y el uso de los servicios tecnológicos, que es indispensable la creación, adaptación y desarrollo de las políticas de información, para fines de regulación sobre el uso de la infraestructura y medidas preventivas en la conducta de los individuos respecto a la información. Para Elizabeth Orna, el concepto de políticas de información³ tiene sus orígenes en el contexto de los años posteriores a la Segunda Guerra Mundial como todo aquel sistema de control, censura y acceso a la información gubernamental. Elizabeth Orna hace hincapié en que además de lo anteriormente mencionado, las políticas de información son actualmente la vía de mediación para el acceso, la utilidad y la protección de los datos personales obtenidos por el *Estado-nación*. De esta manera se entiende que las políticas de información son instrumentos para regular el acceso y el uso de la información, ambos elementos clave para la certidumbre, el control, el beneficio, la ventaja y el progreso para el *Estado-nación*.

² Council of the American Library Association. 2008. Standards for accreditation of master's programs in library & information studies. **American Library Association**. Recuperado en: http://www.ala.org/accreditedprograms/sites/ala.org.accreditedprograms/files/content/standards/standards_2008.pdf [Consultado 24 de agosto de 2016]

³ Orna, Elizabeth. "Information policies: yesterday, today, tomorrow". En **Information science in transition**. (London: Facet, 2009). Pág. 250 - 251

Para el *Estado-nación* la gestión de la información es de suma importancia, por lo que los servicios de información⁴ forman parte de las divisiones administrativas centrales, que a groso modo se categorizan en: asuntos jurídicos, economía, educación y bienestar social, el entorno y los recursos naturales, la defensa nacional, gobernanza, administración pública y, los servicios de información gubernamental. A su vez las políticas de información como lo señala Luis Fernando Ramos Simón, referentes a estos servicios de información en las bibliotecas, archivos y museos (BAM) se orientan principalmente hacia la digitalización, los datos abiertos, la preservación, la reutilización, los costos/participación del sector privado, las licencias y las tarifas, el dominio público y las bases de datos, el derecho de autor y las obras huérfanas.⁵

Cabe destacar que las bibliotecas al tener los medios tecnológicos como el servicio de conexión a Internet, proporcionan al usuario la posibilidad de acceder a ciertos servicios no regulados, lo cual no significa que sean ilícitos, sino que simplemente le permiten al usuario (con conocimientos informáticos avanzados) el acceso a otra clase de contenidos de forma anónima, sin ser monitoreados por los Proveedores del Servicio de Internet, los bibliotecarios y los sistemas de monitoreo del *Estado-nación*. Es a raíz de esta posibilidad ya sea por medio de un servicio de suscripción particular de conexión a Internet o por medio de las bibliotecas que el individuo puede acceder a ciertas herramientas digitales que le proveen en primera instancia del anonimato, como es el caso de la “*web profunda*”^{**}.

⁴ Chartrand, Robert y Milesvski, Sandra. “Congressional research service”. En *Encyclopedia of library and information science* 43, suplemento 8. (New York: Marcel Dekker, 1988). Pág. 70

⁵ Ramos Simón, Luis Fernando. 17 de agosto de 2016. “Políticas de información en bibliotecas, archivos y museos”. En **Seminario de investigación sobre políticas de información**. Conferencia pronunciada en la Universidad Nacional Autónoma de México.

^{**}Se utilizan las comillas para diferenciar a la web profunda bajo el concepto social, siendo que en realidad se trata de una red oscura llamada Tor. Además de Tor existen otras redes oscuras.

Es a partir de los estudios de la información que es posible realizar la gestión de los contenidos de la “*web profunda*” así como de entender sus políticas de acceso mediante una perspectiva bibliotecológica y obtener una aproximación a la complejidad del acceso a la “*web profunda*”. Como antecedente general se conoce que, los servicios de información en esta web, comúnmente se centran en la reutilización de la información, la compra-venta ilícita de las bases de datos y en la vulneración del derecho de autor. De modo que, existen similitudes en el acceso a los contenidos y servicios de la “*web profunda*” respecto a las políticas de información y sus orientaciones en torno al acceso como lo son: el bienestar o el estímulo, las necesidades de certidumbre y la ventaja. Las bibliotecas que proporcionan el servicio de Internet suelen ser el punto medio entre los sistemas de monitoreo del *Estado-nación* y las necesidades de información, el anonimato, la privacidad, el derecho a la información y la libertad de expresión, ello debido a su apertura de acceso para la sociedad.

El acceso a la información en línea, se encuentra sujeto a normas, privilegios, controles y regulaciones por parte del *Estado-nación*, las empresas, las compañías, las instituciones y los laboratorios que se dedican a la producción de información relevante, la cual es regulada mediante filtros de acceso. En este sentido Sandra Braman⁶ indica que, la información es un recurso que le proporciona preeminencia y comodidad al individuo, siempre y cuando, el individuo la capitalice y le dé un enfoque utilitario para ampliar su conocimiento o bien para propiciar el ocio, según sea la situación y contexto.

Partiendo de lo anteriormente mencionado, para obtener el acceso a los contenidos digitales⁷ en línea, es imprescindible el uso de computadoras personales o medios con la capacidad de conexión a Internet, que permitan

⁶ Braman, Sandra. “Defining information: an approach for policy-makers”. *Telecommunications Policy* 13, no. 3 (1989): 233-242. Recuperado en: http://people.tamu.edu/~Braman/bramanpdfs/003_defining.pdf [Consultado 14 de enero de 2016]

⁷ Véase Torres Vargas, Georgina Araceli y Juárez Santamaría, Beatriz. “Los sistemas de organización del conocimiento y el manejo de contenidos digitales”. *Biblioteca Universitaria* 11, no. 1 (2008): 3-12. Recuperado en: <http://www.redalyc.org/pdf/285/28512651002.pdf> [Consultado 22 de junio del 2016]

acceder a la Web. Dichos medios y computadoras personales actualmente son utilizados para realizar la conexión a Internet con el fin de efectuar o complementar actividades domésticas, lúdicas, técnicas, de entretenimiento, fiscales, financieras, administrativas, académicas y laborales.

Internet al ser una infraestructura tecnológica para la transmisión de datos, es parte de la red de telecomunicaciones. Las telecomunicaciones se conforman por medio de distintas tecnologías enfocadas a la comunicación a distancia, como lo son: los sistemas de transmisión de radio, el teléfono, la televisión, la telefonía móvil y el Internet. Puntualmente se puede decir que, las telecomunicaciones⁸ se orientan a toda emisión, transferencia de señales, signos y códigos de cualquier naturaleza que codifiquen, decodifiquen y representen la información mediante el uso de medios de transmisión. Es decir que las telecomunicaciones⁹ son el conjunto de todas las infraestructuras dedicadas a los distintos sistemas para la transmisión de la información. Por tanto, se puede decir que las telecomunicaciones son **la infraestructura de comunicación**.

Históricamente las telecomunicaciones han evolucionado, adaptando nuevos métodos de transmisión y optimizando la tecnología en curso, en este sentido Sara Hedberg¹⁰ menciona que, las redes de comunicación convencionales son adaptadas y optimizadas para nuevos servicios de telecomunicación y nuevas tecnologías de conexión y velocidad en la transmisión. Sin embargo para Robert Walp, Mehmet Ulema y Mary Michel¹¹ las redes de telecomunicaciones no son

⁸ México. Cámara de diputados. 7 de junio de 1995. **Ley Federal de Telecomunicaciones**. Reforma publicada DOF 16-01-2013. Capítulo I, Disposiciones generales. Recuperado en: http://www.sct.gob.mx/fileadmin/migrated/content/uploads/Ley_Federal_de_Telecomunicaciones.pdf [Consultado 8 de marzo de 2015]

⁹ Instituto Latinoamericano de la Comunicación Educativa. 2012. Redes de telecomunicaciones. **Biblioteca digital ILCE**. Recuperado en: http://bibliotecadigital.ilce.edu.mx/sites/ciencia/volumen3/ciencia3/149/htm/sec_8.htm [Consultado 13 de marzo de 2016]

¹⁰ Hedberg, Sara. "The telecommunications network of the new millennium". **IEEE** 4, no. 1 (1996): 6-8. Recuperado en: <http://ieeexplore.ieee.org/xpl/articleDetails.jsp?arnumber=481661&newsearch=true&queryText=telecommunications%20network%20of%20the%20new%20millennium> [Consultado 13 de marzo de 2016]

¹¹ Walp, Robert., Ulema Mehmet y Michel, Mary. "Economic engineering for improving access to the worldwide telecommunications network". **IEEE** 47, no. 11 (2009): 180-185. Recuperado en: <http://ieeexplore.ieee.org/xpl/login.jsp?tp=&arnumber=5307483&url=http%3A%2F%2Fieeexplore.ieee.org%2Fiel5%2F35%2F5307452%2F05307483.pdf%3Farnumber%3D5307483> [Consultado 13 de marzo de 2016]

asequibles para los individuos con escasos recursos económicos, por otro lado los mismos autores señalan que, la cobertura geográfica de las telecomunicaciones es un indicador de desarrollo tecnológico para una nación.

De ser cierto lo anterior, se vislumbra la importancia en el acceso a la información, de manera que al acceder y/o darle una utilidad, es posible obtener cierta recreación y/o nuevos conocimientos. De esta manera el individuo consigue un panorama sobre el funcionamiento del mundo social, así como un amplio entendimiento de las leyes del entorno natural y tecnológico. Por ello, el punto clave del asunto se fundamenta en la regulación por la adquisición de nuevas habilidades y conocimientos sobre tecnologías, procedimientos, acontecimientos y asuntos que socialmente son considerados como importantes o críticos, puesto que a raíz de la apertura que exista a ellos se crearán situaciones de riesgo para el resto de los grupos e individuos que procuran su continuidad, comodidad y calidad de vida.

Para ello, es primordial identificar, seleccionar y clasificar la relevancia de la información presentada en los contenidos digitales, ya sea en texto, expresiones matemáticas, imágenes, fotografías, ilustraciones, símbolos, mapas, signos, grabaciones sonoras, videos, esquemas, multimedia, planos, estadísticas, etc. La recuperación de la información comprende el proceso de la discriminación y selección de aquellos contenidos considerados como relevantes para el individuo. En este sentido, el acceso a los contenidos digitales en línea, depende de la autorización o de la restricción con la que la información haya sido concebida, creada, resguardada y evaluada.

La Web, al ser un conjunto de contenidos digitales de toda índole es también un medio de acceso a la información digital y/o digitalizada. En la Web existen elementos de accesibilidad y de complejidad que a pesar de no ser percibidos con esta óptica, condicionan la dinámica en cuanto al acceso y a la libertad de expresión. La “*web profunda*”, es un concepto que se ha socializado en la *web*

superficial, dicho concepto representa un conjunto de servicios y contenidos particulares e ilícitos, en donde aparentemente no existen los procesos jurídicos que regulen el comportamiento inadecuado de los individuos, no obstante Alex Winter manifiesta que existen consecuencias legales sustentadas en leyes nacionales y acuerdos internacionales.¹² La apropiación social del concepto de *web profunda* ha adquirido cierto cariz, inercia, difusión y confusión en la *web superficial*, por lo que consecuentemente el concepto ha influenciado parte del entorno profesional vinculado a los aspectos tecnológicos.

En el inicio de la investigación, el concepto de la “*web profunda*” (deep web) fue el punto de partida para la búsqueda y recopilación de los elementos y las herramientas de estudio, sin embargo, conforme se presentaron los avances, se pondera de manera preeminente el concepto de *red oscura*.

La “*web profunda*” como construcción conceptual bajo la percepción social, también involucra la libertad de expresión, anonimato y privacidad, que de alguna manera se han acotado a la sociedad. Esta “*web profunda*” es también entendida a un nivel social como un medio para la transferencia y el acceso a la información privilegiada, la cual es un recurso informativo que puede alterar la situación social, económica, profesional y laboral del individuo.

La presente investigación propone clarificar el concepto de *web profunda*, puesto que con base en la documentación oficial obtenida en los sitios web de los desarrolladores del software para acceder a la “*web profunda*”, se han obtenido los argumentos para aclarar tanto el concepto como el uso de: la *web profunda* y las *redes oscuras*.

¹² Epix network. **Deep Web**. DVD. Dirigido por Alex Winter. Estados Unidos: Epix network, 2015.

Asimismo se presenta la problemática, puesto que a partir de todo lo anteriormente mencionado sobre el tema se ha detectado a nivel conceptual la utilización errónea de la *web profunda* en la *web superficial*. Mientras que a nivel práctico se han detectado inconvenientes en el acceso, la configuración y la navegación para el usuario común a la *red oscura* **Tor: *The onion routing***.

Ante este planteamiento se presentan las siguientes preguntas de investigación:

- ¿Qué es la *web profunda*?
- ¿Cuál es la diferencia entre la *web profunda*, *web invisible*, *web opaca* y redes oscuras?
- ¿En qué momento se bifurca el concepto de la *web profunda* e incide con el concepto de las *redes oscuras*?
- ¿Cómo se ha socializado el concepto de la *web profunda*?
- ¿Cuál es la dificultad de acceso a las herramientas tecnológicas?
- ¿Cuáles son las herramientas mínimas que deben de tener los usuarios para acceder a lo que se conoce socialmente como *web profunda*?
- ¿Cuáles son las políticas de acceso por parte de los colectivos desarrolladores del software de acceso?

De acuerdo a lo anterior se establece como objetivo general, estudiar y analizar el concepto de la *web profunda* así como algunos contenidos de las *redes oscuras*, sus complejidades y el acceso a las mismas.

Y como objetivos específicos:

1. Analizar la literatura referente a la teoría correspondiente al acceso a la información, así como los elementos de complejidad en la Web.
2. Identificar la estratificación de la Web y explicar la diferencia entre la *web profunda* y las *redes oscuras*.

3. Analizar la complejidad de acceso a las *redes oscuras* para su exploración, con el fin de entender sus políticas de acceso.

De esta manera, se formularon los siguientes supuestos para responder a las preguntas planteadas:

1. Tanto las habilidades del usuario común como las herramientas para acceder a las *redes oscuras* poseen una similitud de usabilidad y dificultad que las de la *web superficial*.
2. En la actualidad, existen herramientas suficientes para acceder a las *redes oscuras* de forma segura.
3. Las *redes oscuras* utilizan las mismas tecnologías de acceso y navegación que en la *web superficial*.
4. Al parecer la *web profunda* y las *redes oscuras* tienen propósitos, características y objetivos similares, sin embargo estas similitudes no son indicativos de ser sinónimos.

Mediante una investigación exploratoria¹³ se analizaron diversos sitios, portales y páginas web, con el firme propósito de recuperar los recursos de información que sirvieron para dar un sustento teórico desde la perspectiva de la Bibliotecología y en los procesos de análisis mediante los estudios de la información, complementándose con los estudios de la Ingeniería de las Telecomunicaciones. Siendo el método deductivo¹⁴ la vía para encontrar los elementos adecuados y de esta forma distinguir las diferencias conceptuales entre *web profunda* y *red oscura*. El enfoque bibliotecológico proporcionó las corrientes teóricas sobre el acceso a la información, permitiendo conocer los

¹³ Gómez Mendoza, Miguel Ángel., Deslaires, Jean-Pierre y Álzate Piedrahita, María Vitoria. **Como hacer Tesis de Maestría y Doctorado**. (Bogotá: Ecoe ediciones, 2010). Pág. 63

¹⁴ Cisneros Estupiñan, Mireya. **Cómo elaborar trabajos de grado**. (Bogotá: Ecoe Ediciones, 2012). Pág. 44

antecedentes y el contexto de la Web y, consecuentemente el panorama de las *redes oscuras* bajo el paradigma cualitativo¹⁵ (o interpretativo).

Respecto a la metodología de investigación, se inicia con la recopilación de la documentación sobre el acceso a la información, la estratificación de la Web y las *redes oscuras*. Dando paso a la documentación acerca de los requisitos mínimos para acceder a las *redes oscuras*. Posteriormente se realiza la exploración previa mediante pruebas piloto en las *redes oscuras Tor, Freenet e I2P* para designar los elementos de identificación. Se efectúa el acceso y navegación a los contenidos de las *redes oscuras Tor, Freenet e I2P* para proceder a la observación, lectura y recopilación de los datos correspondientes a los elementos de identificación en las cedulas que conforman la bitácora. La bitácora se encuentra compuesta por 60 cedulas como instrumento para el análisis y la discusión de los datos, cada cedula está conformada por 13 elementos de identificación. En los elementos de identificación se aplican los enfoques teóricos correspondientes a los criterios de autoría de la información y clasificación de la información, los cuales permiten entender y estructurar la descripción de las características conforme al análisis y la recuperación de la información. El periodo de investigación parte del 23 de febrero al 18 de marzo del año 2016.

Esta tesis está estructurada en tres capítulos, el primer capítulo trata de los antecedentes y aspectos concernientes a la infraestructura de Internet y sus índices de cobertura nacional, con base a las estadísticas del Instituto Nacional de Estadística y Geografía, el Gabinete de Comunicación Estratégica y, la Asociación Mexicana de Internet. Se abordan conceptos teóricos como: el acceso a la información, la recuperación de la información, la restricción a la información, la vigilancia, el anonimato y la privacidad.

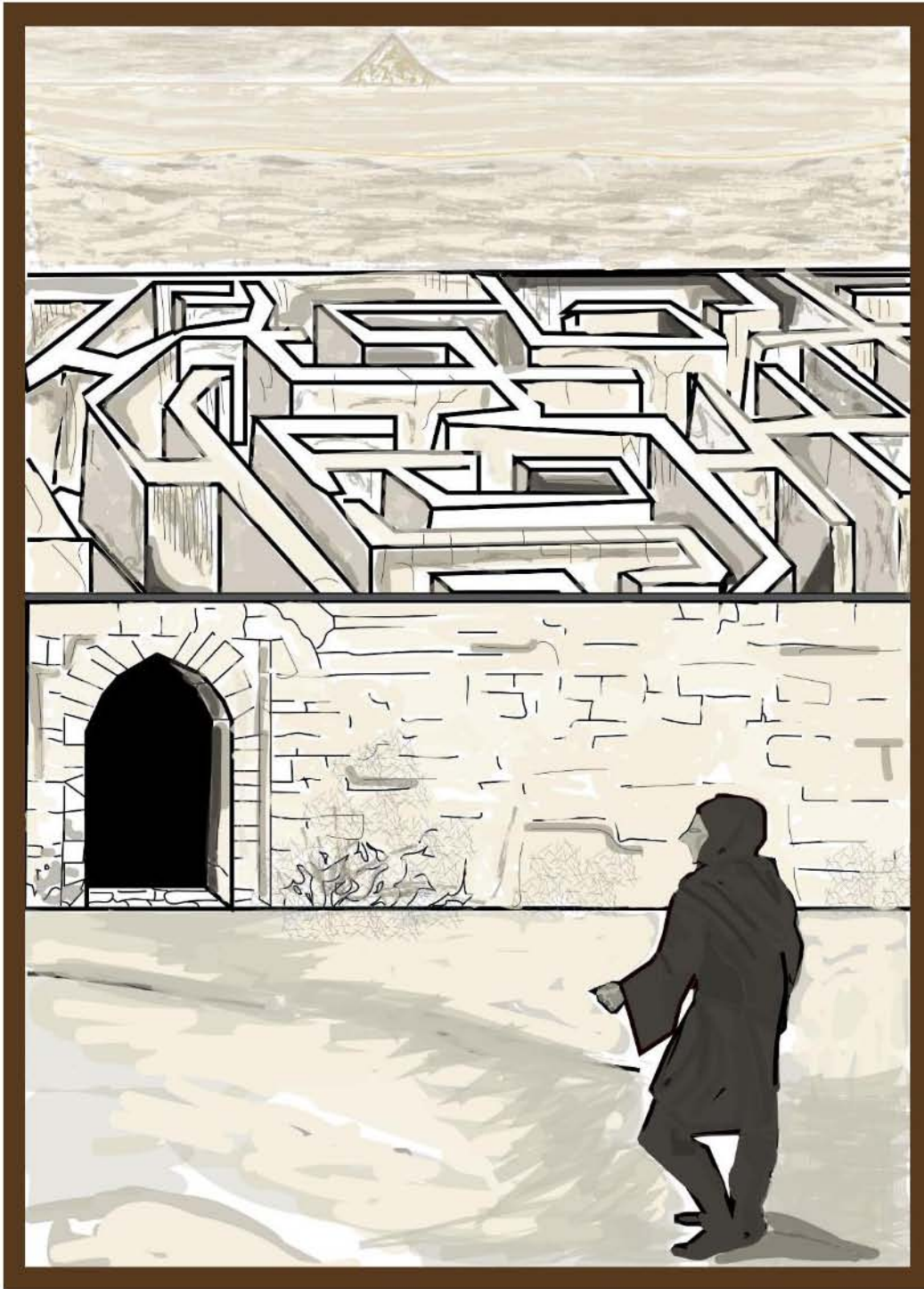
¹⁵ ¹⁵ Cisneros Estupiñan, Mireya. Ídem. Pág. 45

En el segundo capítulo se expone la estratificación conceptual de la Web, mediante el diálogo entre distintos autores, con el objetivo de clarificar las diferencias entre la *web profunda* y las *redes oscuras*. Se desarrolla un apartado dedicado a la conceptualización social de la *web profunda* del periodo 2012 al 2015, y posteriormente se trata a grandes rasgos sus antecedentes, funcionamiento, riesgos de acceso, contenidos y servicios.

En el tercer capítulo se exponen los antecedentes de las *redes oscuras* y se hace énfasis en adquirir o utilizar una computadora para el acceso a las *redes oscuras*. Se mencionan los principales sistemas operativos y como estos pueden determinar y condicionar la instalación del software para el acceso y navegación en las *redes oscuras*. Finalmente se realiza un breve análisis sobre los contenidos de las *redes oscuras* y se menciona la importancia de los aspectos legales en el uso de los contenidos y servicios ilícitos, con el fin de procurar la seguridad tanto para el usuario como para las bibliotecas que proporcionan el servicio de Internet.

Por último, se incluye un apartado de conclusiones en donde se plantean los resultados obtenidos del tercer capítulo, utilizando los fundamentos y aspectos teóricos del primer capítulo, con el fin de destacar las coincidencias, diferencias y características de las tres *redes oscuras* en comparación con los resultados del análisis del monitoreo.

Capítulo 1
Acceso a la Web



Pintura del enmascarado entrando al laberinto que conduce al mar: creación propia basada en la cuarta lámina del libro de *El Club Dumas*, de Arturo Pérez-Reverte.

1.1 Introducción

Este capítulo se trata acerca del acceso a la Web y los conceptos teóricos sobre las diferencias tanto de Internet (como una infraestructura) y, de la Web (como el conjunto de contenidos digitales en línea). Así como los antecedentes militares de Internet y su actual incidencia en la vida civil. Se aborda el tema en cuanto a los requerimientos de conexión y los tipos de comportamiento en la conexión al servicio de Internet en México, con base en datos proporcionados por el Instituto Nacional de Estadística y Geografía.

Se clarifican los conceptos de acceso y disponibilidad desde un enfoque bibliotecológico, ello con el fin de proporcionar un fundamento teórico para su posterior aplicación en los siguientes capítulos. Del mismo modo se tratan temas como la navegación en la Web, la recuperación de la información y el acceso.

Se mencionan los elementos de accesibilidad como: la restricción, el control, la censura y el poder, así como los elementos de la complejidad en la Web, tales como: la vigilancia, la seguridad, el anonimato y la privacidad. Por otro lado, se aborda la relevancia y la utilidad de la Web en torno a los servicios en línea. Además de una tipificación a groso modo sobre los tipos de usuarios en la Web.

Finalmente se mencionan las características de un documento o contenido fiable para su consumo informativo, así como el concepto de la información privilegiada.

1.2 Antecedentes

Fue a principios de los años sesenta en donde se dan los inicios de Internet, basados en las necesidades militares de comunicación a nivel global tanto para los Estados Unidos de América como de la anteriormente llamada Unión Soviética (actualmente Rusia). Juan Corcuera y Ricardo Arnaus¹⁶ señalan que, la creación de las redes de comunicación descentralizadas fue un tema de prioridad para los sistemas de defensa militar de los años sesenta, puesto que, la descentralización de las redes de comunicación no sólo permite una pronta recuperación de la red, sino que también posibilita la ventaja de no tener un punto específico de vulnerabilidad en la comunicación militar.

Años más tarde, fue en los Estados Unidos de América en donde surge en 1969 el proyecto de ARPANET posteriormente llamado DARPA (Defense Advanced Research Projects Agency Network),¹⁷ separado de la parte militar en el año de 1983 y posteriormente desmantelado en 1990. En 1991 fue creada Internet como la red para la comunicación entre los individuos por medio de lenguajes y protocolos informáticos, con el objetivo de intercambiar información. Además de la infraestructura se incorporaron otros recursos abstractos¹⁸ como el hipervínculo y el navegador.

En 1993 Internet es accesible para los ciudadanos, y al paso de la década de los noventa se populariza «la red de redes» conocida públicamente como Internet. La cual según Lawrence Lessig¹⁹ posee una dualidad en tanto su utilidad académica como para fines de ocio.

¹⁶ Corcuera, Juan y Arnaus, Ricardo. *Internet para todos* (Madrid: Prensa Técnica, 1998). Pág. 19

¹⁷ Morán Espinosa, Alejandra., Servín Caamaño, Abraham y Alquicira Gálvez, Oscar. "TIC (Internet) y ciberterrorismo". *Revista Seguridad Cultura de prevención para TI*, no. 23 (2015): 25-29. Recuperado en: <http://revista.seguridad.unam.mx/numeros/numero-23> [Consultado 12 de abril de 2015]

¹⁸ Todd, Stephen. "A guide to the Internet and World Wide Web". *Structural Survey* 17, no. 1 (1999): 36-41. Recuperado en: <http://www.emeraldinsight.com.pbidi.unam.mx:8080/doi/full/10.1108/02630809910263614> [Consultado 14 de enero de 2016]

¹⁹ Lessig, Lawrence. *El código y otras leyes del ciberespacio*. Traducido por Ernesto Alberola. (Madrid: Grupo Santillana, 2001). Pág. 59

En sus inicios Internet, no estaba diseñada para el uso comercial,²⁰ pero conforme a la regulación de los servicios y el desarrollo tecnológico de protocolos de transferencia se sistematizó el comercio de bienes y servicios. Dominique Wolton²¹ menciona que la utilidad de la red en los primeros años se enfocaba en la integridad del contenido de los paquetes de información más allá de la estabilidad de la infraestructura. No obstante en los años venideros la velocidad y la capacidad de transferencia se convertirían en pieza fundamental para los Proveedores del Servicio de Internet (por sus siglas en inglés ISP).

1.3 Internet y la Web

Internet es un conjunto de equipos interconectados por medio de redes para el intercambio y almacenamiento de datos e información digital. Los equipos que almacenan los contenidos digitales son denominados «servidores» en los cuales se alojan datos, información y las aplicaciones que permiten brindar un servicio a distancia. Parte de la infraestructura de Internet se compone de estándares y reglas, con el fin de establecer canales de comunicación entre los distintos equipos de cómputo y medios con la capacidad de conexión a Internet como lo son: computadoras portátiles y teléfonos inteligentes.

La Web e Internet no son sinónimos puesto que Internet es el medio físico para navegar en la Web. La Web es el conjunto de todos los contenidos vinculados mediante el hipertexto. Thomas Sheldon,²² Juan Corcuera y Ricardo Arnaus,²³ Jordi Guim²⁴ y José Huidobro²⁵ mencionan que, Internet es un conjunto de computadoras en red. Sumado a ello Gonzalo Álvarez²⁶ señala que, Internet es un servicio de conexión.

²⁰ Lessig, Lawrence. Ídem. Pág. 83.

²¹ Wolton, Dominique. *Sobrevivir a internet: conversaciones con Oliver Jay*. (España: Gedisa, 2000). Pág. 76

²² Sheldon, Thomas. *LAN times: enciclopedia de redes networking*. Traducido por Isabel Arroyo Et al. (México: McGraw-Hill Interamericana, 1994). Pág. 501

²³ Corcuera, Juan y Arnaus, Ricardo. Ídem. Pág. 14.

²⁴ Guim, Jordi. *Internet: La guía más fácil para dominar la red*. (España: Ediciones Gestión, 1997). Pág. 23.

²⁵ Huidobro, José Manuel. *Todo sobre comunicaciones*. (Madrid: Paraninfo, 1998). Pág. 141

²⁶ Álvarez Marañón, Gonzalo. *¿Qué sabemos de? Cómo protegernos de los peligros de internet*. (España: Consejo Superior de Investigaciones Científicas, 2009). Pág. 93

La Internet se ha definido como una "red de redes". Dicha red abrió nuevas perspectivas para quienes buscaban la información durante la década de los noventa. Internet se ha convertido en una amplia difusión de medios populares y comerciales de comunicación, asimismo procura la accesibilidad a millones de personas y organizaciones. En el presente, una vasta cantidad de información se pone a disposición de los individuos y organizaciones a través de Internet como servicio de información.²⁷

Stephen Todd²⁸ y Dominique Wolton²⁹ argumentan que, Internet es un conjunto de redes que permiten la transferencia de datos. Por tanto el servicio de Internet es todo aquel conjunto de señales, antenas, cableado y protocolos para acceder a los servicios digitales, es pues una infraestructura.

Por otro lado, la Web es todo aquel conjunto de sitios web, páginas, aplicaciones en línea, servicios y contenidos que se visualizan mediante un navegador o interfaz. Christian Crumlish,³⁰ Stephen Todd³¹ además de John Levine, Carol Baroudi, y Margaret Levine³² sostienen que, la Web es un conjunto de páginas y documentos alojados en servidores. Además de que ciertos sitios web tienen el atributo de prestar alguna clase de servicio especial.

²⁷ Traducción libre véase Singh, Shashi Prabha. "Collection management in the electronic environment". *The Bottom Line: Managing Library Finances* 17, no. 2 (2004): 55-60. Recuperado en: <http://www.emeraldinsight.com/journals.htm?articleid=860825&show=html> [Consultado 10 de enero de 2014]

²⁸ Todd, Stephen. *Ibíd.* Recuperado en: <http://www.emeraldinsight.com.pbidi.unam.mx:8080/doi/full/10.1108/02630809910263614> [Consultado 14 de enero 2016]

²⁹ Wolton, Dominique. *Loc. Cit.*

³⁰ Crumlish, Christian. *Diccionario de Internet*. Traducido por Jorge Becerra. (Santafé de Bogotá; México: McGraw-Hill, 1996). Pág. 212

³¹ Todd, Stephen. *Op. Cit.*

³² Levine, John R., Baroudi, Carol y Levine Young, Margaret. *Internet para dummies*. Traducido por Rita Benavides. (México: ST editorial, 2006). Pág. 97

La Web es un servicio de transferencia de información en línea que permite distribuir texto, imagen y sonido, posibilita la comunicación, facilita la realización de transacciones y del entretenimiento, es, por tanto, uno de los grandes activos de la red. Se trata de un sistema normalizado de presentación, consulta y distribución de información.³³

La Web es un servicio que en apariencia puede llegar a ser gratuito y accesible para todo tipo de persona. Sin embargo para acceder a la Web es necesario contar idealmente con un servicio de conexión mediante la suscripción para el acceso a Internet.

1.4 El servicio de Internet

Para tener acceso a Internet es necesario contar con un Proveedor de Servicio de Internet (por sus siglas en inglés ISP), de modo que no todos los individuos pueden acceder de forma directa. Una forma común para acceder al servicio de Internet de forma gratuita es a través de los servicios gubernamentales o en las bibliotecas públicas. Thomas Sheldon³⁴ señala que, el espectro de las señales de transferencia de datos es acaparado por las sucursales gubernamentales junto con de las empresas privadas, las cuales al tener un alto poder de acceso a los recursos merman la calidad de los servicios para el ciudadano común.

John Levine, Carol Baroudi y Margaret Levine³⁵ mencionan que, es imprescindible pagar a un ISP por el acceso a la red de redes. Además de contar con el servicio a disposición del cliente sin importar horarios, de esta manera el usuario evita los registros previos en los servicios gratuitos (o de bajo costo) de acceso a Internet. James Katz y Ronald Rice³⁶ mencionan que, una vez solucionado el acceso al servicio de Internet es viable la navegación por la Web para la consulta, la lectura y reproducción de contenidos relacionados a la

³³ Rodríguez, Blanca. *El documento: entre la tradición y la renovación*. (España: Trea, 2002). Pág. 178

³⁴ Sheldon, Thomas. Ídem. Pág. 503

³⁵ Levine, John R., Baroudi, Carol y Levine Young, Margaret. Ídem. Pág. 14

³⁶ Katz, James y Rice, Ronald. *Consecuencias sociales del uso de Internet*. Traducido por Mónica Torres. (Barcelona: UOC, 2005). Pág. 107

cultura; o a la manufactura de artefactos bélicos. Diane Kovas y Angela Elkordy³⁷ plantean que, el acceso a Internet permite conocer distintos tipos de recursos de información.

Cabe aclarar que el servicio de conexión a Internet no sólo representa un beneficio para los que hoy en día utilizan los servicios digitales de la Web para su bienestar académico, cultural y económico, sino que Internet es también una fuente de ingresos para el *Estado-nación*, puesto que de las instalaciones y del desarrollo de la infraestructura se derivan los pagos de los derechos e impuestos por el uso de los espacios públicos.

1.4.1 Conexión

Para realizar la conexión al servicio de Internet se requiere de una computadora con los componentes de transmisión para el envío y recepción de datos. Además de la computadora u otro medio de conexión es indispensable contar con los conectores y los puntos de acceso, tales como las antenas y el cableado de los ISP en combinación con los componentes de transmisión intangibles para la conexión como: la dirección IP (Protocolo de Internet) del equipo de origen y el destino, como lo anota Lawrence Lessig.³⁸ Es decir el lenguaje de comunicación.

Las computadoras personales y teléfonos inteligentes con conexión al servicio de Internet no sólo poseen la etiqueta de identificación IP, sino que además cuentan con un identificador físico llamado Control de Acceso al Medio (por sus siglas en inglés MAC),³⁹ es decir que, es posible rastrear el origen de la computadora a pesar de que el usuario modifique la dirección IP pública con el fin de ocultar la identidad de la computadora o cualquier medio de conexión con el que accede al sitio, página o aplicación web. Sin embargo existen

³⁷ Kovacs, Diane K., y Elkordy, Angela. "Collection development in cyberspace: building an electronic library collection". *Library Hi Tech* 18, no. 4 (2000): 335-361. Recuperado en: <http://www.emeraldinsight.com/journals.htm?articleid=861248&show=html> [Consultado 21 de enero de 2016]

³⁸ Lessig, Lawrence. Ídem. Pág. 71.

³⁹ Dhanjani, Nitesh., Ríos, Billy y Hardin, Brett. *La nueva generación hacker*. Traducido por Bruno Gorjón. (Madrid: Anaya Multimedia, depósito legal, 2009). Pág. 185

procedimientos para modificar la IP y realizar el enmascaramiento de la MAC; así como existen métodos para revertir el anonimato. Aunque no es vital para el usuario común conocer la operatividad abstracta en la conexión, cuando menos si resulta ser conveniente saber el margen de costo-beneficio en el servicio de Internet. En México, al paso del tiempo se han propiciado y matizado ciertas características tanto en el perfil de usuario como en el desarrollo de la cobertura.

1.4.2 Conexión a Internet en México 2012 – 2015

En el último lustro, instituciones como la Asociación Mexicana de Internet (AMIPICI), la empresa privada Gabinete de Comunicación Estratégica (GCE) y el Instituto Nacional de Estadística y Geografía (INEGI) han generado una serie de encuestas que permitieron reconocer la situación en que se encuentra la conexión a Internet en México, sin embargo los estudios carecen de periodicidad. Para fines de este trabajo se han realizado cuatro tablas, que de manera general reúnen los resultados obtenidos por estas instituciones de acuerdo a los temas que se consideran relevantes en la conexión a Internet.

En el caso concreto de México (país en donde se realizó esta investigación), la cobertura, los medios para acceder y la estabilidad de conexión son factores económicos y sociales que inciden en la experiencia de acceso, navegación y uso de los servicios de la Web. De modo que, en primera instancia, es la cobertura geográfica un factor esencial que no depende del individuo sino de las circunstancias vinculadas al desarrollo tecnológico nacional e inversión empresarial. No obstante, en cuanto a los medios de conexión existe una tendencia hacia los teléfonos inteligentes, de acuerdo con la AMIPICI y el GCE se infiere que, la oferta y la demanda (en el uso del servicio de Internet) están orientadas hacia los jóvenes adultos.

	2012	2013	2014	2015
AMIPICI ⁴⁰		1.- 12 – 17 años 2.- 18 – 24 años 3.- 25 – 34 años	1.- 12 – 17 años 2.- 25 – 34 años 3.- 35 – 44 años	1.- 13 – 18 años 2.- 19 – 24 años 3.- 25 – 34 años
INEGI ⁴¹	1.- 12 – 17 años 2.- 18 – 24 años 3.- 25 – 34 años	1.- 12 – 17 años 2.- 18 – 24 años 3.- 25 – 34 años	1.- 12 – 17 años 2.- 18 – 24 años 3.- 25 – 34 años	
GCE ⁴²				1.- 18 – 29 años 2.- 30 – 39 años 3.- 40 – 49 años

Tabla 1. Mayor rango de edad en los usuarios que realizan la conexión a Internet.

Creación propia.

De acuerdo con las encuestas realizadas, se observa un vínculo entre la edad y las necesidades de conexión a Internet principalmente en los jóvenes adultos anteriormente adolescentes en el periodo 2012.

⁴⁰ Asociación Mexicana de Internet. 2012. *Hábitos de los usuarios de Internet en México*. Recuperado en: https://www.amipci.org.mx/estudios/habitos_de_internet/2012HabitosUsuariosInternetMx.pdf. [Consultado 14 de enero de 2015]. ----- 2013. *Hábitos de los usuarios de Internet en México 2013*. Recuperado en: https://www.amipci.org.mx/estudios/habitos_de_internet/estudio_habitos_internet_2013.pdf. [Consultado 14 de enero de 2015]. ----- 2014. *Hábitos de los usuarios de Internet en México 2014*. Recuperado en: https://www.amipci.org.mx/estudios/habitos_de_internet/Estudio_Habitos_del_Internauta_Mexicano_2014_V_MD.pdf. [Consultado 14 de enero de 2015] y ----- 2015. *11º estudio sobre los hábitos de los usuarios de Internet en México 2015*. Recuperado en: https://www.amipci.org.mx/images/AMIPCI_HABITOS_DEL_INERNAUTA_MEXICANO_2015.pdf [Consultado 14 de enero de 2015]

⁴¹ Instituto Nacional de Estadística y Geografía. 2014. *Hogares con Internet por medio de conexión, 2001 a 2014*. Recuperado en: <http://www3.inegi.org.mx/sistemas/sisept/default.aspx?t=tnf202&s=est&c=19352> [Consultado 14 de enero de 2015]. ----- 2014. *Usuarios de Internet por grupos de edad, 2001 a 2014*. Recuperado en: <http://www3.inegi.org.mx/sistemas/sisept/default.aspx?t=tnf214&s=est&c=19446> [Consultado 14 de enero de 2015] y ----- 2014. *Hogares con conexión a Internet por entidad federativa, 2014*. Recuperado en: <http://www3.inegi.org.mx/sistemas/sisept/default.aspx?t=tnf241&s=est&c=26489>. [Consultado 14 de enero de 2015]

⁴² Gabinete de Comunicación Estratégica. 2015. *¿Qué tan conectado está México?* Recuperado en: http://en2015.gabinete.mx/static/conectividad/Conectividad_mexico_2015.pdf [Consultado 14 de enero de 2015]

	2012	2013	2014	2015
AMIPICI ⁴³	1.- PC 2.- Laptop 3.- Smartphone		1.- Smartphone 2.- PC 3.- Laptop 4.- Teléfono móvil	1.- Laptop 2.- Smartphone 3.- PC 4.- Teléfono móvil
GCE ⁴⁴				1.- Smartphone 2.- PC 3.- Laptop 4.- Tableta

Tabla 2. Medios de conexión más utilizados. Creación propia.

A pesar de que la AMIPICI no reporta datos en el 2013 si cuenta con antecedentes del uso del teléfono inteligente, desde el año 2012. En este sentido los teléfonos inteligentes (smartphone) como medios de conexión han comenzado a tener mayor preferencia, lo cual podría deberse al incremento en la capacidad de procesamiento, facilidad en las tarifas de pago y conexión a Internet que en otrora resultaba complejo y limitado para el teléfono inteligente.

Los teléfonos inteligentes son un medio de conexión ideal para acceder a determinados servicios mediante aplicaciones móviles (por su abreviación en inglés *apps*), para poder realizar un proceso específico como el de consultar el clima, conocer la mejor ruta de traslado, solicitar servicios a domicilio, mensajería y transmisión de contenidos, gestión de documentos digitales etc. Cabe

⁴³ Asociación Mexicana de Internet. 2012. *Hábitos de los usuarios de Internet en México*. Recuperado en: https://www.amipci.org.mx/estudios/habitos_de_internet/2012HabitosUsuariosInternetMx.pdf. [Consultado 14 de enero de 2015] ----- 2013. *Hábitos de los usuarios de Internet en México 2013*. Recuperado en: https://www.amipci.org.mx/estudios/habitos_de_internet/estudio_habitos_internet_2013.pdf. [Consultado 14 de enero de 2015] ----- 2014. *Hábitos de los usuarios de Internet en México 2014*. Recuperado en: https://www.amipci.org.mx/estudios/habitos_de_internet/Estudio_Habitos_del_Internauta_Mexicano_2014_V_MD.pdf. [Consultado 14 de enero de 2015] y ----- 2015. *11º estudio sobre los hábitos de los usuarios de Internet en México 2015*. Recuperado en: https://www.amipci.org.mx/images/AMIPCI_HABITOS_DEL_INERNAUTA_MEXICANO_2015.pdf [Consultado 14 de enero de 2015]

⁴⁴ Gabinete de Comunicación Estratégica. 2015. *¿Qué tan conectado está México?* Recuperado en: http://en2015.gabinete.mx/static/conectividad/Conectividad_mexico_2015.pdf [Consultado 14 de enero de 2015]

mencionar que además de los servicios típicos existen aplicaciones para la navegación anónima, como es el caso de *Orbot*,⁴⁵ no obstante se suele utilizar un sistema físico y abstracto con una arquitectura más compleja para realizar dichos procesos de navegación y transmisión de datos de forma anónima.

En cuanto a los servicios de conexión, según el INEGI, la suscripción mediante un contrato exclusivo de conexión a Internet mediante una línea dedicada ha sido una constante junto con la suscripción a la televisión por cable. Por otro lado, el uso de la línea telefónica ha quedado rezagado posiblemente a causa de los nuevos sistemas, las tecnologías de comunicación y los planes de pre pago en las llamadas locales, nacionales e internaciones de los teléfonos inteligentes. Por lo que se infiere que, la línea telefónica al paso de los últimos años ha comenzado a perder la preferencia por los usuarios en México como servicio de conexión y probablemente como medio de comunicación.

	2012	2013	2014	2015
INEGI ⁴⁶	1.- Línea telefónica dedicada 2.- TV Cable 3.- Línea telefónica 4.- Medios inalámbricos	1.- Línea telefónica dedicada 2.- TV Cable 3.- Medios inalámbricos 4.- Línea telefónica	1.- Línea telefónica dedicada 2.- TV Cable 3.- Medios inalámbricos 4.- Línea telefónica	

Tabla 3. Servicios de conexión a Internet. Creación propia.

En la siguiente tabla se muestran los estados de México en donde se realiza la mayor conexión a Internet.

⁴⁵ Guardian Project. 2014. Orbot: Tor for Android. *Guardian Project*. Recuperado en: <https://guardianproject.info/apps/orbot/> [Consultado 23 de junio de 2016]

⁴⁶ Instituto Nacional de Estadística y Geografía. 2014. *Hogares con Internet por medio de conexión, 2001 a 2014*. Recuperado en: <http://www3.inegi.org.mx/sistemas/sisept/default.aspx?t=tin202&s=est&c=19352> [Consultado 14 de enero de 2015] ----- 2014. *Usuarios de Internet por grupos de edad, 2001 a 2014*. Recuperado en: <http://www3.inegi.org.mx/sistemas/sisept/default.aspx?t=tin214&s=est&c=19446> [Consultado 14 de enero de 2015] y --- ----- 2014. *Hogares con conexión a Internet por entidad federativa, 2014*. Recuperado en: <http://www3.inegi.org.mx/sistemas/sisept/default.aspx?t=tin241&s=est&c=26489>. [Consultado 14 de enero de 2015]

	2012	2013	2014	2015
AMIPICI	1.- Estado de México 2.- Ciudad de México 3.- Jalisco			Zona central del país
INEGI			1.- Aguascalientes 2.- Baja California 3.- Baja california Sur 4.- Campeche 5.- Coahuila de Zaragoza 6.- Colima 7.- Chiapas 8.- Chihuahua 9.- Ciudad de México 10.- Durango	
GCE				1.- Baja california Sur 2.- Nuevo León 3.- Baja California 4.- Quintana Roo 5.- Campeche 6.- Querétaro 7.- Tabasco 8.- Tamaulipas 9.- Sonora 10.- Ciudad de México

Tabla 4. Estados de donde se realiza la mayor conexión a Internet. Fuentes de la Tabla 2 y 3. Creación propia.

Los estudios de la AMIPICI muestran que la región Centro sur (Estado de México y Ciudad de México) tuvo un alto índice de conexión al servicio de Internet en el año 2012. La Ciudad de México al ser el punto geográfico en donde se realizó la conexión al servicio de Internet para el caso práctico de la investigación puede ser considerada como uno de los lugares privilegiados en el acceso a Internet, pero no el mejor. No obstante en el 2014 el INEGI proporciona un incremento de conexión en la región Noroeste (Baja California, Baja California sur, Chihuahua y Durango) lo que denota un alto desarrollo en cuanto a la infraestructura para el acceso a Internet. Mientras que para el año del 2015 la AMIPICI proporciona el dato sobre mayor conexión en la región Centro del país. En este mismo sentido el GCE provee un estudio del año 2015 sobre el nivel de conexión en la región Noroeste (Baja California sur, Baja California y Sonora) además de la región Sureste (Quintana Roo, Campeche y Tabasco).

En síntesis se puede agregar que, en México existe una notable desigualdad en cuanto a la cobertura geográfica del servicio de Internet, además de que el usuario promedio es el joven adulto (con un rango de los 18 a los 30 años de edad), dicho usuario puede utilizar los servicios de la Web para realizar parte de sus necesidades cotidianas y/o solicitar servicios adicionales mediante aplicaciones móviles para optimizar los tiempos y obtener ventajas. Pero por otro lado, se puede interpretar que, el joven adulto como el usuario con mayor dependencia del servicio de conexión a Internet puede llegar a ser víctima del espionaje, la vigilancia, control remoto y robo tanto de sus datos personales como de la información laboral, académica, financiera y sensible. Ante este panorama son las buenas prácticas en el uso del servicio Internet y los servicios de la Web una alternativa ante la carencia de conocimientos técnicos sobre el uso de tecnologías electrónicas y abstractas.

En cuanto a la interpretación de los estudios proporcionados por la AMIPICI, el INEGI y el GCE resulta complicado establecer un criterio sobre en qué región del territorio nacional se realiza un mayor índice de conexión a Internet, puesto que

como se señaló en el inicio del apartado, existe una carencia de periodicidad en los estudios sobre la cobertura geográfica. Por lo que no es viable comparar los resultados en este caso, dado que las perspectivas de los tres estudios son distintas y hay pocos elementos en común. Sin embargo a partir de las coincidencias en los años 2014 y 2015 se revela un incremento en ciertas regiones del país.

De acuerdo a esta situación existe cierta dificultad en cuanto a un seguimiento sobre el nivel de cobertura de conexión al servicio de Internet por lo que se deberían de establecer lineamientos en cuanto al establecimiento de estándares de evaluación, periodicidad y profundidad en los estudios concernientes respecto a los índices de conexión a Internet en México.

1.5 Acceso y disponibilidad

Con el objetivo de aclarar el concepto de acceso, es primordial establecer las diferencias de la accesibilidad y la disponibilidad. A continuación a manera de diálogo entre distintos autores se muestran enfoques sobre el acceso y la disponibilidad.

Para acceder al servicio de Internet, idealmente se necesita de liquidez económica, es decir del dinero o acceso a los recursos, tal como lo anota Pekka Himanen.⁴⁷ El poder adquisitivo es la principal variable de acceso así como el contexto social, el cual se relaciona con la calidad de la infraestructura⁴⁸ por lo que la brecha digital repercute en la experiencia en el uso de los recursos digitales y no basta con saber de su existencia sino que es vital realizar el proceso de conexión y navegación, según lo anotan James Katz y Ronald Rice.⁴⁹

⁴⁷ Himanen, Pekka. *La ética del hacker y el espíritu de la era de la información*. (España: Destino, 2002). Recuperado en: <http://eprints.rclis.org/bitstream/10760/12851/1/pekka.pdf> [Consultado 1 de marzo de 2013]

⁴⁸ UNESCO. *Memoria del mundo: directrices para la salvaguarda del patrimonio documental*. Edición revisada por Ray Edmondson. (París: UNESCO, División de la sociedad de la información, 2002). Pág. 14

⁴⁹ Katz, James y Rice, Ronald. Op. Cit., Pág. 28

Además del capital financiero es primordial contar con un capital técnico-cultural que permita establecer un criterio en la adquisición de nueva información y selección en los servicios, tal como lo mencionan Maureen McCreadie y Ronald Rice, puesto que para poder tener acceso a un recurso informativo es menester contar inicialmente con la capacidad de interpretar la información preliminar así como el de interactuar con el recurso digital.⁵⁰ Josep Vallés⁵¹ agrega que, el acceso delimita quién puede y quién no. Peter Suber⁵² añade que, también existen otras barreras en el acceso como las diferencias de idioma, personas con capacidades diferentes y la velocidad de conexión a Internet.

Por lo anteriormente mencionado, el acceso es todo aquello que regula al individuo mediante filtros o requerimientos tanto previos como posteriores. De manera que es a través de los parámetros selectivos que el individuo tiene privilegios de acceso a los servicios y los contenidos en la Web. Neil Randall⁵³ argumenta que, el acceso divide a quien puede utilizar todas las funciones tanto de la infraestructura de Internet como de la navegación en la Web, ello dependiendo si el usuario es el titular del servicio o sólo tiene acceso al servicio por medio de su adscripción a alguna institución académica o gubernamental.

Mike Chapple, Bill Ballard, Tricia Ballard y Erin Banks⁵⁴ argumentan que, el acceso es la capacidad de interacción entre el sujeto con el objeto, siendo el objeto al que se le han asignado las restricciones mediante la autorización o la denegación por medio de controles de acceso. Por tanto, se puede interpretar que el acceso a la red es una interacción regulada entre el deseo, las necesidades y las expectativas; en contraste con las limitaciones de conexión y navegación.

⁵⁰ McCreadie, Maureen y Rice, Ronald. "Trends in analyzing access to information. Part I: cross-disciplinary conceptualizations of access". *Information processing and management: an international journal archive* 35, no. 1, (1999): 45-76

⁵¹ Vallés, Josep. *Ciencia política: una introducción*. 2a ed. (España: Ariel, 2002). Pág. 19

⁵² Suber, Peter. 21 de junio de 2004. Open Access Overview. *Legacy earlham*. Recuperado en: <http://legacy.earlham.edu/~peters/fos/overview.htm> [Consultado 27 de marzo de 2015]

⁵³ Randall, Neil. *Aprendiendo Internet en 21 días*. Traducido por Enrique Palos. (México: Prentice Hall, 1995). Pág. 42

⁵⁴ Chapple, Mike Et al. *Access control, authentication, and public key infrastructure*. 2a ed. (Burlington, Massachusetts: Jones & Bartlett Learning, 2014). Pág. 4

En contraparte, la disponibilidad es todo aquello que no se encuentra regulado con restricciones, pero aun así cumple con elementos de autoría, identificación y procedencia, por lo que es posible hacer uso de los recursos. La disponibilidad según Antonio Miranda⁵⁵ es el acceso a los contenidos con la condición de que los recursos se encuentren organizados para su consulta. En ese mismo aspecto Ángeles Maldonado y Luis Rodríguez⁵⁶ apuntan que, en el acceso abierto a la literatura científica debe imperar la disponibilidad de los contenidos, es decir sin restricciones económicas, electrónicas y horarios de acceso. Por otro lado Juan Voutssás Márquez⁵⁷ argumenta que, el acceso corresponde a la capacidad tecnológica, mientras que la disponibilidad delimita el grado de interacción con los contenidos digitales.

José Martínez⁵⁸ agrega que, la disponibilidad es también la posibilidad de adquirir o consultar de forma regulada los materiales y contenidos informativos de una biblioteca o librería, según sea el caso. Por otro lado Estela Morales⁵⁹ añade que, la disponibilidad tiende a facilitar el acceso basándose en la organización y la visibilidad.

De lo anterior se ha optado que para poder acceder a algún servicio o producto es primordial contar con liquidez económica pero también es viable el acceso mediante las facilidades proporcionadas por terceras personas, el entorno social, el capital técnico y el capital cultural. De modo que estos son elementos determinantes para obtener los mejores productos así como la información adecuada, que en cierto modo provee de mejores expectativas, puesto que al contar con cierta estabilidad económica aunada a una amplia gama de opciones en cuanto a los productos, es viable la adquisición de beneficios y satisfacciones

⁵⁵ Miranda, Antonio. "La sociedad de la información: contenidos y accesos en perspectiva". En *Infodiversidad y cibercultura: globalización e información en América latina*. (Argentina: Alfagrama, 2006). Pág. 136

⁵⁶ Maldonado Martínez, Ángeles y Rodríguez Yunta, Luis. *La información especializada en internet*. 2a ed. (España: CSIC, 2006). Pág. 156

⁵⁷ Voutssás Márquez, Juan. "Preservación documental digital y seguridad informática". *Investigación bibliotecológica* 24, no. 50 (2010): 127-155. Recuperado en: <http://www.journals.unam.mx/index.php/ibi/article/view/21416> [Consultado 18 de junio de 2016]

⁵⁸ Martínez de Sousa, José. *Diccionario de bibliología y ciencias afines*. 2a ed. (Madrid: Pirámide, 1993). Pág. 5

⁵⁹ Morales Campos, Estela. "Sociedad e información". *Revista AIDBA* 12, no. 2 (1991): 21-28

con base en la mejor decisión. De esta manera se optimiza la interacción con la tecnología y consecuentemente se fortalecen y se obtienen nuevas habilidades.

En síntesis, el acceso es entonces una brecha que selecciona, clasifica y divide a los individuos de acuerdo a los parámetros selectivos basados en filtros, restricciones y requerimientos como lo son: las capacidades cognitivas, los conocimientos, la identidad personal, la documentación, el poder adquisitivo y los vínculos sociales. El acceso, también se manifiesta en nuevos servicios, percibidos actualmente como parte de las necesidades usuales de consumo, como el servicio de Internet.

1.5.1 Acceso a Internet

Tal como lo señala Diego de Charras,⁶⁰ Internet posee una naturaleza excluyente, puesto que para acceder al servicio es primordial contar con una serie de aspectos basados en la certidumbre económica, educación académica (o capital cultural) y habilidades intelectuales, por lo que no es suficiente ser propietario de algún medio de conexión o computadora personal. Internet no es un medio de comunicación y transmisión de datos para todos. Complementario a esto, el uso de las herramientas adecuadas para la conexión determina una mejor experiencia y disminuye la frustración en los usuarios, según lo comenta Andrew Treloar.⁶¹

Para acceder a Internet es primordial la suscripción mensual o mediante algún contrato anual.⁶² Una vez que se ha efectuado dicho contrato o suscripción al servicio, el usuario en cuestión recibirá privilegios de conexión de acuerdo al costo-beneficio del servicio contratado.⁶³

⁶⁰ De Charras, Diego. *Redes, burbujas y promesas: algunas reflexiones críticas acerca del proyecto sociedad de la información y la nueva economía*. (Argentina: Prometeo libros, 2006). Pág. 88

⁶¹ Treloar, Andrew. "Classifying Internet Access Tools". *Resource Sharing & Information Networks* 9, no. 2 (1994): 19-37. Recuperado en: http://www.tandfonline.com/doi/abs/10.1300/J121v09n02_04 [Consultado 19 de enero de 2016]

⁶² McGraw-Hill, ed. *Diccionario de internet y redes de Microsoft*. Traducido por Vuelapluma. (Madrid; México: McGraw-Hill, 2003). Pág. 4

⁶³ Complutense, ed. *Diccionario de Internet*. (Madrid: Editorial complutense, 2002). Pág. 1

Respecto a la brecha de acceso a Internet James Katz y Ronald Rice⁶⁴ mencionan que, el acceso a Internet reprime a los individuos que realmente lo necesitan como medio para informarse en temas referentes a la actividad económica, el contexto social, sucesos nacionales e internacionales y la política, de manera que, su desventaja se incrementa frente a los que tienen la posibilidad de conectarse a Internet y navegar en la Web para cualquier clase de asunto.

1.5.2 Navegación en la Web

Navegar en la Web usualmente implica el hecho de haber instalado y configurado un navegador, junto con un motor de búsqueda para localizar un sitio web, servicio o contenido determinado. Una forma de acceder a los sitios, contenidos y servicios es mediante la dirección URL (Localizador de Recursos Uniforme), lo cual permite recuperar la ubicación exacta. Respecto a este tema, Jonas Fransson⁶⁵ señala que, las direcciones URL están estructuradas en distintos esquemas que indican su tipo de protocolo, nivel de seguridad y acceso a los servicios de la Web, como los protocolos HTTP, HTTPS y FTP entre otros y, por sus datos como: directorios, puertos, archivos, fechas de creación, dominios y subdominios, etc. De este modo se puede interpretar la autenticidad, nivel jerárquico de los contenidos o la tipología de un sitio web con base en la anatomía de su URL.

Cabe agregar que, Timothy John Berners-Lee fundador del Consorcio World Wide Web (por sus siglas en inglés W3C),⁶⁶ creo el protocolo HTTP (Protocolo de Transferencia de Hipertexto) el cual permite la transferencia de datos y la comunicación e interacción entre los usuarios y los servidores que alojan los contenidos digitales, el protocolo HTTP es una tecnología elemental para el

⁶⁴ Katz, James y Rice, Ronald. Ídem. Pág. 26

⁶⁵ Fransson, Jonas. *Efficient information searching on the Web: a handbook in the art of searching for information*. (New Delhi, India: Ess Ess Publications, 2011). Pág. 79

⁶⁶ World Wide Web Consortium. 30 de junio de 2016. Tim Berners-Lee. **W3C**. Recuperado en: <https://www.w3.org/People/Berners-Lee/> [21 de agosto de 2016]

funcionamiento de la Web, puesto que permite el acceso a los sitios, páginas y contenidos que ofrecen información y/o prestan alguna clase de servicio.

La anatomía de la URL:⁶⁷

(ejemplo) http://en.wikipedia.org/wiki/Middle_Ages

1. protocolo: **http (protocolo de transferencia de hipertexto)**
2. nombre del servidor Web: **en** (con frecuencia **www**)
3. sistema de nombre del dominio: **Wikipedia**
4. dominio de nivel superior: **org**
5. nombre del directorio: **wiki**
6. nombre del archivo: **Middle_Ages**

Figura 1. La anatomía de la dirección URL. Traducción libre.

La anatomía de la URL es útil para conocer la autenticidad de las direcciones. De manera que hay direcciones URL en donde se desglosan los datos como el nombre y el tipo del archivo, así como la fecha de creación del sitio web. En el caso de encontrar un desglose irregular como por ejemplo *http://127.0.0.1:8888/USK@wNW1q*. Denota ciertos datos atípicos como la dirección de la computadora (127.0.0.1) desde donde se realiza la petición de datos, por lo que la URL no es común.

Por otro lado, los motores de búsqueda utilizan la lógica de Boole⁶⁸ con los operadores de Y, O y NO. Actualmente la tecnología de dichos buscadores interpreta los espacios entre cada concepto, término y palabra, facilitando al usuario la recuperación de los contenidos mediante las listas de resultados, permitiendo obtener una mejor experiencia en la navegación.

⁶⁷ Fransson, Jonas. Ídem. Pág. 79

⁶⁸ Ídem. Pág. 74

Para Jonas Fransson dos métodos muy frecuentes para navegar, son: el primero, siguiendo algún menú o listado de datos en donde se delimitan los contenidos agrupados en conjuntos, a partir de sus atributos y elementos en común, y el segundo, la navegación aleatoria. Ello depende en gran medida de las características de los sitios y páginas web, la composición gráfica y la estructura de los hipervínculos para avanzar o retroceder. Lola García⁶⁹ señala que, si el usuario comprende la operatividad en las herramientas del navegador, la recuperación de la información será precisa o exhaustiva según sea el caso. En este sentido José Cordón⁷⁰ indica que, la información puede llegar a ser pertinente para el usuario, siempre y cuando, se le proporcione difusión a los servicios y contenidos en línea, o bien los contenidos tengan un alto nivel de visibilidad en los primeros resultados del motor de búsqueda.

Un factor importante a considerar en la localización e identificación de los sitios web de interés para los usuarios, es la deshabilitación de los contenidos, recursos y sitios, ello se debe a la carencia en el interés por administrador web, o simplemente los contenidos en cuestión fueron eliminados, a este fenómeno se le conoce como «evaporización» tal como lo señala Paul Pedley.⁷¹ A esta concepción, Peter Lyman⁷² agrega que, la Web está en constante movimiento y hay sitios que desaparecen mientras otros comienzan a posicionarse en los primeros resultados de la búsqueda.

La Web así como Internet es en apariencia accesible para todos los individuos ya que en ella se ofrecen una gama de servicios de información, pero existen servicios que no se encuentran disponibles para todos los usuarios, según lo

⁶⁹ García Santiago, Lola. *Extraer y visualizar información en internet: el web mining*. (España: Trea, 2003). Pág. 203

⁷⁰ Cordón García, José. *Las nuevas fuentes de información: información y búsqueda documental en el contexto de la web 2.0*. (Madrid: Ediciones Pirámide, 2010). Pág. 359

⁷¹ Pedley, Paul. *The invisible web: searching the hidden parts of the internet*. (London: Aslib-IMI, 2001). Pág. 7

⁷² Lyman, Peter. "Archiving the World Wide Web". En *Building a national strategy for preservation: issues in digital media archiving*. (Washington: Council on Library and Information Resources, 2002). Recuperado en: <http://www.clir.org/pubs/reports/pub106/pub106.pdf> [Consultado 30 de enero de 2016]

indica Richard Rubin.⁷³ En ese mismo tenor Lola García⁷⁴ hace énfasis en que, a pesar de que la información pueda ser recuperada, la Web posee una dualidad que distingue a los grupos de elite, en esta supuesta igualdad se percibe fragmentación y un discurso de democratización. Navegar en la Web no implica un costo extra pero si a sus servicios y contenidos exclusivos. Por otro lado, para obtener los mismos contenidos de forma parcial (o similares en su defecto) mediante otros servicios, se requiere de ciertas habilidades en la recuperación de la información.

1.5.3 Recuperación de la información

Peter Ingwersen⁷⁵ comenta que, el enfoque clásico de la recuperación de la información tiene sus orígenes en los tiempos de la antigua Roma, la recuperación consistía en separar los distintos tipos de documentos según su asunto administrativo. En la era moderna, José Salvador⁷⁶ menciona que después de la Segunda Guerra Mundial (1945) la explosión de la información fue una consecuencia de los avances científicos, derivando en la crisis de la información en cuanto a su acceso y recuperación. José Salvador y José Angos⁷⁷ agregan que, el concepto de la recuperación se le atribuye a Calvin Mooers en 1950, a este respecto Collen Cool y Nicholas Belkin⁷⁸ añaden que, a finales de ese mismo año el concepto de la recuperación de la información comenzó a popularizarse, coincidiendo con el advenimiento del equipo de cómputo y el procesamiento automatizado de los datos, y posteriormente consolidándose en la década de los sesenta con el nacimiento y desarrollo de las bases de datos en línea, para solucionar los problemas en las búsquedas de información, como lo acota José Salvador.⁷⁹

⁷³ Rubin, Richard E. *Foundations of library and information Science*. (Estados Unidos de América: Neal Schuman Publishers, 2004). Pág. 171

⁷⁴ García Santiago, Lola. Ídem. Pág. 63

⁷⁵ Ingwersen, Peter. *Information retrieval interaction*. (Londres: Taylor Graham Publishing, 2002). Pág. 61

⁷⁶ Salvador Oliván, José A. *Recuperación de la información*. (Buenos Aires: Alfagrama, 2006). Pág. 86

⁷⁷ Salvador Oliván, José Antonio y Angos Ullate, José. *Técnicas de recuperación de información: aplicación con Dialog*. (Gijón, Asturias: Trea, 2000). Pág. 23

⁷⁸ Cool, Collen y Belkin, Nicholas. "Interactive information retrieval: history and background". En *Interactive information seeking, behaviour and retrieval*. (London: Facet Publishing, 2011). Pág. 1

⁷⁹ Salvador, José A. Op. Cit. Pág. 111

Ricardo Baeza-Yates y Berthier Ribeiro-Neto⁸⁰ mencionan que, las bibliotecas fueron parte de las primeras instituciones en adoptar el sistema automatizado de recuperación de la información basado en la organización de autores, títulos y fechas de sus obras, para posteriormente desarrollar una arquitectura de datos más compleja por parte de sus proveedores comerciales. José Salvador⁸¹ añade que, los pioneros en cuanto a la recuperación de la información en línea fueron los profesionales de la información.

Siguiendo a Arlene Taylor⁸² un punto total a considerar en la recuperación de la información es la correcta organización de los datos y su diseño lógico en las bases de datos. Mientras que Peter Ingwersen⁸³ agrega que, los lenguajes libres y controlados afectan el resultado en la recuperación de la información puesto que tradicionalmente la búsqueda al ser planteada de forma textual, proporciona consecuentemente un resultado textual.

Nuria Ferrán⁸⁴ expone que, el proceso en la recuperación de la información no es de carácter lineal, ya que existe una retroalimentación o transacción constante, la cual modifica la dinámica del usuario con la Web (o del lector con el contenido) y sus sistemas de búsqueda. Julian Warner⁸⁵ subraya que, las características de los buscadores permiten ampliar el espectro de los resultados esperados. No obstante, uno de los principales conflictos de la Web es la carencia de fiabilidad sobre la información recuperada por medio de los motores de búsqueda, según lo anotan Adrian Stacey y Alison Stacey⁸⁶ en concordancia con José Cordon⁸⁷ quien agrega que, los resultados pueden estar limitados, erróneos y sesgados.

⁸⁰ Baeza-Yates, Ricardo y Ribeiro-Neto, Berthier. *Modern information retrieval: the concepts and technology behind search*. 2da ed. (New York: Addison Wesley, 2011). Pág. 3

⁸¹ Salvador, José A. Ídem. Pág. 118

⁸² Taylor, Arlene. *The organization of information*. 2a ed. (Colorado: libraries Unlimited, 2004). Pág. 2

⁸³ Ingwersen, Peter. Ídem. Pág. 49

⁸⁴ Ferrán Ferrer, Nuria. *Búsqueda y recuperación de la información*. (Barcelona: UOC, 2009). Pág. 14

⁸⁵ Warner, Julian. *Human information retrieval*. (Cambridge, Massachusetts: Massachusetts Institute of Technology, 2010). Pág. 1

⁸⁶ Stacey, Adrian y Stacey, Alison. *Effective information retrieval from the Internet: an advanced user's guide*. (Oxford: Chandos, 2004). Pág. 4

⁸⁷ Cordon García, José. Ídem. Pág. 45

Cabe mencionar que existe una divergencia entre la recuperación de la información y la recuperación de datos, esta última, consiste en determinar cuáles son los documentos que contienen los conceptos, términos y palabras clave; en contraste con la recuperación de la información la cual está orientada hacia un tema concreto, como lo mencionan Ricardo Baeza-Yates y Berthier Ribeiro-Neto.⁸⁸ Por otro lado, Stephen Todd⁸⁹ adiciona que, la captura de la información es un proceso de respaldo y resguardo de aquellos sitios, páginas o contenidos visitados y considerados como relevantes en la navegación.

Finalmente Jesús Tramullas y María Olvera⁹⁰ manifiestan que, la recuperación de la información es una actividad propia y constante del ser humano, la cual persigue como objetivo primordial, el de resolver alguna duda o sustentar un conocimiento previo. Es en este sentido que, el bibliotecólogo actual debe de interactuar de manera continua con las nuevas tecnologías digitales y electrónicas (orientadas a la gestión y recuperación documental) conocidas como tecnologías disruptivas⁹¹ las cuales tienen la característica de tener bajo costo y un alto desempeño, creando en ocasiones brechas digitales y generacionales. No obstante son los aspectos teóricos, el desarrollo de políticas, la voluntad, la apertura y la práctica, los cimientos esenciales para abordar el fenómeno de las tecnologías disruptivas. Empero es importante considerar que, la información relevante en la Web suele estar regulada mediante controles de acceso.

⁸⁸ Baeza-Yates, Ricardo y Ribeiro-Neto, Berthier. Ídem. Pág. 5

⁸⁹ Todd, Stephen. *Ibid.* Recuperado en:

<http://www.emeraldinsight.com.pbidi.unam.mx:8080/doi/full/10.1108/02630809910263614> [Consultado 14 de enero de 2016]

⁹⁰ Tramullas Saz, Jesús y Olvera Lobo, María. ***Recuperación de la información en Internet.*** (Madrid: Ra-Ma, 2001). Pág. 15

⁹¹ Torres Vargas, Georgina Araceli Et al. "The Blended Librarian and the Disruptive Technological Innovation in the Digital World". ***Open Access Library Journal*** 2, (2015): 1-9. Recuperado en: https://www.researchgate.net/publication/280947367_The_Blended_Librarian_and_the_Disruptive_Technological_Innovation_in_the_Digital_World [Consultado 25 de junio de 2016]

1.5.4 Acceso a la información

El acceso autorizado o restringido a la información se establece de acuerdo al tipo de institución u organización que genera, difunde y resguarda la información según su valor y uso potencial, de modo que, existen diferencias en el acceso a la información dependiendo de la instancia que la gestione. Comúnmente el acceso a la información depende de los filtros y políticas para acceder a los datos, documentos o contenidos. La razón de esta accesibilidad se fundamenta en la protección, la seguridad financiera e integridad de los propietarios de la información. Puesto que la información es un instrumento de poder para el desarrollo del conocimiento, la certidumbre y la comprensión de los entornos. A continuación se mencionan algunas similitudes y diferencias del acceso a la información, según distintos autores.

Peter Ingwersen⁹² comenta que, el acceso a la información se divide principalmente en acceso conceptual y acceso físico. El acceso conceptual implica el entendimiento de los contenidos, mientras que el físico es el acceso a los objetos y sus contenidos. Mientras que Ian Rowlands⁹³ establece que hay dos tipos de acceso, el acceso abierto para la ciudadanía y los consumidores mientras que por otro lado, el acceso restringido comprende los datos personales, la información reservada, la seguridad nacional, los avances tecnológicos y las patentes.

En ese mismo sentido de clasificación de acceso, Guillermo Cosentino junto con Chapple, Bill Ballard, Tricia Ballard y Erin Banks exponen los siguientes niveles en cuanto a la clasificación de acceso.

⁹² Ingwersen, Peter. "The role of libraries and libraries in organising digital information". *Libri*, no. 49 (1999): 11-15. Recuperado en: <http://www.librijournal.org/pdf/1999-1pp11-15.pdf> [Consultado 20 de enero de 2016]

⁹³ Rowlands, Ian. *Understanding information policy: proceedings of a workshop held at Cumberland Lodge, Windsor Great Park*. (New Providence, New Jersey: Bowker-Saur, 1997). Pág. 15

Clasificación (de la información judicial) ⁹⁴	Nivel de accesibilidad
Común	Información que pertenece al ámbito público
Accesible	Información a la que se puede tener acceso parcial
Reservada	Información con acceso restringido

Tabla 5. Clasificación de la información judicial. Fuente: creación propia.

Por otro lado Mike Chapple, Bill Ballad, Tricia Ballad y Erin Banks proponen una clasificación sobre la información gubernamental, según su grado de sensibilidad de la información.

Clasificación (información gubernamental) ⁹⁵	Nivel de accesibilidad
Sin clasificación	Información pública
Confidencial	Información que de ser difundida, puede causar daños a la nación
Secreta	Información que de ser difundida, puede causar graves daños a la nación
Altamente secreta	Información que de ser difundida, puede causar daños extremadamente perjudiciales a la nación

Tabla 6. Clasificación de la información gubernamental. Fuente: Traducción libre y creación propia.

Tanto el sistema político gubernamental como el sistema judicial tienen distintos niveles de clasificación, de modo que, la clasificación de la información judicial

⁹⁴ Cosentino, Guillermo. "La información judicial es pública, pero contiene datos privados. Cómo enfocar esta dualidad". *En El acceso a la información judicial en México: una visión comparada*. (México, D.F.: UNAM, Instituto de Investigaciones Jurídicas, 2005). Pág. 250

⁹⁵ Chapple, Mike Et al. Ídem. Pág. 44

ofrece un acceso a todo público y otro acceso parcial, sin embargo queda a reserva un conjunto de documentos y contenidos en donde la información es únicamente accesible para los individuos autorizados; la clasificación gubernamental tiene un nivel de acceso para todo público, no obstante posee más niveles de acceso, ya que de revelarse dicha información podría causar graves daños a la imagen, integridad y operatividad del gobierno, además de atentar contra la seguridad del *Estado-nación*.

En la siguiente tabla, los mismos autores exponen la clasificación de la información de las empresas privadas de acuerdo a la sensibilidad de los datos privados.

Clasificación (de la información de las empresas privadas) ⁹⁶	Nivel de accesibilidad
Pública	Información con disponibilidad para todo público
Interna	Información controlada para cierto tipo de personas
Sensible	Información que puede causar graves daños a la empresa
Altamente sensible	Información que puede causar daños extremadamente perjudiciales a la empresa

Tabla 7. Clasificación de la información de las empresas privadas. Fuente: Traducción libre y creación propia.

La clasificación de la información de las empresas, se percibe de otra forma a diferencia de la clasificación judicial y gubernamental puesto que, la información se considera un recurso de ventaja sobre otras empresas dedicadas a objetivos similares, además de proporcionar productos y servicios, su objetivo primordial es el de obtener ganancias para garantizar su preservación a partir de la gestión

⁹⁶ Chapple, Mike Et al. Ídem. Pág. 45

de la información de sus clientes, las patentes, las estadísticas, los proyectos en desarrollo y el historial administrativo.

Como se ha observado en las tablas anteriores, la información suele estar clasificada según el grado de importancia de quien la gestione, de manera que a groso modo, existen tres niveles de acceso:

1. información disponible para el público en general,
2. información reservada e
3. información altamente reservada

Conforme a este respecto la clasificación de la información en el sector empresarial y gubernamental no tiene niveles intermedios de acceso, sin embargo pueden existir vacíos legales en el acceso a la información gubernamental como por ejemplo, la transparencia de la información en las declaraciones patrimoniales.⁹⁷ Y en el caso de la información judicial, el acceso a la información es gradualmente regulado de acuerdo a su relevancia para los interesados que la requieren,⁹⁸ en donde se hace permisible mantener ciertos expedientes de una zona gris a una zona inaccesible.⁹⁹

En cuanto a la utilidad de la información se entiende que:

- La información judicial, se enfoca hacia la resolución de los conflictos legales con el fin de poder resolver, administrar e impartir justicia en los ciudadanos.

⁹⁷ Excelsior. 6 de febrero de 2015. Por seguridad, senadores optan por la opacidad. *MSN noticias*. Recuperado en: <http://prodiqy.msn.com/es-mx/noticias/mexico/%E2%80%9Cpor-seguridad%E2%80%9D-senadores-optan-por-la-opacidad/ar-AA93c8N> [15 de febrero de 2015]

⁹⁸ Cossío Díaz, José Ramón y Hernández Chávez, María Luisa. 2014. *La Transparencia y el acceso a la Información en los expedientes judiciales*. (México: Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales, 2015). Recuperado en: <http://inicio.ifai.org.mx/Publicaciones/Transparencia%20y%20Acceso%20a%20la%20Informaci%C3%B3n%20en%20los%20Expedientes%20Judiciales.pdf> [10 de julio de 2016]

⁹⁹ Huerta, Irving. 27 de junio de 2016. Tlatlaya: cierran en definitiva acceso a expediente. *Aristegui noticias*. Recuperado en: <http://aristeguinoticias.com/2706/mexico/tlatlaya-cierran-en-definitiva-acceso-a-expediente/> [15 de febrero de 2015]

- En cuanto a la información gubernamental, su utilidad radica en el desarrollo de proyectos sociales, presupuestos, licitaciones, creación de nuevos programas gubernamentales y asuntos referentes a la seguridad nacional.
- La información de las empresas privadas, es utilizada como un recurso de ventaja frente a la competitividad. Dicha información abarca desde los perfiles de usuarios, datos personales, preferencias de consumo, patentes, prototipos y estadísticas prospectivas entre otros aspectos.

Cabe destacar que, dichos autores aportan su perspectiva personal acerca de la clasificación de la información, de modo que, es una forma de entender la operatividad en cuanto a las políticas de información de las instituciones y empresas privadas.

Por otro lado, la solicitud que los usuarios hacen en cuanto a la información, judicial, gubernamental y empresarial corresponde a distintas necesidades y requerimientos de información, de manera que, se puede hablar de una variedad de individuos interesados en los sectores sociales, institucionales, empresariales e industriales.

Independientemente de la clasificación con la que sea etiquetada la información, un factor vital para su utilidad es la comprensión en el lector y el uso potencial de la misma. En este aspecto Maureen McCreadie y Ronald Rice¹⁰⁰ hacen mención que, en el acceso a la información se da un proceso de retroalimentación o transacción para quien hace uso de ella, pero sólo si dicha información es relevante para quien la consulta, interpreta y analiza.

¹⁰⁰ McCreadie, Maureen y Rice, Ronald E. Loc. Cit.

José Usero y Pablo Lara¹⁰¹ agregan que, el acceso a la información mediante el uso de la Web facilita la accesibilidad, siempre y cuando exista igualdad en la adquisición de computadoras personales y el servicio de conexión a Internet. Guillermo Cosentino¹⁰² añade que, el acceso nos conduce a la información, aunque existen limitantes como lo son principalmente: la seguridad del *Estado-nación*, las investigaciones penales y el interés económico justificado por el *Estado-nación*. A lo que finalmente Estela Morales¹⁰³ comenta que, en ocasiones no es posible tener acceso a la información debido a los intereses del *Estado-nación*, los grupos de poder y de las empresas privadas.

En síntesis, las distintas perspectivas en cuanto al acceso a la información pueden ser cohesionadas bajo un enfoque general. Iniciando con el acceso a la información ya sea al sistema judicial, gubernamental o empresarial propuesto por algunos autores (como Guillermo Cosentino junto con Mike Chapple, Bill Ballad, Tricia Ballad y Erin Banks), pasando por controles físicos de acceso (manifestados por Peter Ingwersen) y bifurcándose en dos sentidos: lo restringido y lo abierto (ambos propuestos por Ian Rowlands). Posteriormente (Peter Ingwersen agrega que) se requiere de un entendimiento conceptual, es decir de una decodificación cognitiva sobre la información. A partir de estas perspectivas es viable adaptar los procesos de acceso a otro tipo de entornos y dinámicas. El enfoque general puede representarse gráficamente de la siguiente manera.

¹⁰¹ Martínez Usero, José y Lara Navarra, Pablo. *La accesibilidad de los contenidos web*. (España: editorial UOC, 2006). Pág. 10

¹⁰² Cosentino, Guillermo. Ídem. Pág. 253

¹⁰³ Morales Campos, Estela. Loc. Cit.

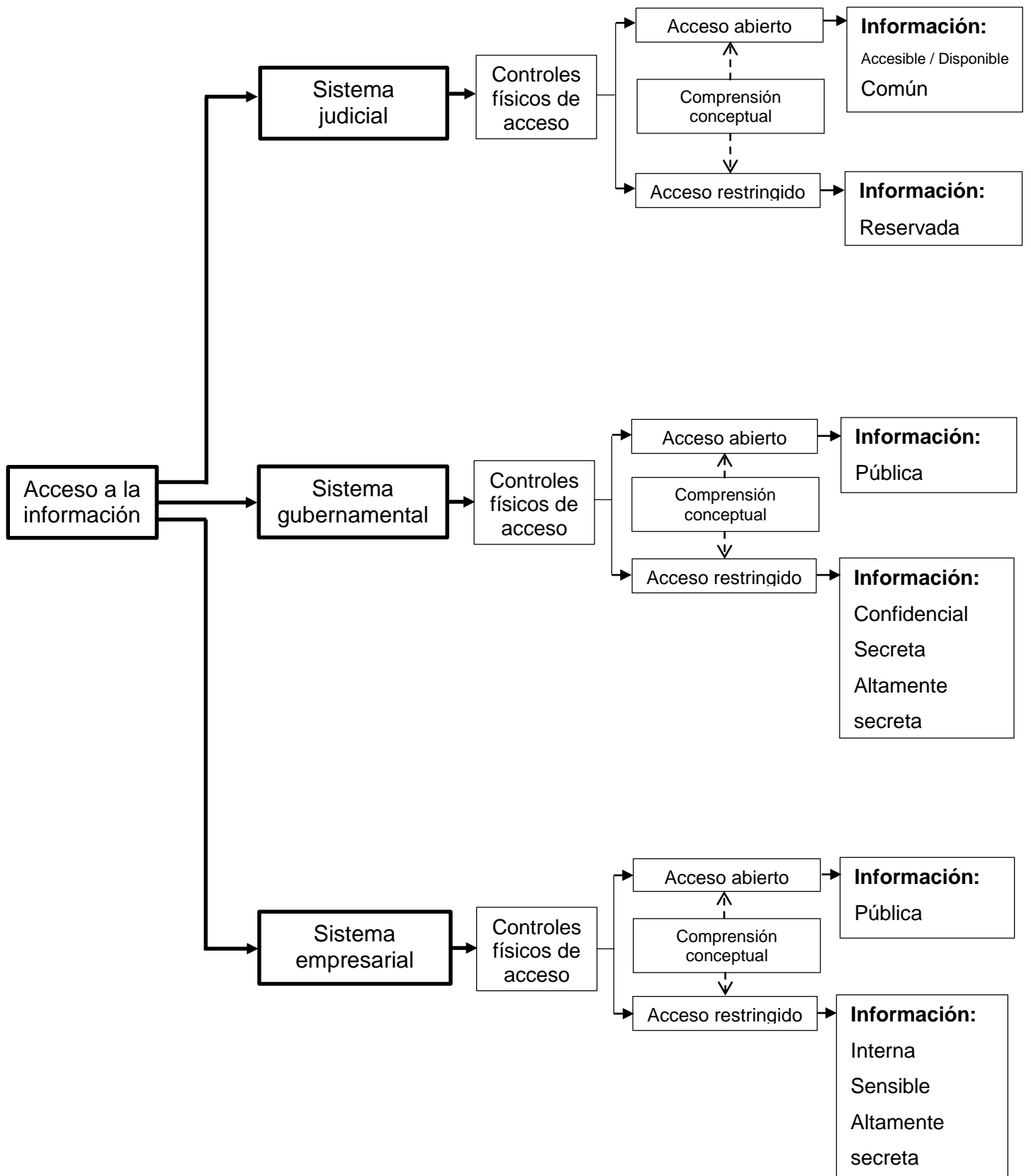


Figura 2. Enfoque general en el acceso a la información. Fuente: creación propia.

1.6 Elementos de accesibilidad

James Katz y Ronald Rice¹⁰⁴ hacen hincapié en los factores y catalizadores de la accesibilidad, desde la carencia del suficiente capital cultural, habilidades intelectuales y la patente brecha digital, puesto que para el acceso a Internet, la Web u otros entornos (como las *redes oscuras*) es fundamental contar con el conocimiento elemental de acceso y navegación incluyendo la computadora personal o medio de conexión.

La accesibilidad también puede entenderse como un conjunto de elementos que regulan los beneficios de quienes utilizan los contenidos para entretenerse, informarse y comunicarse. Existen diversos intereses en la regulación del acceso a Internet y a los contenidos ofrecidos mediante los servicios de la Web. Las formas de regulación van desde la restricción, el control hasta la censura de la información que atenta en contra de los grupos de poder, ya sea la iniciativa privada o el *Estado-nación*. A continuación se describen los elementos de la accesibilidad a la información.

1.6.1 Restricción

La restricción de acceso es un tema muy particular ligado a la regulación de los recursos por parte del *Estado-nación*, dicha restricción se fundamenta en la ideología de gobierno hasta las leyes de propiedad sobre los contenidos impresos o digitales. Además de las limitaciones de la propiedad intelectual, son necesarias las restricciones para la sociedad. Siguiendo a María Marván y Roberto Corona¹⁰⁵ el costo en el consumo de recursos supondría una serie de gastos para el *Estado-nación* en la compra, renta y mantenimiento de la infraestructura, así como de la ingeniería informática la cual permite la operatividad de los medios de transmisión de datos. Por lo que la restricción permite ajustar la oferta y la demanda.

¹⁰⁴ Katz, James y Rice Ronald. Ídem. Pág. 28

¹⁰⁵ Marván, María y Corona, Roberto. "El instituto federal de acceso a la información pública: una institución para la rendición de cuentas en México". En *Democratización, rendición de cuentas y sociedad civil participación ciudadana y control social*. (México, D.F.: H. Cámara de Diputados, LIX Legislatura, 2006). Pág. 578

Dominique Wolton¹⁰⁶ advierte que, la restricción no sólo se debe a una forma de gobierno y administración sino a la desigualdad frente a otros países, en donde existe una gran diferencia en la realidad económica, académica, industrial, geográfica y sanitaria por lo que el contacto con la tecnología de las comunicaciones se complica. Jesús Ibáñez¹⁰⁷ añade a esta idea que, Internet no es una infraestructura a la que todos los individuos puedan acceder sin restricción, puesto que se requiere de un pago a los monopolios que proveen del servicio de conexión.

Lawrence Lessig¹⁰⁸ argumenta que, el *Estado-nación* no puede regular en absoluto la operatividad de la red de redes, pero si puede segmentar a los individuos que quieren hacer uso de Internet, siendo que al *Estado-nación* le interesa conocer lo que no es regulable para poder reglamentarlo según convengan las circunstancias. De este modo se restringe el acceso en la conexión y la navegación, y consecuentemente se origina la condición de uso.

1.6.2 Control

El control de la información se centra en la organización de la información pero con un acceso restringido, puesto que según Maureen McCreadie y Ronald Rice,¹⁰⁹ los individuos que poseen el control de la información obtienen certidumbre y pueden hacer movimientos asertivos para ellos y para el grupo al que pertenecen, con lo que se obtiene una ventaja sobre los demás. Manuel Guerrero¹¹⁰ afirma que, con el control en el acceso a la información se cubren los errores y las faltas en la gestión gubernamental, creando opacidad en los procesos administrativos.

¹⁰⁶ Wolton, Dominique. Ídem. Pág. 135

¹⁰⁷ Ibáñez Balears, Jesús. "Acceso a la información y aprendizaje informal en Internet". *Revista Científica de Comunicación y Educación*, no. 21 (2003): 31-38. Recuperado en: http://www.google.com.mx/url?sa=t&rct=j&q=&esrc=s&source=web&cd=1&ved=0CBwQFjAA&url=http%3A%2F%2Fwww.revistacomunicar.com%2Fverpdf.php%3Fnumero%3D21%26articulo%3D21-2003-05&ei=WNoDvLDClmZgwTj14HACw&usg=AFQjCNEmc_kJ4qAexqPCFX0JzRln7daXuw [Consultado 21 de enero de 2016]

¹⁰⁸ Lessig, Lawrence. Ídem. Pág. 90

¹⁰⁹ McCreadie, Maureen y Rice, Ronald E. Loc. Cit.

¹¹⁰ Guerrero, Manuel Alejandro. *Medios de comunicación y la función de transparencia*. (México: Instituto Federal de Acceso a la Información y Protección de Datos, 2006. Cuadernos de transparencia, 11). Pág. 13

Para Rosemary Righter¹¹¹ en el caso de los medios de comunicación, la importancia en el control de la información se basa en el registro de los acontecimientos relevantes con el objetivo de ser difundidos bajo un enfoque imparcial pero al mismo tiempo la información es editada de acuerdo a la postura ideológica o financiera. La información también se controla por medio del seguimiento en el quehacer político del país y la relación con otros países extranjeros, de manera que, con el control de la información se obtiene un panorama histórico y actual sobre la administración gubernamental con el fin de que los grupos políticos entiendan las amenazas y las oportunidades. Por otro lado Cherie Givens¹¹² indica que, en una biblioteca también se cuenta con un control de la información, primordialmente en la organización de los documentos, su estado de conservación, préstamo a domicilio, reprografía, preservación e índice de consultas así como en el comportamiento de los usuarios.

1.6.3 Censura

De acuerdo con Ian Cornelius¹¹³ la censura es una forma de omitir la inconformidad en los individuos, comportamientos atípicos, ideas o pensamientos. El mismo autor señala que, la censura controla la adquisición de la materia prima y, en consecuencia también controla los contenidos informativos. Usualmente mediante la censura se prioriza evitar que, los ideales, los movimientos de oposición, productos, servicios y contenidos sean percibidos y difundidos. La censura no únicamente se limita a ocultar, también tiende a manipular la naturaleza de las expresiones del ser humano. Teresa Páramo¹¹⁴ explica que, por un lado la censura es un filtro natural en cada individuo mientras que por otro lado la censura permite ocultar la comunicación entre los individuos.

¹¹¹ Righter, Rosemary. *El control de la información: política, prensa y tercer mundo*. Traducido por Belén Garrigues y Asunción Rodríguez. (Madrid: Pirámide, 1982). Pág. 19

¹¹² Givens, Cherie. *Information privacy fundamentals for librarians and information professionals*. (Lanham, Maryland: Rowman & Littlefield, 2015). Pág. 72

¹¹³ Cornelius, Ian. *Information policies and strategies*. (London: Facet, 2010). Pág. 90

¹¹⁴ Páramo, Teresa. *Sociedad y comunicación: una mirada al siglo XXI*. (México: UAM, Unidad Iztapalapa: Plaza y Valdés, 2006). Pág. 58

En ocasiones el origen de la censura se basa en ideas que atentan a la tradición, a la filosofía o la ideología de otros individuos o grupos dominantes. Porfirio Barroso y John Weckert¹¹⁵ comentan que, son las intenciones con las que se difunden los contenidos las que los hacen ofensivos, los autores argumentan que, la ofensa del agraviado es un factor para inducir a la censura. Jonathan Zittrain y John Palfrey¹¹⁶ señalan que, en ocasiones en la Web, se bloquean o anulan comentarios y a los usuarios que son considerados ofensivos cuando los contenidos de los administradores del sitio o servicio no son del agrado de alguna minoría.

Asimismo Jonathan Zittrain y John Palfrey añaden que, son los *Estados-naciones* que suelen promover y alentar la libertad de expresión entre sus ciudadanos, los mismos que ejercen la censura. De esta manera la censura es un mecanismo para suprimir y regular el comportamiento de los individuos que actúan de una manera atípica para el sistema de control.

1.6.4 Poder

El poder en lo que se refiere al acceso a la información, es el resultado de todo aquello que puede sortear las restricciones, el control y la censura. Maureen McCreadie y Ronald Rice¹¹⁷ explican que, el acceso a la información proporciona al individuo la certidumbre sobre los servicios en su seguridad personal y, en consecuencia lo empodera como un ciudadano participativo con conocimientos; aunque irónicamente son aquellos individuos en mayor desventaja los que desconocen acerca de los servicios y beneficios sociales por falta de información.

¹¹⁵ Barroso, Porfirio y Weckert, John. "Material ofensivo en Internet". En *Deontología y autorregulación informativa: ensayos desde una perspectiva comparada*. (México: Fundación Manuel Buendía, 2000). Pág. 70

¹¹⁶ Zittrain, Jonathan y Palfrey, John. "Access denied: the practice and policy of global internet filtering". En *Internet filtering: the politics and mechanisms of control*. (Reino Unido: Oxford Internet Institute, 2007). Recuperado en: www.oii.ox.ac.uk/research/publications/RR14.pdf [Consultado 28 de enero de 2016]

¹¹⁷ McCreadie, Maureen y Rice, Ronald E. Loc. Cit.

El acceso a la información para Rosemary Righter,¹¹⁸ va más allá de obtener beneficios que le provean al individuo de una mejor calidad de vida; el acceso a la información es la suma de herramientas que coadyuvan a mejorar el entorno social. En ese sentido para María Marván y Roberto Corona¹¹⁹ el acceso a la información genera un funcionamiento favorable en la democracia actual, en donde el ciudadano participa de forma activa para señalar las carencias en las actividades administrativas del gobierno.

Finalmente Rigoberto López¹²⁰ agrega que, el acceso a la Web conlleva beneficios para los usuarios suscritos a ciertos temas informativos, los cuales se adaptan a sus necesidades de información, ya que el acceso a distintos contenidos empodera a estos usuarios frente a otros, señala el autor. De esta forma se puede entender que la accesibilidad está compuesta de distintos elementos que se conjugan en un vaivén de situaciones favorables y desfavorables, según con la óptica con la que se analicen.

1.7 Elementos de la complejidad en la Web

La Web ha evolucionado desde la primera década de su apertura, de manera que se han realizado modificaciones en su operatividad con el fin de mejorar la navegación, capacidad de transmisión de paquetes de datos y también para adaptar su legislación. No obstante, algunos de los elementos de su complejidad se han matizado al paso de los años con el desarrollo de la tecnología y de nuevos servicios, aunado a la forma de navegación de los usuarios en donde la **vigilancia**, el **anonimato**, la **privacidad** y la **seguridad (VAPS)** son los elementos más representativos de la complejidad en la actualidad, dado que los individuos deben seguir ciertos lineamientos para no ser sancionados así como evitar ser vulnerados en su integridad.

¹¹⁸ Righter, Rosemary. Ídem. Pág.17

¹¹⁹ Marván, María y Corona, Roberto. Ídem. Pág. 578

¹²⁰ López y Quezada, Rigoberto. **Cómo obtienen los reporteros la información.** (México, D. F.: Universidad Nacional Autónoma de México, 2013). Pág. 135

A) Vigilancia

Para David Lyon¹²¹ la vigilancia es una actividad que se práctica en las instituciones, lugares públicos y prisiones, con el objetivo de compilar los registros sobre el comportamiento de la población y determinar los patrones de conducta en la sociedad para garantizar el bienestar del *Estado-nación*. Para David Lyon la vigilancia es sustancialmente un sistema de control, puesto que es exclusivamente el personal autorizado quien puede acceder a la información. Lawrence Lessig¹²² añade que, la vigilancia da seguimiento al comportamiento de los individuos por medio del monitoreo, es decir que, se estudian los patrones de conducta anteriores con los actuales para establecer las rutinas y las medidas de regulación correspondientes.

En cuanto al uso de la tecnología, Sergio Contreras¹²³ hace mención que si el *Estado-nación* reconoce como una amenaza la conexión a Internet creará sistemas de regulación en el acceso y control a contenidos subversivos. Para ello Lawrence Lessig¹²⁴ señala que, el *Estado-nación* puede obligar a los Proveedores del Servicio de Internet a proporcionar el acceso a la base de datos de los usuarios que contratan su servicio, así como el historial de navegación de cada usuario que ha contratado el servicio, basándose el *Estado-nación* en los procesos jurídicos para protegerse dentro del marco de la legalidad.

Por otro lado el concepto de espionaje, se centra en la sustracción de la información sin el consentimiento de los individuos, gobiernos extranjeros y empresas. De manera que, en la ejecución del espionaje se desconoce del monitoreo; a diferencia de la vigilancia en donde se hace evidente la observación del comportamiento humano. El espionaje está basado en distintas técnicas de infiltración para recabar datos concretos e información, con el objetivo de obtener una ventaja al exponer los secretos. En la actualidad el espionaje se manifiesta

¹²¹ Lyon, David. *Surveillance as social sorting: privacy, risk and digital discrimination*. (London: Routledge, 2003). Pág. 37

¹²² Lessig, Lawrence. Ídem. Pág. 281

¹²³ Contreras, Sergio. "Los límites en la era digital". *Etcétera: para entender a los medios*, no. 165 (2014). 37-41

¹²⁴ Lessig, Lawrence. Op. Cit., Pág. 103

en la Web y se le conoce como ciberespionaje,¹²⁵ el cual se realiza de forma remota, modificando la operatividad de los sistemas informáticos y sustrayendo los documentos y los contenidos digitales.

B) Seguridad

La seguridad en el acceso a Internet y navegación en la Web abarca distintos aspectos, que van desde la prevención hasta las buenas prácticas de navegación. En el caso de la seguridad preventiva es importante señalar que no todas las conexiones a Internet con posibilidad de acceso gratuito son una buena opción, como bien comentan Nitesh Dhanjani, Billy Ríos y Brett Hardin,¹²⁶ porque existe la probabilidad de exponer los datos personales a algún tercero no autorizado.

En ese mismo sentido José Carballar¹²⁷ agrega que, la seguridad en las computadoras personales y medios con conexión a la red, es crítica, puesto que al no haber barreras físicas existe una alta probabilidad de riesgo. Siguiendo a Gonzalo Álvarez¹²⁸ es importante evitar el uso de equipos públicos y ajenos para acceder a cuentas personales como los son las redes sociales, el correo electrónico y los servicios bancarios.

En el contexto de la seguridad digital, las buenas prácticas son un conjunto de procedimientos que garantizan el óptimo funcionamiento tanto del equipo de conexión como del software con el que interactuamos para la conexión y navegación. En este sentido Bárbara Bécares¹²⁹ recomienda actualizar el sistema operativo así como las aplicaciones de navegación. Gonzalo Álvarez¹³⁰

¹²⁵ Alonso, Chema. 2 de noviembre de 2014. Cómo funciona el software de espionaje de Hacking Team. *El lado del mal*, Recuperado en: <http://www.elladodelmal.com/2014/11/como-funciona-el-software-de-espionaje.html> [Consultado 11 de julio de 2015]

¹²⁶ Dhanjani, Nitesh., Ríos, Billy y Hardin, Brett. Op. Cit., Pág. 188.

¹²⁷ Carballar Falcón, José. *Wi-Fi: lo que se necesita conocer*. (México: Alfaomega grupo editor, 2010). Pág. 141

¹²⁸ Álvarez Marañón, Gonzalo. Ídem. Pág. 102

¹²⁹ Bécares, Bárbara. 14 de agosto de 2015. 10 precauciones básicas para mantener tu dispositivo seguro. *ChannelBiz*. Recuperado en: http://www.channelbiz.es/2015/08/14/10-precauciones-basicas-para-mantener-tu-dispositivo-seguro/?utm_content=buffer658bc&utm_medium=social&utm_source=twitter.com&utm_campaign=buffer [Consultado 14 de agosto de 2015]

¹³⁰ Álvarez Marañón, Gonzalo. Ídem. Pág. 104

insiste en que en un ambiente familiar es importante instalar la computadora del hogar en un lugar visible para el control parental. Asimismo Ángel Avilés¹³¹ exhorta al uso y actualización del software antivirus, que si bien no garantiza la protección del equipo de conexión si reduce la probabilidad de un suceso de ataque.

Matthew Bailey¹³² hace énfasis en la importancia que tiene el *malware* en el contexto de la seguridad, siendo este un código malintencionado con la capacidad de modificar los procesos en el software de las computadoras, teléfonos inteligentes y tabletas con conexión al servicio de Internet. Dicho código es perjudicial y se adquiere por medio de la descarga o por el simple hecho de navegar e interactuar en ciertos sitios web.

Finalmente Ana Martos¹³³ comenta que, en ocasiones, es posible recibir un correo electrónico falso, en donde se solicita determinada información o se ofrece algún tipo de promoción fraudulenta.

C) Anonimato

El anonimato forma parte de la naturaleza de la Web, de modo que le permite a cualquier usuario ocultar o alterar su identidad ya sea para crear, colaborar, impugnar o simplemente para consultar los contenidos y hacer uso de los servicios en línea. El anonimato también se puede propiciar cuando se adquiere una computadora personal, de modo que, el equipo en cuestión usualmente se configura con algunos datos del propietario, a este respecto simplemente pueden ser falsos u omitidos, he ahí la virtud y el problema para cualquier proceso jurídico.

¹³¹ Avilés, Ángel Pablo. *X1red+segura: informando y educando*. (España: Safe creative, 2013). Pág. 88

¹³² Bailey, Matthew. *Complete guide to internet privacy, anonymity and security*. (New York: Cogipas, 2011). Pág. 37

¹³³ Martos Rubio, Ana. *Cómo buscar en internet*. (Madrid: Anaya Multimedia, 2012). Pág. 44

Además de esta arista de la identidad, Diane Fulkenson¹³⁴ comenta que, existen herramientas de conexión y navegación para mantener el anonimato como lo es, el acceso remoto a una Red Privada Virtual (por sus siglas en inglés VPN) el cual es un modelo de transmisión de datos utilizado comúnmente por instituciones y proporcionado por proveedores de conexión segura a contenidos y recursos de acceso controlado. En este mismo aspecto, Matthew Bailey¹³⁵ añade que, una forma de evitar ser identificados es mediante el intercambio de datos encapsulados, utilizando las Redes Privadas Virtuales.

Cabe agregar que un alto porcentaje de esta clase de servicios de VPN requiere de un pago, y no todos los usuarios pueden acceder a estos servicios de anonimato. En primera instancia por conocimiento técnico, y en segundo lugar porque implica un costo extra. Sin embargo, existen otros métodos disponibles para ocultar la identidad, pero implican una investigación y documentación en el entendimiento de su configuración y operatividad. Lawrence Lessig¹³⁶ argumenta que, los individuos siempre buscaran la forma de sortear los controles de identidad, puesto que los creadores del código establecen la dinámica en la Web y no las autoridades del *Estado-nación*, de manera que son los creadores y desarrolladores del código quienes determinan cual es el grado del anonimato y la privacidad en la red de redes.

D) Privacidad

No existe privacidad como tal en la conexión a Internet y en la navegación Web, puesto que todos los movimientos son registrados y preservados. Según Matthew Bailey¹³⁷ cuando el usuario visita un sitio, página o accede a redes sociales queda registrada la dirección IP pública, su localización geográfica y sus movimientos de navegación. Por lo que la privacidad queda anulada, aun así es posible delimitar la privacidad pero depende en gran medida de la prudencia del

¹³⁴ Fulkenson, Diane. *Remote access technologies for library collections: tools for library users and managers*. (Hershey, Pennsylvania: Information Science Reference, 2012). Pág. 83

¹³⁵ Bailey, Matthew. Ídem. Pág. 136

¹³⁶ Lessig, Lawrence. Ídem. Pág. 119

¹³⁷ Bailey, Matthew. Loc. Cit.

usuario en revelar sus datos personales, los cuales comúnmente se proporcionan en el registro de algún servicio en línea para obtener acceso a los productos y contenidos, además de la difusión de la vida personal.

David Treviño¹³⁸ agrega que, la privacidad de los datos personales en manos de terceros autorizados por sí misma no representa ninguna garantía de protección, pero está ligada al control de la información y por tanto el concepto de la privacidad determina quién puede acceder a la información almacenada. En contraste con los datos personales como lo son la edad, raza, nacionalidad, fecha de nacimiento, el nombre, domicilio, etc.; Los datos sensibles¹³⁹ se relacionan con la intimidad del individuo que revela principalmente sus características de preferencias sexuales, creencias religiosas, creencias filosóficas, sentimientos, opiniones políticas, entre otras.

Fernando Escalante¹⁴⁰ menciona que, a diferencia de la privacidad, la intimidad es un vínculo entre los individuos en cuanto a la confidencialidad de su comportamiento mutuo, y la intimidad quedara vulnerada cuando se dé a conocer públicamente la vida personal del individuo. El mismo autor señala que definir la privacidad y la intimidad¹⁴¹ en el plano político es complicado, puesto que cualquier dato o información que altere el prestigio de los políticos y funcionarios públicos puede resultar interesante para la oposición, con la posibilidad de modificar la realidad de la esfera política y la percepción social acerca de los funcionarios públicos.

¹³⁸ Treviño, David “¿Quién te conoce?” *Revista Seguridad Cultura de prevención para TI*, no. 24 (2015): 30-32. Recuperado en: http://revista.seguridad.unam.mx/sites/revista.seguridad.unam.mx/files/revistas/pdf/24_RevistaSeguridad-Aproximacion_al_malware.pdf [Consultado 28 de enero de 2016]

¹³⁹ González, Isai Rojas Et al. “Leyes de protección de datos personales en el mundo y la protección de datos biométricos – Parte I”. *Revista Seguridad Cultura de prevención para TI*, no. 13 (2012): 4-8. Recuperado en: <http://revista.seguridad.unam.mx/numeros/numero-13> [Consultado 30 de enero de 2016]

¹⁴⁰ Escalante Gonzalbo, Fernando. *El derecho a la privacidad*. (México: Instituto Federal de Acceso a la Información y Protección de Datos, 2004. Cuadernos de transparencia, 2). Pág. 35

¹⁴¹ Ídem. Pág. 40

1.8 La utilidad de la Web

La Web es un conjunto de ideas, aportaciones, datos, imágenes y acontecimientos vinculados, de índole social, nacional e internacional, en donde los individuos informan en tiempo real sobre algún suceso o tema por medio de las tecnologías de comunicación. Sin embargo para Lola García¹⁴² en la Web cualquier usuario tiene la posibilidad de contribuir con sus aportaciones pero también puede causar ruido con información errónea y caos en la forma de clasificar u organizar los contenidos.

Por otro lado, el papel esencial de la Web es el hecho de ser una plataforma digital para concretar los negocios y proporcionar visibilidad a los bienes y servicios. Manuel Castillo y Jesús Montenegro¹⁴³ comentan que, al incrementar el acceso a la información los mercados obtienen mayor productividad puesto que los costos se minimizan. Los mismos autores señalan que, los beneficios no sólo son para la iniciativa privada sino también para la economía del *Estado-nación* y sus relaciones exteriores. Mientras que para Leandro Olguín y José López,¹⁴⁴ los bancos se han interesado en proporcionar servicios digitales para agilizar los trámites de sus clientes debido a los bajos costos que les significan esta clase de servicios financieros.

El comercio electrónico y la Web reducen los límites geográficos a cambio de un valor agregado en el envío de los productos, y por otro lado también se reduce el costo de los productos tangibles creando alternativas digitales como lo es la literatura académica, la música, el arte visual y el software, entre otros. Cabe aclarar que, tanto el acceso como el comportamiento no sólo dependen del poder adquisitivo del usuario; su astucia puede ser crucial para obtener el acceso, junto

¹⁴² García Santiago, Lola. Ídem. Pág. 29

¹⁴³ Castillo, Manuel y Lechuga, Jesús. "Las tecnologías de la información y la nueva economía". En **Reflexiones acerca de la era de la información (new economics)**. (México: UAM, Unidad Azcapotzalco, 2005). Pág. 31

¹⁴⁴ Olguín, Leandro y López, José. "El comercio electrónico via Internet: seguridad y bajo costo en las transacciones". En **Reflexiones acerca de la era de la información (new economics)**. (México: UAM, Unidad Azcapotzalco, 2005). Pág. 72

con su personalidad y habilidades, las cuales determinan el tipo de usuario que es, en la interacción con los servicios en línea.

1.8.1 Servicios en línea

Joann Wasik¹⁴⁵ argumenta que, los servicios en línea tienen sus orígenes vinculados a la biblioteca, ya que el servicio de referencia (en donde el usuario hace una solicitud para obtener cierta información), tiene su punto histórico a la pauta del servicio de Internet en 1992 y posteriormente es en 1995 cuando dicho servicio de Internet se consolida en las bibliotecas públicas de los Estados Unidos de América. Para la Asociación de Servicios a Usuarios y Referencia (por sus siglas en inglés RUSA), el servicio de referencia virtual¹⁴⁶ parte del uso de los medios tradicionales (como el teléfono) para la transmisión y comunicación, hasta llegar a las tecnologías electrónicas y digitales en línea. Es decir que la ideología de los servicios digitales pretende emular la interacción presencial entre el usuario y la biblioteca.

Georgina Torres¹⁴⁷ comenta puntualmente que, para el acceso en línea en el caso de las bibliotecas, la cooperación interbibliotecaria como la operatividad institucional es pieza fundamental para optimizar el tiempo del usuario, así como el de proporcionar un mayor grado de visibilidad a los documentos y contenidos. Adicionalmente Juan Corcuera y Ricardo Arnaus¹⁴⁸ mencionan que, la radio, la prensa y la televisión fueron medios tradicionales que adaptaron sus servicios a la Web, con algunas variaciones en sus contenidos. Pero no significa que el acceso total a sus contenidos en línea sea gratuito, ya que como lo subrayan

¹⁴⁵ Wasik, Joann. 1999. Building and maintaining digital reference services. *ERIC Digest*. Recuperado en: <http://files.eric.ed.gov/fulltext/ED427794.pdf> [Consultado 31 de enero de 2016]

¹⁴⁶ Reference and User Services Association, 2010. Guidelines for Implementing and Maintaining Virtual Reference Services. **American Library Association**. Recuperado en: <http://www.ala.org/rusa/sites/ala.org.rusa/files/content/resources/guidelines/virtual-reference-se.pdf> [Consultado 31 de enero de 2016]

¹⁴⁷ Torres Vargas, Georgina. "Hacia un modelo de servicios en la biblioteca digital". *Investigación Bibliotecológica* 17, no. 35 (2003): 32-44. Recuperado en: <http://www.revistas.unam.mx/index.php/ibi/article/view/4021/3571> [Consultado 31 de enero de 2016]

¹⁴⁸ Corcuera, Juan y Arnaus, Ricardo. Ídem. Pág. 24

Víctor Salgado, Jorge Bustamante y Mauricio Varela¹⁴⁹ existen productos tradicionales que al ser creados específicamente para una plataforma digital pueden llegar a tener un costo mayor, de manera que no todos los productos y servicios son gratuitos en la Web, como consecuencia de su diseño, desarrollo y actualización, así como de la oferta y la demanda.

1.8.2 Tipos de usuario

El usuario común que accede a la Web, tiene el potencial para convertirse o asumir el papel de un ciudadano digital como aquel que observa las deficiencias del código para señalarlas o corregirlas; pero también para explotar sus vulnerabilidades. El usuario también puede optar por acceder ilegalmente a los contenidos aprovechándose de las deficiencias de acceso o simplemente para divertirse engañando a otros usuarios. Un usuario podría adoptar más de un rol en la Web, dependiendo de sus necesidades, contexto, perfil psicológico y conocimientos.

A continuación se describen los principales tipos de usuario que interactúan con el usuario común en la Web.

- **Hacker:** es una persona curiosa en los sistemas computacionales, actúa con el objetivo de favorecer a la sociedad además de promover la descentralización en el control de la información y no depender de alguna figura de autoridad en la Web.¹⁵⁰ Es un experto en informática para solucionar los problemas en un sólo proceso, y así mejorar la ingeniería del sistema.¹⁵¹

¹⁴⁹ Salgado, Víctor., Bustamante, Jorge y Varela, Mauricio. "El valor de los intangibles en la nueva economía". En **Reflexiones acerca de la era de la información (new economics)**. (México: UAM, Unidad Azcapotzalco, 2005). Pág. 191

¹⁵⁰ Sánchez, Antulio. **Territorios virtuales: de internet hacia un nuevo concepto de la simulación**. (México: Taurus, 1997). Pág. 184

¹⁵¹ Véase Álvarez Marañón, Gonzalo. Op. Cit., Pág. 9. González Sánchez, José. **Autopistas de la información e Internet: tecnología, servicios, peajes y normas de navegación**. (Caceres: Universidad de Extremadura, 1998). Pág. 405 y McClure, Stuart., Scambray, Joel y Kurtz, George. **Hackers: secretos y soluciones para la seguridad de redes**. Traducido por Fulgencio Gómez. (Madrid; México: Osborne/McGraw-Hill, 2000). Pág. xxix

- **Cracker:** posee los conocimientos de los *Hackers* pero hace uso de ellos para su propio beneficio y en consecuencia comete delitos informáticos.¹⁵² Acceden a los sistemas vulnerando el código de seguridad por diversión y/o beneficio económico.¹⁵³
- **Hacktivista:** es aquel usuario con conocimientos en los sistemas computacionales que comunica a través de la Web para reivindicar el sentir sobre comunidades, agrupaciones o minorías, utilizando las vulnerabilidades del sistema, por medio de mensajes de alto impacto.¹⁵⁴
- **Ciberpunk:** se deleita con la conceptualización de la decadencia de un mundo distópico en donde la tecnología ha sobrepasado los aspectos éticos, el ciberpunk es producto de la civilización norteamericana y de un movimiento ideológico globalizado que ha influenciado a otras culturas y naciones.¹⁵⁵
- **Phreaker:** es el usuario que busca la manera de pagar lo mínimo por algún servicio, producto o contenido. Y en el mejor de los casos evita pagar por el acceso.¹⁵⁶
- **Troll:** es aquel individuo que se divierte provocando la molestia de los demás para generar controversia,¹⁵⁷ con datos e información falsa y comentarios fuera de lugar. El Troll¹⁵⁸ se manifiesta con expresiones

¹⁵² Álvarez Marañón, Gonzalo. Ídem. Pág. 8

¹⁵³ González Sánchez, José. Ídem. Pág. 405

¹⁵⁴ Alonso, Chema. 25 de noviembre de 2015. Introducción: Hacker, cibercriminal y hacktivismo. Episodio 1. **Flooxer**. Recuperado en: <http://www.flooxer.com/video/chema-alonso-risk-alert-introduccion-hacker-ciber-criminal-hacktivismo/5655a4887e31f20cbf9ceb20> [Consultado 19 de diciembre de 2015]

¹⁵⁵ Sánchez, Antulio. Ídem. Pág. 192

¹⁵⁶ González Sánchez, José. Loc. Cit.

¹⁵⁷ Croll, Alistair. **Técnicas de monitorización Web**. Traducido por Jorge Garrido. (Madrid: Anaya Multimedia, 2010). Pág. 78

¹⁵⁸ Lozano Aguilar, César Iván "Los trolls cibernéticos". **Revista Seguridad Cultura de prevención para TI**, no. 17 (2013): 26-29. Recuperado en: <http://revista.seguridad.unam.mx/numeros/numero-17> [Consultado 14 de enero de 2015]

violentas mediante el texto e imágenes desagradables, mediante el anonimato

- **Spamer:** está interesado en saturar con su información la sección de comentarios.¹⁵⁹ Su objetivo es el de acaparar dichos espacios con comentarios o enlaces de publicidad referentes a contenidos, productos o servicios.
- **Ciberdepredador:** es el usuario que tiene una fijación por los menores de edad,¹⁶⁰ pretendiendo su excitación y la relación sexual mediante el uso de la Web.
- **Phisher:** es aquel individuo especializado en el robo de identidades y datos personales mediante la ingeniería social,¹⁶¹ la cual es el monitoreo de las actividades y la recolección de contenidos personales de la víctima.
- **Blended librarian:** es todo aquel bibliotecario profesional con fundamentos teóricos, el cual tiene la capacidad de interactuar con las tecnologías disruptivas orientadas a la transferencia, gestión, organización, recuperación de la información y servicios en línea.¹⁶²

La distinción de los usuarios inicia desde el momento de conexión al servicio de Internet para acceder a los contenidos y servicios de la Web. Cada usuario posee diferentes habilidades de acuerdo a sus intereses y su formación ideológica, técnica, académica o autodidacta, dicha formación repercute en el uso de las herramientas digitales y su interacción con el código informático en línea. El

¹⁵⁹ Croll, Alistair. Loc. Cit.

¹⁶⁰ Avilés, Ángel Pablo. Ídem. Pág. 177

¹⁶¹ Voutssás Márquez, Juan. "Preservación documental digital y seguridad informática". *Investigación bibliotecológica* 24, no. 50 (2010): 127-155. Recuperado en: <http://www.journals.unam.mx/index.php/ibi/article/view/21416> [Consultado 18 de junio de 2016]

¹⁶² Torres Vargas, Georgina Araceli Et al. Ibíd. Recuperado en: https://www.researchgate.net/publication/280947367_The_Blended_Librarian_and_the_Disruptive_Technological_Innovation_in_the_Digital_World [Consultado 25 de junio de 2016]

comportamiento suele derivar del tipo de habilidades que posee el individuo, de modo que, la aplicación del conocimiento depende del criterio, madurez y responsabilidad que los usuarios deseen asumir para mejorar o perjudicar el entorno digital. En lo general no se puede encasillar a los usuarios debido a que cada individuo hace uso del servicio de Internet y los servicios de la Web de acuerdo a su realidad social, económica, política y cultural, por lo que además de los tipos de usuario anteriormente presentados se podrían considerar también como actitudes, de acuerdo a la complejidad en la vida de cada individuo.

Cabe aclarar en primera instancia que, el *Hacker* es el opuesto por antonomasia al *Cracker* siendo el primero un actor con aportaciones positivas sin fines de lucro al resto de la comunidad de usuarios. Por otro lado, existe un vínculo entre el *Hactivista* con el *Hacker*, puesto que el *Hactivismo* como corriente ideológica, es el medio para señalar los procesos inadecuados por parte de las autoridades y los actos que inciden en la sociedad considerados como injustos. No obstante estos comportamientos de manifestación al estar basados en pasiones y provocaciones resultan consecuentemente una tergiversación de la cultura *Hacker*.

El *Phreaker* por su parte, está vinculado al *Cracker* ya que existe una relación de oferta-demanda con base en las necesidades de acceso a los servicios y contenidos regulados por un medio de pago o suscripción. Es entonces el *Cracker*, el proveedor de los usuarios (*Phreaker*) que no están interesados en pagar la totalidad del precio para acceder a los productos, contenidos y servicios digitales.

En cuanto al *Troll* y el *Spamer* se refiere, ambos comparten elementos en común como lo es la creación de ruido textual, sonoro y visual además de la constante incidencia beligerante en el orden, organización y convivencia con el resto de los usuarios que hacen uso de los servicios de la Web, como lo es la comunicación y el diálogo sobre algún tema. Sin embargo, un atributo particular del *Troll* es la

provocación con base a una inadecuada actitud premeditada comúnmente ligada al anonimato.

Finalmente el *Phisher*, el *Ciberdepredador* y el *Ciberpunk* poseen conductas muy particulares. El *Ciberpunk* crea y al mismo tiempo es parte de una atmosfera en donde la tecnología y la supervivencia humana se entremezclan entre conflictos filosóficos, al tiempo que busca la simbiosis electrónica dentro de un mundo sin reglas. Mientras que el *Ciberdepredador* tiene elementos de ser un individuo anónimo con fijaciones pedófilas en busca del estímulo sexual a partir de la interacción mediante los servicios de la Web. El *Phisher* por su parte, dedica su tiempo y habilidades a la recolección de datos y contenidos ajenos, con el objetivo de crear un perfil de su víctima potencial, este tipo de usuario comparte elementos en común con el *Ciberdepredador*, dado que tienen un interés en conocer la vida privada y la intimidad de terceros.

A manera de inclusión, el *Blended librarian* es la antítesis del *Troll*, el *Ciberdepredador*, el *Spamer* y el *Cracker* puesto que su objetivo es el de clarificar el caos, es pues un aliado potencial del *Hacker* ya que su función es la de brindar servicios de búsqueda y recuperación de los contenidos para el bien del usuario común, mediante los distintos tipos de acceso a la información.

La siguiente figura muestra gráficamente los vínculos entre los tipos de usuario conforme a lo anteriormente mencionado.

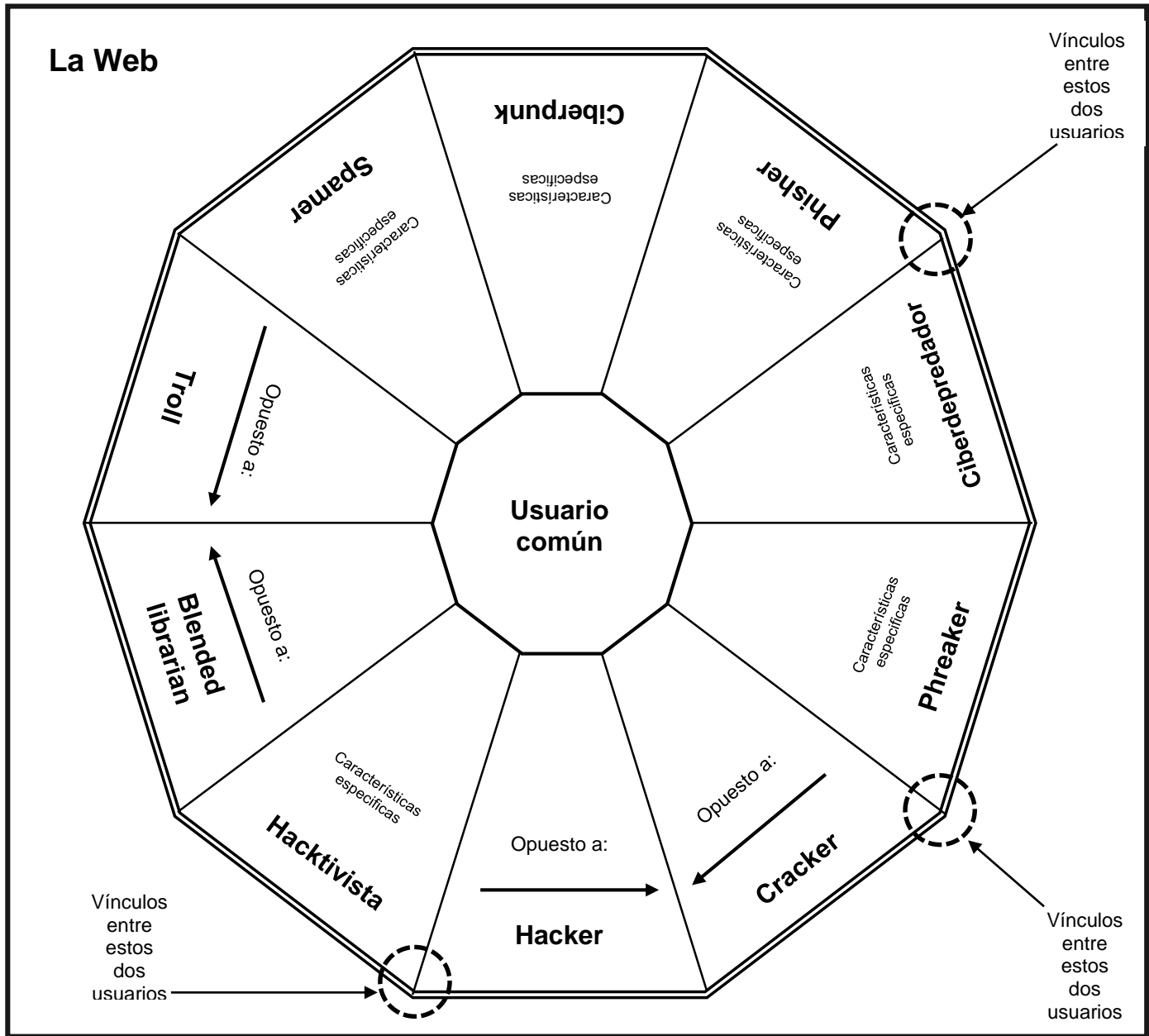


Figura 3. La Web y sus tipos de usuario. Fuente: creación propia.

1.8.3 Veracidad de la información

En la Web existe información correcta, imprecisa, incompleta, errónea y tergiversada, ello como consecuencia de los distintos tipos de usuarios que inciden en el entorno digital, además de los controles relacionados a la propiedad intelectual, el derecho de autor y el derecho de copia. Por tanto, la información debe de ser analizada y contar con criterios de credibilidad, como lo son: el autor, la procedencia geográfica, la fecha, la adscripción institucional, el dominio de red, entre otros, para ser considerada con atributos de sustentabilidad.

Criterios (de autoría) ¹⁶³	características
Autoría	La autoría debe pertenecer a algún autor, institución, publicación periódica, diario o semanario. Si el documento es anónimo, no es fiable.
Contexto	Institución, laboratorio, agencia, empresa, publicación periódica, diario, semanario, etc.
Actualización	Fecha de publicación

Tabla 8. Criterios de autoría de la información. Fuente: creación propia.

La autoría no sólo se manifiesta en los contenidos académicos, institucionales, científicos y administrativos de orden gubernamental, sino también en otro tipo de contenidos alojados en la Web como lo son: blogs de opinión, videos, audios, pinturas digitales, fotografías, imágenes, etc. Los sitios web además de contar con cierta estética visual también deben de poseer elementos de organización, clasificación y descripción para su referencia, entendimiento e interacción.

¹⁶³ Martos Rubio, Ana. Ídem. Pág. 45

Criterios (de sitios web) ¹⁶⁴	características
Autoría	Autor, institución, órgano gubernamental, asociación, organización, etc.
Exactitud	Fuentes de información, fuentes bibliográficas, obras consultadas
Accesibilidad gráfica	Visualización del texto, animaciones, imágenes, gráficas, etc.
Estructura	Organización jerárquica en la composición visual y de su información
Disponibilidad de enlaces	Actualización de enlaces a otros sitios o documentos

Tabla 9. Criterios de sitios web. Fuente: creación propia.

Una vez que se han localizado algunos o la mayoría de los criterios de estructura y autoría, será necesaria la observación en el contenido. Francisco Cisterna¹⁶⁵ hace hincapié en que, el análisis de la información consiste en interpretarla para conocer la intención del mensaje y posteriormente se deberá efectuar una triangulación de la información, la cual consiste en comparar más de un documento o contenido, con el objetivo de complementar la idea esencial del tema, además de ampliar el contexto histórico y documental.

¹⁶⁴ Singh, Shashi Prabha. *Ibíd.* Recuperado en:

<http://www.emeraldinsight.com/journals.htm?articleid=860825&show=html> [Consultado 10 de enero 2014]

¹⁶⁵ Cisterna Cabrera, Francisco. "Categorización y triangulación como procesos de validación del conocimiento en investigación cualitativa". *Theoria* 14, no. 1 (2005): 61-71. Recuperado en: <http://www.redalyc.org/articulo.oa?id=29900107> [Consultado 17 de febrero de 2016]

La información, según Cesar Vargas¹⁶⁶ para ser interpretada debe poseer relevancia, de modo que el individuo pueda comprender el mensaje además de que la información debe ser confiable, concisa, coherente y verificable. Retomando a Ana Martos¹⁶⁷ la información en la Web al no ser verificada puede conducir a errores simplemente graves o lamentables según sea el caso. En ese sentido Mayelín Travieso¹⁶⁸ menciona que, en la Web no hay alguna autoridad que controle la calidad de todas las publicaciones consideradas de carácter científico y académico, refiriéndose explícitamente a las que no pertenecen a alguna editorial, o bien estas publicaciones no sean arbitradas.

Los criterios para valorar la información son fundamentales, puesto que de ellos se puede inferir el grado de sustentabilidad sobre el contenido en cuestión. En primera instancia los criterios de autoría de la información pueden ser considerados como punto de partida para toda clase de documentos y contenidos, en este tenor es viable considerar los puntos de autoría a partir de algunas preguntas como:

- a) ¿Quién es el responsable del contenido?
- b) ¿Cuál es el origen de procedencia?
- c) ¿Cuál es la fecha de publicación?

Consecuentemente dichos criterios de autoría pueden adaptarse y/o complementarse al contexto digital. A continuación se presentan los criterios de sitios web basados en cinco puntos a valorar mediante las siguientes preguntas:

- 1. ¿A quién se le atribuye el contenido?
- 2. ¿En qué información se fundamenta el contenido?
- 3. ¿Existe una interacción adecuada con el contenido?

¹⁶⁶ Vargas, César. "Indicadores de gestión en materia de transparencia y su impacto en el desarrollo económico". En **Derecho a la información: reflexiones contemporáneas**. (México: UAM, 2012). Pág. 205

¹⁶⁷ Martos Rubio, Ana. Ídem. Pág. 43

¹⁶⁸ Travieso Aguilar, Mayelín. "Las publicaciones electrónicas: una revolución en el siglo XXI". **ACIMED** 11, no. 2 (2003): Recuperado en: <http://eprints.rclis.org/5101/1/publicaciones.pdf> [Consultado 4 de febrero de 2016]

4. ¿Hay una estructura y desarrollo temático?
5. ¿Cuál es el grado de acceso o disponibilidad a los contenidos enlazados?

Tanto los criterios de autoría de la información como los criterios de sitios web son de utilidad para el bibliotecólogo, puesto que son elementos que coadyuvan a la identificación para posteriormente tomar una decisión de selección o descarte. Sin embargo, dichos criterios son considerados en un entorno ideal, de manera que, en ocasiones los contenidos alojados en la Web carecen de elementos de autoría, procedencia, fecha de publicación o fecha de modificación, referencias bibliográficas, estructura temática y disponibilidad de sus enlaces a otros recursos en línea.

1.8.4 Información privilegiada

En cuanto a la información privilegiada se refiere, Daniel Entrena¹⁶⁹ comenta que, es toda aquella información que no es habitual para el experto o el individuo especializado en el tema. Es información sumamente valiosa que no se encuentra al alcance por las vías del acceso común. En este sentido Marta Torres¹⁷⁰ menciona que, la información es un producto de consumo orientado a aspectos económicos y rentables. Mientras que José Salvador¹⁷¹ agrega que, la información es un elemento de gran valor político y estratégico para tomar decisiones asertivas. Juan Castaingts¹⁷² argumenta que, la información privilegiada junto con la astucia favorece la fortuna en el escenario de la corrupción.

A partir de estos argumentos se puede ratificar que, la información privilegiada proporciona certidumbre para ejecutar un movimiento específico, el cual

¹⁶⁹ Entrena Ruiz, Daniel. *El empleo de información privilegiada en el mercado de valores: un estudio de su régimen administrativo sancionador*. (Cizur Menor, Navarra: Thomson Civitas, 2006). Pág. 53

¹⁷⁰ Torres Santo Domingo, Marta. "La función social de las bibliotecas universitarias". *Boletín de la Asociación Andaluza de bibliotecarios* 20, no. 80 (2005): 310-314. Recuperado en: <http://dialnet.unirioja.es/servlet/dcart?info=link&codigo=2173486&orden=95050> [Consultado 28 de enero de 2016]

¹⁷¹ Salvador, José A. *Recuperación de la información*. (Argentina: Alfagrama, 2008). Pág. 111

¹⁷² Castaingts Teillery, Juan. *Simbolismos del dinero: antropología y economía una encrucijada*. (México: UAM; Anthropos, 2002). Pág. 76

garantiza la ventaja sobre los adversarios. La información privilegiada¹⁷³ es ornato y poder en el individuo que la posee y la ejerce. Sin embargo, es menester tener cuidado de donde proviene la supuesta información privilegiada, ya que como lo advierten Raúl Canseco y Perla Gómez¹⁷⁴ los canales informales en una institución pública tergiversan la información, por lo que al ser liberada o filtrada puede llegar a ser perjudicial para quien la utiliza y difunde.

En síntesis se puede interpretar que, los individuos comunes tienen acceso limitado al servicio de Internet, además de que el servicio de conexión no es para todos, de manera que se requiere de cierto nivel de poder adquisitivo para cubrir los costos de gama alta. Internet se ha convertido en un servicio básico puesto que la comunicación, la interacción social y los trámites administrativos se han acoplado a los servicios de la Web. La Web por su parte puede llegar a propiciar el acceso a los recursos y nuevos contenidos generando nuevas experiencias de aprendizaje.

El acceso es por tanto, un filtro para la segregación, porque con base a requerimientos de autenticidad delimita quien puede disponer a la experiencia, el entorno, el objeto o contenido. Por ende el acceso se fundamenta en políticas de información las cuales son creadas para regular el interés y el beneficio. En este sentido en la Web se crea un nuevo paralelismo de segmentación para acceder a los contenidos y a los servicios en línea, de manera que, suele ser el poder adquisitivo un elemento para incrementar la apertura en el acceso.

Es importante recalcar que, la recuperación de la información se debe al desarrollo de los proyectos militares y avances científicos, además de ser la recuperación de la información un acto reflejo del ser humano para garantizar su

¹⁷³ Tapscott, Don., Ticoll, David y Lowy, Alex. *Capital digital: el poder de las redes de negocios*. Traducido por María Córdor Orduña. (Madrid; México: Santillana, 2001). Pág. 23

¹⁷⁴ Canseco, Raúl y Gómez, Perla. "La diseminación de la información y la transparencia informativa". En *Derecho a la información: reflexiones contemporáneas*. (México: UAM, 2012). Pág. 67

preservación y prosperidad en la sociedad y, en el entorno natural. La información, es un recurso de insumo en el mundo moderno.

No sólo existen restricciones a los contenidos en la Web por parte de particulares, la propiedad intelectual, el derecho de autor y el derecho de copia sino que también es el *Estado-nación* el que regula con base a las leyes el acceso a la infraestructura como a los contenidos y servicios en línea. En este sentido, es el control de la información lo que permite a las instituciones, medios de comunicación y empresas privadas conocer la situación administrativa, legal y social para poder determinar una decisión acertada basada en la certidumbre. La censura por su parte, complementa y polariza el control de la información como regulador en la conducta de los individuos.

De esta manera se puede detectar una complejidad en la Web puesto que la privacidad al ser reducida por la vigilancia, comparte nexos con el control y la censura. Por su parte, la seguridad informática puede ser considerada como un punto en común entre los individuos, las instituciones y las empresas privadas incluso es un elemento crucial para la integridad del *Estado-nación*, porque es el usuario con conocimientos avanzados en el acceso a la Web el que puede explotar las vulnerabilidades de seguridad y acceder a la información reservada de las empresas privadas, del gobierno y de otros usuarios.

El anonimato en la Web se ha redimensionado como un elemento para evitar las sanciones, las restricciones y la censura, de modo que, surgen nuevas posibilidades para acceder anónimamente a los contenidos considerados como prohibidos por la censura. A estos entornos de anonimato y contenidos sin restricción se les conoce socialmente como la “**web profunda**”^{*} o la “**deep web**”.

* Se utilizan las comillas para diferenciar a la web profunda bajo el concepto social, siendo que en realidad se trata de una red oscura llamada Tor. Además de Tor existen otras redes oscuras.

Capítulo 2

La web profunda



Pintura del mar y la complejidad en el acceso al iceberg (o la travesía del enmascarado): creación propia basada en la metáfora de la web profunda.

2.1 Introducción

A continuación se describe el concepto de *web profunda*. Así como la estratificación de la Web, con el objetivo de delimitar los conceptos de *web superficial*, *web semántica*, *web opaca*, *web propietaria* y *web invisible*. Se presentan esquemas sobre su estratificación, con la finalidad de mostrar una conceptualización gráfica sobre las diferencias entre cada tipo de web.

Consecuentemente se aborda el concepto de la *web profunda* bajo la percepción social, el cual se ha delimitado para fines de esta investigación a partir del año 2012 al 2015, ello con el fin primordial de establecer las diferencias con las *redes oscuras*. Asimismo, se presentan los antecedentes acerca de la conceptualización de la invisibilidad de los contenidos en la Web. Del mismo modo, se mencionan los aspectos generales sobre el funcionamiento del software para acceder a las *redes oscuras*. Se exponen esquemas realizados por terceros sobre la conceptualización gráfica de la *web profunda* y sus respectivos elementos, características y niveles de acceso.

Finalmente se mencionan los riesgos tanto en la navegación como en la adquisición de productos, contenidos y servicios que pueden derivar tanto en consecuencias legales como psicológicas en el individuo.

2.2 Estratificación de la Web

La Web conceptualmente hablando se encuentra segmentada de acuerdo a la navegabilidad, recuperación y acceso a los contenidos. Dicha estratificación se debe a que los distintos conjuntos de sitios y contenidos comparten las mismas características. En este apartado es menester aclarar algunos conceptos como el ciberespacio y la nube, con el objetivo de presentar un mayor margen de claridad en la estratificación de la Web.

En cuanto al ciberespacio Lawrence Lessig manifiesta que, este es un entorno multidimensional en donde el individuo puede realizar distintas actividades a la vez; la Web, por su parte no necesariamente cumple con particularidades de interacción y representación gráfica a detalle, como en el caso del ciberespacio.¹⁷⁵ A diferencia de la Web a la cual se accede por medio de la conexión a Internet; el ciberespacio es considerado como todo aquel conjunto de entornos virtuales que recrean la realidad, es decir que el usuario interactúa con el entorno y con otros individuos representados mediante un personaje digital.

Por otro lado el cómputo en nube mejor conocido como, *la nube*, es todo aquel conjunto de servicios para el respaldo y acceso a contenidos de índole personal, empresarial e institucional. *La nube*¹⁷⁶ es básicamente un servicio para la conexión y actualización del software, además del alojamiento masivo de los contenidos digitales. Cabe mencionar que, un servicio de alojamiento o almacenamiento, es aquel que le permite al usuario guardar y descargar sus contenidos digitales por medio de la conexión a Internet sin importar su ubicación y horario geográfico. *La nube* al igual que los sitios web, almacena los datos en servidores ubicados en distintas partes del planeta, a diferencia de la Web que representa la totalidad de los servicios y contenidos en línea, *la nube* restringe el acceso y en algunos casos no existe transparencia en su servicio de respaldo,

¹⁷⁵ Lessig, Lawrence. Ídem. Pág. 23

¹⁷⁶ Rouse, Margaret. Junio de 2011. Cloud storage service. **Tech target**. Recuperado en: <http://searchcloudstorage.techtarget.com/definition/cloud-storage-service> [Consultado 27 de abril de 2016]

puesto que no se tiene conocimiento sobre los procesos de transferencia, ingesta o conversión de los contenidos así como de su código informático para su almacenamiento, del mismo modo que se desconoce el grado de confidencialidad y privacidad por parte de las empresas que se dedican a brindar el servicio en *nube*. Para Francisco Martínez y Beatriz Gutiérrez,¹⁷⁷ *la nube* además de ser un servicio de almacenamiento de contenidos y acceso a los servicios, ha comenzado a adquirir un cariz en la comprobación de la autenticidad en la licencia de uso del software de productividad y software de entretenimiento. La estratificación de la Web se diversifica según sus características fundamentales, la cuales son:

- **La web superficial;** que se encuentra compuesta por sitios, páginas y contenidos indexados por los motores de búsqueda. Nigel Yazdan¹⁷⁸ señala que, la *web superficial* es el conjunto de páginas fijas elaboradas con código HTML. Mientras que para Juan Becerra¹⁷⁹ la *web superficial* tiene la característica esencial de ser un conjunto de documentos y contenidos vinculados, los cuales están orientados a la navegación. La *web superficial* es el estrato más visible para los motores de búsqueda y en consecuencia los sitios, páginas y contenidos poseen un alto grado de visibilidad para el usuario común.
- **La web semántica;** Lluís Codina¹⁸⁰ explica que, la *web semántica* es un conjunto de iniciativas tecnológicas que tienen por objetivo el de representar y dotar de visibilidad a la información, mediante conexiones temáticas. El mismo autor hace énfasis en la importancia de regular la

¹⁷⁷ Martínez, Francisco y Gutiérrez, Beatriz. "Cómputo en Nube: Ventajas y Desventajas". *Revista Seguridad Cultura de prevención para TI*, no. 8 (2010): 1-7. Recuperado en: <http://revista.seguridad.unam.mx/numero-08/c%C3%B3mputo-en-nube-ventajas-y-desventajas> [Consultado 12 de abril de 2015]

¹⁷⁸ Yazdan Mansourian, Nigel Ford. "The invisible web: an empirical study of cognitive invisibility". *Journal of Documentation*, no. 62 (2006): 584-596. Recuperado en: <http://www.emeraldinsight.com/doi/abs/10.1108/00220410610688732> [Consultado 12 de abril de 2015]

¹⁷⁹ Becerra, Juan. "Mitos y realidades de la Internet profunda". *Revista Seguridad Cultura de prevención para TI*, no. 20 (2014): 8-11. Recuperado en: <http://revista.seguridad.unam.mx/numeros/numero-20> [Consultado 3 de agosto 2015]

¹⁸⁰ Codina, Lluís. "Internet invisible y web semántica: ¿El futuro de los sistemas de información en línea?". *Revista Tradumática*, no. 2, (2003): Recuperado en: <http://www.fti.uab.es/tradumatica/revista> [Consultado 20 de enero 2016]

representación de los contenidos, con el uso de vocabulario controlado y la clasificación para la asociación y posterior recuperación de temas, ideas, conceptos, palabras clave, conceptos y terminología.

- **La web opaca;** que Paul Pedley¹⁸¹ define como el conjunto de sitios que debido a la capacidad limitada de las tecnologías de búsqueda no aparecen en los resultados de los motores de búsqueda. Mientras que Nigel Yazdan¹⁸² agrega que, debido a la preferencia de las compañías que brindan el servicio de búsqueda se omite la visibilidad de otros sitios, páginas y contenidos potenciales. En relación a lo anterior, se puede inferir que la *web opaca* puede ser considerada como la omisión de los resultados potencialmente pertinentes y relevantes.
- **La web invisible;** la cual Paul Pedley¹⁸³ indica que, es un conjunto de páginas y sitios con las características de ser únicamente visibles en su interfaz de inicio, restringiendo parcial o completamente sus contenidos a los motores de búsqueda, como es el caso de la industria del entretenimiento, los catálogos en línea de bibliotecas y las bases de datos académicas. Mientras que Lluís Codina¹⁸⁴ describe a la *web invisible* como el conjunto de contenidos de los sitios web, que los motores de búsqueda no pueden indizar. En tanto que Idoia Salazar¹⁸⁵ menciona que, la *web invisible* son los sitios, páginas y contenidos que no pueden ser recuperados mediante los métodos de búsqueda convencionales. Finalmente Jonas Fransson¹⁸⁶ recalca que, nada es invisible en la Web, no obstante es viable ocultarlo.

¹⁸¹ Pedley, Paul. *The invisible web: searching the hidden parts of the internet*. (London: Aslib-IMI, 2001). Pág. 6

¹⁸² Yazdan, Nigel. Ibíd. Recuperado en: <http://www.emeraldinsight.com/doi/abs/10.1108/00220410610688732>

[Consultado 12 de abril de 2015]

¹⁸³ Pedley, Paul. Op. Cit. Pág. 4

¹⁸⁴ Codina, Lluís. Ibíd. Recuperado en: <http://www.fti.uab.es/tradumatica/revista> [Consultado 20 de enero 2016]

¹⁸⁵ Salazar García, Idoia. *Las profundidades de Internet: accede a la información que los buscadores no encuentran y descubre el futuro inteligente de la red*. (Asturias: TREA, 2005). Pág. 63

¹⁸⁶ Fransson, Jonas. Ídem. Pág. 97

- **La web propietaria;** es descrita por Nigel Yazdan¹⁸⁷ como los recursos excluidos en los resultados de los motores de búsqueda, porque intencionalmente dichos recursos poseen etiquetas en su código para evitar su visibilidad. Por su parte Paul Pedley¹⁸⁸ agrega que, para acceder a los recursos de un sitio de la *web propietaria* es necesario ingresar una contraseña. Comúnmente las empresas, las compañías, las instituciones y los laboratorios poseen recursos en línea que no son recuperados por los motores de búsqueda.
- **La web profunda;** la cual comparte atributos que definen tanto a la *web propietaria* como a la *web invisible*. De acuerdo a Gerry McKiernan,¹⁸⁹ la *web profunda* se compone de contenidos especializados y bases de datos que no pueden ser rastreados, porque cuentan con sistemas de protección, o como lo señala Kristin Finklea¹⁹⁰ simplemente no es del interés (del administrador del sitio) que los servicios sean visibles bajo ninguna circunstancia. Asimismo Qiuyan Huang y colaboradores¹⁹¹ señalan que, los contenidos de la *web profunda* están restringidos por medio de una interfaz de acceso. En este tenor Nigel Yazdan¹⁹² agrega que, los creadores y administradores no pretenden que sus sitios, páginas y contenidos sean indexados por los motores de búsqueda. Jane Devine y Francine Egger-Sider¹⁹³ definen que, la *web profunda* es el conjunto de recursos sentenciados al olvido y la marginación. Idoia Salazar¹⁹⁴ añade que, la *web profunda* se encuentra dividida de acuerdo a los niveles de

¹⁸⁷ Yazdan, Nigel. Op. Cit.

¹⁸⁸ Pedley, Paul. Ídem. Pág. 14

¹⁸⁹ McKiernan, Gerry. "The Hidden Web". *Science & Technology Libraries* 20, no. 4 (2001): 65-74. Recuperado en: http://www.tandfonline.com/doi/abs/10.1300/J122v20n04_08#preview [Consultado 28 de febrero de 2016]

¹⁹⁰ Finklea, Kristin, 7 de julio de 2015. Dark Web. *Congressional Research Service*. Recuperado en: <https://www.fas.org/sqp/crs/misc/R44101.pdf> [Consultado 30 de septiembre de 2016]

¹⁹¹ Huang, Qiuyan Et al. "An Approach to Incremental Deep Web Crawling Based on Incremental Harvest Model". *Procedia Engineering* 29, (2012): 1081-1087. Recuperado en: <http://www.sciencedirect.com/science/article/pii/S1877705812001038> [Consultado 30 de enero de 2016]

¹⁹² Yazdan, Nigel. Íbid. Recuperado en: <http://www.emeraldinsight.com/doi/abs/10.1108/00220410610688732> [Consultado 12 de abril de 2015]

¹⁹³ Devine, Jane y Egger-Sider, Francine. *Going beyond Google: The invisible web in learning and teaching*. (New York: Neal Schuman Publishers, 2009). Pág. 3

¹⁹⁴ Salazar García, Idoia. Ídem. Pág. 73

visibilidad. Por lo anteriormente mencionado, el objetivo esencial en la creación de sitios, páginas y contenidos pertenecientes a la *web profunda* podría estar enfocado a la inaccesibilidad para cualquier tecnología de rastreo y carecer de toda visibilidad, exceptuando a sus administradores y usuarios autorizados.

La Web es por tanto la totalidad de sus estratificaciones, las cuales se deben a las distintas características de los sitios, páginas y contenidos web agrupados en conjuntos, según sus utilidades, grado de acceso y visibilidad. A grandes rasgos la Web puede dividirse en tres niveles:

1. **Nivel 1:** Contenidos visibles con disponibilidad
2. **Nivel 2:** Contenidos parcialmente visibles con controles de acceso
3. **Nivel 3:** Contenidos no visibles

A manera de homologación, conforme al nivel de accesibilidad a la información se puede agregar que, existe una relación entre el nivel de acceso de acuerdo a la visibilidad.

- a) Contenidos visibles – información disponible para el público en general
- b) Contenidos parcialmente visibles – información reservada
- c) Contenidos no visibles – información altamente reservada

Respecto al primer nivel de visibilidad se puede considerar en primera instancia a la *web superficial*, pero también es la *web semántica* un sistema mediador entre la *web superficial* y la *web opaca*, no obstante a pesar de la intención por parte de la *web semántica*, los motores de búsqueda pueden llegar a realizar exclusiones en sus resultados de búsqueda.

Parte de la *web superficial* podría presentar atributos de un segundo nivel, de acuerdo al tipo de acceso a los servicios y contenidos ofrecidos. De manera que,

es complejo establecer una línea indiscutiblemente sólida entre cada nivel. En este sentido, La *web opaca* podría ser considerada como la zona profunda de la *web superficial* debido a su ambigüedad de visibilidad y desconocimiento en sus contenidos, es decir que, es un vacío entre la *web superficial* y la *web invisible*, razón por la cual forma parte del segundo nivel. La *web invisible* es considerada como todo aquel conjunto de sitios, páginas y contenidos con un acceso parcial, de manera que se desconoce a plenitud la intención y utilidad de la información, por lo que también forma parte del segundo nivel.

Mientras que en un tercer nivel de visibilidad, la *web propietaria* y la *web profunda* poseen códigos de programación para no ser indexadas por los motores de búsqueda, además de restringir el acceso a sus contenidos mediante sistemas de seguridad basados en políticas de información. Un bosquejo para representar la estratificación de la Web se puede ver en la siguiente figura.


Primer nivel (Contenidos visibles con disponibilidad)	web superficial	web semántica (fomenta la visibilidad de los contenidos)	Mayor visibilidad Mayor accesibilidad  Menor visibilidad Menor accesibilidad
Segundo nivel (Contenidos parcialmente visibles con controles de acceso)			
Segundo nivel	web opaca		
Segundo nivel	web invisible		
Tercer nivel (Contenidos no visibles)	web propietaria		
Tercer nivel	web profunda		

Figura 4. Esquematzación de acceso y visibilidad en la estratzificación Web. Fuente: creación propia basada en la estratzificación de la Web.

En cuanto a la esquematización de acceso y visibilidad en la estratzificación de la Web, se muestra una amplia visibilidad en la *web superficial* así como una mayor probabilidad de disponibilidad en sus recursos, servicios y contenidos. De este modo, la accesibilidad se ve gradualmente reducida en la *web opaca*, *web invisible*, *web propietaria* y *web profunda*.

Conforme a lo mencionado en cuanto a la estratzificación de la Web, la visibilidad y la accesibilidad, se puede añadir que, también existen servicios, documentos y contenidos que poseen un alto nivel de visibilidad, sin embargo el acceso a

ellos se encuentra regulado mediante una contraseña, pago y/o suscripción (como en el caso de la *web invisible*). No obstante es menester mencionar que, existen otras alternativas en cuanto al consumo y solicitud de servicios, una de estas alternativas es mediante el uso y acceso a las *redes oscuras*.

2.2.1 La red oscura y su vínculo con la web profunda

Una *red oscura*¹⁹⁵ es un conjunto de servidores y computadoras personales conectados y sincronizadas mediante la conexión a Internet, con un cifrado particular para la transmisión de datos. Su objetivo principal es el de preservar el anonimato de los usuarios por medio de tecnologías de cifrado en constante desarrollo por los colectivos interesados en el anonimato y en ampliar la privacidad. Para Tao Ban y colaboradores¹⁹⁶ la *red oscura* es definida como un tejido abstracto de comunicación en línea, en donde no todos los servicios se encuentran habilitados las 24/7, por lo que depende del horario geográfico del usuario y del administrador el cual aloja sus contenidos en un servidor dedicado o mediante una computadora personal, comúnmente este tipo de servicios son proporcionados por individuos con intereses particulares; y no de instituciones, laboratorios u organizaciones reconocidas.

Un estudio por parte de *Digital Citizens Alliance and RiskIQ shows*¹⁹⁷ menciona que, el concepto de *red oscura* se utiliza para referirse a una red de comunicación anónima con intenciones ilícitas. Hans Graux¹⁹⁸ señala que, una *red oscura* está dedicada al intercambio de información, procurando no revelar

¹⁹⁵ Véase Rouse, Margaret. Diciembre de 2011. Darknet. **Tech target**. Recuperado en: <http://searchnetworking.techtarget.com/definition/darknet> [Consultado 17 de abril de 2016]

¹⁹⁶ Ban, Tao Et al. "Behavior Analysis of Long-term Cyber Attacks in the Darknet". En **Neural information processing**. (Berlín: Springer, 2012). Recuperado en: http://link.springer.com/chapter/10.1007%2F978-3-642-34500-5_73 [Consultado 17 de abril de 2016]

¹⁹⁷ Digital Citizens Alliance and RiskIQ shows. Diciembre de 2015. How content theft sites and malware are exploited by cybercriminals to hack into internet users' computers and personal data. **Digital Citizens Alliance**. Recuperado en: <https://media.gractions.com/314A5A5A9ABBBBC5E3BD824CF47C46EF4B9D3A76/0f03d298-aedf-49a5-84dc-9bf6a27d91ff.pdf> [Consultado 19 de diciembre de 2015]

¹⁹⁸ Graux, Hans. "Darknets and the future of expression in the information society". En **Facing the Limits of the Law**. (Berlín: Springer, 2008). Recuperado en: http://link.springer.com/chapter/10.1007%2F978-3-540-79856-9_24 [Consultado 17 de abril de 2016]

el origen y el destino de conexión. Además de que en este tipo de red no existen restricciones legales.

Las *redes oscuras* son consideradas como sospechosas bajo el criterio de los *Estados-naciones*, puesto que se desconoce el contenido de los datos transmitidos, así como el origen de conexión que permite conocer la ubicación e identidad de los usuarios de acuerdo con su IP pública.

2.3 Conceptualización social de la web profunda (2012 - 2015)

Anteriormente se han señalado las características entre la *web profunda* y una *red oscura*, sin embargo es menester mencionar el origen del concepto y su evolución al paso del tiempo, dado que posiblemente la confusión entre la *web profunda* y las *redes oscuras* surge a raíz del sincretismo en sus objetivos y utilidades. Por ello se muestran a continuación las disparidades en el concepto de *web profunda*, de acuerdo a la cronología y los acontecimientos que han modificado el concepto.

De acuerdo con Idoia Salazar,¹⁹⁹ fue en el año de 1994 cuando la Doctora Jill Ellsworth acuñó el concepto de Internet invisible. Posteriormente, Jane Devine y Francine Egger-Sider²⁰⁰ agregan que, en el año 2000 se realizó un estudio elaborado por Michael Bergman para determinar el tamaño de la *web invisible* (también conocida como *Internet invisible* o *web profunda*). Años más tarde en un estudio de Vincenzo Ciancaglini y colaboradores²⁰¹ se argumenta que, la “*web profunda*”^{*} alcanzó su auge en el 2013 y consecuentemente es identificada por la Oficina Federal de Investigaciones (por sus siglas en inglés FBI) de los Estados Unidos de América, como un medio para la compra-venta de productos y servicios que operan fuera de la legalidad.

¹⁹⁹ Salazar García, Idoia. Ídem. Pág. 63

²⁰⁰ Devine, Jane y Egger-Sider, Francine. Loc. Cit.

²⁰¹ Ciancaglini, Vincenzo Et al. ***Below the surface: exploring the Deep Web***. (Reino Unido: Trend Micro, 2015). Recuperado en: <http://www.trendmicro.co.uk/media/wp/exploring-the-deep-web-whitepaper-en.pdf> [Consultado 2 de agosto de 2016]

* Se utilizan las comillas para diferenciar a la web profunda bajo el concepto social, siendo que en realidad se trata de una red oscura llamada Tor. Además de Tor existen otras redes oscuras.

De lo anteriormente mencionado, se puede entender que *Internet invisible*, *web invisible* y *web profunda* son conceptos relacionados con características similares; siendo que cada tipo de web posee atributos específicos. De modo que, Internet es la infraestructura y el conjunto de protocolos para la transmisión de datos, por tanto, en el estricto orden de la palabra, Internet invisible tendría que referirse a un sistema de conexión intangible, sin antenas, ni cables y circuitos, etc. O bien, un conjunto de redes inalámbricas ocultas. Y por otro lado el concepto de la *web invisible* es todo aquello que no puede ser recuperado en su totalidad; la *web profunda* es todo aquello que no debe ser recuperado por los programas desarrollados para encontrar e indexar.

La presente investigación se enfoca en el periodo 2012–2015 puesto que en este lapso de tiempo se recopilaron documentos y contenidos para coadyuvar a definir el concepto de *web profunda*, además de ser un momento crucial, ya que se concreta el desarrollo, auge y disolución de algunos servicios ilícitos. Para fines de concordancia con la literatura recopilada, se utilizará a continuación el concepto de *web profunda (deep web)*, para referirse a lo que posteriormente se identificara de acuerdo al canon como **redes oscuras**.

A grandes rasgos, esta *web profunda* es conocida en la *web superficial* como una caverna submarina en donde se encuentran contenidos referentes a la ilegalidad, contenido bizarro y herramientas digitales para vulnerar la seguridad informática,²⁰² entre otros temas.

Concretamente esta clase de *web profunda* es utilizada por grupos terroristas²⁰³ empero, no se puede generalizar en absoluto su nexos con el terrorismo o actos

²⁰² Véase Pacheco, Wilberto. 11 de febrero de 2015. ¿Cómo entrar a la deep web y qué cosas necesitas saber al respecto? **Batanga**. Recuperado en: <http://www.batanga.com/tech/55817/como-entrar-a-la-deep-web-y-que-cosas-necesitas-saber-al-respecto> [Consultado 27 de enero de 2015]. Internautas21. 2014. Deep web: mi experiencia entrando a la Internet profunda. **Internautas21**. Recuperado en: <http://internautas21.com/mi-experiencia-entrando-a-la-deep-web/> [Consultado 27 de enero de 2015] y Emmanuel, Hery. 2014. ¿Qué es la Deep Web? **Marcianos**. Recuperado en: <http://marcianosmx.com/que-es-la-deep-web/> [Consultado 27 de enero de 2015].

²⁰³ Kumar, Mohit. 10 de diciembre de 2015. France will not ban public Wi-Fi or Tor Network, Prime Minister Valls confirms. **The hacker news**. Recuperado en: http://thehackernews.com/2015/12/France-tor-ban_10.html [Consultado 19 de diciembre de 2015]

ilícitos. Según Carlos Zahumenszky²⁰⁴ la supuesta *web profunda* es una red superpuesta en la Web, dedicada al anonimato, y tan sólo una de las tantas redes que no son visibles y accesibles al usuario común.²⁰⁵ Por su parte Amaya Quincoces²⁰⁶ menciona que, dichas redes no son del todo inexpugnables. Juan Becerra²⁰⁷ describe a las *redes oscuras* como un conjunto de túneles virtuales para proporcionar anonimato y privacidad a sus usuarios, con el fin de reducir la vigilancia. Vicente Motos²⁰⁸ sugiere que, además de alojar contenidos, es una de las principales vías para mantener el anonimato en el acceso a los contenidos de la *web superficial*.

Cooper Quintin²⁰⁹ agrega que, es posible navegar de forma anónima con el sistema de navegación de **Tor** ocultando el origen y el destino en la conexión del usuario, para evitar la vigilancia en el análisis de tráfico. Dicho análisis²¹⁰ además de ser implementado para la vigilancia puede ser de utilidad para realizar ataques por parte de *Crackers* hacia otros usuarios. En concordancia, Lucian Constantin²¹¹ menciona que, este método para navegar, oculta la actividad de los usuarios hacia sus Proveedores del Servicio de Internet (ISP).

²⁰⁴ Zahumenszky, Carlos. 8 de junio de 2013. La red cifrada TOR recomienda abandonar Windows. **Gizmodo en español**. Recuperado en: <http://es.gizmodo.com/la-red-cifrada-tor-recomienda-abandonar-windows-1043218659> [Consultado 10 de diciembre de 2013]

²⁰⁵ Segu Info. 8 de marzo de 2014. TOR confirma que el anonimato en la Deep Web fue roto. **Segu Info: noticias sobre seguridad de la información**. Recuperado en: http://blog.segu-info.com.ar/2014/08/tor-confirma-que-el-anonimato-en-la.html?utm_source=feedburner&utm_medium=feed&utm_campaign=Feed%3A+NoticiasSeguridadInformativa+%28Noticias+de+Seguridad+de+la+Informaci%C3%B3n%29 [Consultado 3 de agosto de 2014]

²⁰⁶ Quincoces, Amaya. 2 de agosto de 2015. Internet profundo: El mundo ilegal en la Web. **Sin embargo**. Recuperado en: <http://www.sinembargo.mx/02-08-2015/1435895> [Consultado 3 de agosto de 2015]

²⁰⁷ Becerra, Juan. Ibíd. Recuperado en: <http://revista.seguridad.unam.mx/numeros/numero-20> [Consultado 3 de agosto de 2015]

²⁰⁸ Motos, Vicente. 21 de diciembre de 2015. Script para detectar nodos maliciosos en Tor. **Hack players**. Recuperado en: <http://www.hackplayers.com/2015/12/script-para-detectar-nodos-maliciosos-en-tor.html> [Consultado 21 de diciembre de 2015]

²⁰⁹ Quintin, Cooper. 6 de agosto de 2013. Tor Is For Everyone: Why You Should Use Tor? **Electronic Frontier Foundation**. Recuperado en: <https://www.eff.org/deeplinks/2014/06/why-you-should-use-tor> [Consultado 2 de agosto de 2014]

²¹⁰ The onion router. 2016. Tor: Overview. **Tor**. Recuperado en: <https://www.torproject.org/about/overview.html.en> [Consultado 28 de enero de 2016]

²¹¹ Constantin, Lucian. 20 de enero de 2016. Privacy-conscious users rejoice: you can now use Facebook's Android app over Tor. **CSO**. Recuperado en: http://www.csoonline.com/article/3024779/security/privacy-conscious-users-rejoice-you-can-now-use-facebooks-android-app-over-tor.html#tk.rss_all [Consultado 23 de enero de 2016]

En cuanto a los datos duros se refiere, el estudio realizado por Vincenzo Ciancaglini y colaboradores²¹² indica que, los idiomas más recurrentes en la *red oscura Tor* son: inglés, ruso, francés y coreano. El mismo estudio revela que en esta supuesta *web profunda* se venden productos como el cannabis, medicamentos farmacéuticos y anfetaminas. Los contenidos más buscados son los códigos y herramientas maliciosas informáticas, junto con la pornografía infantil. Kyle Wilhoit y Stephen Hilt²¹³ añaden que, en dicha *web profunda* existen bienes y servicios enfocados principalmente al cibercrimen, robo de datos, documentos falsos, drogas y armas.

Carlos Zahumenszky²¹⁴ anota que, El FBI y la Agencia de Seguridad Nacional de los Estados Unidos de América (por sus siglas en inglés NSA) desarrolló un *malware* para los sistemas operativos Windows que utilizan el software de navegación anónima de la *web profunda*, con el objetivo principal de rastrear a los usuarios con actividades sospechosas e ilícitas. De forma reiterativa²¹⁵ la NSA y el Cuartel General de Comunicaciones del Gobierno del Reino Unido (por sus siglas en inglés GCHQ) han tratado de quebrantar el anonimato de los usuarios que navegan por la *web profunda*. A esta aparente *web profunda* se le conoce también con el nombre de **T O r** (The onion routing), una *red oscura*.

²¹² Ciancaglini, Vincenzo Et al. *Ibíd.* Recuperado en: <http://www.trendmicro.co.uk/media/wp/exploring-the-deep-web-whitepaper-en.pdf> [Consultado 2 de agosto de 2016]

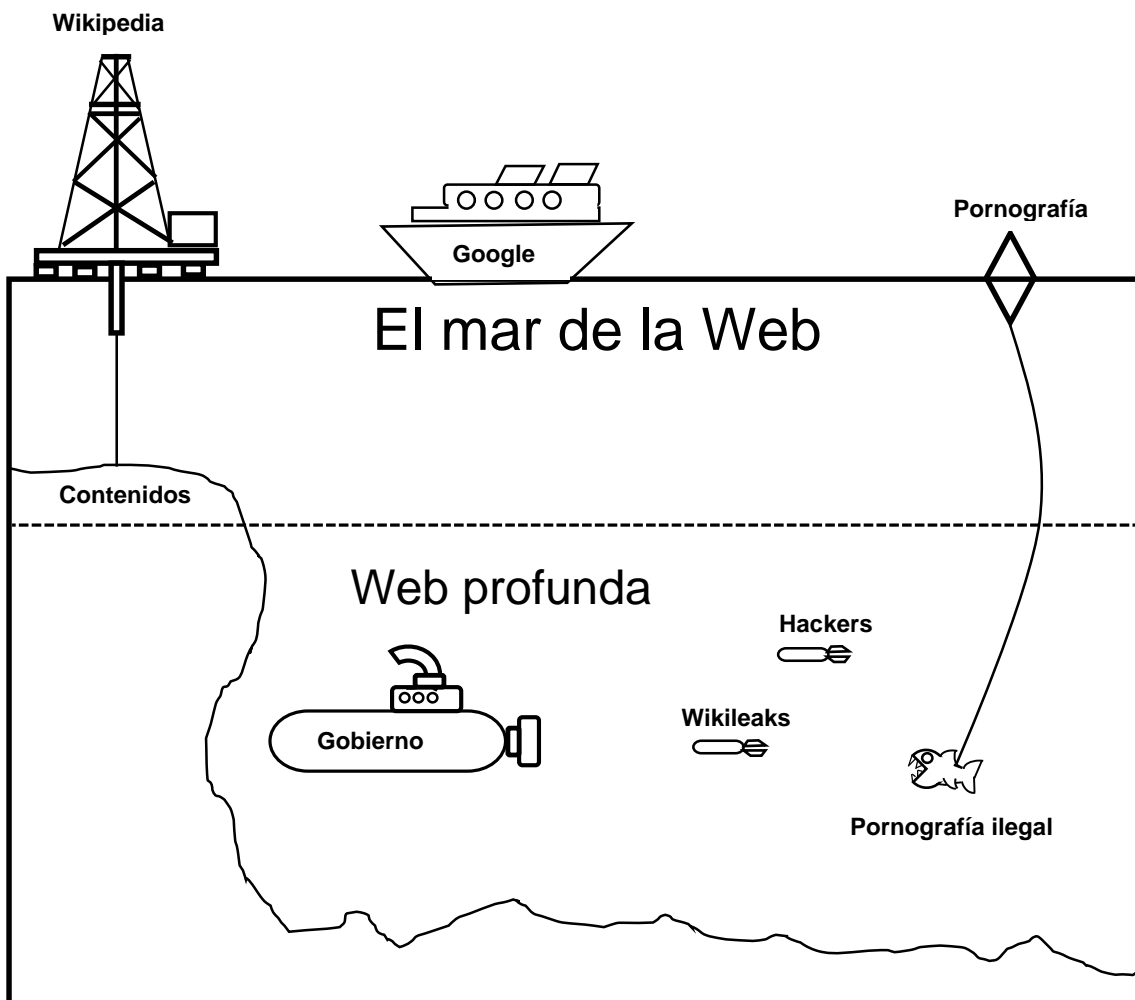
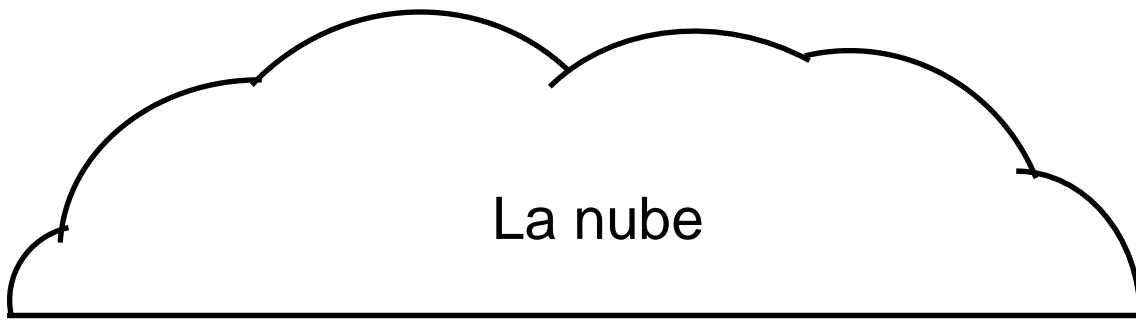
²¹³ Wilhoit, Kyle y Hilt, Stephen. *North American underground: the glass Tank*. (Estados Unidos: Trend Micro, 2015). Recuperado en: <http://www.trendmicro.com/cloud-content/us/pdfs/security-intelligence/white-papers/wp-north-american-underground.pdf> [Consultado 21 de diciembre de 2015]

²¹⁴ Zahumenszky, Carlos. *Ibíd.* Recuperado en: <http://es.gizmodo.com/la-red-cifrada-tor-recomienda-abandonar-windows-1043218659> [Consultado 10 de diciembre de 2013]

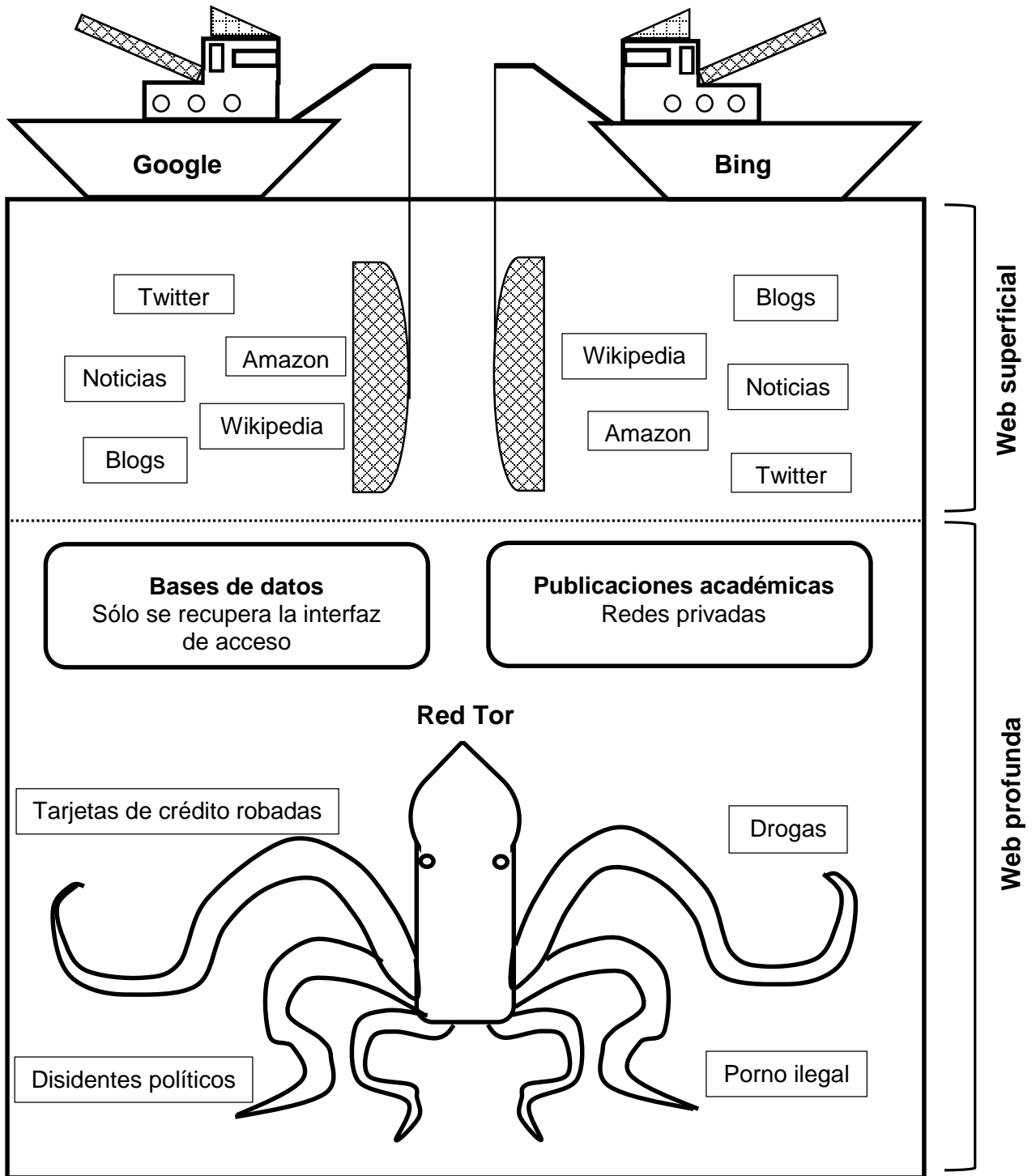
²¹⁵ RT. 23 de enero de 2016. Tor Project moves to lessen dependency on US gov't. *RT*. Recuperado en: <https://www.rt.com/usa/329870-tor-govt-funding-crowdsourcing/> [Consultado 23 de enero de 2016]

A continuación se presentan tres esquemas sobre como la *web profunda* (la *red oscura* The onion routing) es socialmente conceptualizada en la *web superficial*:

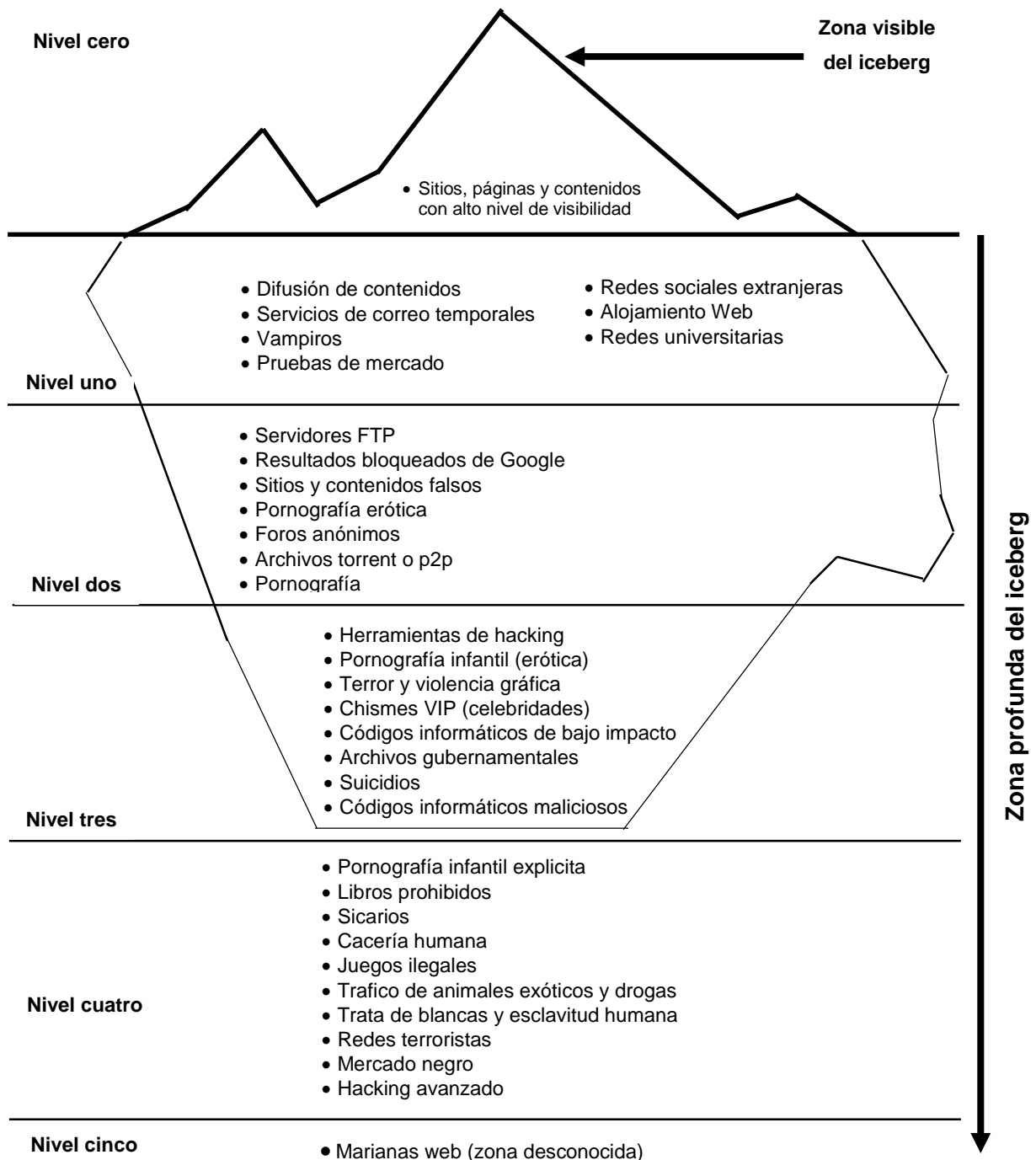
1. El primer esquema muestra los dos aspectos elementales de la Web bajo la metáfora de un océano, la visibilidad de la *web superficial* y dificultad de acceso a la supuesta *web profunda*, como sinónimo de un entorno en constante conflicto y hostil para el usuario común (véase esquema 1, pág. 70).
2. El segundo esquema se enfoca a la capacidad de recuperación de los motores búsqueda (Google y Bing) y a la visibilidad de los servicios de la *web superficial*; además de la complejidad referente a la seguridad, contenidos, servicios ilícitos, acceso y navegación en la *web profunda* (véase esquema 2, pág. 71).
3. El tercer esquema presenta la metáfora del iceberg, en donde la parte visible simboliza a la *web superficial*; mientras que el resto de sus niveles se encuentran agrupados según sus características ilícitas hasta llegar a una zona desconocida nombrada como las *marianas web* (véase esquema 3, pág. 72).



Esquema 1. ¿Qué tan profunda es tu Web? Fuente: creación propia a partir de la imagen postada: Brandpower. 2011. How deep is your Web. Brandpower. Recuperado en: <http://www.brandpowder.com/how-deep-is-your-web/> [Consultado 23 de julio de 2013]



Esquema 2. ¿Qué es la web profunda? Fuente: creación propia a partir de la imagen postada: CNN México. 2014. ¿Qué es el internet profundo? Tics y formación. Recuperado en: <https://ticsyformacion.com/2014/03/13/que-es-internet-profundo-o-deep-web-infografia-infographic-internet/> [Consultado 23 de noviembre de 2014]



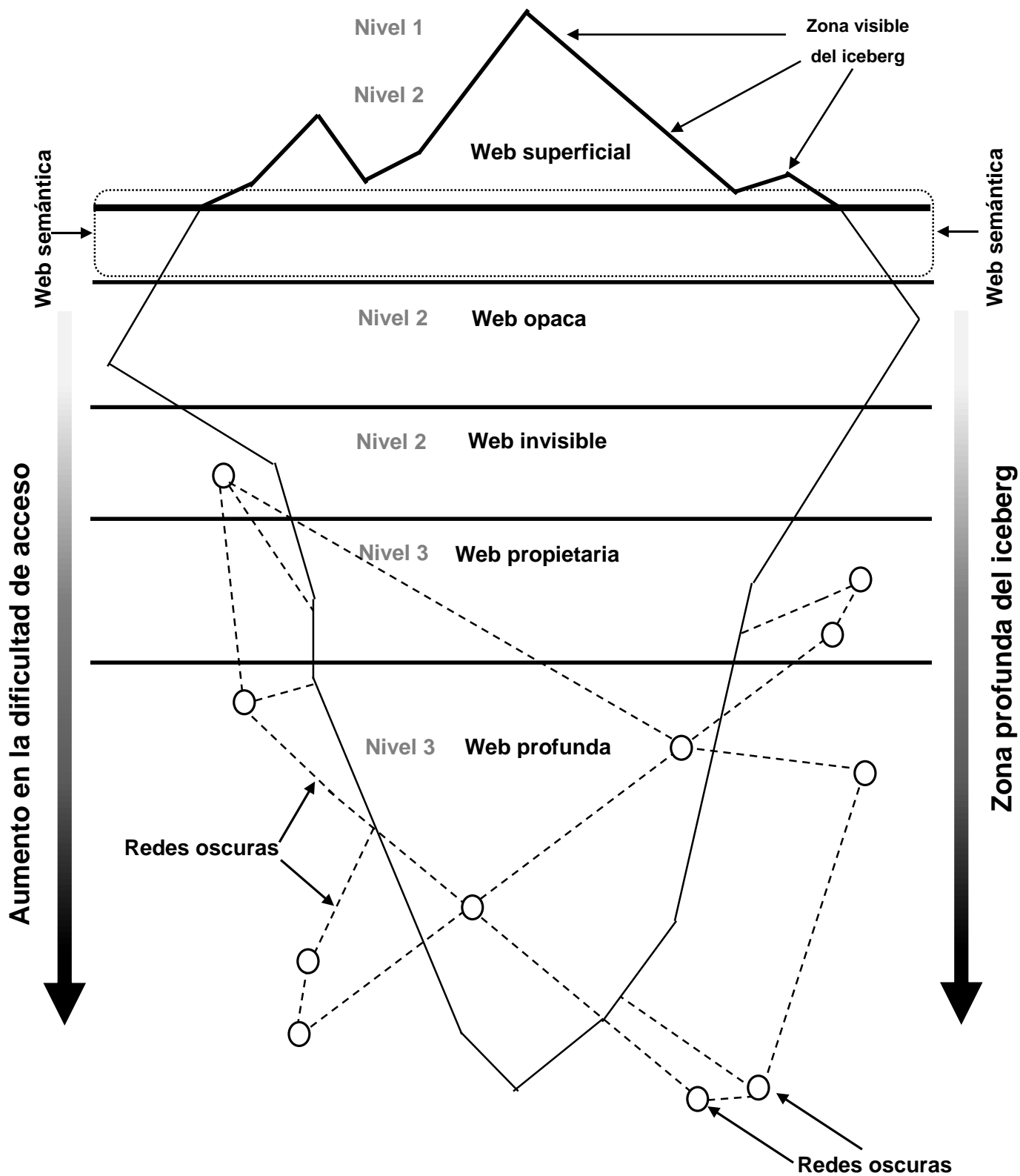
Esquema 3. Traducción de esquema de la deep web en sus diferentes niveles.
 Fuente: creación propia a partir de la imagen postzada: Valenzuela Medina, Luis. 2012.
 Deep web - Lo que hay del otro lado de la red. La balada de Quiro. Recuperado en:
http://labaladadequiro.blogspot.mx/2012_06_01_archive.html [Consultado 24 de julio de 2013]

Finalmente se presenta un cuarto esquema, a manera de propuesta, el diseño se fundamenta con base en la documentación acerca de la estratificación de la Web y las *redes oscuras*. Se utiliza la metáfora del iceberg del tercer esquema con el objetivo de optimizar la imagen más representativa del concepto bajo la percepción social de la supuesta *web profunda*.

- El cuarto esquema se enfoca en mostrar de manera gráfica la visibilidad y la posibilidad de acceso a las *redes oscuras*, por lo que si se tuviera que plantear una conceptualización gráfica acerca de los distintos tipos de web según su estratificación, las *redes oscuras* se encontrarían en la parte más profunda de dicha estratificación visual, puesto que no forman parte de la *web profunda*, *web propietaria*, *web opaca* o *web invisible* sin embargo poseen el atributo de ser (en cierta medida) inaccesibles para el usuario común. El presente esquema se enfoca en la estratificación de la Web de acuerdo a los 3 niveles de visibilidad 1) **disponibilidad**, 2) **acceso parcial** y 3) **acceso restringido**.

Las *redes oscuras* se encuentran aisladas de la parte inferior del iceberg. Estas *redes oscuras* son un sistema de comunicación, almacenamiento de contenidos y transmisión de paquetes de información ocultos de toda visibilidad en la *web superficial*.

Como primer elemento a distinguirse en el cuarto esquema, es la adición de las *redes oscuras*, las cuales están constituidas por líneas punteadas, dichas líneas representan la autonomía y la comunicación de las *redes oscuras*. En la parte superior del iceberg se localiza la *web superficial* como todo aquel conjunto de sitios, servicios, recursos y contenidos visibles, los cuales en su mayor parte se encuentran disponibles para el usuario. Por su parte, la *web semántica* coadyuva (en la medida de lo posible) a la visibilidad de la *web opaca* con la finalidad de optimizar y crear conexiones temáticas en la Web.



Esquema 4. La metáfora del iceberg: niveles de acceso y visibilidad. Fuente: creación propia a partir de las teorías de la estratificación y los esquemas anteriores.

2.3.1 The onion routing network: **T o r**

The onion routing (**Tor**)²¹⁶ castellanizado como «el proyecto de enrutamiento de la cebolla», recibe su nombre en alusión a las capas de una cebolla roja,²¹⁷ en donde cada capa cubre a las otras. La metáfora se vincula a las capas que protegen los datos de transferencia en **Tor**. Los orígenes de este proyecto comienzan en el año de 1996,²¹⁸ en donde se inician los experimentos de cifrado para ocultar el origen del equipo conectado a una red.

Es al paso de los siguientes años a raíz de los acontecimientos históricos relacionados al terrorismo, que los gobiernos comienzan a tomar cartas en el asunto. David Lyon²¹⁹ comenta que, los atentados del 11 de septiembre del año 2001 en los Estados Unidos de América, fueron un catalizador para los sistemas de vigilancia por parte de los gobiernos, con el objetivo primordial de estudiar e identificar los patrones de comportamiento en los ciudadanos. En este tenor Richard Rubin²²⁰ anota que, los atentados del 2001 propiciaron modificaciones al sistema de seguridad nacional y vigilancia de los Estados Unidos de América. Consecuentemente, para el año 2002 la versión de prueba de **Tor** que fue desarrollada por Roger Dingledine, Nick Mathewson y Paul Syverson²²¹ es liberada para su descarga y uso masivo.

Desde el 2004 y por un periodo de aproximadamente un año, la fundación sin fines de lucro *Electronic Frontier Foundation*,²²² comenzó a patrocinar a **Tor** para defender tanto la libertad de expresión en respuesta a la vigilancia por parte de

²¹⁶ The onion router. 2016. Why is it called Tor? **Tor**. Recuperado en: <https://www.torproject.org/docs/faq.html.en#WhyCalledTor> [Consultado 28 de enero de 2016]

²¹⁷ Carballude González, Pablo. "Fingerprinting Tor". *Information Management & Computer Security* 21, no. 2 (2013): Recuperado en: <http://www.emeraldinsight.com/journals.htm?articleid=17090719> [Consultado 28 de enero de 2016]

²¹⁸ Syverson, Paul. 2013. Onion Routing. *Onion Router*. Recuperado en: <http://www.onion-router.net/> [Consultado 28 de enero de 2016]

²¹⁹ Lyon, David. *Identifying citizens: ID cards as surveillance*. (Cambridge, United Kingdom: Polity, 2009). Pág. 54

²²⁰ Rubin, Richard E. Ídem. Pág. 129

²²¹ Dingledine, Roger. 2002. Pre-alpha: run an onion proxy now! *Archives Seul*. Recuperado en: <http://archives.seul.org/or/dev/Sep-2002/msg00019.html> [Consultado 28 de enero de 2016]

²²² Palmer, Chris. 21 de diciembre de 2004. EFF Joins Forces with Tor Software Project. *Electronic Frontier Foundation*. Recuperado en: <https://www.eff.org/press/archives/2004/12/21-0> [Consultado 28 de enero de 2016]

los *Estados-naciones*. En el año 2010,²²³ **Tor** es reconocido por la *Free Software Foundation*, fundación que busca alentar el uso y desarrollo del software libre.

2.3.2 Funcionamiento

Tor funciona por medio de una red de servidores y computadoras personales conectadas a Internet. La particularidad en la dinámica de la navegación con **Tor** en la *web superficial* radica esencialmente en modificar la dirección IP pública,²²⁴ siempre y cuando el usuario utilice la interfaz de navegación (Tor browser). Por otro lado, el usuario no puede acceder a todos los servicios de la *web superficial* a través de **Tor**, puesto que existen mecanismos de seguridad que solicitan ciertos protocolos de origen para cotejar si se trata de un usuario o un programa informático capaz de simular el comportamiento de navegación de un usuario.

El funcionamiento de **Tor** puede ser conceptualizado como un laberinto en constante cambio. El laberinto o circuito en cuestión está conformado por puntos de conexión, tales como servidores y computadoras convencionales dedicadas a la administración de los enlaces. Lucian Constantin²²⁵ señala que, sólo el punto de conexión actual conoce el punto anterior y el siguiente, no obstante dicho punto desconoce la totalidad de la conexión del resto de los puntos. Nicole Arce²²⁶ argumenta que, a pesar de que pueden proliferar los puntos de conexión, son vulnerables a ser neutralizados o eliminados por las agencias del gobierno o grupos dedicados a vulnerar sistemas.²²⁷

²²³ Sullivan, John. 2011. 2010 Free Software Awards announced. *Free Software Foundation*. Recuperado en: <https://www.fsf.org/news/2010-free-software-awards-announced> [Consultado 28 de enero 2016]

²²⁴ The onion router. 2016. Don't enable or install browser plugins. **Tor**. Recuperado en: <https://www.torproject.org/download/download.html.en> [Consultado 28 de enero 2016]

²²⁵ Constantin, Lucian. Ibíd. Recuperado en: http://www.csoonline.com/article/3024779/security/privacy-conscious-users-rejoice-you-can-now-use-facebooks-android-app-over-tor.html#tk.rss_all [Consultado 23 de enero de 2016]

²²⁶ Arce, Nicole. 27 de diciembre de 2014. Anonymous to Lizard Squad: Keep Your Hands off Tor. *Tech times*. Estados Recuperado en: <http://www.techtimes.com/articles/23248/20141227/anonymous-to-lizard-squad-keep-your-hands-off-tor.htm> [Consultado 30 de diciembre de 2014]

²²⁷ RT. 12 de noviembre de 2015. Tor Project accuses FBI of paying university to 'deanonymize' users without warrant. *RT*. Recuperado en: <https://www.rt.com/usa/321756-tor-project-fbi-cmu-attack/> [Consultado 23 de diciembre de 2016]

Armando Becerra²²⁸ menciona que, algunos usuarios deciden ceder parte de su ancho de banda para el uso de la red **Tor** a nivel mundial. Mientras que Ilya Khrennikov²²⁹ manifiesta que, la red encamina el tráfico de cada usuario a través de varios puntos de conexión distribuidos en el planeta. De modo que, se puede interpretar que esta solidaridad es un conjunto de saberes y recursos anónimos sin fines de lucro.

En esencia **Tor** es un software que permite crear una *red oscura* entre sus usuarios, la cual está integrada por distintas computadoras personales y servidores distribuidos en el planeta, con el objetivo de diseminar el rastro de navegación, origen y destino de los datos y, la identidad del equipo de cómputo (la computadora personal).²³⁰

2.3.3 Usuarios

Los usuarios de **Tor** no solamente son terroristas, para Lucian Constantin²³¹ la *red oscura* es útil para los periodistas, activistas e individuos que no pueden acceder a ciertos contenidos en su país. Pero también es de utilidad para los proveedores de productos ilegales,²³² al igual que los contrabandistas.²³³ **Tor** también puede llegar a ser utilizado por los usuarios avanzados, los cuales deshabilitan el bloqueo de los Proveedores del Servicio de Internet (ISP) para acceder a servicios y contenidos restringidos. Por otro lado la *red Tor*, es de utilidad para los departamentos de policía, profesionales del mercado de valores,

²²⁸ Becerra, Juan. *Ibíd.* Recuperado en: <http://revista.seguridad.unam.mx/numeros/numero-20> [Consultado 3 de agosto de 2015]

²²⁹ Khrennikov, Ilya. 29 de julio de 2014. Putin Sets \$110,000 Bounty for Cracking Tor as Anonymous Internet Usage in Russia Surges. **Bloomberg**. Recuperado en: <http://www.bloomberg.com/news/2014-07-29/putin-sets-110-000-bounty-for-cracking-tor-as-anonymous-internet-usage-in-russia-surges.html> [Consultado 3 de agosto de 2014]

²³⁰ Tic beat. 16 de febrero de 2015. La red anónima TOR, en peligro de ciberataques en 2015. **Tic beat**. Recuperado en: http://www.ticbeat.com/seguridad/la-red-anonima-tor-en-peligro-de-ciberataques-en-2015/?utm_content=buffercb547&utm_medium=social&utm_source=twitter.com&utm_campaign=buffer [Consultado 11 de julio de 2015]

²³¹ Véase Marin, Eduardo. 25 de noviembre de 2015. Anonymous comienza a eliminar la propaganda a favor de ISIS en la dark web. **Gizmodo en español**. Recuperado en: <http://es.gizmodo.com/anonymous-comienza-a-eliminar-la-propaganda-a-favor-de-1744630985> [Consultado 19 de octubre de 2015] y Constantin, Lucian. *Ibíd.* Recuperado en http://www.csoonline.com/article/3024779/security/privacy-conscious-users-rejoice-you-can-now-use-facebooks-android-app-over-tor.html#tk.rss_all [Consultado 23 de enero de 2016]

²³² RT. *Ibíd.* Recuperado en: <https://www.rt.com/usa/321756-tor-project-fbi-cmu-attack/> [Consultado 23 de diciembre de 2016]

²³³ Tic beat. *Loc. Cit.*

profesionales en las tecnologías de información e incluso para la Marina de los Estados Unidos de América (por sus siglas en inglés USN).²³⁴

En la *red oscura Tor*, es probable que el usuario común se encuentre a merced de los *Crackers*, los cuales como se ha mencionado anteriormente sólo están interesados en vulnerar la seguridad informática para lucrar con la ingenuidad y carencia de conocimiento informático de otros usuarios. En este aspecto de la vulnerabilidad, el *Ciberdepredador* puede llegar a tener atributos de *Cracker* o simplemente puede adoptar un personaje de bajo perfil para recolectar información sobre sus víctimas potenciales, como el *Phisher*.

2.3.4 Niveles de acceso

La información acerca de los niveles de acceso de lo que socialmente se conoce en la *web superficial* sobre *Tor* suele estar orientada hacia la ambigüedad, la perversidad y el misterio sobre sus contenidos, así como la dificultad de acceso.²³⁵ Por otro lado existen discrepancias sobre dicha información²³⁶ de modo que, este panorama pone en duda la veracidad sobre las experiencias de navegación en los niveles más profundos, puesto que la información es similar y tiende a ser somera.²³⁷

De acuerdo a la literatura sobre la supuesta *web profunda* y la literatura de las *redes oscuras* se puede interpretar que, en *Tor* no existe un sistema de niveles jerárquicos como tal, ya que la estructura de acceso se fundamenta en el grado de visibilidad y difusión que posean los contenidos y servicios de la *red oscura*, es decir que además de la carencia de visibilidad hay restricciones de acceso en

²³⁴ The onion router. 2016. Inception. *Tor*. Recuperado en: <https://www.torproject.org/about/torusers.html.en> [Consultado 28 de enero de 2016]

²³⁵ Self.deepweb. 2015. *Does the internet really have 8 layers/levels?* *Reddit*. Recuperado en: https://www.reddit.com/r/deepweb/comments/35ei8s/does_the_internet_really_have_8_layerslevels/ [Consultado 30 de enero de 2016]

²³⁶ Keerthi, Rahul. 2015. What is the Marianas web? *Quora*. Recuperado en: <https://www.quora.com/What-is-the-Marianas-web> [Consultado 30 de enero de 2016]

²³⁷ Enriquekpo. 2013. Mi experiencia en la DeepWeb y los niveles 5, 6, 7 y 8. *Taringa*. Recuperado en: <http://www.taringa.net/posts/info/16786901/Mi-experiencia-en-la-DeepWeb-y-los-niveles-5-6-7-y-8.html> [Consultado 30 de enero de 2016]

donde se requiere un registro previo o bien de un nombre de usuario y contraseña de acceso, como es el caso del mercado negro.²³⁸ Por otro lado, lo que vendría siendo la parte más inaccesible de la *red oscura* considerada para algunos usuarios como la zona más profunda en visibilidad y acceso, son las *Marianas web*²³⁹ un conjunto de sitios, contenidos y herramientas digitales completamente inaccesibles para cualquier tipo de usuario común. Mariana Cortez²⁴⁰ agrega que, el nombre de *Marianas web* se debe al lugar más profundo del planeta. La fosa de las Marianas se encuentra ubicada geográficamente en el pacífico occidental, cerca de la isla de Guam.²⁴¹

A pesar de que no hay pruebas sólidas sobre la existencia de las *Marianas web*, la idea sobre el acceso al núcleo del control informático, se asemeja a lo que John Vaca²⁴² describe como la guerra de la información, la cual implica desactivar la infraestructura electrónica de un *Estado-nación*, en donde los adversarios en cuestión pueden acceder a los servidores que controlan la operatividad electrónica y lógica de un gobierno. Sin embargo, Tom Simonite²⁴³ hace énfasis en que, algunas empresas carecen de políticas de información y mantienen malas prácticas en no reforzar la seguridad de sus servidores centrales y por tanto, se expone la información relacionada a datos personales y transacciones bancarias.

²³⁸ Howell O'Neill, Patrick. 4 de marzo de 2014. I made my own Deep Web black market, and it took just 60 seconds.

DeepIstweb. Recuperado en: <http://www.dailydot.com/business/deepify-make-your-own-deep-web-black-market/> [Consultado 30 de enero de 2016]

²³⁹ Ist sara. 25 de noviembre de 2014. Deep Web - casos reales. **DeepIstweb.** Recuperado en: <http://deepIstweb.blogspot.mx/2014/11/mariana-web.html> [Consultado 30 de enero de 2016]

²⁴⁰ Cortez, Mariana. 2015. Mariana's Web. **Revistas Bolivianas.** Recuperado en: http://www.revistasbolivianas.org.bo/pdf/rits/n9/n9_a14.pdf [Consultado 30 de enero de 2016]

²⁴¹ Than, Ker. 25 de marzo de 2012. James Cameron completes record-breaking mariana trench dive. **National Geographic.** Recuperado en: <http://news.nationalgeographic.com/news/2012/03/120325-james-cameron-mariana-trench-challenger-deepest-returns-science-sub/> [Consultado 30 de enero de 2016]

²⁴² Vaca, John R. **Los secretos de la seguridad en internet.** Traducido por Marcos Sagrado. (España: Anaya Multimedia, 1997). Pág. 714

²⁴³ Simonite, Tom. 7 de agosto de 2015. Los datos más sensibles se guardan en los ordenadores más vulnerables. **Technology review.** Recuperado en: <http://www.technologyreview.es/informatica/47938/los-datos-mas-sensibles-se-guardan-en-los/> [Consultado 10 de agosto de 2015]

2.4 Riesgos de consulta y acceso

El acceso a la *red oscura* proporciona anonimato y cierta privacidad, aun así cabe señalar que los servicios y productos ofrecidos no carecen de dudosa procedencia. La información consultada en la *red Tor* no es sinónimo de garantía, puesto que los servicios y productos pueden llegar a ser falsos con el único fin de atraer a los curiosos e ingenuos. Por ello, es preciso hacer mención en la importancia de un servicio regulado por las instancias correspondientes y sólo entonces bajo estas circunstancias es viable obtener garantías como usuario en la adquisición de productos en línea. En cuanto a las *redes oscuras*, su valor principal es el hecho de adquirir algo ilegal o prohibido, ya sea un contenido o producto censurado, pero también una experiencia clandestina.

2.4.1 El arte de la duda

El acceso a Internet y a la creación de contenidos tales como blogs en línea, plataformas para la difusión de contenidos audiovisuales, sitios web, foros, enciclopedias colectivas, entre otros, ha favorecido la proliferación en la consulta de la información en línea, en este punto Liu Ziming²⁴⁴ menciona que, los bajos costos para la publicación de los contenidos en la Web crean un problema en la revisión en cuanto a la veracidad de la información, como es el caso de los foros, blogs y wikis. Nicholas Carr²⁴⁵ agrega en este aspecto que, los contenidos digitales se han incrementado debido a la preferencia de los usuarios por la inmediatez de adquisición y consumo.

Peter Herson²⁴⁶ por su parte señala que, en la Web existe información con errores e intencionalmente falsa, Ana Martos²⁴⁷ se suma a esta postura y añade que, es común encontrar datos históricos incorrectos así como literatura

²⁴⁴ Ziming, Liu. "The evolution of documents and its impacts". *Journal of Documentation* 60, no. 3 (2004): 279-288. Recuperado en: <http://www.emeraldinsight.com/journals.htm?articleid=864247&show=html> [Consultado 30 de enero de 2016]

²⁴⁵ Carr, Nicholas. *¿Qué está haciendo internet con nuestras mentes?* Traducido por Pedro Cifuentes. (México: Taurus, 2011). Pág. 113

²⁴⁶ Herson, Peter. *U.S. government on the Web: getting the information you need*. (Estados Unidos: Libraries Unlimited, 2003). Pág. 18

²⁴⁷ Martos Rubio, Ana. Ídem. Pág. 42

científica sin respaldo editorial o con discrepancias en el desarrollo de la investigación. Inclusive, para Federico Di Trocchio,²⁴⁸ los científicos profesionales pueden llegar a presentar resultados confusos en sus investigaciones. A lo que Mayelín Travieso²⁴⁹ adiciona que, en la Web pueden existir contenidos complejos que a pesar de tener un alto grado de visibilidad y disponibilidad para los usuarios, estos mismos contenidos científicos no pueden ser comprendidos e interpretados por cualquier individuo, por lo que existe un problema de acceso conceptual.

De lo mencionado anteriormente, se puede deducir que si en la *web superficial* y en las revistas académicas arbitradas existe la posibilidad de encontrar inconsistencias así como cierta carencia en la transparencia de sus contenidos; las *redes oscuras* como **Tor**, pueden alojar contenidos muy ilustrativos pero también es probable encontrar información superflua y falsa.

2.4.2 El marco de la legalidad

Cuando un usuario realiza la navegación en los sitios con servicios y contenidos ilícitos es potencialmente sospechoso de un acto delictivo, pero al no haber alguna transacción de compra y venta no se está cometiendo ninguna clase de delito.²⁵⁰ Sin embargo todo ello depende del código penal de cada país.²⁵¹ En el caso de la pornografía infantil, el usuario puede comenzar a ser monitoreado por las autoridades policiales a pesar de no haber descargado contenidos a su computadora personal.²⁵²

²⁴⁸ Di Trocchio, Federico. *Las mentiras de la ciencia: por qué y cómo engañan los científicos*. Traducido por Constanza V. (Madrid: Alianza, 1998). Pág. 7

²⁴⁹ Travieso Aguilar, Mayelín. *Ibid.* Recuperado en: <http://eprints.rclis.org/5101/1/publicaciones.pdf> [Consultado 4 de febrero de 2016]

²⁵⁰ Véase Spotz, Kenny. 12 de agosto de 2014. Lo que he aprendido como traficante de drogas de Internet. *Motherboard*. Recuperado en: <http://motherboard.vice.com/es/read/lo-que-he-aprendido-siendo-traficante-de-drogas-en-internet> [Consultado 19 de diciembre de 2015]. y Becerra, Juan Armando. Programa de radio transmitido el 23 de noviembre de 2015. *Deep Web, un lugar para bucear*. Resistencia modulada, Radio UNAM.

²⁵¹ Franganillo, Marina. 15 de junio de 2015. Cuando buscar en Google se convierte en un delito. *El diario*. Recuperado el 1 de febrero de 2016, en: http://www.eldiario.es/hojaderouter/ilegales/Google-busquedas-delito-conspiracion-provocacion-tentativa_6_397620277.html [Consultado 19 de diciembre de 2015]

²⁵² Whitley, Susie. 12 de enero de 2007. Prison time for viewing porn? *ABC News*. Recuperado en: <http://abcnews.go.com/2020/LegalCenter/prison-time-viewing-porn/story?id=2785054> [Consultado 1 de febrero de 2016]

Además de la navegación, el simple hecho de arrendar espacios virtuales y facilitar la transferencia de los contenidos ilícitos es causa de la investigación y detención policial, a pesar de ello, **Tor** no es una red utilizada únicamente para cometer actos delictivos.²⁵³

Alberto Sánchez²⁵⁴ comenta que, la Oficina Europea de Policía (Europol), junto con el órgano de la Unión Europea llamado Eurojust y el Departamento de Justicia de los Estados Unidos de América (por sus siglas en inglés DOJ) son las autoridades internacionales con la capacidad de coordinar investigaciones, incautaciones y detenciones sobre los servicios y contenidos ilícitos a nivel internacional. En México, el Centro Nacional de Respuesta a Incidentes Cibernéticos (CERT-MX)²⁵⁵ es la división científica responsable sobre el monitoreo, seguridad, investigación y delitos electrónicos.

Otro aspecto a mencionar es que al adquirir un equipo de cómputo, teléfono inteligente (smartphone), tableta (tablet), netbook o laptop mediante la compra en línea o bien de forma presencial en algún centro de venta, se genera en el historial del cliente al momento de realizar el pago con la tarjeta de crédito, un vínculo con el número de serie del producto junto con los datos personales del comprador. Por lo que puede ser de utilidad para cualquier aclaración relacionada a los procesos jurídicos; aunque también dicho registro de compra, puede considerarse como un factor para determinar hallazgos, evidencias o pruebas de algún delito informático.

²⁵³ Véase BBC. 30 de noviembre de 2012. Austrian police raid privacy network over child porn. **BBC News**. Recuperado en: <http://www.bbc.com/news/technology-20554788> [Consultado 9 de enero de 2015]. y Télam. 25 de julio 2014. Rusia ofrece 110 mil dólares al que logre hackear la red anónima Tor. **Télam: Agencia nacional de noticias**. Recuperado en: <http://www.telam.com.ar/notas/201407/72368-rusia-ofrece-110-mil-dolares-al-que-logre-hackear-la-red-anonima-tor.html> [Consultado 5 de agosto de 2014]

²⁵⁴ Sánchez, Alberto. 12 de noviembre de 2014. 17 detenidos en la operación ONYMOUS contra el crimen organizado en la Deep Web. **Hipertextual**. Recuperado en: <http://hipertextual.com/2014/11/onymous-deep-web> [Consultado 21 de diciembre de 2014]

²⁵⁵ Diario 24 horas. 12 de marzo de 2012. Vigila policía federal red informática del país. **Diario 24 horas**. Recuperado en: <http://www.24-horas.mx/vigila-policia-federal-red-informatica-del-pais/> [Consultado 10 de enero de 2014]

En síntesis se puede interpretar que, al haber una apertura en el acceso a los contenidos, existe la probabilidad de que estos no se encuentren regulados o soportados por alguna instancia y ello derive en errores o accidentes al momento de poner en práctica la información adquirida,²⁵⁶ De modo que, se manifiesta ante el acceso conceptual; el criterio para la interpretación y el análisis de los contenidos. También existen riesgos al instalar software propietario alterado por terceros para su operatividad gratuita, puesto que nada es gratis.

2.5 Servicios, productos y contenidos

Óscar de la Cruz Yagüe²⁵⁷ jefe del Grupo de Delitos Telemáticos de la Guardia Civil (en España) comenta que, se han dado casos en que los servicios referentes a la contratación de sicarios, venta de órganos y armas de fuego tienen el objetivo de estafar a los usuarios que acceden a esta clase de servicios ilícitos. Por otro lado, José Antonio Álvarez Bermejo²⁵⁸ profesor de la asignatura de Arquitectura y Tecnología de Computadores en la Universidad de Almería, menciona que, existen ciertos grupos de usuarios que se interesan en temas de interés privado a los que sólo se puede acceder por medio de una invitación. A lo que Santiago Camacho²⁵⁹ añade que, dichos actos privados son útiles para la venta de arte robado.

En cuanto a los productos más comunes se encuentran las drogas como el cannabis o marihuana,²⁶⁰ elaborada con distintos elementos tanto naturales como químicos. Las falsificaciones de armas de fuego²⁶¹ así como las armas modificadas²⁶² las cuales son productos que suelen encontrarse en **Tor**. Kristin

²⁵⁶ Véase Revilla, Ángel David. 12 de febrero de 2014. Los cristales de 4chan. Episodio 22. **DrossRotzank**. Recuperado en: <https://www.youtube.com/watch?v=P7pdXv1BS7U> [Consultado 26 de junio de 2016] y Imgur. 2013. How to grow crystals. **Imgur**. Recuperado en: <http://imgur.com/gallery/BuF31> [Consultado 26 de junio de 2016]

²⁵⁷ Falla, Fernando (Conductor). 7 de abril de 2013. Los huesos de nadie. Episodio 30. **Cuarto milenio**. Recuperado en: <http://fansmilenio3.com/cuarto-milenio-8x30-los-huesos-de-nadie-07042013/> [Consultado 29 de febrero de 2016]

²⁵⁸ *Ibíd.*

²⁵⁹ *Loc. Cit.*

²⁶⁰ Gamella, Juan y Álvarez, Arturo. **Las rutas del éxtasis: drogas de síntesis y nuevas culturas juveniles**. (Barcelona: Ariel, 1999). Pág. 80

²⁶¹ Wilhoit, Kyle y Hilt, Stephen. *Ibíd.* Recuperado en: <http://www.trendmicro.com/cloud-content/us/pdfs/security-intelligence/white-papers/wp-north-american-underground.pdf> [Consultado 21 de diciembre de 2015]

²⁶² Labrousse, Alain. **La droga, el dinero y las armas**. (México: Siglo XXI, 1993). Pág. 52

Finklea²⁶³ hace mención que, los delincuentes dependen cada vez más del servicio de Internet para perpetrar sus actividades. En este sentido Siddharth Kara²⁶⁴ comenta que, los grupos delictivos en la trata de personas pueden llegar a utilizar los servicios digitales para la adquisición ilícita de pasaportes falsos²⁶⁵ en las *redes oscuras*.

Los contenidos que se ofrecen en la *red oscura Tor* se enfocan concretamente en los datos personales y datos financieros.²⁶⁶ Por otro lado, Para Kristin Finklea²⁶⁷ la exhibición de la pornografía infantil es un tema muy delicado para las autoridades en seguridad, ya que existen sitios que sólo son vistos en una ocasión y no pueden volverse a recuperar para dar seguimiento a la investigación. Por su parte Santiago Camacho²⁶⁸ señala que, los contenidos comercializados sobre la tortura, los asesinatos y las ejecuciones son parte de las tendencias en la difusión del poder y la violencia de cárteles latinoamericanos y grupos extremistas de medio oriente.

Autores como Cale Guthrie (A),²⁶⁹ Charles McFarland, François Paget y Raj Samani (B),²⁷⁰ Amaya Quincoces (C),²⁷¹ Hiroshi Takahashi (D),²⁷² Kyle Wilhoit y

²⁶³ Finklea, Kristin. *Ibíd.* Recuperado en: <https://www.fas.org/sgp/crs/misc/R44101.pdf> [Consultado 30 de septiembre de 2016]

²⁶⁴ Kara, Siddharth. *Tráfico sexual: el negocio de la esclavitud moderna*. Traductor Dimitri Fernández. (Madrid: Alianza, 2010). Pág. 28

²⁶⁵ Wilhoit, Kyle y Hilt, Stephen. *Loc. Cit.*

²⁶⁶ Véase Alonso, Chema. 9 de agosto de 2014. Ganar dinero con 1.200 Millones de identidades robadas. *El lado del mal*. Recuperado en: <http://www.elladodelmal.com/2014/08/ganar-dinero-con-1200-millones-de.html> [Consultado 10 de agosto de 2014] y Finklea, Kristin. *Ibíd.* Recuperado en: <https://www.fas.org/sgp/crs/misc/R44101.pdf> [Consultado 30 de septiembre de 2016]

²⁶⁷ Ward, Mark. 2 de enero de 2015. Drogas y pornografía, los sitios más populares en la red oscura. *BBC*. Recuperado en: http://www.bbc.com/mundo/noticias/2015/01/141231_tecnologia_tor_red_oscura_paginas_populares_trafico_ig [Consultado 12 de julio de 2015]

²⁶⁸ Falla, Fernando (Conductor). *Ibíd.* Recuperado en: <http://fansmilenio3.com/cuarto-milenio-8x30-los-huesos-de-nadie-07042013/> [Consultado 29 de febrero de 2016]

²⁶⁹ Guthrie, Cale. 8 de mayo de 2015. 9 things you can hire a hacker to do and how much it will (generally) cost. *Search data center*. Recuperado en: <http://www.businessinsider.com/9-things-you-can-hire-a-hacker-to-do-and-how-much-it-will-generally-cost-2015-5?op=1> [Consultado 17 de mayo de 2015]

²⁷⁰ McFarland, Charles., Paget, François y Samani, Raj. *Data economy, the Marketplace for stolen digital information*. (Estados Unidos: Intel Security Group, 2015). Recuperado en <http://www.mcafee.com/us/resources/reports/rp-hidden-data-economy.pdf> [Consultado 18 de enero de 2016]

²⁷¹ Quincoces, Amaya. 2 de agosto de 2015. Internet profundo: el mundo ilegal en la Web. *Sin embargo*. Recuperado en: <http://www.sinembargo.mx/02-08-2015/1435895> [Consultado 3 de agosto de 2015]

²⁷² Takahashi, Hiroshi. "La mafia digital secuestra México". *Revista emeequis*, no. 51 (2015): 42-51

Stephen Hilt (E),²⁷³ Andy Greenberg (F)²⁷⁴ y algunos sitios web como DTIC Editores (G)²⁷⁵ y SlashDot (H)²⁷⁶ han publicado algunos precios de los servicios, productos y contenidos más populares en el mercado negro de la *redes oscuras*. En la siguiente tabla se elaboró un concentrado sobre los productos y contenidos en el mercado negro de las *redes oscuras* del periodo 2014-2015.

Referencia	Servicios y productos	Precio en dólar
(A)	Contraseñas de Netflix	USD\$2.00
(A)	Cifrado y descifrado parcial de datos para vulnerar sistemas	USD\$5.00
(A)	Lecciones de ataques sencillos	USD\$20.00
(B)	Tarjetas de crédito (claves de acceso)	USD\$45.00
(A)	Acceso a cuentas de Gmail	USD\$90.00
(C)	Cuenta robada de eBay o PayPal	USD\$110.00
(B)	Acceso a cuentas bancarias	USD\$190.00
(A)	Eliminar críticas negativas y poner criticas favorables	USD\$350.00
(G)	Herramienta de acceso remoto	USD\$1000.00
(A)	Acceder a un sitio Web, como administrador	USD\$2000.00
(D)	Membresía mensual y servicio de soporte para herramientas de infección digital	USD\$3000.00
(C)	Pasaportes falsos	USD\$6000.00
(H)	Exploit para iCloud	USD\$17,000.00
(A)	Acceder a cuentas de Facebook	USD\$20,000.00
(E)	Servicio de asesinato de personas comunes	USD\$45,000.00
(F)	Sistema operativo para iOS	USD\$250,000.00
(E)	Servicio de asesinato de personas públicas	USD\$300,000.00

Tabla 10. Precios de productos, servicios y acceso en el mercado negro de la web profunda. Fuente: creación propia.

²⁷³ Wilhoit, Kyle y Hilt, Stephen. *North American underground: the glass Tank*. (Estados Unidos: Trend Micro, 2015). Recuperado en: <http://www.trendmicro.com/cloud-content/us/pdfs/security-intelligence/white-papers/wp-north-american-underground.pdf> [Consultado 21 de diciembre de 2015]

²⁷⁴ Greenberg, Andy. 17 de abril de 2015. New Dark-Web Market Is Selling Zero-Day Exploits to Hackers. *Wired*. Recuperado en: <http://www.wired.com/2015/04/therealdeal-zero-day-exploits/> [Consultado 12 de julio de 2015]

²⁷⁵ DTIC Editores. 29 de julio de 2014. Trustwave presenta precios de Malware en el mercado negro. *Securitic*. Recuperado en: <http://www.securitic.com.mx/noticias/1073-trustwave-presenta-precios-de-malware-en-el-mercado-negro> [Consultado 1 de agosto de 2014]

²⁷⁶ SlashDot. 28 de mayo de 2015. The real deal market: venta de exploit en la Deep Web. *Segu Info*. Recuperado en: <http://blog.segu-info.com.ar/2015/05/therealdeal-market-venta-de-exploit-en.html> [Consultado 12 de julio de 2015]

Una de las formas más comunes de pagar por el servicio, producto o contenido es mediante el *Bitcoin*,²⁷⁷ el cual funge como una moneda digital descentralizada de la economía mundial, con el *Bitcoin* es viable realizar transferencias y pagos de forma anónima. Andy Greenberg²⁷⁸ añade que, el *Bitcoin* es utilizado en el mercado negro, como moneda de cambio.

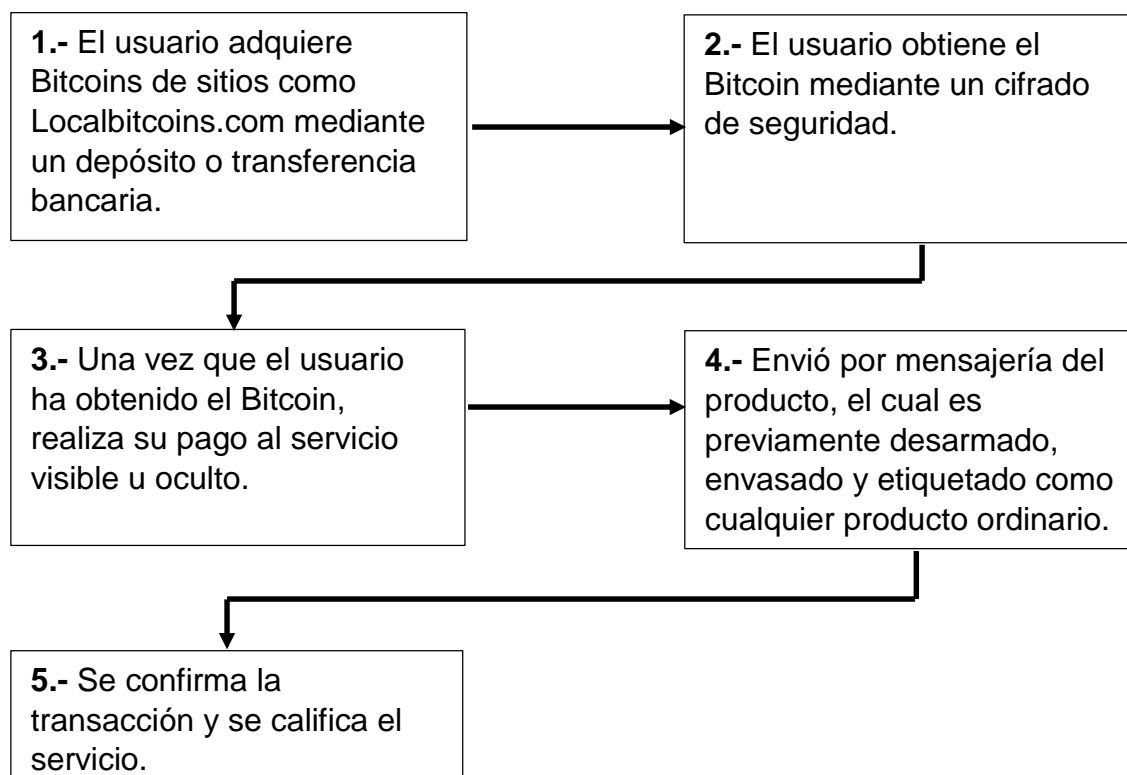


Figura 5. Proceso de pago para la adquisición de servicios, productos y contenidos. Fuente: Traducción libre y creación propia a partir de: Wilhoit, Kyle y Hilt, Stephen. North American underground: the glass Tank. (Estados Unidos: Trend Micro, 2015). Recuperado en: <http://www.trendmicro.com/cloud-content/us/pdfs/security-intelligence/white-papers/wp-north-american-underground.pdf> [Consultado 21 de diciembre de 2015]

²⁷⁷ Bitcoin. 2015. Bitcoin es una innovadora red de pagos y una nueva clase de dinero. *Bitcoin*. Recuperado en: <https://bitcoin.org/es/> [Consultado 30 de enero de 2016]

²⁷⁸ Greenberg, Andy. 17 de abril de 2015. New Dark-Web Market Is Selling Zero-Day Exploits to Hackers. *Wired*. Recuperado en: <http://www.wired.com/2015/04/therealdeal-zero-day-exploits/> [Consultado 12 de julio de 2015]

2.5.1 Consecuencias psicológicas de los servicios, contenidos y productos

La curiosidad y el miedo juegan un papel determinante en la conducta del individuo, puesto que al existir elementos misteriosos, ocultos y secretos el ser humano es impulsado por la duda y el deseo de conocer. Carlo Mongardini²⁷⁹ explica que, el individuo busca el insumo informativo pero al mismo tiempo no soporta las consecuencias en asimilar la experiencia o, de poseer el conocimiento, puesto que ello implica atenerse al canon social y las leyes que lo limitan para hacer uso del conocimiento adquirido.

A este respecto Thorstein Veblen²⁸⁰ agrega que, las clases sociales marginadas se limitan a observar y si es posible a imitar el comportamiento de las clase ociosa. La clase ociosa es aquella sociedad beligerante con acceso a los recursos, la cual busca nuevas experiencias, «una más intensa a la anterior», señala el autor. En las *redes oscuras* como en la *web superficial*, existe una variedad de servicios, productos y contenidos enfocados al aprendizaje y el entretenimiento, no obstante no todos pueden acceder a ellos.

Los usuarios que acceden a los contenidos de las *redes oscuras* pueden ser víctimas de algún tipo de representación gráfica o audiovisual de carácter desagradable, el cual posteriormente podría derivar en un trauma. Respecto a este asunto Aida Alayarian²⁸¹ comenta que, un trauma emocional puede ser producto de alguna experiencia desagradable, aunque el autor aclara que no todos los individuos son afectados en el mismo grado, ello depende de su estructura de personalidad individual. Finalmente, es menester hacer hincapié en que no todo lo presentado en las *redes oscuras* obedece a un ambiente perverso; un alto porcentaje del material gráfico es matizado y tergiversado de su contexto original.²⁸²

²⁷⁹ Mongardini, Carlo. *Miedo y sociedad*. Traducido por Josefa Linares. (Madrid: Alianza, 2007). Pág. 61

²⁸⁰ Veblen, Thorstein. *Teoría de la clase ociosa*. Traducido por Vicente Herrero. (México: Fondo de Cultura Económica, 1992). Pág. 90

²⁸¹ Alayarian, Aida. *Trauma, torture and dissociation: a psychoanalytic view*. (Londres: Karnac, 2011). Recuperado en: <http://unam.ebib.com.pbidi.unam.mx:8080/patron/Login.aspx?r=needlogin> [Consultado 30 de enero de 2016]

²⁸² Dimensión macabra. 24 de junio de 2014. Desmintiendo fotos de la Deep Web. Episodio 1. *Dimensión macabra*. Recuperado en:

2.6 ¿Quién busca la información privilegiada?

La información privilegiada es una variable que coadyuva a modificar los sucesos presentes, en ocasiones los individuos desconocen de dicha información, puesto que se encuentra resguardada por las esferas de poder. Para Teresa Páramo²⁸³ los poderes establecidos están interesados en anular las oportunidades de cambio, lo que conlleva a regularizar los canales y medios para la comunicación de ciertos grupos de prensa o colectivos en oposición.

De este modo, las *redes oscuras*²⁸⁴ son viables para el intercambio de información de interés público por parte de los periodistas. Para estos casos dichas redes²⁸⁵ son de gran utilidad ya que en la *web superficial* se carece de anonimato para el administrador y los usuarios que acceden a la información altamente reservada, como es el caso de los procesos judiciales. Carlos Gràcia²⁸⁶ agrega que, además de ser la información judicial un tema de interés para los periodistas es también un recurso en demanda por parte de las empresas privadas, puesto que la información privilegiada permite (guardadas las proporciones) predecir y modificar el comportamiento de los individuos y consecuentemente, obtener un control en su conducta al vulnerar la privacidad.

Por otro lado Armando Bartra²⁸⁷ señala que, el secuestro de la información financiera define el curso en el rumbo económico y en consecuencia este tipo de información comienza a ser atesorada por los empresarios. Finalmente cabe mencionar que, no sólo los empresarios, los periodistas, los agentes de valores y los políticos buscan la información privilegiada. Por su parte el bibliotecólogo

<https://www.youtube.com/watch?v=sPqevB3jZxl&index=1&list=PLEqhKxfHwY4U5i6tNSNXfrQH5AQJZfAj9> [Consultado 13 de febrero de 2016]

²⁸³ Páramo, Teresa. Ídem. Pág. 50

²⁸⁴ El Universal. 14 de marzo de 2015. Presentan México Leaks, una plataforma para información anónima. *El universal*. Recuperado en: <http://www.eluniversal.com.mx/computacion-tecno/2015/mexico-leaks-plataforma-anonima-102719.html> [Consultado 21 de marzo de 2015]

²⁸⁵ Proceso. 17 de octubre de 2014. Colaboradora de Valor por Tamaulipas, sufrió amenazas antes de ser asesinada. *Proceso*. Recuperado en: <http://www.proceso.com.mx/?p=385068> [Consultado 17 de mayo de 2015]

²⁸⁶ Gràcia, Carlos. "Internet, transparencia y acceso a la información judicial". En *El acceso a la información judicial en México: una visión comparada*. (México, D.F.: UNAM, Instituto de Investigaciones Jurídicas, 2005). Pág. 233

²⁸⁷ Bartra, Armando. *El hombre de hierro: los límites sociales y naturales del capital*. (México, D.F.: Universidad Autónoma de la Ciudad de México, 2008). Pág. 112

aunque no está condicionado a conocer acerca del tema de las *redes oscuras* y la información privilegiada, podría incorporar dichos conocimientos y habilidades a su bagaje técnico como un *Blended librarian*, dado que es el bibliotecólogo el que realiza los servicios de referencia y se encuentra vinculado al servicio de acceso a Internet, la navegación en la Web, la búsqueda y la recuperación de la información para acceder a los contenidos que puedan tener elementos de información privilegiada para el usuario.

Realizando un balance puntual se puede comentar que, la Web se encuentra segmentada con base en:

- a) La visibilidad de los contenidos disponibles y,
- b) Contenidos con controles de acceso.

A este respecto es oportuno mencionar que el usuario con habilidades de búsqueda y recuperación de la información puede obtener los elementos suficientes para aplicar otros métodos de búsqueda, con el objetivo de ampliar las posibilidades de encontrar, consultar o descargar el contenido sin ninguna clase de control de acceso.

No obstante dentro de esta compleja estratificación en la Web, la *web propietaria*, la *web invisible* y la *web profunda* requieren de elementos de identificación para proporcionar un acceso a sus servicios y contenidos. En este sentido ya no se habla estrictamente de la profundidad, sino de la visibilidad y accesibilidad que tienen los servicios y contenidos en línea. De manera que, no se trata concretamente de un atributo de profundidad virtual sino de visibilidad y de acceso.

En lo que se podría considerar como el uso adecuado del concepto, la *web profunda* es todo aquel conjunto que incluye a todos los sitios web que no son en absoluto del conocimiento público y que requieren de una contraseña de

acceso. En este sentido, el acceso suele estar vinculado a la visibilidad de la información, dicha relación se debe a distintos factores como: la propiedad intelectual, el grado de sensibilidad de la información, el derecho de copia, el derecho de autor, el valor del contenido, entre otros.

La *web profunda* no es sinónimo de contenidos ilícitos, no obstante al ser estos contenidos y servicios especiales, oscuros, prohibidos, ocultos, bizarros e ilícitos han sido catalogados socialmente como parte de una *web profunda* en relación a cierta oscuridad en la condición humana. Con base en los antecedentes históricos anteriormente mencionados, el concepto de la *web profunda* sufre de un conflicto polisémico desde sus orígenes en la década de los noventa. No obstante, respecto a este conflicto se puede considerar como válido que socialmente la *web profunda* es igual a **Tor**, sin embargo, es menester reflexionar acerca de las características y utilidades que posee la *web profunda* y la *web invisible* como todo aquel conjunto de sistemas de acceso a contenidos reservados y regulados por medio de controles de acceso para el uso académico, científico, institucional e industrial.

La **red Tor** no es la *web profunda*²⁸⁸, la **red Tor** es un conjunto de sitios a los que únicamente se puede tener acceso autorizado mediante el software (navegador Tor browser), además de ser una herramienta de anonimato para la navegación. La **red Tor** pasó de ser un medio de anonimato, a un constante objetivo de vigilancia por parte del *Estado-nación*, a causa de su alto nivel de difusión en la *web superficial* y el incremento en el uso de la herramienta por parte del usuario común, aunado al abuso de los contenidos y servicios ilícitos de dicha red. De modo que la **red Tor** no es ni tan anónima, ni tan grande, ni tan segura y tampoco tan profunda como se considera socialmente en la *web superficial*. No obstante la utilidad de la **red Tor** adquiere el atributo de la dualidad como resultado del

²⁸⁸ Newitz, Annalee. 8 de noviembre de 2015. 9 datos básicos sobre seguridad que los expertos desearían que supieras. **Gizmodo en español**. Recuperado en: <http://es.gizmodo.com/9-datos-basicos-sobre-seguridad-que-los-expertos-desear-1723071993> [Consultado 15 de noviembre de 2015]

conflicto sempiterno, derivado de la necesidad de libertad y la imposición del control sobre el individuo occidental.

Las malas prácticas en el uso y publicación de los contenidos personales e institucionales propician un punto clave de oportunidades para la filtración y sustracción de la información privada o reservada. De manera que, esta concatenación de actitudes, situaciones y eventos pueden ser uno de los principales factores que originan algunos canales para la información privilegiada. Por tanto, si hay carencia de políticas de información y carencia de buenas prácticas; consecuentemente habrá un alto riesgo de vulneración a la privacidad y a la intimidad.

La *red oscura Tor* es un reflejo de las necesidades de información, así como de los deseos ocultos y reprimidos en la sociedad por parte del sistema de gobierno del *Estado-nación*. En consecuencia, se genera un mercado negro en línea utilizando las herramientas de alojamiento, acceso y navegación anónima. Respecto a este asunto concerniente al criterio que va desde el libre albedrío hasta los daños y perjuicios, las *redes oscuras* han establecido poco a poco políticas de información con el objetivo de regular el uso de estos sistemas anónimos enfocados a fomentar la disponibilidad de acceso a los contenidos. No obstante dichas políticas de información llegan a ser contradictorias en cuanto a la supuesta libertad que se pretende brindar hacia los usuarios. De modo que, el *quid* de la cuestión radica en la responsabilidad y en el sentido común de cada individuo por procurar una apertura a la información y no pretender el lucro de servicios y contenidos con el propósito de daños a terceros.

El acceso a las *redes oscuras* requiere de cierto capital técnico, económico y cultural, de modo que, son estos elementos los que determinan la experiencia de navegación y permiten sortear los riesgos informáticos así como los contenidos agresivos, ilustrativos, falsos y tergiversados tanto en la *web superficial* como en las *redes oscuras*.

Capítulo 3

Acceso a las redes oscuras



Pintura del desenmascaramiento: creación propia basada en la escena final del largometraje *Eyes wide shut* (1999), dirigido por Stanley Kubrick.

3.1 Introducción

En este capítulo se presentan los antecedentes de las *redes oscuras* *Tor*, *Freenet* e *I2P*, creadas y desarrolladas bajo los contextos de la vigilancia y la censura siendo consecuentemente utilizadas para fines de anonimato y privacidad. Se exponen las características esenciales de estas *redes oscuras* conforme a la postura ideológica de los colectivos que las han desarrollado.

Se describe la complejidad en cuanto a la adquisición de computadoras personales, sistemas operativos y la prevención de riesgos informáticos. Además, se aborda el tema de los conocimientos básicos de acceso a Internet y navegación en la Web, que en cierto modo repercuten en la configuración y navegación de las *redes oscuras*.

Consecuentemente se realiza un breve ejercicio de instalación de software, configuración y acceso a las *redes oscuras* **Tor**, *Freenet* e *I2P*. Se elabora una bitácora de monitoreo para determinar la actividad, vigencia o ausencia de los contenidos alojados en los sitios de las *redes oscuras*, lo que permitirá determinar e interpretar las constantes y variables en la temática, en comparación con el contexto del periodo 2012–2015.

Se mencionan aspectos éticos a groso modo, con el propósito de brindar un panorama sobre las consecuencias legales que potencialmente pueden derivar con el uso de contenidos y servicios tanto de la *web superficial* como de las *redes oscuras*.

Finalmente, se ofrecen alternativas para coadyuvar a la seguridad informática y el uso del servicio de Internet en las bibliotecas. Sean las bibliotecas como el lugar en donde es viable acceder a la información ya sea impresa, digital, multimedia y en línea.

3.2 Redes oscuras

A mediados de la década de los noventa surgen las primeras *redes oscuras*,²⁸⁹ con la necesidad de compartir los contenidos digitales mediante la transferencia en línea. Las *redes oscuras* desde entonces utilizaban la infraestructura de Internet para poder conectar las computadoras de los usuarios con el fundamento ideológico de compartir los contenidos digitales como texto, imágenes y música. No obstante, la popularidad de estas herramientas de acceso, almacenamiento y transferencia ha sido un factor que proporciona un conocimiento popular de estas tecnologías generando una reacción en oposición por parte de los afectados, ya sea en la industria editorial, industria discográfica, industria del cine y el mismo *Estado-nación*.

A partir de una documentación sobre el concepto de la *web profunda* y posteriormente acerca de los temas referentes a la *red Tor*, es viable determinar si dicha red cumple con los atributos de ser una *red oscura*. Con el objetivo de clarificar y reiterar las diferencias se describen las características más representativas de *Tor* según las fuentes y autores mencionados en el capítulo anterior en la siguiente tabla.

²⁸⁹ Biddle, Peter., England, Paul., Peinado, Marcus y Willman Bryan. 2002. The darknet and the future of content distribution. En *FRField's Page*, Recuperado en: <http://msl1.mit.edu/ESD10/docs/darknet5.pdf> [Consultado 13 de febrero de 2016]

Autor / Fuente	Características de Tor	usuarios
Tor Project	Red de navegación protegida mediante el cifrado de datos.	Usuarios que requieren del anonimato. Profesionales del mercado de valores y profesionales en las tecnologías de la información.
Lucian Constantin	El sistema de conexión de la red Tor funciona a través de una ruta dinámica y descentralizada.	Periodistas, activistas e individuos que no pueden acceder a ciertos contenidos en su país.
Electronic Frontier Foundation	Red orientada al anonimato en la Web.	
Nicole Arce	Los puntos de conexión son blanco constante de los ataques informáticos por parte del Estado-nación.	Usuarios que requieren del anonimato.

Tabla 11. Características de Tor como red oscura. Fuente: creación propia.

Después de haber presentado algunas características de **Tor** como *red oscura*, se presenta una tabla referente a la *web profunda* con el objetivo de diferenciar de manera concisa y puntual las divergencias entre la *web profunda* y la *red oscura*.

Autor / Fuente	Características de la web profunda	usuarios
Gerry McKiernan	Contenidos especializados y bases de datos que no pueden ser rastreados, porque cuentan con sistemas de protección.	Usuarios autorizados.
Kristin Finklea	No es del intereses del administrador del sitio que los servicios sean visibles bajo ninguna circunstancia.	Usuarios autorizados.
Qiuyan Huang, Qingzhong Li, Hong Li y Zhongmin Yan	Los contenidos están restringidos por medio de una interfaz de acceso.	Usuarios autorizados.
Nigel Yazdan	Los administradores no pretenden que sus sitios, páginas y contenidos sean indexados por los motores de búsqueda.	Usuarios autorizados.
Devine y Francine Egger-Sider	Es el conjunto de recursos sentenciados al olvido y la marginación.	

Tabla 12. Características de la web profunda. Fuente: creación propia.

Con base en las tablas anteriores se puede concluir que, la *web profunda* es todo aquel conjunto de contenidos especializados y bases de datos a los cuales sólo el usuario autorizado en cuestión accede mediante una interfaz con controles de acceso, en consecuencia los contenidos o recursos pueden llegar a ser proclives al olvido y al desconocimiento de los usuarios potenciales de dichos recursos, no obstante esta decisión de aislamiento depende del administrador, institución o empresa privada. En contraste, una *red oscura* tiene la característica fundamental del acceso mediante un software específico para su uso. Las *redes*

oscuras utilizan la visibilidad de la *web superficial* para difundir la información acerca de su software de acceso, no obstante su operatividad es independiente a la de la Web. Por tanto, una *red oscura* está enfocada a un público selecto con necesidades y actividades específicas que no son propias de la cotidianidad de la *web superficial*. Comúnmente estas necesidades son el resultado como oposición ante la vigilancia del *Estado-nación* y los monopolios de la Web, pero también es un acto de cofradía.

En cuanto a la oposición hacia el control por parte del *Estado-nación*²⁹⁰ se puede agregar que, se debe al sentimiento de inconformidad ante los sistemas de gestión en las sociedades, lo cual da origen a la creación y desarrollo de las *redes oscuras* como una alternativa para propiciar la privacidad y preservar la difusión de ideas y contenidos censurados.

Las *redes oscuras* cumplen con el objetivo primordial de evitar el monitoreo por parte de los Proveedores del Servicio de Internet, además de garantizar el anonimato y procurar la privacidad en los usuarios que hacen uso de las redes, protegidas con capas de cifrado. En este sentido, la cuestión técnica con las *redes oscuras* es que, además de tener un proceso de instalación particular, algunas de ellas tienden a presentar una configuración compleja para el usuario común. Sin embargo, para este tipo de sistemas de comunicación entre computadoras, es viable la consulta de artículos, foros, manuales y tutoriales²⁹¹ para ampliar la comprensión en cuanto a la instalación, configuración y operatividad del software. A continuación se mencionan cuatro *redes oscuras*

²⁹⁰ UNESCO “De la sociedad de la información a las sociedades del conocimiento”. En *Hacia las sociedades del conocimiento*. (UNESCO: Francia, 2005). Recuperado en: <http://unesdoc.unesco.org/images/0014/001419/141908s.pdf> [Consultado 13 de febrero de 2016]

²⁹¹ Véase Conrad, Bernd y Shirazi, Fatemeh. 2014. A survey on Tor and I2P. *Geti2p*, Recuperado en: https://geti2p.net/static/pdf/icimp_2014_1_40_30015.pdf. [Consultado 13 de febrero de 2016] Ask Ubuntu. 2016. Hot answers tagged: tor. *Ask Ubuntu*. Recuperado en: <http://askubuntu.com/tags/tor/hot>. [Consultado 13 de febrero de 2016] Infante, Andre. 2013. Unofficial guide to Tor: really private browsing. *Sluug*. Recuperado en: http://www.sluug.org/resources/presentations/2013/2013-12-11_TOR.pdf [Consultado 13 de febrero de 2016] y Mendoza, Miguel. 14 de julio de 2014. Cómo configurar Tor utilizando Vidalia. *We live security*. Recuperado en: <http://www.welivesecurity.com/la-es/2014/07/14/como-configurar-tor-utilizando-vidalia/> [Consultado 13 de febrero de 2016]

referentes al anonimato, la privacidad y la transmisión de contenidos potencialmente censurables.

1) The onion routing; Como ya se ha mencionado anteriormente, **Tor** (The onion routing o The onion routing network) ha sido socialmente conceptualizado como la *web profunda*,²⁹² siendo que es una *red oscura* en donde se conectan distintos equipos de cómputo y servidores que alojan contenidos y servicios por medio de un circuito dinámico en constante cambio. Además de ello, **Tor** cuenta con una aplicación, la cual no requiere ser instalada en el sistema operativo, su función primaria es la de proporcionar una ventana para la navegación anónima, tanto en la *web superficial* como en los servicios de la *red Tor*.²⁹³

- **Fecha de lanzamiento al público:** 2002
- **Desarrolladores iniciales:** Roger Dingledine, Nick Mathewson y Paul Syverson
- **Utilidad:** anonimato en la *web superficial* y acceso a la *red Tor*
- **Requerimientos mínimos de instalación:** Sistema Operativo Windows (32–64 bits). XP, Vista, 7, 8, y 10. OS X 10.6 (64 bits). Linux (32–64 bits)
- **Nivel de conocimiento informático:** accesible para el usuario común.

²⁹² Zavia, Matías. 11 de febrero de 2015. Una semana en la deep web: esto es lo que me he encontrado. **Xataka**. Recuperado en: <http://www.xataka.com/analisis/una-semana-en-la-deep-web-esto-es-lo-que-me-he-encontrado> [Consultado 15 de febrero de 2016]

²⁹³ Velasco, Rubén. 14 de septiembre de 2015. La red Tor gana seguridad gracias a los nuevos dominios .onion. **Redes zone**. Recuperado en: http://www.redeszone.net/2015/09/14/la-red-tor-gana-seguridad-gracias-a-los-nuevos-dominios-onion/?utm_content=buffer420a8&utm_medium=social&utm_source=twitter.com&utm_campaign=buffer [Consultado 13 de diciembre de 2015]

2) **Freenet**; diseñada en el año de 1999 y posteriormente liberada en el año 2000²⁹⁴ para su uso público. *Freenet*²⁹⁵ es una *red oscura* basada en un sistema de comunicación de red entre pares, lo que significa que se pueden transferir paquetes de información entre los usuarios que conforman dicha red, así como la consulta de los contenidos aportados por la comunidad mediante la navegación dentro de la red. *Freenet* es una red para alojar y compartir contenidos que podrían ser censurados por el *Estado-nación*.

La interfaz de *Freenet* permite al usuario configurar el nivel de la seguridad dependiendo de sus necesidades y la censura en su región o nación, la cual difiere según en cada contexto social. Por otro lado, la filosofía de *Freenet* se sustenta bajo la libertad de expresión y el derecho a la información.²⁹⁶

- **Fecha de lanzamiento al público:** 2000
- **Desarrollador inicial:** Ian Clarke
- **Utilidad:** promueve el anonimato en la navegación de la *Freenet* además de alentar la difusión de contenidos sin censura
- **Requerimientos mínimos de instalación:** Multiplataforma: Sistema Operativo Windows (con máquina virtual de Java de 32 bits). OS X 10.8. Linux (con Java Runtime Environment)
- **Nivel de conocimiento informático:** medianamente accesible para el usuario común.

²⁹⁴ Clarke, Ian Et al. *Freenet: a distributed anonymous information storage and retrieval system*. (Stanford: Estados Unidos, 2001). Recuperado en: <http://snap.stanford.edu/class/cs224w-readings/clarke00freenet.pdf> [Consultado 17 de febrero de 2016]

²⁹⁵ The Freenet Project Inc. 2015. "What is Freenet?" *Freenet project*. Recuperado el 17 de febrero de 2016, de <https://freenetproject.org/about.html> [Consultado 17 de febrero de 2016]

²⁹⁶ Ídem.

3) **I2P**; *Invisible Internet Project* (I2P) es una red cifrada, liberada para el uso público en el año 2003.²⁹⁷ A diferencia de **Tor** y *Freenet*, *I2P* opera mediante túneles de entrada y salida de datos, lo que significa que su arquitectura lógica es robusta. Dicha *red oscura* permite la navegación, comunicación y transferencia de datos de una forma anónima. Los contenidos dentro de *I2P* además de estar organizados para su recuperación pueden ser consultados aun cuando el equipo del usuario que los gestiona no está en línea.²⁹⁸

La red *I2P* fue creada para optimizar y crear alternativas de comunicación anónima en entornos hostiles, asociados a la carencia de privacidad y exceso de vigilancia. Dicha *red oscura* no está del todo orientada al anonimato de sus usuarios; su enfoque como herramienta digital se centra hacia la comunicación privada de los mensajes y contenidos.

- **Fecha de lanzamiento al público:** 2003
- **Desarrolladores iniciales:** desarrolladores conocidos bajo seudónimos
- **Utilidad:** proporciona anonimato a sus usuarios y fomenta la privacidad en la comunicación y transmisión de archivos
- **Requerimientos mínimos de instalación:** Java Runtime Version 7 o superior. Sistema Operativo Windows. OS X. GNU/Linux / BSD / Solaris. Debian. Ubuntu y Android
- **Nivel de conocimiento informático:** presenta cierta dificultad para el usuario común.

²⁹⁷ Castillo, Pedro. 18 de noviembre de 2015. I2P: una red anónima que deberías conocer. **Security inside**. Recuperado en: <http://securityinside.info/i2p-una-red-anonima-que-deberias-conocer/> [Consultado 19 de diciembre de 2015]

²⁹⁸ The Invisible Internet Project. 2015. *I2P. The Invisible Internet Project*. Recuperado en: <https://geti2p.net/es/comparison/freenet> [Consultado 17 de febrero de 2016]

4) **Hyperboria**; en el año 2012 el proyecto *Meshnet* desarrolló los lineamientos tecnológicos para la creación de la *red Hyperboria*.²⁹⁹ *Hyperboria* no es una *red oscura* como tal, puesto que es un sistema alternativo a Internet en comunicación y transmisión de datos mediante el protocolo de comunicaciones *Cjdns*. El creador del protocolo en cuestión Caleb DeLisle³⁰⁰ hace hincapié en que, se deben de crear iniciativas en torno a un sistema de comunicación, transferencia de datos y navegación independientes de la Web, con el fin de establecer una convivencia de libertad entre los usuarios y reducir la dependencia de los monopolios que proporcionan el servicio de conexión y recuperación de la información.

El objetivo primordial del proyecto *Meshnet*,³⁰¹ es el de crear una visibilidad horizontal en cuanto a los contenidos y disminuir la jerarquía tradicional de la *web superficial*. La red *Hyperboria* se enfoca esencialmente en la lucha contra la censura y el control de la información digital. *Hyperboria*, al ser una red alejada de la escena popular, podría ser considerada como una de las *redes oscuras* más complejas por su ideología descentralizada, además de que dicha red de comunicación depende de las comunidades locales para una conexión nacional e internacional a largo plazo.

²⁹⁹ Blake Curran. 26 de septiembre de 2012. Bitcoin 2012: Caleb James Delisle. Episodio 7. **Blake Curran**. Recuperado en: <https://www.youtube.com/watch?v=sCFmzGknUew> [Consultado 17 de febrero de 2016]

³⁰⁰ Macbroadcast. 9 de noviembre de 2013. Cjdns - The modular isp, the internet of the future? Episodio 23. **Blake Curran**. Recuperado en: <https://www.youtube.com/watch?v=NRhMY-gdXDw> [Consultado 17 de febrero de 2016]

³⁰¹ Hyperboria. 2015. Frequently Asked Questions. **Hyperboria**. Recuperado en: <https://docs.meshwith.me/faq/general.html> [Consultado 17 de febrero de 2016]

- **Fecha de lanzamiento al público:** 2012
- **Desarrollador inicial:** Caleb James DeLisle
- **Utilidad:** aunque no promueve el anonimato en primera instancia, su utilidad se fundamenta en una mayor privacidad y optimización de los recursos tecnológicos para acelerar la velocidad en la transmisión de archivos digitales.
- **Requerimientos mínimos de instalación:** Sistema Operativo Linux. Android. OpenWrt y OS X
- **Nivel de conocimiento informático:** conocimientos avanzados para el usuario común.

Las cuatro *redes oscuras*: **Tor**, *Freenet*, *I2P* e *Hyperboria*, fueron identificadas como tales a partir de una indagación en la *web superficial*, no obstante pueden existir otras *redes oscuras*. Consecuentemente con base en el análisis de sus características particulares se puede interpretar que, cada *red oscura* puede aportar un elemento en oposición concerniente al control de accesibilidad y, elementos en pro de la optimización frente a la complejidad de la Web, es decir que, la *red Tor* está orientada al anonimato en la *web superficial* y acceso exclusivo a su red de usuarios.

Mientras que la *Freenet* está encaminada la difusión de contenidos sin censura. La *red oscura I2P* por su parte promueve la privacidad en la comunicación y transmisión de archivos dentro de su comunidad de usuarios. Finalmente *Hyperboria* es una iniciativa para alentar una red independiente a los servicios de conexión a Internet y los intereses económicos que permean en la Web, además de robustecer la seguridad informática mediante el cifrado de datos. De esta manera las cuatro *redes oscuras* (en teoría) se conjugan para contrarrestar y desestabilizar (guardadas las proporciones) la accesibilidad y la complejidad de la Web.

La siguiente tabla representa a las *redes oscuras* como elementos en oposición a la accesibilidad y la complejidad, con base en la postura ideológica de sus usuarios con el rol de *actores-agentes*. Manuel Serrano³⁰² define al *actor-agente* como aquel individuo con la capacidad de alterar el entorno que le rodea con actitudes antagonistas y acciones expresivas, físicas e intelectuales para modificar la percepción de otros individuos. Bajo el contexto de las *redes oscuras*, estos *actores-agentes* tienen la posibilidad de incidir en los elementos de la accesibilidad, que son: restricción, control, censura y poder, además de los elementos de la complejidad de la Web: vigilancia, anonimato, privacidad y seguridad.

³⁰² Martín Serrano, Manuel. *La producción social de comunicación*. 2da ed. (Madrid: Alianza, 1993). Pág. 224

Elementos de:		Red oscura	Carencias y riesgos
Accesibilidad	Restricción	Hyperboria como elemento en oposición a la restricción.	
	Control		Ausencia de organización, jerarquía y estructura temática en las redes oscuras.
	Censura	Freenet como elemento en oposición a la censura.	
	Poder	Hyperboria, The onion routing, I2P y Freenet como elementos en oposición a la centralización del poder.	
Complejidad de la Web	Vigilancia		El Estado-nación constantemente pretende vulnerar la operatividad de las redes oscuras.
	Seguridad	Hyperboria como elemento en pro de la optimización de la seguridad informática.	
	Anonimato	The onion routing como elemento en pro del anonimato.	
	Privacidad	I2P como elemento en pro de la privacidad.	

Tabla 13. Redes oscuras como elementos de oposición a la accesibilidad y en pro de la optimización en la complejidad de la Web. Fuente: creación propia.

De acuerdo a lo presentado en la tabla anterior en la sección de carencias y riesgos se interpreta que, el *Estado-nación* trabaja constantemente en mecanismos y políticas de información para regular, disminuir, dismantelar y erradicar cualquier tipo de tecnología que ponga en desventaja su jurisdicción. Por otro lado se puede interpretar que, el control de la información es un punto débil en las *redes oscuras* de modo que no existe una conexión, jerarquización, vinculación y unificación que le permita a estas redes emular la operatividad de la Web; aunque cabe resaltar de manera puntual que esta misma ausencia de control y descentralización de la información, forma parte de la naturaleza de las *redes oscuras*.

En cuanto al poder como elemento de accesibilidad con carta de naturalidad exclusiva para las instituciones y grupos dominantes, las *redes oscuras* podrían ejercer el poder como una vía hacia la visibilidad y disponibilidad de contenidos, recursos, productos y servicios en favor de sus usuarios, no obstante dichas redes tendrían que cohesionarse además de compartir recursos físicos y abstractos a manera de un movimiento de hardware y software libre, gestionado tanto por los administradores como por sus usuarios avanzados. A falta de esta cohesión, las *redes oscuras* están condenadas a ser constantemente monitoreadas, vigiladas, atacadas, deshabilitadas y reguladas por el *Estado-nación*, en donde el control de la información si es un recurso de certidumbre para fragmentar y disolver la autonomía de las *redes oscuras*.

3.3 Recursos para acceder a las redes oscuras

Para que el usuario pueda acceder a las *redes oscuras* se requiere de la instalación del software de acceso a cada red, por tanto es imprescindible cubrir los requisitos mínimos de instalación. Por otro lado el usuario debe tener en consideración que, no sólo existen riesgos en el acceso a las *redes oscuras* sino también en la *web superficial*, por ello es recomendable contar (en el mejor de los casos) con una computadora personal para el acceso a la Web, desvinculando los intereses, contenidos o proyectos referentes al contexto personal, social, familiar y laboral. Cabe mencionar que además de las computadoras personales, son también los medios electrónicos con la capacidad de conexión a Internet como: los teléfonos inteligentes, computadoras portátiles y tabletas, los recursos que usualmente se utilizan con base a su portabilidad y alto nivel de utilidad para la comunicación. No obstante, el acceso a las *redes oscuras* demanda cierta capacidad y estabilidad, que de momento proporcionan las computadoras personales.

Para acceder a la *web superficial* y sustancialmente a las *redes oscuras* es recomendable conocer el fin principal que cumplirá la computadora personal, es decir que, se deben de considerar las consecuencias a las que se expone tanto el software como el hardware. De modo que, los documentos personales como tareas académicas, proyectos laborales, datos personales e información sensible podrían quedar expuestos a un ataque informático. Sin embargo, esta clase de ataques está orientada comúnmente a las empresas privadas, instituciones y laboratorios. A pesar de ello, se recomienda considerar la aplicación de las medidas preventivas.

En cuanto al tema de la navegación en las *redes oscuras*, se exhorta al usuario común a tener la misma prudencia que en la *web superficial*. Carlos Zahumenszky³⁰³ menciona que, en el caso de la *red oscura Tor* el tiempo de

³⁰³ Zahumenszky, Carlos. 22 de enero de 2015. Cómo empezar a utilizar el navegador anónimo Tor, paso a paso. *Gizmodo en español*. Recuperado en: <http://es.gizmodo.com/los-mejores-consejos-para-mantener-de-verdad-tu-privaci-1681089272> [Consultado 23 de enero de 2015]

navegación es crucial, puesto que a mayor tiempo de exposición en la conexión anónima, aumenta la probabilidad de ser monitoreado por instancias gubernamentales o por algún *Cracker* avanzado. En cuanto a la descarga de contenidos o archivos, lo mejor es evitar cualquier tipo de descarga, porque se desconoce la intención real del contenido, el cual podría tratarse de una simple broma de muy mal gusto; o en el peor de los casos un programa malicioso que corrompa el sistema operativo y en consecuencia ocurra algún daño a los componentes físicos de la computadora personal.

En este sentido de riesgo en la navegación de *redes oscuras*, vale la pena redimensionar la importancia de la computadora personal, puesto que es la computadora personal (personal desktop computer o PC desktop),³⁰⁴ un conjunto de hardware y software para la creación, desarrollo e interacción en las actividades vinculadas al ámbito académico, laboral y del entretenimiento; a diferencia de una computadora institucional o estación de trabajo utilizada para fines específicos, con el respaldo del personal técnico en informática; pero también con limitaciones de operatividad y acceso. Una computadora personal posee la característica fundamental de poder ser configurada y modificada según sea el gusto, el conocimiento técnico y las necesidades del usuario.

A este respecto Lincoln Spector³⁰⁵ menciona que, las computadoras de escritorio permiten pasar a la siguiente generación de procesadores, tarjetas gráficas y componentes de memoria RAM con una inversión considerable, siempre y cuando exista compatibilidad entre los componentes y una arquitectura física adecuada para realizar la modificación. En cuanto a los fallos de sus

³⁰⁴ Pingdom. 28 de agosto de 2012. The incredible story of the first PC, from 1965. *Tech blog*. Recuperado en: <http://royal.pingdom.com/2012/08/28/the-first-pc-from-1965/> [Consultado 19 de febrero de 2016]

³⁰⁵ Spector, Lincoln. 16 de septiembre de 2013. Why you may want a desktop instead of a laptop. *PC world*. Recuperado en: <http://www.pcworld.com/article/2048257/why-you-may-want-a-desktop-instead-of-a-laptop.html> [Consultado 17 de febrero de 2016]

componentes Ángel Sánchez³⁰⁶ agrega que, la reparación de las computadoras de escritorio es más económica que la de las computadoras portátiles.

De acuerdo a estas posturas cabe señalar que, el usuario común en ocasiones adquiere una computadora personal con los componentes elementales para cumplir con sus necesidades, no obstante no se vislumbra a mediano o largo plazo la disminución en el rendimiento de la computadora en relación al aumento de requerimientos de nuevas aplicaciones, software de productividad y para el entretenimiento. Por ello, es menester que el usuario sea consiente del rendimiento (o nivel de prestación) en cuanto a la velocidad de procesamiento y capacidad de almacenamiento en los componentes.

Finalmente en lo que atañe a las computadoras personales portátiles, el usuario deberá ser consciente de que el equipo de cómputo en cuestión presentará limitantes en cuanto a su rendimiento y durabilidad a largo plazo. Juan Corcuera y Ricardo Arnaus³⁰⁷ comentan que, lo recomendable ante el desconocimiento en la adquisición del equipo de cómputo la mejor opción es la investigación, documentación y asesoría con algún experto en computadoras personales. En estos casos el experto en cuestión tendría que ser un mediador entre las distintas marcas de computadoras, con el fin de dar una opinión neutral y objetiva. Por tanto, es a partir de este conjunto de opiniones sobre la adquisición del equipo de cómputo, las alternativas para el usuario común conforme a sus necesidades, además de las herramientas y fundamentos esenciales encaminados a una adecuada adquisición de recursos, junto con las mejores opciones en cuanto a los servicios, contenidos y productos de la Web. En este sentido también se comprende el acceso a las *redes oscuras* como un elemento extra hacia nuevos niveles de acceso para el usuario común.

³⁰⁶ Sánchez, Ángel. 24 de abril de 2015. Resuelve de forma sencilla tus dudas entre un PC de escritorio y uno portátil. **Computadoras about**. Recuperado en: <http://computadoras.about.com/od/comprar-computadora/bb/Antes-De-Comprar-Una-Computadora.htm> [Consultado 17 de febrero de 2016]

³⁰⁷ Corcuera, Juan y Arnaus, Ricardo. Ídem. Pág. 52.

3.3.1 Sistema operativo

Además de la variedad en cuanto a las computadoras personales, existen sistemas operativos, programas de productividad y software de entretenimiento que requieren para su instalación un mínimo de 64 bits en procesador, aunque también existen sistemas operativos que requieren tan sólo 32 bits, sin embargo hay una tendencia hacia los 64 bits, ya que los programas informáticos demandan cada vez una mayor capacidad en cuanto al procesamiento, por esa razón es importante conocer qué tipo de sistema operativo, software de productividad y software de entretenimiento se instalará en la computadora personal. Es importante señalar que, no todos los sistemas operativos soportan los mismos programas y aplicaciones, de modo que, al momento de adquirir una computadora personal será fundamental establecer la prioridad en su usabilidad.

El sistema operativo (Operating System, por sus siglas en inglés OS) es un conjunto de programas que hacen posible la operatividad de una computadora.³⁰⁸ Cuando se adquiere una computadora personal de marca, en la mayoría de los casos cuenta con un sistema operativo previamente instalado,³⁰⁹ lo cual conlleva a ciertas desventajas, puesto que el costo del equipo de cómputo aumenta considerablemente, además de que, para habilitar los programas de productividad tales como los editores de texto, hojas de cálculo y el sistema antivirus, es necesario realizar un pago extra para la suscripción o compra del programa. Cabe mencionar que, el sistema operativo propietario impide cualquier modificación en su código fuente, sin importar si dicha modificación es para la mejora de la operatividad o seguridad informática.

A manera de ejemplo, Ubuntu³¹⁰ es un sistema operativo distribuido como software libre, lo cual significa que, el sistema operativo puede ser modificado

³⁰⁸ Calvin College. 2001. What is an Operating System? **Calvin College**. Recuperado en: <http://www.calvin.edu/~rbobeldy/tutorials/os/basics.htm> [Consultado 22 de febrero de 2016]

³⁰⁹ Franklin, Curt y Coustan, Dave. 2016. How operating systems work. **Computer how stuff works**. Recuperado en: <http://computer.howstuffworks.com/operating-system.htm> [Consultado 22 de febrero de 2016]

³¹⁰ Ubuntu. 2016. Página de inicio, Ubuntu. **Ubuntu**. Recuperado en: <http://www.ubuntu.com/> [Consultado 22 de febrero de 2016]

por los usuarios dependiendo de sus necesidades específicas ya sea para el trabajo de oficina, la programación informática o para el entretenimiento. El sistema operativo Ubuntu se puede descargar e instalar en las computadoras personales de forma gratuita, tanto en las computadoras de escritorio como en las computadoras portátiles. Ubuntu es soportado por Canonical, una empresa orientada a la venta y servicios sobre productos informáticos.

Cabe mencionar que, a pesar de las necesidades y el presupuesto de cada usuario, la comodidad visual de interacción con la interfaz y la fácil configuración en el sistema operativo son elementos en la preferencia por la adquisición de las computadoras de marca.³¹¹ De modo que, no es necesario contar con cierto nivel de conocimientos y documentación para la interacción con el equipo de cómputo; en contraste con la adquisición de componentes para su ensamblado personalizado, así como la instalación y configuración de un sistema operativo adecuado a los gustos y necesidades de cada usuario.

Si bien existe un grado de dificultad en cuanto a la adquisición de computadoras personales ensambladas e instalación de sistemas operativos distribuidos como software libre. Los contenidos, tutoriales y servicios en su mayor parte gratuitos, se encuentran disponibles en la Web, y están orientados hacia la enseñanza de aspectos relacionados en la compra de componentes y armado de computadoras, por lo que consecuentemente dichos contenidos han dado pauta a reducir la brecha digital referente al software libre. Por lo que se hace viable para el usuario común y también para la biblioteca conocer otras alternativas concernientes al uso de la tecnología digital, aunque de ello depende en gran medida la voluntad y la disposición de aprendizaje en cada individuo.

³¹¹ Jmaturana TI. 21 de enero de 2008. ¿Por qué Linux no sustituirá a Windows? **Silicon**. Recuperado en: http://www.silicon.es/por_que_linux_no_sustituira_a_windows-8111 [Consultado 21 de febrero de 2016]

3.3.2 Prevención de riesgos informáticos

Todos los sistemas operativos son vulnerables sin importar su popularidad o su alto nivel de complejidad en cuanto a su seguridad informática.³¹² Dicho esto, las vulnerabilidades no deben de ser un factor desalentador, sino por el contrario, se deben de tomar las medidas preventivas así como el hecho de tener conciencia sobre las implicaciones que representa utilizar una computadora personal o para su uso público. Para el caso concreto de la navegación en la Web³¹³ y posteriormente en las *redes oscuras*, una alternativa para reducir los riesgos y la inversión es la de instalar un sistema operativo distribuido como software libre,³¹⁴ aunque ello dependerá de la compatibilidad con los componentes que integran la computadora, por lo que se deberán considerar las opciones en las distintas distribuciones³¹⁵ que mejor se adapten a la computadora personal.

Para fines académicos, el software libre es una opción puntual a las necesidades de profesores y alumnos, sin embargo suele ser común que, en las instituciones educativas se tenga una partida del presupuesto destinada a la compra del equipo de cómputo (por distintos motivos o acuerdos) con determinados proveedores, lo cual significa una contradicción en cuanto al fomento por la apropiación y estudio de la tecnología sin fines de lucro. En este tenor, las *redes oscuras* aunque no son propiamente desarrolladas para fines académicos reflejan en cierto sentido esa aura del libre acceso tecnológico, seguridad informática y apertura a la información.

³¹² Kemp, Steve. 18 de marzo de 2014. Mitos en linux. *Ingenierasa's blog*. Recuperado en: http://www.ingenierasa.org/blog/Mitos_en_linux.html [Consultado 22 de febrero de 2016]

³¹³ Méndez, Manuel. 15 de abril de 2014. Tails, el OS anónimo, en USB y gratuito que utiliza Edward Snowden. *Gizmodo en español*. Recuperado en: <http://es.gizmodo.com/tails-el-os-anonimo-y-en-usb-que-edward-snowden-aconse-1563333168> [Consultado 23 de febrero de 2015]

³¹⁴ Craig, Charles. 2014. Advantages and disadvantages of Linux. *Renewablecs*. Recuperado en: <https://renewablepcs.wordpress.com/about-linux/advantages-of-using-linux/> [Consultado 22 de febrero de 2016]

³¹⁵ Kavindra, Buddhi. 2016. The best Linux distros – 2016. *Buddhilive*. Recuperado en: <http://www.buddhilive.com/2016/01/the-best-linux-distros-2016.html> [Consultado 22 de febrero de 2016]

3.3.3 Tipo de conexión a Internet

La conexión a Internet suele ser el siguiente paso después optar por una computadora personal. En este sentido Sergio Talens y José Hernández³¹⁶ mencionan que, existen varias formas de acceder a Internet, ya sea mediante el uso de la red escolar o laboral. De no ser el caso, es vital saber cuáles son las mejores opciones de suscripción al servicio de Internet. Conforme a esto, Preston Gralla³¹⁷ añade que, los mejores servicios de Internet están vinculados a la velocidad de transmisión de datos; no obstante el costo es proporcional a la calidad de conexión y velocidad.

Una vez que se ha optado por un servicio de Internet acorde con las necesidades y el presupuesto. Comúnmente ocurre que, después de firmar un contrato de suscripción para el hogar o institución, el personal técnico lleva acabo tanto la instalación del cableado como del dispositivo de conexión, sin embargo es recomendable contar con el manual de usuario (impreso o digital), con el fin de cambiar posteriormente la configuración predeterminada de fábrica del router,³¹⁸ el cual suele ser el dispositivo de conexión entre la computadora personal del usuario hacia la infraestructura del Proveedor de Servicio de Internet que se ha contratado. En cuanto a la configuración inalámbrica Wi-Fi se refiere, es necesario evaluar la posibilidad de cifrar la señal mediante el sistema WPA o WPA2³¹⁹ (o superior) siendo el segundo la mejor opción, puesto que al tener la señal inalámbrica abierta, esta puede ser utilizada por personas ajenas y consecuentemente derivar en una disminución de la velocidad en la transmisión de datos y en el peor de los casos, posibles riesgos de seguridad informática.

En cuanto al tema de la seguridad de la red inalámbrica doméstica, cabe señalar que, a pesar de no detectar riesgos visibles, el usuario común puede ser víctima

³¹⁶ Talens, Sergio y Hernández, José. *Internet: redes de computadores y sistemas de información*. (Madrid: Paraninfo, 1997). Pág. 112

³¹⁷ Gralla, Preston. *Cómo funciona Internet*. Traducido por Beatriz Tarancón. (Madrid: Anaya Multimedia, 2007). Pág. 27

³¹⁸ Computer hope. 2016. Router. *Computer hope*. Recuperado en: <http://www.computerhope.com/jargon/r/router.htm> [Consultado 27 de febrero de 2016]

³¹⁹ Álvarez Marañón, Gonzalo. Ídem. Pág. 88

de algún *Cracker* ejecutando un testeo (o auditoria) de redes, con el objetivo de conectarse al servicio de Internet o para fines maliciosos.³²⁰ Por ello, como se ha mencionado anteriormente, es importante realizar la modificación del nombre de usuario (User ID) y la contraseña (Password) del router, así como de un cambio en la contraseña de acceso Wi-Fi, ya sea de forma semanal o mensual.

En cuanto al tema de la velocidad de conexión, cuando se realiza la suscripción al servicio de conexión a Internet, usualmente se desconoce de la velocidad real de conexión. La velocidad de conexión es un factor importante en la experiencia de navegación, ya que al comparar los valores de velocidad ofrecidos por el Proveedor de Servicio de Internet junto con los valores obtenidos a través de los servicios de medición por terceros en la Web³²¹ es posible comparar y esclarecer la calidad del servicio de conexión. Respecto a este tema es primordial saber que, la velocidad de conexión se encuentra comúnmente estratificada en tres aspectos:³²²

- 1) **Velocidad de bajada**, implica el tiempo para descargar los programas, documentos y contenidos.
- 2) **Velocidad de subida**, se refiere al tiempo para enviar contenidos a los servicios de alojamiento, servicios de mensajería y redes sociales.
- 3) **Latencia**, es un conjunto de pausas en la transmisión, decodificación y visualización de los contenidos, lo que afecta directamente la experiencia

³²⁰ Pash, Adam. 1 de septiembre de 2012. How to crack a Wi-Fi network's WPA password with Reaver. *Life hacker*. Recuperado en: <http://lifehacker.com/5873407/how-to-crack-a-wi-fi-networks-wpa-password-with-reaver> [Consultado 27 de febrero de 2016]

³²¹ Ookla. 2016. Página de inicio, Speed test. *Speed test*. Recuperado en: <http://www.speedtest.net/> [Consultado 28 de febrero de 2016]

³²² Véase Hruska, Joel. 23 de abril de 2015. How to Test Your Internet Speed. *Speed test*. Recuperado en: <http://www.speedtest.net/articles/how-to-test-your-internet-speed/>. [Consultado 28 de febrero de 2016] Speed of me. 2016. Página de inicio, Speed of me. *Speed of me*. Recuperado en: <http://speedof.me/> [Consultado 28 de febrero de 2016] y Sherali, Stephanie. An analysis of tools for online anonymity. *International Journal of Pervasive Computing and Communications* 11, no. 4. (2015): 436-453. Recuperado en: <http://dx.doi.org/10.1108/IJPC-08-2015-0030> [Consultado 28 de febrero de 2016]

de navegación e interacción, así como la frustración en el usuario al interactuar con los servicios en línea.

Como se ha mencionado anteriormente, a mayor costo mayor beneficio en la velocidad de transmisión de bajada, subida y bajos niveles de la latencia. De manera que, dichos aspectos se polarizan en las *redes oscuras*, por lo que la velocidad se verá notablemente reducida junto con un aumento en la latencia a causa del cifrado de cada *red oscura*, en donde se procura cierto nivel de anonimato y privacidad.

3.3.4 Alternativas para evitar el monitoreo

Algunas de las herramientas para conocer la velocidad de conexión a Internet proporcionan el dato de la IP pública, el cual es el código de identificación en la Web. Básicamente la dirección IP pública es un número asignado³²³ para que la computadora personal independientemente de su sistema operativo y navegador pueda acceder a la Web, al mismo tiempo que la computadora es identificada. En este sentido es el Proveedor de Servicio de Internet³²⁴ quien asigna la IP pública para que la computadora pueda comunicarse con los servicios de la Web.

La gestión de las direcciones IP públicas no sólo deriva del Proveedor de Servicio de Internet, las IP públicas son administradas de manera global³²⁵ por la IANA³²⁶ (Internet Assigned Numbers Authority) entidad en supervisión de las direcciones IP, en coordinación con la ICANN³²⁷ (Internet Corporation for Assigned Names and Numbers) organización multinacional orientada a la asignación e identificación de las direcciones IP.

³²³ IP location. 2016. What is the difference between public and private IP address? *IP Location*. Recuperado en: <https://www.iplocation.net/public-vs-private-ip-address> [Consultado 1 de marzo de 2016]

³²⁴ Vratonjic, Nevena Et al. A location-privacy threat stemming from the use of shared public IP Addresses. *IEEE transactions on mobile computing* 13, no. 11 (2014): 2445-2457. Recuperado en: <http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=6757043&isnumber=6913596> [Consultado 3 de marzo de 2016]

³²⁵ Carballar Falcón, José. Ídem. Pág. 39

³²⁶ The Internet Assigned Numbers Authority. 2016. IANA. *The Internet Assigned Numbers Authority*. Recuperado en: <http://www.iana.org/> [Consultado 3 de marzo de 2016]

³²⁷ Internet Corporation for Assigned Names and Numbers. 2016. "ICANN". *Internet Corporation for Assigned Names and Numbers*. Recuperado en: <https://www.icann.org/> [Consultado 3 de marzo de 2016]

En caso de que el usuario se interese en modificar su dirección pública con el objetivo de tener una navegación anónima en la Web, puede hacerlo mediante distintos métodos. Uno de ellos es por medio de proxys. No obstante existe un riesgo latente en el uso de estos servicios, puesto que al utilizarlos se proporcionan datos como la ubicación geográfica y la identidad del Proveedor de Servicio de Internet.³²⁸ A pesar de ello, cabe resaltar que algunos de los sitios web convencionales a los que el usuario accede, también tienen acceso a estos datos. Por otro lado, existen servicios llamados Web Proxy,³²⁹ que permiten cambiar la identidad de origen sin realizar modificaciones en la configuración del navegador. Las *redes oscuras* en este sentido también son una alternativa para evitar el monitoreo, empero es menester mencionar que el uso de dichas redes está enfocado a contenidos y servicios ajenos a la *web superficial*.

Otra alternativa al problema del monitoreo en la Web, es el uso de los servicios de las Redes Virtuales Privadas (por sus siglas en inglés VPN)³³⁰ las cuales ofrecen privacidad por medio de sus túneles para el anonimato en la navegación, sin embargo la mayoría de estas redes requieren de la suscripción a sus servicios. Estas redes virtuales no sólo se utilizan para el anonimato, puesto que los servicios bibliotecarios también implementan este tipo de tecnologías para el acceso remoto y acceso a los recursos digitales.³³¹

3.4 Caso práctico de navegación en las redes oscuras

Conforme a la previa indagación documental es menester mencionar que, para fines de esta investigación las opciones idóneas son la computadora personal de escritorio o computadora portátil, puesto que es la arquitectura tanto física como abstracta de este tipo de computadoras personales la que permite la instalación, configuración y ejecución de los programas para la navegación en las *redes*

³²⁸ Metz, Paul. "Principles of selection for electronics resources". *Library Trends* 48, no. 4 (2000): 711-728

³²⁹ Bailey, Matthew. Ídem. Pág. 129

³³⁰ Op. Cit. Pág. 136

³³¹ Dirección General de Bibliotecas UNAM. 2011. Servicio de acceso remoto a BIDI UNAM. *BIDI UNAM*. Recuperado en: http://bidi.unam.mx/web/sbdsite/mailling/foll_bidiago/foll_bidiagoAR.html [Consultado 3 de marzo de 2016]

oscuras; caso contrario a los medios con la capacidad de conexión a Internet como los teléfonos inteligentes y las tabletas.

A continuación se describe un caso práctico de acceso y navegación en las *redes oscuras* *Tor*, *Freenet* e *I2P* descartando a *Hyperboria* por su dificultad de instalación, aun así es importante hacer mención de ella como iniciativa de conexión y recuperación de la información independiente a la Web convencional. Para acceder a las *redes oscuras* se ha optado por una computadora personal portátil laptop, ya que su arquitectura lógica permite la instalación de programas robustos así como la disminución de daños informáticos a causa de un posible ataque informático. En el siguiente cuadro se describen las características y los componentes de la computadora en cuestión.

Computadora	Portátil laptop
Marca	ASUS
Modelo	K45VD
Gráficos	NVIDIA 610M 2GB
Tipo de sistema	64 bits
Procesador	Intel Core i5-3210M 2.50 GHz
Memoria	8 GB RAM
Almacenamiento	Samsung SSD EVO 250 GB
Sistema operativo	Windows 8 / Ubuntu 14.04 LTS

Tabla 14. Características de la computadora personal y sistema operativo. Fuente: creación propia.

La selección de la computadora personal para realizar las actividades de monitoreo se fundamenta en las tendencias de compra, estadísticas, críticas y sugerencias sobre el desempeño de los equipos de cómputo a nivel nacional del periodo 2012, 2014 al 2015³³² en añadidura con los puntos de vista a nivel

³³² Véase Revista del consumidor. 2012. "Estudio de calidad: Computadoras portátiles y tabletas, tu mundo". *Revista del consumidor*. Recuperado en: http://www.consumidor.gob.mx/wordpress/wp-content/uploads/2012/08/RC426_Computadoras_OK.pdf. [Consultado 23 de enero de 2016] Revista del consumidor. 2014. "Estudio de calidad: dile hola a tu nueva computadora Laptops, ultraportátiles y todo en uno". *Revista del*

internacional del año 2013 al 2015,³³³ ello con el objetivo de ampliar el conocimiento sobre la adquisición de una computadora adecuada.

	2012	2013	2014	2015
Contexto Nacional	1.- Sony (Vaio SVE14113ELW) 2.- Toshiba (Satellite L745-SP4288KM) 3.- Hewlett Packard (Pavilion G4-1283LA)		1.- Lanix (Neuron V) 2.- Lenovo (IdeaPad Z410 20292) 3.- Toshiba (Satellite S50t-A5163SM)	1.- Toshiba (Tecra Z40-A4162SM) 2.- Toshiba (Satellite L55t-B5164WM) 3.- Lanix (Neuron RII)
Contexto Internacional		1.- Apple 2.- Lenovo 3.- Asus	1.- Asus (Transformer book T100) 2.- Acer (Aspire E1-510P) 3.- Asus (K200MA)	1.- Acer (Aspire E5-571P) 2.- Asus (Zenbook UX305FA) 3.- Lenovo (IdeaPad U430)

Tabla 15. Las mejores marcas y modelos de computadoras portátiles laptop en el contexto internacional y nacional. Fuente: creación propia basada en los documentos consultados.

consumidor. Recuperado en: <http://www.consumidor.gob.mx/wordpress/?p=17652> [Consultado 23 de enero de 2016] y Revista del consumidor. 2015. "Estudio de calidad: las computadoras más impersonales a revisión". **Revista del consumidor.** Recuperado en: http://www.consumidor.gob.mx/wordpress/wp-content/uploads/2015/09/computadoras_impersonales.pdf [Consultado 23 de enero de 2016]

³³³ Véase Dachis, Adam. 20 de noviembre de 2013. Las mejores y peores marcas: cómo escoger un portátil que no falle. **Gizmodo en español.** Recuperado en: <http://es.gizmodo.com/las-mejores-y-peores-marcas-como-escoger-un-portatil-g-1468106074>. [Consultado 17 de febrero de 2016] Corona, Eder. 19 de agosto de 2014. Las mejores laptops económicas. **Vive USA.** Recuperado en: <http://www.viveusa.mx/articulo/2014/08/19/compras/las-mejores-laptops-economicas> [Consultado 17 de febrero de 2016] y Žygimantas. 28 de julio 2015. 8 Best hackintosh laptops with guides and comparison. **Pick notebook.** Recuperado en: <http://picknotebook.com/blog/best-hackintosh-laptop/> [Consultado 21 de marzo de 2016]

Conforme a los datos presentados sobre las mejores opciones en cuanto a marcas y modelos de computadoras portátiles (laptop), se deduce que, el mercado nacional está orientado a ciertas marcas, ya sea por sus convenios de importación con los proveedores o por la accesibilidad de sus costos al público en general; contrastando con algunos ejemplos en el contexto internacional.

La presente computadora (adquirida de segunda mano) fue formateada y posteriormente fueron instalados dos sistemas operativos. La elección del sistema operativo Windows se debe en principio porque existen programas y aplicaciones populares que están destinadas a los sistemas operativos propietarios. Por otro lado, Ubuntu es un sistema operativo de distribución libre, el cual permite la instalación de programas y aplicaciones destinadas a las distribuciones Linux, las cuales no suelen ser adaptadas para los sistemas operativos propietarios. Ambos sistemas operativos pueden convivir en la misma computadora personal, de manera que al encenderla se puede elegir con cual sistema operativo se desea trabajar. Windows 8 y Ubuntu 14.04 LTS complementan las necesidades de ocio, entretenimiento y trabajo, pero para fines de esta investigación el sistema operativo utilizado, es Ubuntu, el cual corresponde a la línea de GNU/Linux.³³⁴ Cabe aclarar que, un sistema operativo basado en GNU/Linux no es enteramente seguro e infalible a los ataques informáticos, sin embargo gran parte de los programas maliciosos están enfocados a los sistemas operativos propietarios debido a su consumo en el mercado y su usabilidad tanto en los hogares como en las instituciones.³³⁵

Ubuntu 14.04 LTS es un sistema operativo con el potencial para fines académicos, laborales y del entretenimiento. Además de ello, las distribuciones basadas en GNU/Linux suelen tener mayor estabilidad y compatibilidad en la instalación y configuración de programas para acceder a las *redes oscuras*.

³³⁴ Stallman, Richard. 2016. Linux y el sistema GNU. **GNU**. Recuperado en: <http://www.gnu.org/gnu/linux-and-gnu.es.html> [Consultado 7 de marzo de 2016]

³³⁵ Contreras, Manu. 3 de abril 2015. Windows XP aún sigue siendo más usado que Windows 8.1. **Fayer wayer**. Recuperado en: <https://www.fayerwayer.com/2015/04/windows-xp-aun-sigue-siendo-mas-usado-que-windows-8-1/> [Consultado 7 de marzo de 2016]

3.4.1 Instalación y configuración para la navegación

En el caso del software para acceder a la *red Tor* su instalación en Ubuntu es asequible, puesto que solo se debe descargar del sitio oficial la versión que corresponda a la arquitectura del sistema operativo, ya sea de 32 bits o de 64 bits de procesador. El navegador anónimo de *Tor* puede ser descargado desde la *web superficial* en su sitio oficial,³³⁶ una vez que se ha descargado, se descomprime y se ejecuta como aplicación, sin la necesidad de ser instalado en el sistema operativo.

En cuanto a la *Freenet*, la instalación tiene variantes puesto que para su instalación se debe de utilizar la terminal del sistema operativo Ubuntu, e ingresar la línea de comando que corresponde a la descarga de Ubuntu.³³⁷ Para realizar el proceso de instalación *Freenet* recomienda instalar previamente OpenJDK Java 7, disponible en «El centro de software de Ubuntu» del mismo sistema operativo. Después de ejecutar la línea de comando se procede a la configuración mediante la interfaz gráfica para establecer las preferencias de idioma, ubicación en el disco duro, creación de carpetas y creación de íconos para el acceso. En el último paso se configura el nivel de anonimato, capacidad de almacenamiento, seguridad y ancho de banda.

Finalmente en lo que respecta a la instalación de *I2P*, en algunos casos ocurren conflictos de compatibilidad con la extensión de archivo (*.jar*), para evitar este problema se recomienda realizar la instalación por medio de la terminal de Ubuntu, con las respectivas líneas de comando que se proporcionan en la página de descargas del sitio oficial de *I2P*.³³⁸ Una vez que ha concluido la instalación, se debe de configurar tanto el proxy (localhost 127.0.0.1 y asignar el puerto 4444) así como las tasas de transferencia, de acuerdo a la velocidad de bajada y

³³⁶ The onion router. 2016. Download. *Tor*, Recuperado en: <https://www.torproject.org/download/download.html.en> [Consultado 7 de marzo de 2016]

³³⁷ The Freenet Project Inc. 2015. Download. *Freenet project*. Recuperado en: <https://freenetproject.org/download.html#note> [Consultado 7 de marzo de 2016]

³³⁸ The Invisible Internet Project. 2015. Descargas. *The Invisible Internet Project*. Recuperado en: <https://geti2p.net/es/download> [Consultado 17 de febrero de 2016]

velocidad de subida correspondientes. Para designar la configuración de velocidad, se utiliza el dato de la velocidad del Proveedor de Servicio de Internet (como dividendo) entre 1.5 o 2 (como divisor), utilizando el cociente de la división para determinar un estándar de velocidad en *I2P*.

3.4.2 Bitácora de monitoreo

Se presenta la bitácora de monitoreo de las *redes oscuras* **Tor**, *Freenet* e *I2P*, ello con el objetivo de obtener un panorama general sobre la temática y el uso de las *redes oscuras*. El criterio en la cantidad de los sitios monitoreados de cada *red oscura* parte de su complejidad de instalación, configuración, acceso y navegación. En total son 60 sitios monitoreados a manera de muestra: 30 sitios de la *red Tor*, 20 sitios de *Freenet* y 10 sitios de *I2P*. En esta bitácora de monitoreo se aplican los enfoques teóricos correspondientes a los criterios de autoría de la información y clasificación de la información, los cuales permiten entender y estructurar tanto la descripción de las características conforme al análisis y la recuperación de la información. En este sentido de interpretación, la asignación del vocabulario controlado permite delimitar las temáticas y elaborar los datos comparativos sobre los resultados del monitoreo.

La metodología de trabajo se desarrolla a partir de la adquisición de direcciones URL de la *red Tor*, como punto de partida referente al concepto social de *web profunda*, dichas direcciones URL fueron obtenidas en su mayoría en los años 2014 y 2015 en las redes sociales y plataformas sociales de la *web superficial*, por lo que al verificar la existencia de sus contenidos se hizo notable la deshabilitación de muchos sitios, de modo que, fue descartado un alto porcentaje de las direcciones URL. La bitácora en cuestión se encuentra conformada por 60 cedulas compuestas por datos de identificación. Los datos fueron desarrollados durante los periodos de acceso a las *redes oscuras*, ello con el objetivo de establecer uniformidad en los resultados basados en la interpretación y comparación de cada *red oscura*. A continuación se muestran los datos de identificación utilizados y desarrollados en cada cedula.

- Nombre de la red oscura
- Número de sitio investigado
- Nombre del sitio
- Autor
- URL
- Materia general
- Idioma
- Fecha de adquisición de la URL
- Fecha de acceso
- Tipo de acceso conceptual
- Clasificación de la información
- Contenido
- Última fecha de actualización del sitio

En el caso específico de la *red Tor* los números de los sitios investigados no tienen un orden consecutivo debido a que, algunos contenidos se consideraron irrelevantes o tenían elementos insuficientes para su descripción. El dato de la autoría no representa un factor determinante, dado que no existe certidumbre acerca de la identidad de los autores, creadores o administradores de los sitios en las *redes oscuras*. Respecto a las *redes oscuras Freenet e I2P* las direcciones URL fueron obtenidas mediante la navegación en la interfaz de inicio de cada red, por lo que no hubo necesidad de adquirir las direcciones URL en la *web superficial*, por terceros o por otros medios. Los números de los sitios investigados tienen una relación cruzada con su respectiva dirección URL, ello con el objetivo de agilizar la navegación en la computadora portátil utilizando únicamente estos dos datos de identificación para posteriormente conformar las cédulas en una computadora personal de escritorio. Cabe recalcar que, los fundamentos teóricos de la Bibliotecología y estudios de la información proporcionaron los elementos adecuados para realizar una estrategia de trabajo y posteriormente la descripción y el análisis de los contenidos.

El criterio para describir el dato de «materia general» se fundamenta en la afinidad de los contenidos temáticos de los sitios, conforme al vocabulario controlado de los registros obtenidos en los resultados del catálogo en línea LIBRUNAM de la Universidad Nacional Autónoma de México.³³⁹ En cuanto al idioma, en algunos casos fue necesario realizar una traducción mediante un traductor³⁴⁰ de servicio libre multilingüe en línea.

La fecha del periodo de investigación parte del 23 de febrero al 18 de marzo del año 2016. En la *red Tor* se accedió el día 23 de febrero, 12 de marzo y de forma aleatoria del 14 al 18 de marzo. Mientras que en la *Freenet* se accedió el día 26 de febrero, 12 de marzo y de forma aleatoria del 14 al 18 de marzo. Finalmente se accedió a la *red I2P* el día 28 de febrero, 12 de marzo y de forma aleatoria del 14 al 18 de marzo. El dato sobre el tiempo de navegación al igual que la fecha de acceso se registra a modo de indicador del tiempo transcurrido en la exploración, finalmente el análisis proporciona una interpretación con base en la lectura y observación de los contenidos para determinar los datos representativos de cada sitio.

El dato de «tipo de acceso conceptual» deriva de la interpretación en cuanto a la complejidad temática de cada uno de los sitios de las *redes oscuras*, de manera que, para hacer uso de los servicios y contenidos es imprescindible contar con un conocimiento específico acerca del uso, beneficios y consecuencias en la utilidad de la información de ciertos sitios. Por lo que el acceso conceptual queda segmentado en:

- tipo de acceso **conceptual requerido** o,
- tipo de acceso **conceptual no requerido**.

³³⁹ UNAM. 2016. Catálogos y Recursos Electrónicos. *Bibliotecas UNAM*. Recuperado en: <http://bibliotecas.unam.mx/index.php/catalogos> [Consultado 22 de febrero de 2016]

³⁴⁰ Traductor de Google. 2016. Página de inicio, Traductor de Google. *Translate Google*. Recuperado en: <https://translate.google.com/?hl=es> [Consultado 23 de febrero de 2016]

En cuanto a la clasificación de la información, el criterio se fundamenta en la disponibilidad de los contenidos y servicios. Aunque en algunos casos se requiere de un registro previo para el acceso o bien, se desconoce la intención de los contenidos a descargar, además del argot en determinados sitios de opinión. De esta manera se clasifica a la información si esta tiende a ser:

- a) **pública accesible** (para cualquier usuario),
- b) **reservada** (con requerimientos de acceso) o,
- c) **interna** (asuntos particulares de alguna comunidad de usuarios).

En lo que concierne a los datos del contenido de los sitios, se describen las características más representativas así como sus servicios, temáticas y posturas ideológicas, en caso de ser explícitamente manifestadas. Finalmente se aporta un dato de actualización para determinar la antigüedad y el transcurso en los contenidos y servicios.

En síntesis se puede agregar que, la descripción y el análisis de los contenidos se derivan de un proceso de catalogación y clasificación mediante la lectura, la investigación y la normatividad, puesto que se asignan valores de distinción y concordancia, así como la construcción de una estructura compuesta por los datos representativos.

3.4.3 Resultados del monitoreo

Durante el ejercicio del monitoreo se detectaron las características de cada *red oscura*, siendo que en **Tor** existe una línea temática en donde se destaca el interés de sus usuarios por la crítica hacia el control social, así como una economía basada en los servicios y productos ilícitos dentro de la *red oscura*. Por otro lado, la *red oscura Freenet* mantiene un discurso generalizado hacia las conspiraciones y como el código informático puede coadyuvar a disminuir la vigilancia por parte del *Estado-nación*. En lo que respecta a la *red oscura I2P*, su

eje temático se encuentra orientado hacia los servicios de almacenamiento y desarrollo de tecnologías para procurar el anonimato.

En cuanto al anonimato como tema medular se puede interpretar que, las tres *redes oscuras* manifiestan el interés de sus usuarios hacia la incidencia de la vigilancia en la privacidad de los individuos. Por lo que la intención del presente ejercicio de monitoreo, navegación e interpretación de los sitios se orienta a comprobar la necesidad de los usuarios que buscan alternativas ante los sistemas de regulación en la Web, en primera instancia por el *Estado-nación* y por los Proveedores del Servicio de Internet.

A continuación se presentan las tablas comparativas de las tres *redes oscuras* monitoreadas, ello con el objetivo de establecer sus características, similitudes y diferencias de acuerdo a sus temas, servicios e idiomas, además de aportar un nuevo punto de comparación, de acuerdo al concepto de *web profunda* bajo la percepción social. En la sección del anexo se encuentran las cédulas correspondientes a **Tor** (véase anexo A, pág. 201), de igual forma se encuentran las cédulas de *Freenet* (véase anexo B, pág. 216) e *I2P* (véase anexo C, pág. 228). Los temas presentados en la siguiente tabla son una muestra de lo que se puede encontrar en las *redes oscuras* **Tor**, *Freenet* e *I2P*.

Afinidades temáticas	Tor	Freenet	I2P
Documentos sobre informática		Seguridad informática y Programas de código abierto para computadoras	Alojamiento web y Desarrollo de sitios web
Contenidos sobre el anonimato	Anonimato, Vigilancia, Control social, Libertad de expresión y Libertad de información	Anonimato, Vigilancia y Control social	Anonimato, Seguridad informática, Libertad de expresión y Libertad de información
Servicios y contenidos ilícitos	Tráfico de armas, Tráfico de drogas, Cibercrimen y Piratería	Espionaje	Piratería
Opinión sobre aspectos sociales	Terrorismo, Política mundial	Xenofobia, Opinión pública extranjera sobre el Islam, Espionaje, Conspiraciones y Globalización	
Ocio y entretenimiento	Películas y series de TV, Libros digitales y digitalizados	Literatura, Manga y anime, Comics y Juegos de rol	Películas y series de TV
Interés sobre la sexualidad	Arte erótico y Pornografía	Literatura inmoral, Sexo en la literatura, Sadomasoquismo y Aspectos eróticos	

Tabla 16. Comparación de los contenidos temáticos de las redes oscuras: Tor, Freenet e I2P. Fuente: creación propia.

	Tor	Freenet	I2P
Servicios principales	Navegación anónima en la web superficial	Anonimato en su red de pares	Red de comunicación anónima
Servicios secundarios	Almacenamiento de contenidos	Almacenamiento de contenidos	Almacenamiento de contenidos
	Trasferencia de moneda digital		Trasferencia de moneda digital
	Motores de búsqueda		
	Correo electrónico		

Tabla 17. Servicios de las redes oscuras: Tor, Freenet e I2P. Fuente: creación propia.

El anonimato es el servicio esencial que proporcionan las tres *redes oscuras*, seguido del almacenamiento y gestión de contenidos, ya sea para la difusión de intereses personales o para brindar servicios alternativos a los de la Web a causa de la carencia de anonimato, libertad de expresión y libertad a la información, siendo estos los temas frecuentes en las *redes oscuras*.

	Tor	Freenet	I2P
Temas frecuentes	<ul style="list-style-type: none"> • Libertad de expresión • Libertad de información 	<ul style="list-style-type: none"> • Vigilancia 	<ul style="list-style-type: none"> • Anonimato • Seguridad informática

Tabla 18. Comparación de los temas frecuentes en las redes oscuras: Tor, Freenet e I2P. Fuente: creación propia.

Por otro lado, se divisa en las *redes oscuras* el idioma inglés como lengua franca seguido del alemán, ruso y francés por lo que se puede interpretar que, el uso de estas tecnologías ocurre en el mundo occidental, concretamente en los países anglosajones y europeos. Países en los que en la medida de lo posible, han superado los conflictos bélicos dentro de sus territorios nacionales (como las Guerras Mundiales); en contraste con sus sistemas de vigilancia creados y desarrollados en respuesta a los atentados terroristas acontecidos en dichos países.

	Tor	Freenet	I2P
Idiomas recurrentes	1.- Inglés 2.- Alemán 3.- Polaco 4.- Finlandés 5.- Portugués	1.- Inglés 2.- Francés 3.- Alemán 4.- Español 5.- Polaco	1.- Inglés 2.- Ruso 3.- Francés 4.- Alemán 5.- Chino

Tabla 19. Idiomas recurrentes de las redes oscuras de acuerdo a su índice de frecuencia. Fuente: creación propia.

Sortear el acceso conceptual, es un requerimiento indispensable para comprender la información presentada, puesto que ello determina el entendimiento de los contenidos, en primera instancia para identificar la validez o falsedad de la información y por otro lado para capitalizar el nuevo conocimiento sobre las posibilidades, beneficios o riesgos al utilizar estos servicios y contenidos, así como de solicitar los productos ofrecidos. Con base en los datos cuantitativos de los sitios monitoreados y analizados, el entendimiento conceptual tiende a ser un requisito fundamental en el uso de los servicios de *Freenet* e *I2P*; mientras que en la *red oscura Tor* se detectó que lo es, parcialmente.

	Tor	Freenet	I2P
Acceso conceptual	Requerido / no requerido	Preferentemente requerido	Preferentemente requerido

Tabla 20. Tipo de acceso conceptual. Fuente: creación propia.

A partir de los datos obtenidos se puede señalar que, por lo general en las tres *redes oscuras* no es indispensable realizar un registro previo para acceder a los servicios y contenidos, de modo que, la información tiende a ser pública para todo aquel que utilice el software de acceso y navegación correspondiente a cada *red oscura*. Cabe señalar que en *I2P* los contenidos en su mayoría se relacionan a temas altamente especializados para ciertas comunidades de usuarios.

	Tor	Freenet	I2P
Clasificación de la información	1.- Pública accesible 2.- Reservada 3.- Interna	1.- Pública accesible 2.- Reservada 3.- Interna	1.- Pública accesible 2.- Interna 3.- Reservada

Tabla 21. Clasificación de la información de acuerdo a la cantidad de sitios detectados con este atributo. Fuente: creación propia.

Finalmente, con base en la triangulación de los resultados obtenidos sobre las tres *redes oscuras*, se puede determinar que, la *red Tor* denota una mayor apertura hacia los temas, servicios y contenidos; mientras que *Freenet* e *I2P* manifiestan un perfil más elitista que va desde la instalación del software de navegación hasta los contenidos y servicios, por lo que existe una brecha de acceso para el usuario común. A este respecto es menester realizar un ejercicio

de reflexión en los sucesos que provocaron que las *redes oscuras Freenet e I2P* modificaran sus políticas de información.

A manera de síntesis se puede agregar que, el acceso a los contenidos es preminente puesto que de ello depende la adquisición de conocimientos mediante el análisis de la información ya sea para tomar la decisión adecuada o para conocer la probabilidad de riesgo. La triangulación de la información permite ampliar los horizontes acerca del contexto, objeto o sujeto en cuestión. Por tanto, el acceso y el uso a las *redes oscuras* es tan sólo una extensión sobre nuestra condición cultural y socioeconómica, puesto que el criterio, la lectura del mundo, los conocimientos y el sentido común se aplican a estas mismas instancias.

3.5 Las redes oscuras después del 2015

El concepto social de la *web profunda* (la *red oscura Tor*) comenzó a popularizarse desde el año 2011 hasta el año 2013³⁴¹ por lo que dicho concepto tuvo resonancia en los años posteriores, incluso a principios del 2016. Con base en estos antecedentes en cuanto al concepto social, existe una complejidad en el intento por pretender asignar una nomenclatura adecuada a la tecnología de alojamiento de contenidos, transferencia de archivos, anonimato y privacidad, conocida por antonomasia como *redes oscuras*. Cabe aclarar que, es a finales del año 2015³⁴² que el concepto de *redes oscuras* (darknet) tiene mayor índice de búsqueda en la *web superficial* en Europa; mientras en ese mismo año el concepto de *web profunda* (*deep web*) tiene un mayor índice de interés en Latinoamérica. Razón por la cual se puede deducir el alto impacto y la aceptación

³⁴¹ Epix network. *Deep Web*. DVD. Loc. Cit.

³⁴² Google. 2016. Página de inicio, Google trends. *Google trends*. Recuperado en: <https://www.google.com/trends/> [Consultado 23 de marzo de 2016]

social en los años venideros por el concepto de la *web profunda*, *deep web*³⁴³ o *dark web*.³⁴⁴

Aun en el año 2016 en donde se finaliza la investigación sobre el acceso a las *redes oscuras*, persisten temas y servicios (en el caso de **Tor**), concernientes a las opiniones políticas, la globalización, la vigilancia, el secreto de *Estadonación*, el anonimato, la anarquía, la seguridad informática, compra y venta de documentos oficiales apócrifos, tráfico de armas y venta de drogas; con base a los antecedentes del periodo 2012–2015 se ha notado la aparente ausencia en cuanto a los contenidos sobre la pornografía infantil. Por otro lado, un aspecto a destacar sobre el uso que puede conllevar más allá de la legalidad de la propiedad intelectual o la libertad a la información, es el almacenamiento y descarga de literatura de cualquier índole, lo que da pauta a la disponibilidad de libros y contenidos, sin importar las barreras ideológicas, geográficas y políticas.

A principios del año 2016 se dio a conocer que Matthew Edman³⁴⁵ aparentemente ex colaborador del proyecto **Tor**, se incorporó al equipo de trabajo del FBI desde el año 2012, para crear un *malware* dedicado a desenmascarar a los usuarios de **Tor**, con la intención de dismantelar los servicios del sitio *Silk Road* y de esta manera obtener los elementos legales para arrestar a su administrador en cuestión, por tráfico de narcóticos. A mediados del año 2016 el comportamiento del mercado negro en las redes oscuras, se ha orientado hacia la venta del software para el control remoto de los dispositivos y

³⁴³ Marin, Eduardo. 19 de agosto de 2016. 5 motivos para dejar de usar Google como buscador por defecto. **Gizmodo en español**. Recuperado en: <http://es.gizmodo.com/5-motivos-para-dejar-de-usar-google-como-buscador-por-d-1785519010> [Consultado 21 de agosto de 2016]

³⁴⁴ Crespo, Adrián. 14 de agosto de 2016. La red Tor gana seguridad gracias a los nuevos dominios .onion. **Redes zone**. Recuperado en: <http://www.redeszone.net/2016/08/14/troyano-bancario-scylex-aparece-la-dark-web/> [Consultado 21 de agosto de 2016]

³⁴⁵ Khandelwal, Swati. 27 de abril de 2016. Former tor developer created malware for FBI to unmask tor users. **The hacker news**. Recuperado en: <http://thehackernews.com/2016/04/tor-unmask-malware.html> [Consultado 8 de mayo de 2016]

computadoras personales³⁴⁶ y, a la venta de cuentas de acceso³⁴⁷ referentes a los servicios de la Web. No obstante existen proyectos de investigación³⁴⁸ orientados a mejorar en la medida de lo posible la seguridad de **Tor**, en contraparte, existe una constante oposición por parte del *Estado-nación* y empresas privadas en averiguar la operatividad de **Tor**, mediante la suplantación operativa a través de servidores maliciosos.³⁴⁹ Sumado a esta problemática sempiterna, la *red oscura Tor* debe adaptarse a los nuevos protocolos, como lo es el caso del Protocolo de Internet versión 6 (por sus siglas en inglés IPv6)³⁵⁰ el cual es una actualización para la asignación del número de identificación IP, ello a causa del incremento de usuarios con acceso al servicio de Internet.

En cuanto a la *red oscura Freenet*, el tipo de usuarios se refleja en cierto modo por los contenidos e ideología acerca de temas sobre la vigilancia, el control social del *Estado-nación*, la censura y las vulnerabilidades en el servicio de Internet. En *Freenet* los contenidos están encauzados a grupos más definidos y con necesidades de información orientadas a temas referentes a la informática, la crítica al extremismo ideológico, la geopolítica y la vigilancia. En esta *red oscura* comienzan a manifestarse algunas prácticas sociales y legalmente inadecuadas que propiciaron el cierre de varios sitios de la *red oscura Tor*. No obstante al parecer sólo se trata de casos aislados en la *Freenet*.

³⁴⁶ Crespo, Adrián. 7 de agosto de 2016. Remcos, otro malware que está a la venta en la Dark Web. **Redes zone**. Recuperado en: <http://www.redeszone.net/2016/08/07/remcos-otro-malware-que-esta-a-la-venta-en-la-dark-web/> [Consultado 13 de agosto de 2016]

³⁴⁷ Gabilondo, Pablo. 5 de agosto de 2016. Deep web: el mercado clandestino de las cuentas robadas. **El confidencial**. Recuperado en: <http://www.elconfidencial.com/tecnologia/2016-08-05/precio-cuentas-robadas-deep-web-1242837/> [Consultado 13 de agosto de 2016]

³⁴⁸ Conti, Mauro Et al. "Selfrando: Securing the Tor Browser against De-anonymization Exploits". **Proceedings on Privacy Enhancing Technologies**, no. 4 (2016): 1-16. Recuperado en: https://www.ics.uci.edu/~perl/pets16_selfrando.pdf [Consultado 20 de junio de 2016]

³⁴⁹ García, Alberto. 25 de julio de 2016. Un experimento detecta 110 servidores maliciosos en la red Tor. **Grupo ADSL Zone**. Recuperado en: <http://www.adszone.net/2016/07/25/experimento-detecta-110-servidores-maliciosos-la-red-tor/> [Consultado 31 de julio de 2016]

³⁵⁰ Velasco, Rubén. 19 de agosto de 2016. La red Tor no está preparada para trabajar con conexiones IPv6. **Redes zone**. Recuperado en: <http://www.redeszone.net/2016/08/19/la-red-tor-no-esta-preparada-trabajar-conexiones-ipv6/> [Consultado 21 de agosto de 2016]

En la *red oscura I2P*, los servicios de almacenamiento y descarga de contenidos son más notables que en las redes anteriormente mencionadas. *I2P* se caracteriza por el enfoque de sus contenidos temáticos en torno a la configuración, operatividad y optimización de su tecnología de comunicación anónima, la cual es el servicio principal para su comunidad de usuarios.

3.6 ¿Se recupera la misma información en la web superficial?

Si bien en la *web superficial* existe un mayor número de contenidos, las *redes oscuras* no pretenden tener visibilidad, sin importar la veracidad o falsedad de la información, aunada a la legitimidad o ilegalidad de sus servicios. En las *redes oscuras*, la intención de la información no es la misma que en la *web superficial*, dado que se trata esencialmente de pensamientos e ideas que son parte de la paranoia, la fantasía, el secreto, la proyección psicológica o el sentir más profundo de los individuos; caso contrario de los contenidos de la *web superficial* en donde se busca la visibilidad y en ocasiones aunque sea de forma anónima, se pretende el reconocimiento.

Los contenidos en las *redes oscuras* tienden a ser difusos, lacónicos, someros y breves; en la *web superficial* se genera constantemente la retroalimentación sobre un tema de interés público, ello debido a la inmediatez y a la vinculación entre las distintas redes sociales, lo que da pauta a un constante cambio y crecimiento en los contenidos. Razón por la cual, la comparación en cuanto a la recuperación de la información no es viable, ya que los enfoques difieren. El origen de procedencia de los contenidos es un aspecto a destacar en cuanto a la recuperación de la información en la *web superficial* y las *redes oscuras*, ya que en ocasiones se desconoce si el texto, imagen, audio, video o software pertenece explícitamente a las *redes oscuras* o si proviene de la *web superficial*.

Incluso si no es decisión del administrador del sitio retirar sus contenidos en las *redes oscuras* los sitios pueden llegar a quedar deshabilitados a largo plazo según sea considerado y tipificado legalmente como material o actividad delictiva

por parte de las autoridades competentes de cada país. Concretamente no se recupera la misma información.

3.7 Aspectos legales en torno a los servicios y contenidos

Toda actividad y transacción ilícita ya sea en la *web superficial* como en las *redes oscuras* puede acarrear consecuencias negativas para el usuario. De manera que existen autoridades tanto en el plano internacional como en el nacional que regulan e investigan de forma particular o coordinada el comportamiento de los individuos en la Web. En consecuencia, los elementos de la complejidad en la Web inciden y modifican la conducta de los usuarios, como reacción natural ante el control de sus actividades.

Para tener un panorama general en cuanto a la relevancia de la regulación de Internet y el monitoreo de los usuarios en la Web, se mencionan a continuación algunos casos a nivel internacional sobre la vigilancia, censura y actos ilícitos.

3.7.1 Contexto internacional

En lo que respecta al continente asiático, las autoridades de China³⁵¹ aseguran que su seguridad informática es altamente vulnerable, por lo que se podrá exigir a los Proveedores del Servicio de Internet, la información que consideren pertinente, así como de analizar y regular la información potencialmente relacionada al terrorismo. Mientras que en Turquía³⁵² se dio el caso de un individuo condenado por fraude bancario y robo de identidad, por medio de los servicios de la Web.

En el continente europeo concretamente en Austria³⁵³ una persona fue allanada y sus equipos de cómputo confiscados, puesto que se le encontró culpable por

³⁵¹ Álvarez, Raúl. 27 de diciembre de 2015. China ya podrá exigir a cualquier compañía información confidencial de sus usuarios. *Xataka*. Recuperado en: <http://www.xataka.com/legislacion-y-derechos/china-ya-podra-exigir-a-cualquier-compania-informacion-confidencial-de-sus-usuarios> [Consultado 9 de enero de 2016]

³⁵² Wei, Wang. 11 de enero de 2016. 26-Year-Old Hacker Sentenced to Record 334 Years in Prison. *The hacker news*. Recuperado en: <http://thehackernews.com/2016/01/hacker-sentenced-prison.html> [Consultado 11 de enero de 2016]

³⁵³ BBC. 30 de noviembre de 2012. Op. Cit., Recuperado en: <http://www.bbc.com/news/technology-20554788> [Consultado 9 de enero de 2015]

la distribución de imágenes de pornografía infantil en la *red oscura*. En España,³⁵⁴ un hombre fue acusado y condenado por obtener información íntima de su expareja sentimental, mediante un software de espionaje. Otros dos casos sucedieron en Alemania, el primero³⁵⁵ se trata de un individuo arrestado por utilizar la *red oscura* para la venta de narcóticos. En cuanto al segundo caso,³⁵⁶ otro individuo fue puesto bajo custodia y en espera de la extradición a los Estados Unidos de América, por los cargos de distribución de pornografía infantil. Mientras que en Francia,³⁵⁷ a raíz de los actos terroristas a la revista *Charlie Hebdo*, se planteó la prohibición en el uso de la *red oscura Tor*.

En los Estados Unidos de América³⁵⁸ los delitos federales persiguen los juegos de apuesta en línea toda vez que no se encuentren regulados, es decir, que el estado del territorio americano en donde el usuario realiza la conexión al servicio web sea regulado y, el estado en donde se encuentre geográficamente el hardware para dicha transacción, sea legal. Por otro lado, los grupos o personas involucrados en ciberataques³⁵⁹ que no se encuentren geográficamente dentro de los Estados Unidos de América pueden ser sancionados de forma financiera, por lo que existen consecuencias sin importar las divisiones geográficas.

En el año 2015 un hombre fue identificado por el FBI como el administrador del sitio *Silk Road versión 2.0*³⁶⁰ en la *red Tor*, en donde se ofrecía el servicio de

³⁵⁴ El país. 18 de enero 2016. Dos años por espiar a su exnovia con un programa en el móvil. *El país*. Recuperado en: http://politica.elpais.com/politica/2016/01/17/actualidad/1453069620_328953.html [Consultado 28 de abril de 2016]

³⁵⁵ Locker, Theresa. 3 de noviembre de 2015. Germany's most notorious Darknet drug dealer sentenced to only 7 years. *Motherboard*. Recuperado en: <http://motherboard.vice.com/read/germanys-most-notorious-darknet-drug-dealer-sentenced-to-only-7-years> [Consultado 19 de diciembre de 2015]

³⁵⁶ Peachey, Paul. 23 de agosto de 2013. Eric Eoin Marques: 28-year-old architect's son from Dublin accused of being world's biggest dealer in child abuse images. *Independent*. Reino Unido. Recuperado en: <http://www.independent.co.uk/news/world/europe/eric-eoin-marques-28-year-old-architect-s-son-from-dublin-accused-of-being-world-s-biggest-dealer-in-8782756.html> [Consultado 31 de enero de 2016]

³⁵⁷ Pastor, Javier. 10 de diciembre de 2015. Cómo ha cambiado internet después de las filtraciones de Snowden. *Xataka*. Recuperado en: <http://www.xataka.com/privacidad/como-ha-cambiado-internet-despues-de-las-filtraciones-de-snowden> [Consultado 9 de enero de 2016]

³⁵⁸ Lessig, Lawrence. Ídem. Pág. 112.

³⁵⁹ Reuters. 1 de abril de 2015. Lanza EU plan de sanciones financieras contra ciberataques. *La Jornada en internet*. Recuperado en: <http://www.jornada.unam.mx/ultimas/2015/04/01/lanza-estados-unidos-programa-de-sanciones-a-ciberataques-3017.html> [Consultado 1 de abril de 2015]

³⁶⁰ Khandelwal, Swati. 4 de abril de 2016. Silk Road 2.0 dark-web admin pleads guilty. *The hackers news*. Recuperado en: <http://thehackernews.com/2016/04/silk-road-dark-web.html> [Consultado 6 de abril de 2016]

venta de narcóticos, además, el administrador fue declarado culpable por posesión de contenidos digitales relacionados a la pornografía infantil con una posible condena de 8 años de prisión. Mientras que, a principios del año 2016 se presentó por parte del Comité Asesor sobre Normas Federales de Procedimiento Criminal, una propuesta para que la Corte Suprema de los Estados Unidos de América actualice la regla 41 del procedimiento penal,³⁶¹ de aprobarse definitivamente dicha actualización a finales del año 2016, permite el acceso a las *redes oscuras*, las Redes Privadas Virtuales y los servicios proxy además del libre acceso de forma remota a las computadoras personales, en caso de que el juez en turno lo considere.

3.7.2 Contexto nacional

Un estudio proporcionado por el Centro de Innovación para la Gobernanza Internacional (CIGI) a través de la empresa de estudios de mercado *Ipsos*,³⁶² revela que los habitantes entrevistados en México, opinan que las *redes oscuras* deberían cerrarse, cabe mencionar que, dicho estudio sólo muestra a groso modo los porcentajes de los distintos países en donde la percepción de las *redes oscuras* es negativa.

En lo que se refiere a la privacidad del usuario, el Acuerdo Comercial Anti-falsificación³⁶³ (ACTA), busca la cooperación internacional, la cual incluye a México, dicha cooperación tiene como objetivo el de regular el intercambio de información y la solicitud a los Proveedores del Servicio de Internet en caso de tener usuarios bajo sospecha, a pesar de que ello atente en contra de la privacidad y la intimidad del usuario. De este modo se vulnera la confidencialidad de los datos de conexión.

³⁶¹ Reitman, Rainey. 30 de abril de 2016. With rule 41, little-known committee proposes to grant new hacking powers to the government. **Electronic Frontier Foundation**. Recuperado en: <https://www.eff.org/deeplinks/2016/04/rule-41-little-known-committee-proposes-grant-new-hacking-powers-government> [Consultado 8 de mayo de 2016]

³⁶² Centre for International Governance Innovation. 29 de marzo de 2016. Seven in ten (71%) global citizens say the dark net should be shut down. **CIGI online**. Recuperado en: https://www.cigionline.org/sites/default/files/factum_2016_cigiippos_survey_darknet_0.pdf [Consultado 8 de mayo de 2016]

³⁶³ Locker, Theresa. 3 de noviembre de 2015. Op. Cit., Recuperado en: <http://motherboard.vice.com/read/germanys-most-notorious-darknet-drug-dealer-sentenced-to-only-7-years> [Consultado 19 de diciembre de 2015]

Respecto a la vulnerabilidad de datos personales, la compañía AT&T³⁶⁴ en el año 2015, pago una multa millonaria por la venta de datos sobre sus clientes. En esta operación estuvieron involucrados empleados que laboraban en México, Filipinas y Colombia. En respuesta a este tipo de sucesos, se ha creado la iniciativa llamada Defensa de Derechos Digitales (por sus siglas R3D),³⁶⁵ misma que presentó un proyecto para defender los derechos del cliente ante los Proveedores del Servicio del Internet en México.

En cuanto al tema de la seguridad y el orden público en el plano digital, es la Policía de Ciberdelincuencia Preventiva³⁶⁶ la fuerza de seguridad responsable en el monitoreo para la detección de pornografía infantil, trata de personas, fraudes, extorciones y robo de identidad en la Ciudad de México³⁶⁷ (anteriormente llamada Distrito Federal). Mientras que por otro lado, la Policía Federal³⁶⁸ tiene una División Científica para brindar apoyo en materia de ciberinteligencia. La División Científica actúa cuando se identifican actos que vulneran la seguridad informática de las empresas financieras. En este sentido Alejandra Morán, Abraham Servín y Oscar Alquicira³⁶⁹ comentan que, cualquier individuo por experto que sea en el tema de la informática y en el acceso a la infraestructura tecnológica, es proclive a ser localizado y sometido a los principios jurídicos. Cabe señalar que, en este aspecto hay precedentes, puesto

³⁶⁴ La Jornada. 7 de abril de 2015. Multa millonaria a ATT por robo de datos en México y otros países. *La Jornada en internet*. Recuperado en: <http://www.jornada.unam.mx/ultimas/2015/04/08/multa-millonaria-a-att-por-robo-de-datos-en-mexico-y-otros-paises-9222.html> [Consultado 8 de abril de 2015]

³⁶⁵ Bárcenas, Javier. 17 de junio de 2015. Si el gobierno mexicano pide acceso a tus datos, ¿las empresas de telecomunicación se los entregan? *MSN noticias*. Recuperado en: <http://prodigy.msn.com/es-mx/noticias/mexico/si-el-gobierno-mexicano-pide-acceso-a-tus-datos-%C2%BF-las-empresas-de-telecomunicaci%C3%B3n-se-los-entregan/ar-BBleGc1> [Consultado 20 de junio de 2015]

³⁶⁶ Jiménez, Gerardo. 4 de abril de 2013. SSPDF crea la policía cibernética, para evitar delitos por Internet. *Excelsior*. Recuperado en: <http://www.excelsior.com.mx/comunidad/2013/04/04/892055> [Consultado 20 de julio de 2013]

³⁶⁷ México. Cámara de Diputados. 20 de enero de 2016. Comisión Permanente declara constitucional Reforma Política de la Ciudad de México. *Comunicación social, Boletín No. 0824*. Recuperado en: <http://www5.diputados.gob.mx/index.php/esl/Comunicacion/Agencia-de-Noticias/2015/Diciembre/09/1287-Aprueban-diputados-en-lo-general-y-con-cambios-dictamen-de-minuta-del-Senado-sobre-la-reforma-politica-de-la-Ciudad-de-Mexico-y-discuten-58-reservas> [Consultado 9 de marzo de 2016]

³⁶⁸ Nácar, Jonathan. 27 de noviembre de 2015. Policía Federal se fortalece en la lucha contra delitos cibernéticos. *MSN noticias*. Recuperado en: <http://prodigy.msn.com/es-mx/noticias/mexico/polic%C3%ADa-federal-se-fortalece-en-la-lucha-contradelitos-cibern%C3%A9ticos/ar-AAfHUHW?li=AA5a7e&ocid=mailsignout> [Consultado 19 de diciembre de 2015]

³⁶⁹ Morán Espinosa, Alejandra., Servín Caamaño, Abraham Alejandro y Alquicira Gálvez, Oscar. *Ibid.* Recuperado en: <http://revista.seguridad.unam.mx/numeros/numero-23> [Consultado 12 de abril de 2015]

que el portal web de MVS sufrió un ataque en el año 2015 por hacktivistas mexicanos en contra del despido de Carmen Aristegui³⁷⁰ de la empresa MVS.

Conforme a este tipo de situaciones, la Ley Federal de Telecomunicaciones y Radiodifusión establece en el año 2014, en su artículo 178 lo siguiente:

Artículo 178 Bis.- A la persona física o en su caso al representante de la persona moral que sea requerida por el Ministerio Público o por la autoridad competente para colaborar o aportar información para la localización geográfica, en tiempo real de los dispositivos de comunicación en términos de lo dispuesto por la Ley Federal de Telecomunicaciones y Radiodifusión, que estén relacionados con investigaciones en materia de delincuencia organizada, delitos contra la salud, secuestro, extorsión, amenazas o cualquiera de los previstos en el capítulo II del Título Noveno del Código Penal Federal y que se rehusare hacerlo de forma dolosa, se le impondrá una pena de prisión de 3 a 8 años y de cinco mil a diez mil días multa.

Las mismas penas se aplicarán a la persona física, o en su caso al representante de la persona moral que de forma dolosa obstaculice, retrase sin justa causa o se rehusó a colaborar en la intervención de comunicaciones privadas, o a proporcionar información a la que estén obligados, en los términos de la legislación aplicable.

Se aplicarán las mismas penas a la persona física, o en su caso al representante de la persona moral que sea requerida por las autoridades competentes, para colaborar o aportar información para la localización geográfica, en tiempo real de los dispositivos de comunicación en términos de lo dispuesto por la Ley Federal de Telecomunicaciones y Radiodifusión y que se rehusare hacerlo de forma dolosa.³⁷¹

³⁷⁰ Véase Camacho Servín, Fernando y Dávila, Ricardo. 14 de marzo de 2015. Anonymous hackea portal de MVS y publica comunicados apócrifos. **La Jornada en internet**. Recuperado en: <http://www.jornada.unam.mx/ultimas/2015/03/14/anonymous-publica-falso-comunicado-de-mvs-sobre-ex-colaboradores-de-aristegui-6832.html> [Consultado 21 de marzo de 2015]

³⁷¹ México. Congreso de los Estados Unidos Mexicanos. 14 de julio de 2014. **Ley Federal de Telecomunicaciones y Radiodifusión**. Título décimo sexto, capítulo único. Medios de impugnación, Título décimo sexto. Capítulo único, Medios de impugnación. Recuperado en: <http://www.sct.gob.mx/fileadmin/Comunicaciones/LFTR.pdf> [Consultado 9 de marzo de 2015]

De modo que, habrá sanciones en caso de no cooperar u obstruir en el curso de las averiguaciones con las autoridades competentes, sobre las investigaciones concernientes a la información y las telecomunicaciones. Dicho esto, es la tecnología digital un factor que polariza la preeminencia de la biblioteca, dado que las bibliotecas y su personal podrían encontrarse en circunstancias vinculadas a la colaboración con el Ministerio Público y autoridades con facultades legales. En este sentido, el código de ética del Colegio Nacional de Bibliotecarios³⁷² hace mención sobre la confidencialidad, la oposición a la censura y la facilidad de acceso a la información conforme a las leyes del Estado mexicano. Por tanto, es menester para el bibliotecólogo no sólo el de estar informado sobre el código de ética, sino también de conocer los aspectos legales concernientes a la tecnología, el acceso a los servicios y contenidos en la Web.

A pesar de que no se conocen antecedentes relacionados con la biblioteca y las *redes oscuras* en México, es pertinente considerar la regulación nacional en el uso de las telecomunicaciones, puesto que, es el responsable administrativo de la biblioteca un sujeto proclive a los procesos jurídicos así como a las sanciones penales en caso de no cooperar con las autoridades. Por lo que la confidencialidad, el anonimato y la privacidad en la biblioteca son ideales a alcanzar que poco a poco han sido rebasados por los aspectos legales propuestos e impuestos por el *Estado-nación*. Pero también es necesaria la regulación jurídica en el uso del servicio de conexión a Internet y navegación en la Web, con el fin de deslindar responsabilidades.

Mientras que en el contexto internacional, el código de ética de la Federación Internacional de Asociaciones de Bibliotecarios e Instituciones³⁷³ (por sus siglas en inglés IFLA), señala como puntos esenciales, a la confidencialidad y la privacidad de los datos personales, siendo estos debidamente gestionados en la

³⁷² Colegio Nacional de Bibliotecarios. 1991. Código de ética profesional. **CNB**. Recuperado en: <http://www.cnb.org.mx/index.php/documentos/codigo-de-etica> [Consultado 4 de mayo de 2016]

³⁷³ International Federation of Library Associations and Institutions. 2012. Código de ética de la IFLA para bibliotecarios y otros trabajadores de la información. **IFLA**. Recuperado en: <http://www.ifla.org/files/assets/faife/codesofethics/spanishcodeofethicsfull.pdf> [Consultado 4 de mayo de 2016]

biblioteca de manera responsable en los procesos institucionales, administrativos y legales. Asimismo, se hace mención sobre las limitaciones a causa del derecho de autor, el derecho de copia y la propiedad intelectual; así como la alternativa del dominio público y su disponibilidad conforme a las leyes. Finalmente, en lo que respecta al código de ética de la Asociación Americana de Bibliotecas³⁷⁴ (por sus siglas en inglés ALA) se enfatizan aspectos referentes tanto a la confidencialidad, la privacidad y la resistencia a la censura, como el respeto al derecho de autor, la propiedad intelectual y el derecho de copia. En dicho código, también se hace énfasis en el desapego por las convicciones y las posturas ideológicas del bibliotecario, ello con el fin de ser un profesional neutral ante las necesidades del usuario, incluyendo a la biblioteca como mediador social.

En este tenor, el código de ética al ser un conjunto de normas y principios para encaminar al individuo, asociaciones y sociedades a la mediación de la conducta, debe ser congruente a la realidad, por lo que resulta acuciante cuando menos en México establecer una revisión al código de ética del *Colegio Nacional de Bibliotecarios*, en donde se redimensionen los aspectos relacionados a la tecnología digital, el anonimato, la privacidad y los aspectos legales. A este respecto en ocasiones resulta complejo para el bibliotecólogo apearse al código, puesto que en ciertos momentos, su integridad, certidumbre económica y estatus social se ven comprometidos al ejercer la normatividad concerniente al acceso a la información.

Cabe resaltar que, existen contrastes entre el quehacer bibliotecológico como los derechos de autor, los derechos de copia, la confidencialidad, el acceso abierto a los recursos y; la naturaleza anárquica de las *redes oscuras* como resultado del acceso restringido, la vigilancia y la censura. Ante este panorama,

³⁷⁴ American Library Association. 28 de junio de 1995. El código de ética de la Asociación de Bibliotecas de los Estados Unidos. **IFLA.** Recuperado en: <http://www.ala.org/advocacy/sites/ala.org/advocacy/files/content/proethics/codeofethics/coespanishversion/codigodeetica.pdf> [Consultado 4 de mayo de 2016]

el bibliotecólogo deberá de ampliar el espectro en el acceso a la información, además de interactuar con las tecnologías disruptivas e integrarse como colaborador en los aspectos tecnológicos referentes al acceso y la gestión de contenidos, ello con el fin de reducir el rezago tecnológico y financiero al que se enfrenta cotidianamente.

3.8 Las redes oscuras en el quehacer bibliotecario

El antecedente histórico que incide de manera notable entre la biblioteca y las *redes oscuras* se da en el año 2013, con el arresto de Ross William Ulbricht,³⁷⁵ conocido como “*Dread Pirate Roberts*”, quien según el FBI era el administrador del sitio nombrado *Silk Road*, en donde se proporcionaba el servicio de venta de narcóticos mediante la *red oscura Tor*. El arresto tuvo lugar en la biblioteca pública de San Francisco, posteriormente, William Ulbricht fue sentenciado en el año 2015 a cadena perpetua. Respecto a esto, Diane Fulkenson³⁷⁶ menciona que a pesar de las leyes de seguridad por parte del *Estado-nación*, la Asociación Americana de Bibliotecas (ALA) mantiene una postura de protección a la confidencialidad de los usuarios de las bibliotecas de los Estados Unidos de América.

En cuanto al software para el acceso a las *redes oscuras* en las bibliotecas, cabe mencionar que, con el movimiento del software libre se ha dado un advenimiento de nuevas herramientas digitales para la comunicación y transferencia de datos que podrían ser desconocidas para el bibliotecólogo. En este aspecto también hay antecedentes, de manera que Joseph Janes³⁷⁷ hace mención en que, desde la década de los noventa Internet y las nuevas herramientas tanto electrónicas como digitales comenzaron a tener mayor presencia en la biblioteca, por lo que

³⁷⁵ Mac, Ryan. 2 de octubre de 2013. Who is Ross Ulbricht? Piecing together the life of the alleged libertarian mastermind behind Silk Road. *Forbes*. Recuperado en: <http://www.forbes.com/sites/ryanmac/2013/10/02/who-is-ross-ulbricht-piecing-together-the-life-of-the-alleged-libertarian-mastermind-behind-silk-road/#588cfb1122e9> [Consultado 30 de enero de 2016]

³⁷⁶ Fulkenson, Diane. Ídem. Pág. 88

³⁷⁷ Janes, Joseph. The Internet public library: an intellectual history. *Library Hi Tech* 16, no. 2 (1998): 55-68. Recuperado en: <http://dx.doi.org/10.1108/07378839810303983> [Consultado 30 de enero de 2016]

dicha inclusión ha representado desde entonces un esfuerzo extra en el bibliotecario, ya sea con una formación de oficio o de profesión.

Respecto a este asunto Jesse Shera³⁷⁸ manifiesta que, el bibliotecario debe de alejarse del estereotipo institucional, en donde es presentado como el eslabón entre la información y el usuario; el bibliotecario no sólo se limita a ser un mediador, puesto que debe de interesarse en el conocimiento que busca el usuario y la forma en cómo el conocimiento se divulga para el beneficio de la sociedad. En este tenor Kebede Hundie³⁷⁹ agrega que, la capacidad de discernir la información adecuada de la errónea, parte de su análisis y evaluación para determinar si es fiable para el usuario, es decir una triangulación de la información.

Las *redes oscuras* no deberían ser ajenas para el bibliotecólogo, desde un enfoque conceptual en primera instancia, ya que son hoy en día una alternativa para el alojamiento de contenidos, la comunicación y la transferencia de datos a favor de la privacidad y la disponibilidad de los contenidos. Actualmente, las bibliotecas suelen incorporar el servicio de acceso a Internet y navegación en la Web, razón por la cual el bibliotecario tiene que estar informado sobre los alcances de las nuevas tecnologías digitales para la navegación, búsqueda, recuperación, acceso a la información y seguridad informática elemental.

3.8.1 Servicio de Internet en la biblioteca

Las bibliotecas son un espacio para la lectura y el estudio de los contenidos artísticos, literarios y académicos. Las bibliotecas públicas proporcionan un mayor grado de accesibilidad al servicio de Internet; en contraste con las bibliotecas universitarias y especializadas. Marcos Merino³⁸⁰ menciona que, si

³⁷⁸ Shera, Jesse. *Los fundamentos de la educación bibliotecológica*. Traducido por Francisco González. (México: UNAM, Centro Universitario de Investigaciones Bibliotecológicas, 1990). Pág. 114

³⁷⁹ Hundie, Kebede. Library operations and Internet resources. *The Electronic Library* 21, no. 6 (2003): 555-564
Recuperado en: <http://dx.doi.org/10.1108/02640470310509117> [Consultado 20 de marzo de 2016]

³⁸⁰ Merino, Marcos. 29 de noviembre de 2014. ¿Cómo serán las bibliotecas en un futuro cercano? *Tic beat*. Recuperado en: <http://www.ticbeat.com/tecnologias/como-sern-las-bibliotecas-en-futuro-cercano/> [Consultado 6 de marzo de 2016]

bien las bibliotecas además de proveer la consulta de libros electrónicos o digitales, libros impresos y documentos audiovisuales, los servicios bibliotecarios deben de ampliarse a las nuevas tecnologías y herramientas digitales para la comunicación y el acceso a la información. Por lo anteriormente mencionado por el autor, podría interpretarse a los nuevos servicios tales como: el asesoramiento en la adquisición de una computadora personal, sistemas operativos y herramientas digitales de software libre para fines de estudio, además de proporcionar pláticas de orientación en cuanto al uso de datos personales y el uso de la información acreditada como dominio público.

Finalmente Nick Moore³⁸¹ agrega que, las bibliotecas al brindar el servicio de acceso a Internet, deberían de replantear su filosofía e ideología de acceso. De modo que, al cambiar los procesos tecnológicos, el reglamento de uso debe adaptarse a los alcances, limitaciones y riesgos tecnológicos tanto para los bibliotecarios como para los usuarios. Por lo que debe de considerarse una revisión a las políticas de acceso a Internet en la biblioteca.

La biblioteca por otro lado, es un espacio que debe ser valorado por la sociedad, puesto que, en otrora el acceso a las bibliotecas estaba restringido a unos cuantos privilegiados, por lo que se debe de entender a la biblioteca como un privilegio del cual deriva el aprendizaje autónomo y la adquisición de nuevos conocimientos conforme a la interpretación de la información. Razón por la cual es menester entender a la biblioteca como un espacio predilecto en cuanto al estudio, la reflexión, el diálogo y el fomento a la lectura. De este modo, es el servicio de Internet en la biblioteca un aspecto extra en donde se diversifican las posibilidades para los usuarios, puesto que dicho servicio además de complementar la experiencia en el individuo, cubre otras necesidades como el ocio, los trámites administrativos y la comunicación, no obstante, su utilidad requiere de responsabilidad y plena conciencia tanto de la biblioteca como en el

³⁸¹ Moore, Nick. The Internet and the library. *Library Review* 49, no. 9 (2000): 422-428. Recuperado en: <http://dx.doi.org/10.1108/00242530010354029> [Consultado 20 de abril de 2016]

usuario, de modo que, el usuario y la biblioteca no se encuentran aislados de los sistemas de vigilancia y monitoreo por parte del *Estado-nación*.

3.8.2 Políticas de acceso a Internet

Como reflexión final a todos los puntos anteriormente tratados, se puede manifestar que, no existe una fórmula exacta en la elaboración de un reglamento para el uso del servicio de Internet en la biblioteca, puesto que cada biblioteca tiene sus propias características, que van principalmente desde su tipología, comunidad de usuarios y colección documental. Si bien existe cierta libertad de acceso a la información, para el bien de la administración bibliotecaria, se deberá considerar y reflexionar las implicaciones que existen en la dualidad entre el control y la libertad de acceso al servicio de Internet, ya que por un lado se lleva a cabo el monitoreo de las actividades del usuario, al punto de transgredir su privacidad, empero también cabe aclarar que las políticas coadyuvan a los procesos jurídicos para esclarecer y deslindar responsabilidades de cualquier índole, consecuencias o sanciones legales.

En cuanto a la elaboración de políticas, es imprescindible conocer las aristas de los actores con el fin de identificar sus capacidades, de modo que, la biblioteca debe de establecer políticas en el acceso al servicio de Internet dado que existe una asimetría en las habilidades de los usuarios y por tanto, una posible vulneración en la seguridad informática de todo aquel que haga uso del servicio de conexión. Por ello, es indispensable como bibliotecario, el respeto hacia la capacidad intelectual de los usuarios como a los contenidos y las herramientas digitales disponibles en la Web.

Las políticas de información deben basarse en directrices, reglamentos y alcances tecnológicos, optando por la adopción de políticas externas como punto de partida, para después conceptualizarlas y ser entonces utilitarias mediante la adaptación al contexto institucional, empresarial o social, pero sobre todo, las políticas de información deben de complementarse con la normatividad actual de

la biblioteca, puesto que no es viable ignorar el pasado o el presente, ya sea administrativo, cultural o social.

Los siguientes puntos a considerar, están basados en reglamentos orientados a la seguridad informática, control de usuarios, acceso a los contenidos de la Web y sobre el equipo de cómputo en las bibliotecas.³⁸² Con el objetivo de considerar un escenario rígido y otro flexible en el servicio de acceso a Internet, en ambos casos se propone evitar y disminuir los riesgos que afecten al personal de la biblioteca y al usuario. Es sumamente importante que el reglamento tenga visibilidad dentro de la biblioteca y, se informe sobre su existencia al usuario antes de proporcionar el servicio de Internet.

3.8.3 Escenario rígido en el acceso a Internet en la biblioteca

La biblioteca debe controlar y vigilar el acceso al servicio de Internet, además de monitorear las actividades que realiza el usuario en la Web.

Requisitos para el acceso a Internet en caso de que la biblioteca cuente con el servicio de conexión a Internet y/o computadoras para sus usuarios:

- ❖ Se solicitará al usuario una credencial (institucional u oficial) con el fin de acreditar el nombre de la persona además de firmar una ficha de registro.

- ❖ Se utilizarán contraseñas gestionadas por la biblioteca para acceder a la computadora.

³⁸² Véase México. Ayuntamiento de San Gabriel. 26 de abril de 2013. **Reglamento para el uso adecuado de Internet y del equipo de cómputo del H. Ayto. De San Gabriel Jalisco 2010 – 2012**. Recuperado en: <http://www.ordenjuridico.gob.mx/Documentos/Estatal/Jalisco/Todos%20los%20Municipios/wo80785.pdf>. [Consultado 21 de marzo de 2016] Biblioteca de México. 5 de junio de 2014. **Reglamento de acceso y uso de los servicios digitales de la biblioteca de México**. Recuperado en: http://www.bibliotecademexico.gob.mx/documentos_PDF/ReglamentoServiciosDigitales.pdf [Consultado 21 de marzo de 2016] y México. Gobierno de Monterrey. 14 de diciembre de 2015. **Reglamento de bibliotecas públicas municipales de Monterrey**. Recuperado en: http://portal.monterrey.gob.mx/pdf/reglamentos/reg_bibliotecas.pdf [Consultado 21 de marzo de 2016]

- ❖ Se informará al usuario que los puertos USB se encuentran bloqueados de forma física y/o lógica.
- ❖ Se informará con previo aviso al usuario, sobre la vinculación del equipo de cómputo con su nombre y fecha de acceso.
- ❖ Se informará con previo aviso al usuario que, se elaborará una bitácora sobre sus actividades en la Web, siendo esta información resguardada por un periodo determinado por la misma biblioteca, dicha bitácora será confidencial y se utilizará para el uso de procedimientos jurídicos.
- ❖ El usuario tiene derecho a expresar su sentir y proponer sugerencias sobre el servicio.
- ❖ El usuario deberá reportar de inmediato cualquier tipo de falla en la computadora.

De las prohibiciones a los usuarios:

- ❖ Queda prohibida la conexión física e inalámbrica de dispositivos de almacenamiento ajenos al equipo de cómputo de la biblioteca.
- ❖ Queda prohibida la instalación de software ajeno al sistema operativo de las computadoras.
- ❖ Queda prohibido el acceso a páginas de pornografía, material no apto para adultos, juegos de apuesta en línea, venta de drogas y venta de armas.
- ❖ Queda prohibida la descarga y transferencia de cualquier obra protegida bajo los derechos de autor.

- ❖ Queda prohibida la descarga de software propietario que no cuente con los respectivos permisos de licencia de uso.

Sobre el uso de la red inalámbrica:

- ❖ La contraseña de la red inalámbrica se cambiará mensualmente, por lo que el usuario deberá actualizar su clave de conexión inalámbrica.
- ❖ Queda prohibido compartir o ceder el nombre de usuario y la contraseña de conexión inalámbrica.
- ❖ Queda prohibido realizar auditoria o testeado de redes, excepto cuando exista un mandato administrativo o judicial por parte de las autoridades competentes.
- ❖ Queda prohibido realizar ataques informáticos de fuerza bruta o utilizar diccionarios para descifrar claves de acceso a otras redes inalámbricas de la biblioteca o alrededores.
- ❖ Queda prohibida la transmisión de malware a otros usuarios que utilicen la red inalámbrica.

De las recomendaciones y buenas prácticas en la navegación Web:

- ❖ No acceder a los mensajes relacionados a las ofertas, premios, agencias de viajes, advertencias de virus, publicidad erótica, etc.
- ❖ No publicar contenidos e información personal, familiar o laboral en las redes sociales.
- ❖ Borrar el historial de navegación, descargas, cookies, caché y conexiones activas.

Dicho escenario tiende a ser distópico e irracional, puesto que se presentan una serie de restricciones y condiciones para desalentar el uso del servicio de Internet a ultranza, no obstante se garantiza el control en el acceso, navegación e historial de cada usuario.

3.8.4 Escenario flexible en el acceso a Internet en la biblioteca

La biblioteca como espacio de reflexión, recreación y acceso a la información debe de ofrecer las condiciones adecuadas para que el usuario pueda acceder al servicio de Internet, además de que el usuario pueda realizar sus actividades en la Web con privacidad.

Requisitos para el acceso a Internet en caso de que la biblioteca cuente con el servicio de conexión a Internet y/o computadoras para sus usuarios:

- ❖ Se le solicitará de forma amable al usuario registrarse antes de proporcionarle la contraseña de acceso a Internet o antes de habilitarle una computadora para acceder a Internet, según sea el caso.
- ❖ Se utilizarán contraseñas gestionadas por la biblioteca para acceder a la computadora.
- ❖ Se informará con previo aviso al usuario, sobre la vinculación del equipo de cómputo con su nombre y fecha de acceso con el fin de establecer un estudio sobre la frecuencia de acceso al servicio de Internet.
- ❖ Se le informará mediante el reglamento al usuario que, tiene derecho a expresar su sentir y proponer sugerencias sobre el servicio.
- ❖ El usuario deberá reportar cualquier tipo de falla en la computadora.

De las prohibiciones a los usuarios:

- ❖ No se ejercerá ningún control sobre las actividades que realice el usuario en la Web, la responsabilidad sobre el uso del servicio de Internet queda

bajo el criterio de cada usuario. Sin embargo de ser requerido el usuario responderá ante cualquier caso o irregularidad detectada.

Sobre el uso de la red inalámbrica:

- ❖ Queda prohibido realizar auditoria o testeo de redes, excepto cuando exista un mandato administrativo o judicial por parte de las autoridades competentes.
- ❖ Queda prohibido realizar ataques informáticos de fuerza bruta o utilizar diccionarios para descifrar claves de acceso a otras redes inalámbricas de la biblioteca o alrededores.
- ❖ Queda prohibida la transmisión de malware a otros usuarios que utilicen la red inalámbrica.

De las recomendaciones y buenas prácticas en la navegación Web:

- ❖ No acceder a los mensajes relacionados a las ofertas, premios, agencias de viajes, advertencias de virus, publicidad erótica, etc.
- ❖ Evitar publicar contenidos e información personal, familiar o laboral considerada como sensible, en las redes sociales.
- ❖ Borrar el historial de navegación, descargas, cookies, caché y conexiones activas.

Este escenario corresponde a un contexto afable con las facilidades de acceso al servicio de Internet, aunque es esta misma apertura la que conlleva a más responsabilidades para la biblioteca. Por ende, es en este contexto de apertura en que los usuarios deben de ser consientes sobre las consecuencias del uso de los contenidos protegidos bajo la propiedad intelectual, el derecho de autor y el derecho de copia, además de los contenidos y servicios ilícitos.

3.9 La biblioteca como medio de acceso a la información privilegiada

La biblioteca al contar con colecciones temáticas que van de lo general a lo particular, ofrece la posibilidad de vincular acontecimientos actuales e históricos, conceptos, teorías, saberes y posturas acerca de algún tema que se encuentre en boga en las redes sociales, plataformas audiovisuales o en los foros de la *web superficial*. En algunos casos, las bibliotecas cuentan con una hemeroteca, la cual es una sección dedicada a la conservación de publicaciones periódicas referentes a las revistas, publicaciones científicas y acontecimientos históricos, según el tipo de biblioteca a la que se acuda.

Las bibliotecas de acceso al público en general, brindan el servicio de consulta a sus colecciones, de manera que, no sólo es posible acceder a los documentos impresos sino a otro tipo de materiales que abordan el mismo tema pero en distintas manifestaciones, como es el caso de los documentos audiovisuales. De modo que, a partir de la lectura de distintos libros, diarios oficiales, leyes jurídicas, diccionarios especializados, estadísticas, revistas y periódicos se puede efectuar una triangulación de la información en complemento con los contenidos digitales que se recuperan en la *web superficial*. Otras bibliotecas, como las universitarias y especializadas ofrecen servicios de consulta de bajo costo para acceder a los contenidos en línea de revistas científicas, medios oficiales y bases de datos.

La información privilegiada, aparte de ser adquirida de forma sintetizada por intermediarios, puede ser desarrollada desde la investigación y la interpretación en cada individuo, lo que significa un esfuerzo y deseo por incrementar el contexto que vagamente es proporcionado por los medios de comunicación, contenidos web o redes sociales.

3.10 Prospectiva de las redes oscuras

El concepto de la *web profunda* bajo la percepción social, en realidad comprende el conjunto de sitios de la *red oscura Tor*, dedicados al alojamiento de contenidos y servicios ilícitos, pornográficos, atípicos y bizarros. Sin embargo, es menester aclarar que, las *redes oscuras* son utilizadas para fines de anonimato, privacidad y seguridad informática. El periodismo de guerra y la censura, son los principales catalizadores de las *redes oscuras*, creadas y desarrolladas por los colectivos interesados en la libertad de expresión; la visibilidad y la popularidad de estas *redes oscuras* son parte del riesgo en su difusión, puesto que incrementan el interés del *Estado-nación* por conocer y regular este tipo de conexiones anónimas y privadas.

En el futuro inmediato, es viable la migración de los usuarios avanzados de la *red Tor* hacia *redes oscuras* más complejas en su instalación, configuración y acceso, puesto que ello delimita las antípodas digitales de lo popular a lo selecto y confidencial. *Tor* es una *red oscura* con sitios web a los que sólo se puede acceder por medio del navegador *Tor*, el cual permite navegar en la *web superficial* de forma anónima. Hoy en día, hay una apertura hacia el anonimato en el acceso a ciertos servicios y redes sociales, como es el caso de Facebook³⁸³ que permite a sus usuarios acceder a través de *Tor*, desde el año 2014.

Las *redes oscuras* son actualmente un ejercicio de libertad de expresión y libre albedrío mediante el uso de la infraestructura de Internet. El desarrollo continuo en el cifrado de su código es un punto clave, más allá de su composición visual, puesto que su objetivo primordial es la comunicación y difusión de los contenidos, evitando aspectos publicitarios. Por tanto, si se pretenden cuidar estos espacios será indispensable el uso responsable de las *redes oscuras*, con el fin de preservar la privacidad y el anonimato en el acceso a la información.

³⁸³ Hughes, Matthew. 6 de noviembre de 2014. How you can officially browse Facebook over Tor. *Make use of*. Recuperado en: <http://www.makeuseof.com/tag/can-officially-browse-facebook-tor/> [Consultado 12 de marzo de 2016]

Realizando un balance de acuerdo a lo anteriormente presentado en el capítulo, se puede interpretar que, las *redes oscuras* son de utilidad para los usuarios con conocimientos avanzados en la configuración de conexión al servicio de Internet; mientras que los usuarios comunes pueden no estar interesados en su anonimato ya que sus actividades y necesidades son actos convencionales en la Web. En este sentido los servicios de la Web agilizan la adquisición de productos mediante la infraestructura y el código, de manera que, es la inmediatez un factor económico que beneficia a los individuos en la oferta y la demanda, no obstante cabe resaltar que la información no fue gratuita en el pasado y no lo es en el presente (concretamente en la Web), puesto que en el aparentemente acceso gratuito es inevitable cubrir un costo como la publicidad, la incertidumbre, las condiciones de uso y los riesgos informáticos.

Las facilidades de acceso a la Web se han incrementado considerablemente con base en el desarrollo de la infraestructura y la cobertura geográfica, no obstante, las políticas de información emanan de los administradores de los servicios y productos digitales para condicionar el acceso y el uso exclusivo de sus servicios, modificando así la economía mediante la adquisición de datos personales para crear nuevos productos y consecuentemente modificar las necesidades de consumo en el individuo. De modo que, son los datos personales y la conducta del usuario un recurso para los monopolios vinculados a la producción, gestión y análisis de la información. De esta manera, es la información un recurso vital, en la era digital.

Por otro lado, es la *web superficial* un mediador entre lo habitual, la diversidad y la ficción. Ya que es a través de la visibilidad que es permisible encontrar nuevas dimensiones de comunicación e interacción, las cuales obedecen a otra clase de código informático y social, de manera que se busca lo oculto y lo desconocido con el fin de experimentar cierta sensación de exclusividad, privacidad y anonimato. Sin embargo existe también la posibilidad de ser engañado, estafado

o vulnerado a falta del sentido común y criterios de autoría en la información o elementos de certidumbre en la legalidad de los servicios.

La era actual en el acceso al servicio de Internet y a los servicios y contenidos de la Web se encuentra en una situación de conflicto y debate, entre la vigilancia y la privacidad, utilizando como elementos críticos al anonimato y a la seguridad nacional, es decir que, es el anonimato un elemento que puede derivar en un peligro para la sociedad con base en actos de crimen y terrorismo, pero es igualmente la vigilancia del *Estado-nación* un acto de violencia hacia la privacidad e intimidad de cada individuo. A este respecto, son las buenas prácticas en el uso del servicio de Internet y la Web, una opción para sortear la complejidad tecnológica, desde la precaución en proporcionar datos personales, la actualización en el sistema de defensa o antivirus, el control en la difusión de contenidos personales, la precaución en los contenidos recibidos mediante el correo electrónico, la gestión y eliminación en el historial de navegación y, en la medida de lo posible, evitar la descarga de software de procedencia y creación desconocida, entre otros aspectos. Las buenas prácticas también contemplan el cambio periódico en la contraseña de acceso en la conexión inalámbrica y en la creación de contraseñas robustas y alfanuméricas para acceder a los servicios de la Web.

Como consecuencia de la vigilancia y la carencia de privacidad en los servicios de la Web, las conductas socialmente inadecuadas y los comportamientos que atentan contra los intereses del *Estado-nación* se han condensado hacia nuevos entornos como es el caso de las *redes oscuras* **Tor**, *Freenet* e *I2P*. Ello se debe en parte al anonimato y a la disponibilidad de contenidos y servicios, considerados como una amenaza para el *Estado-nación*. Sin embargo, las *redes oscuras* han optado por el desarrollo de políticas, no sólo para su acceso sino para regular el comportamiento de sus usuarios y administradores en cuanto a los términos y condiciones de uso, para impedir la difusión y promoción de actos de daños a terceros.

En este sentido, el bibliotecólogo debe de mantener un código de ética universal basado en la convicción y la neutralidad de la legalidad y la facilidad de acceso a la información. De momento, las *redes oscuras* no representan un factor de debate o incidencia en la biblioteca, pero queda para la reflexión en el bibliotecólogo este tipo de herramientas como factor de cambio, disidencia y libertad en el acceso a la información.

Conclusiones

La investigación teórica permitió entender el fenómeno, dando paso a la exploración empírica, con el propósito de comprender y describir los entornos de las *redes oscuras*, de modo que, fue posible identificar las características de las *redes oscuras* con base en la documentación referente del periodo 2012 al 2015. Asimismo, fueron analizados los contenidos de algunos de los sitios de las *redes oscuras* con base en los aspectos teóricos concernientes al acceso y a la recuperación de la información, en un breve ejercicio de monitoreo.

Lo que permitió aclarar el primer supuesto planteado en esta investigación:

Tanto las habilidades del usuario común como las herramientas para acceder a las *redes oscuras* poseen una similitud de usabilidad y dificultad que las de la *web superficial*.

La dificultad de acceso a las *redes oscuras* si difiere del acceso a la *web superficial*, por lo que existe una brecha de acceso a los sitios de las *redes oscuras*, debido a la demanda de ciertos conocimientos teóricos y técnicos para la instalación, configuración y navegación, que no son imprescindibles en la *web superficial*.

La complejidad de acceso a las *redes oscuras* se compone de varias aristas, la complejidad no sólo se centra en conocimientos de acceso a Internet e instalación del software dedicado a la navegación anónima, sino del acceso a los medios, como las computadoras. Puesto que para realizar el monitoreo se requirió de conocimientos básicos para la adquisición de la computadora personal con ciertas características tecnológicas referentes a la velocidad de arranque en el sistema operativo y los procesos informáticos (para fines de practicidad y operatividad), además de la instalación de un sistema operativo robusto, con la posibilidad de ser instalado una y otra vez en caso de un

incidente. Posteriormente, se realizó una investigación sobre la forma de instalación y configuración del software para acceder a las tres *redes oscuras*.

Por tanto, las herramientas de acceso, van desde la adquisición del hardware y software, en conjunción con los conocimientos y la documentación acerca de la ideología, funcionamiento y operatividad de las *redes oscuras*.

Retomando el segundo supuesto, planteado en la presente investigación:

En la actualidad, existen herramientas suficientes para acceder a las *redes oscuras* de forma segura.

Concretamente si existen las herramientas suficientes para el acceso a las *redes oscuras*, cabe mencionar que, estas herramientas son proporcionadas por los colectivos desarrolladores de las *redes oscuras*, y en el caso de la *red oscura Tor* puede combinarse con otras tecnologías abstractas, las cuales comúnmente pertenecen al software libre, no obstante dichos complementos deben de configurarse según las necesidades de los usuarios avanzados. En este sentido, la configuración y las políticas de acceso dependen de cada *red oscura*, ya que cada una posee características ideológicas particulares, empero es notable que las *redes oscuras* comparten el objetivo primordial del anonimato y la privacidad.

Desde la perspectiva del usuario como herramientas para el acceso, se debe considerar en primera instancia a la literatura y los contenidos sobre la configuración del software de acceso, dando paso a la combinación de técnicas para aumentar el espectro de anonimato. En este tenor es menester mencionar que, la literatura en su mayoría se encuentra en el idioma inglés. Otro aspecto a destacar de las *redes oscuras*, son sus políticas de información, porque son necesarios los requerimientos mínimos de hardware y específicos del software, por tanto, como primer requisito ya representa una dificultad significativa para el

usuario, en caso de no contar con los recursos adecuados para el acceso a los servicios, productos y contenidos.

Respecto al tercer supuesto planteado:

Las *redes oscuras* utilizan las mismas tecnologías de acceso y navegación que en la *web superficial*.

En principio las *redes oscuras* utilizan parte de los protocolos de comunicación de la *web superficial*, como el protocolo HTTP para el acceso, y en algunos casos el protocolo HTTPS para la seguridad en la transferencia de datos. No obstante, los complementos multimedia que proporcionan una mayor experiencia de interacción y de entretenimiento en la *web superficial* quedan deshabilitados en las *redes oscuras* (caso exclusivo del navegador **Tor**) debido a la capacidad de los complementos de la *web superficial* en la recopilación de datos sobre el usuario y solicitud de datos de origen. Los navegadores de las *redes oscuras* *Freenet* e *I2P* son independientes de los navegadores convencionales y no proporcionan el acceso a los contenidos de la *web superficial*, su tecnología no es compatible al estar programados con otro tipo de cifrado y propósito.

A partir de la lectura sobre la anatomía URL de la *red oscura* **Tor** se detectó que, en la mayoría de los sitios explorados se presenta el protocolo HTTP. Se identificó en la URL un código a manera de título del sitio, el cual da la impresión de que se genera de manera aleatoria y no es creado por el administrador de los contenidos, las direcciones URL cuentan con el dominio (*.onion*) y en algunos casos con el nombre del archivo, es decir el formato digital del contenido alojado.

Los motores de búsqueda en **Tor** (*Torch* y *Grams*) aún no cuentan con la tecnología de recuperación de contenidos, palabras, conceptos y términos mediante el uso de operadores booleanos, no obstante emulan algunas

características de los motores convencionales de la *web superficial*, como la presentación gráfica de los resultados.

La navegación en la *red oscura Freenet*, se llevó a cabo mediante su interfaz de inicio. *Freenet* cuenta con documentación relacionada con la operatividad del software de acceso, blogs del equipo de desarrollo y directorios de acceso, en donde continuamente se actualizan nuevos enlaces a los contenidos. La anatomía URL de *Freenet* se encuentra estructurada con la dirección IP «127.0.0.1» de la computadora personal (del usuario) y el puerto «8888» para el envío y recepción de los datos. En la parte final de la URL se encuentra el título del sitio, seguido de un número único de identificación. El motor de búsqueda *Freenet* se encuentra en desarrollo, por lo que resultó compleja la búsqueda de temas, sucesos o conceptos.

En *I2P*, la consola de enrutamiento (o interfaz de inicio) contaba con algunos servicios y contenidos para los nuevos usuarios que no disponen de un enlace o datos para la comunicación con otro usuario. Por medio de estos enlaces en la interfaz, los nuevos usuarios de la *red oscura I2P* pueden acceder a la documentación preliminar, información de distinta índole y descargas de contenidos. Se detectó en la anatomía de la URL el protocolo HTTP, el título del sitio, el dominio (*.i2p*), y en algunos casos el nombre del directorio al que pertenece el archivo.

Aunque la interfaz para la navegación y los protocolos de acceso de las *redes oscuras* posean cierto sincretismo con los navegadores habituales, tanto la conectividad como la seguridad de las *redes oscuras* se componen a partir de lenguajes de programación orientados a proporcionar la estabilidad de sus utilidades en la navegación y la transferencia de datos cifrados.

Finalmente, en cuanto al último supuesto planteado en la parte introductoria de la investigación:

La *web profunda* y las redes oscuras tienen propósitos, características y objetivos similares, sin embargo estas similitudes no son indicativos de ser sinónimos.

A partir de un análisis sobre la literatura concerniente a la *web profunda*, comenzaron a presentarse variantes y discrepancias en cuanto a la nomenclatura, de manera que, se identificaron algunos textos en donde se hacía referencia a las *redes oscuras*. El concepto social de la *web profunda* como el conjunto de sitios (*.onion*), es un concepto que al paso de los años ha sido aceptado y utilizado por los usuarios de la *web superficial*, mediante blogs, videos de opinión y comentarios, aunque es importante señalar que, esta supuesta *web profunda* se trata del conjunto de los sitios de la *red oscura Tor*.

A pesar de no haber encontrado un punto histórico exacto para definir en qué momento se bifurca o amplía el concepto de la *web profunda*, con base en los sucesos ocurridos en la vulneración de la *red oscura Tor*, y posterior cierre de los sitios considerados como ilícitos o bajo sospecha, se concluye con base al arco histórico que, posiblemente fue en el año 2011, dado que las *redes oscuras* tienen su origen a mediados de la década de los noventa. No obstante en 1994 ya se había acuñado de forma aislada el concepto de Internet invisible, siendo en el año de 1996 cuando es creado el sistema de transmisión de datos y comunicación anónima *Tor*. Posteriormente, en el 2002 el software de acceso a la red *Tor* es liberado para el público en general y en el año 2011 es cuando el concepto social de la *web profunda* comenzó a tener auge y sociabilización en la *web superficial*, a causa de la supuesta impunidad sobre ciertos servicios.

Los contenidos de las *redes oscuras* están orientados a la preservación de la privacidad y el anonimato, en ellos se fomenta la apertura a la información concerniente a la configuración del software de navegación con fines de seguridad. Algunos de los sitios ofrecen el servicio de descarga de contenidos y en otros sitios, se crean foros para el intercambio de opiniones de índole política,

social, económica o del entretenimiento. Aparentemente en las *redes oscuras* no hay productos o servicios que no puedan adquirirse por las vías tradicionales del contrabando, o que no puedan ser recuperados en la *web superficial*. El atributo esencial de las *redes oscuras*, es el de la libertad de acceso a los contenidos alojados en cada tipo de red sin importar el origen geográfico. En este aspecto cabe destacar que, los servicios en las *redes oscuras* no tienen la gama de posibilidades de la *web superficial*; en cambio, hay otra clase de servicios que por su naturaleza prohibida son inaccesibles en la *web superficial*, según el contexto político, social y jurídico. De esta manera se finalizan los supuestos planteados en la introducción.

A manera de cierre se puede decir que, las *redes oscuras* no distan de proyectar la dualidad propia del ser humano, puesto que en ellas prevalecen dos ópticas, el libre albedrío y la libertad; ante el libertinaje y el daño a terceros como símbolo de violencia. En lo que respecta al mercado de las *redes oscuras*, se puede interpretar con base a los precios de los productos, los servicios y el acceso a cuentas personales que, en el mercado negro la oferta y la demanda giran en torno a la invasión a la privacidad y el acceso restringido a los contenidos del entretenimiento en general. Respecto a la privacidad y la seguridad, se vislumbra en el corto plazo, servicios de vulnerabilidad para el espionaje en los teléfonos inteligentes con base en las estadísticas del primer capítulo, referentes a los hábitos de la conexión y las zonas geográficas con mayor conexión a Internet, así como al espionaje de datos en los jóvenes adultos como víctimas potenciales. Por lo que respecta a los estados de México con mayor conexión, dichos datos podrían vincularse con otros indicadores relacionados en el acceso a los recursos, acceso a la información en línea, uso de servicios y la calidad de vida.

La información privilegiada considerada como sensible, altamente sensible, reservada, secreta y altamente secreta, aun en las *redes oscuras* no es visible para los usuarios que acceden a los sitios, páginas y contenidos frecuentes de **Tor**, **Freenet** e **I2P**, de manera que, podría inferirse que esta clase de información

puede ser transferida sólo cuando se realizan transacciones para la compra de este insumo de ventaja, como se ha señalado en el tercer capítulo (véase apartado de Contexto internacional) con el caso de AT&T o bien, sea la información privilegiada como toda aquella información en contextos beligerantes, como el periodismo de guerra y en el plano político.

En cuanto al tema de la vigilancia, se puede argumentar que, en todo el planeta existe un sistema global de monitoreo que gestiona a manera de una prisión los comportamientos personales, colectivos y sociales, con el fin de segmentarlos y controlarlos. De tal manera que estos patrones de comportamiento son registrados por el sistema de vigilancia, controlando la información mediante bases de datos y perfiles detallados de comportamiento. La vigilancia comúnmente aumenta y se polariza a raíz de los actos de violencia, como los atentados terroristas, por lo que es confuso establecer si estos actos se permiten por los *Estados-naciones* a pesar de toda su infraestructura de vigilancia o, si la perpetración de estos actos de *lesa humanidad* es parte de las vulnerabilidades de seguridad, malas prácticas de control en la información y los conflictos ideológicos.

Los accesos a la biblioteca central y a la biblioteca del Instituto de Investigaciones Bibliotecológicas y de la Información de la UNAM, así como las revistas electrónicas y bases de datos, mediante el acceso remoto a través de los servicios de la biblioteca digital de la UNAM, permitieron obtener la información relevante para la realización del marco teórico sobre el acceso a las *redes oscuras*. De manera que el acceso por medio de los recursos económicos institucionales y bibliotecarios a la *web invisible* fue un factor determinante en la recuperación de la información arbitrada en el contexto académico y científico. En este sentido cabe señalar la importancia de las bibliotecas, no sólo para la elaboración de tareas, trabajos y proyectos, sino como una oportunidad para el individuo en la obtención de bienes tangibles e intangibles a corto, mediano y largo plazo. Puesto que fueron los servicios bibliotecarios en combinación con el

servicio de conexión a Internet y los servicios de la Web los que permitieron la búsqueda y recuperación de los elementos suficientes para el desarrollo y sustento de la información presentada.

La presente investigación ofrece otros temas a desarrollar, los cuales inciden en la Bibliotecología y Estudios de la Información, como lo son: el desarrollo en la conectividad a Internet en las bibliotecas públicas, la seguridad informática dentro de las bibliotecas, el control de usuarios con acceso a Internet, el uso de los contenidos de la Web, el comercio electrónico de la información y, la adquisición, mantenimiento y gestión del equipo de cómputo en las bibliotecas. Otro posible tema, es el de la autenticidad y el valor monetario de los contenidos digitales elaborados, recuperados, transferidos y resguardados. Por otro lado, en el caso concreto de las *redes oscuras*, los servicios de alojamiento de contenidos y los sistemas de transmisión de datos, mediante el anonimato pueden ser estudiados a fondo, ya sea para fines de uso personal o institucional, como alternativas para posibles situaciones de guerra, vigilancia y censura en el acceso a la información.

Como aspectos relevantes a destacar en esta investigación se exponen los siguientes puntos:

1. Sobre el acceso a la Web;

- El acceso a la Web delimita con base a ciertos requerimientos quien puede disponer de los servicios, los productos y/o los contenidos. De modo que, el servicio de conexión a Internet no es para todos, puesto que demanda cierto poder adquisitivo para cubrir los costos, no sólo de conexión, sino en la velocidad para la transferencia de datos y el acceso exclusivo a los servicios en línea.

- La Web cuenta esencialmente con atributos de visibilidad y controles de acceso a los servicios, productos y contenidos. No obstante, el usuario con habilidades de búsqueda y recuperación de la información, tiene los elementos suficientes para aplicar otros métodos de acceso y, consecuentemente visualizar, consultar o descargar el contenido sin ninguna clase de restricción.
- Respecto a la privacidad y la seguridad, se vislumbran en el corto plazo, los servicios ilícitos de vulnerabilidad para el espionaje en los teléfonos inteligentes, dado que los índices en la adquisición en este tipo de medios de conexión se han incrementado en el último lustro. Por lo que existe la posibilidad de que los servicios bibliotecarios que utilicen la transferencia de datos a través de los teléfonos inteligentes podrían ser afectados.

2. De la *web profunda*;

- La *web superficial* es un mediador entre lo habitual, la diversidad y la ficción. Ya que es a través de la visibilidad en esta web que es permisible encontrar (a modo de invitación) nuevas posibilidades de comunicación e interacción, las cuales obedecen a otra clase de código informático y social, de manera que se busca lo oculto y lo desconocido con el fin de experimentar cierta sensación de intensidad, exclusividad, privacidad y anonimato.
- La *web profunda* es todo aquel conjunto de sitios web que no son del conocimiento público y que requieren de una contraseña de acceso. La *web profunda* no es sinónimo de servicios, productos y contenidos ilícitos, dichas características corresponden a ciertos casos particulares en las *redes oscuras*.

3. En el acceso a las *redes oscuras*;

- Existe una brecha de acceso a los sitios de las *redes oscuras*, debido a la demanda de ciertos conocimientos teóricos y técnicos para la instalación, configuración y navegación, que no son imprescindibles en la *web superficial*.
- La *red oscura Tor* no es ni tan anónima, ni tan grande, ni tan segura, y tampoco tan profunda, como se considera socialmente en la *web superficial*. La *red oscura Tor* es un reflejo de posibles trastornos psicológicos (con base a sus contenidos), y de las necesidades de información referentes a los deseos ocultos y/o reprimidos ya sea por la misma sociedad y por el sistema de gobierno de los *Estados-naciones*.
- Como consecuencia de la vigilancia y la carencia de privacidad en los servicios de la Web, las conductas socialmente inadecuadas y los comportamientos que atentan contra los intereses del *Estado-nación*, se han condensado hacia nuevos entornos, como es el caso de las *redes oscuras Tor, Freenet e I2P*, adquiriendo dichas redes un valor adaptativo.
- De momento, aparentemente las *redes oscuras* no representan un factor de debate o incidencia en las bibliotecas de México, pero queda para la reflexión en el bibliotecólogo este tipo de herramientas tecnológicas como una alternativa para posibles situaciones de guerra, vigilancia y censura en el acceso a la información.

4. Y, de las conclusiones;

- El acceso abierto a la literatura científica y la apertura en la información gubernamental pueden llegar a ser variables contraproducentes para las industrias, los monopolios y evidentemente para los *Estados-naciones*,

puesto que el ser humano tiene el potencial para razonar, aprender, entender y modificar su situación por medio de los datos, la información, el conocimiento y las herramientas tangibles e intangibles. Ejemplo de ello son las *redes oscuras*.

- Las *redes oscuras* al ser una tecnología con fines de anonimato y privacidad en el acceso, la navegación, la transferencia, la comunicación y la consulta de los contenidos; son inaccesibles para la mayoría de los usuarios comunes, debido a su complejidad.
- La *red oscura Tor* ha adquirido parcialmente un sincretismo semántico, visual y operativo similar a la *web superficial*, de modo que es actualmente la *red oscura Tor* un servicio con alta visibilidad derivado de la curiosidad, las necesidades de información y, los productos y servicios bajo el anonimato, como resultado del exceso de vigilancia y censura política.
- La triangulación de la información permite obtener certidumbre acerca de los temas, los contextos históricos, los sucesos presentes, las inversiones, e inclusive de los individuos.
- Las *redes oscuras* suponen un esfuerzo extra, tanto para el usuario común como para el bibliotecario, por lo que es necesario para el bibliotecario cuando menos en el conocimiento conceptual conocer los alcances y utilidades de las *redes oscuras*. Y para el bibliotecólogo además de lo anterior, significa también el hecho de distinguir las diferencias entre el ciberespacio, la Web, la *web semántica* y la *web invisible*.
- Las bibliotecas no sólo proveen del acceso a los servicios de la Web, sino que también cuentan con información académica, científica y cultural elemental y/o especializada con la cual es viable proporcionar, reforzar y

ampliar los conocimientos y habilidades en el individuo, para que posteriormente adquiera conocimientos y expectativas con la posibilidad de crear nuevos servicios, productos y contenidos.

El bibliotecólogo tiene la responsabilidad social en conocer los alcances de la tecnología y su incidencia en la información, de modo que, además de entender los cambios en los paradigmas tecnológicos pueda asesorar en la adquisición de computadoras personales, sistemas operativos, software libre y difundir las buenas prácticas en el acceso a Internet y la navegación en la Web, lo que potencialmente lo proyecta hacia la complejidad tecnológica (Blended librarian), así como el de estar consciente de las sanciones y las repercusiones jurídicas en el uso inadecuado de las tecnologías. Razón por la cual es preciso redimensionar el valor de las bibliotecas como los últimos bastiones en cuanto al acceso a la información, el aprendizaje y el respeto a la privacidad.

Obras consultadas

Alayarian, A. (2011) **Trauma, torture and dissociation: a psychoanalytic view.** En EBL. Recuperado en: <http://unam.ebib.com.pbidi.unam.mx:8080/patron/Login.aspx?r=needlogin> [Consultado 30 de enero 2016]

Alonso, C. (2014) **Cómo funciona el software de espionaje de Hacking Team.** En El lado del mal. Recuperado en: <http://www.elladodelmal.com/2014/11/como-funciona-el-software-de-espionaje.html> [Consultado 11 de julio 2015]

----- (2014) **Ganar dinero con 1.200 Millones de identidades robadas.** En El lado del mal. Recuperado en: <http://www.elladodelmal.com/2014/08/ganar-dinero-con-1200-millones-de.html> [Consultado 10 de agosto 2014]

----- (2015) **Introducción: Hacker, cibercriminal y hacktivismo** [Episodio 1]. En Risk alert. Recuperado en: <http://www.flooxer.com/video/chema-alonso-risk-alert-introduccion-hacker-ciber-criminal-hacktivismo/5655a4887e31f20cbf9ceb20> [Consultado 19 de diciembre 2015]

Álvarez, G. (2009) **¿Qué sabemos de? Cómo protegernos de los peligros de internet.** España: Consejo Superior de Investigaciones Científicas.

Álvarez, R. (2015) **China ya podrá exigir a cualquier compañía información confidencial de sus usuarios.** En Xataka. Recuperado en: <http://www.xataka.com/legislacion-y-derechos/china-ya-podra-exigir-a-cualquier-compania-informacion-confidencial-de-sus-usuarios> [Consultado 9 de enero 2016]

Anwer, J. (2014) **Buying an assembled PC? Keep these points in mind.** En India today. Recuperado en: <http://indiatoday.intoday.in/technology/story/buying-an-assembled-pc-keep-this-in-mind/1/395410.html> [Consultado 18 de febrero 2016]

Arce, N. (2014) **Anonymous to Lizard Squad: Keep Your Hands off Tor.** En Tech times. Recuperado en: <http://www.techtimes.com/articles/23248/20141227/anonymous-to-lizard-squad-keep-your-hands-off-tor.htm> [Consultado 30 de diciembre 2014]

Asociación Mexicana de Internet (2012) **Hábitos de los usuarios de Internet en México.** En AMIPICI. Recuperado en: https://www.amipci.org.mx/estudios/habitos_de_internet/2012HabitosUsuariosInternetMx.pdf [Consultado 14 de enero 2015]

----- (2013) **Hábitos de los usuarios de Internet en México 2013.** En AMIPICI. Recuperado en: https://www.amipci.org.mx/estudios/habitos_de_internet/estudio_habitos_internet_2013.pdf [Consultado 14 de enero 2015]

----- (2014) **Hábitos de los usuarios de Internet en México 2014.** En AMIPICI. Recuperado en: https://www.amipci.org.mx/estudios/habitos_de_internet/Estudio_Habitos_del_Internauta_Mexicano_2014_V_MD.pdf [Consultado 14 de enero 2015]

----- (2015) **11º estudio sobre los hábitos de los usuarios de Internet en México 2015.** En AMIPICI. Recuperado en: https://www.amipci.org.mx/images/AMIPCI_HABITOS_DEL_INERNAUTA_MEXICANO_2015.pdf [Consultado 14 de enero 2015]

Avilés, Á. (2013) **X1red+segura: informando y educando.** España: Safe creative.

Ayuntamiento de San Gabriel (2013) **Reglamento para el uso adecuado de Internet y del equipo de cómputo del H. Ayto. De San Gabriel Jalisco 2010 – 2012.** En Orden jurídico. Recuperado en: <http://www.ordenjuridico.gob.mx/Documentos/Estatal/Jalisco/Todos%20los%20Municipios/wo80785.pdf> [Consultado 21 de marzo 2016]

Aznar, H. y Villanueva E. (2000) **Deontología y autorregulación informativa: ensayos desde una perspectiva comparada.** México: Fundación Manuel Buendía.

Baeza-Yates, R. y Ribeiro-Neto, B. (2011) **Modern information retrieval: the concepts and technology behind search.** 2da ed. New York: Addison Wesley.

Bailey, M. (2011) **Complete guide to internet privacy, anonymity and security.** New York: Cogipas.

Bárceñas, J. (2015) **Si el gobierno mexicano pide acceso a tus datos, ¿las empresas de telecomunicación se los entregan?** En MSN noticias. Recuperado en: <http://prodigy.msn.com/es-mx/noticias/mexico/si-el-gobierno-mexicano-pide-acceso-a-tus-datos-%C2%BFas-empresas-de-telecomunicaci%C3%B3n-se-los-entregan/ar-BBleGc1> [Consultado 20 de junio 2015]

Bartra, A. (2008) **El hombre de hierro: los límites sociales y naturales del capital.** México, D.F.: Universidad Autónoma de la Ciudad de México.

BBC (2012) **Austrian police raid privacy network over child porn.** En BBC News. Recuperado en: <http://www.bbc.com/news/technology-20554788> [Consultado 9 de enero 2015]

Beal, V. (2005) **Cable vs. DSL.** En Webopedia. Recuperado en: http://www.webopedia.com/DidYouKnow/Internet/cable_vs_dsl.asp [Consultado 24 de febrero 2016]

----- (2014) **Types of Internet connections.** En Webopedia. Recuperado en: http://www.webopedia.com/quick_ref/internet_connection_types.asp [Consultado 24 de febrero 2016]

Bécares, B. (2015) **10 precauciones básicas para mantener tu dispositivo seguro.** En ChannelBiz. Recuperado en: http://www.channelbiz.es/2015/08/14/10-precauciones-basicas-para-mantener-tu-dispositivo-seguro/?utm_content=buffer658bc&utm_medium=social&utm_source=twitter.com&utm_campaign=buffer [Consultado 14 de agosto 2015]

Becerra, J. (2014) **Mitos y realidades de la Internet profunda.** En: Revista Seguridad Cultura de prevención para TI, (20). Recuperado en: <http://revista.seguridad.unam.mx/numeros/numero-20> [Consultado 3 de agosto 2015]

Betts, A. (2015) **Wi-Fi vs Ethernet: which should you use and why?** En Make use of. Recuperado en: <http://www.makeuseof.com/tag/wi-fi-vs-ethernet-which-should-you-use-and-why/> [Consultado 26 de febrero 2016]

Biblioteca de México (2014) **Reglamento de acceso y uso de los servicios digitales de la biblioteca de México**. En Biblioteca de México. Recuperado en: http://www.bibliotecademexico.gob.mx/documentos_PDF/ReglamentoServiciosDigitales.pdf [Consultado 21 de marzo 2016]

Biddle, P., England, P., Peinado, M. y Willman B. (2002) **The darknet and the future of content distribution**. En *FRField's Page*. Recuperado en: <http://msl1.mit.edu/ESD10/docs/darknet5.pdf> [Consultado 13 de febrero 2016]

Bitcoin (2015) **Bitcoin es una innovadora red de pagos y una nueva clase de dinero**. En Bitcoin. Recuperado en: <https://bitcoin.org/es/> [Consultado 30 de enero 2016]

Blake Curran (2012) **Bitcoin 2012: Caleb James Delisle** [Episodio 7]. Blake Curran. Recuperado en: <https://www.youtube.com/watch?v=sCFmzGknUew> [Consultado 17 de febrero 2016]

Braman, S. (1989) **Defining information: an approach for policy-makers**. En *Telecommunications Policy*. 13 (3). Recuperado en: http://people.tamu.edu/~Braman/bramanpdfs/003_defining.pdf [Consultado 14 de enero 2016]

Caballero, J. (2005) **El acceso a la información judicial en México: una visión comparada**. México, D.F.: UNAM, Instituto de Investigaciones Jurídicas.

Calvin College (2001) **What is an Operating System?** En Calvin. Recuperado en: <http://www.calvin.edu/~rbobeldy/tutorials/os/basics.htm> [Consultado 22 de febrero 2016]

Camacho, F. y Dávila, R. (2015) **Anonymous hackea portal de MVS y publica comunicados apócrifos**. En La Jornada en internet. Recuperado en: <http://www.jornada.unam.mx/ultimas/2015/03/14/anonymouse-publica-falso-comunicado-de-mvs-sobre-ex-colaboradores-de-aristegui-6832.html> [Consultado 21 de marzo 2015]

Cámara de Diputados (2016) **Comisión Permanente declara constitucional Reforma Política de la Ciudad de México**. En Comunicación social, Boletín N°.0824, Recuperado en: <http://www5.diputados.gob.mx/index.php/esl/Comunicacion/Agencia-de-Noticias/2015/Diciembre/09/1287-Aprueban-diputados-en-lo-general-y-con-cambios-dictamen-de-minuta-del-Senado-sobre-la-reforma-politica-de-la-Ciudad-de-Mexico-y-discuten-58-reservas> [Consultado 9 de marzo 2016]

Carballar, J. (2010) **Wi-Fi: lo que se necesita conocer**. México: Alfaomega grupo editor.

Carballude, P. (2013) **Fingerprinting Tor**. En: **Information Management & Computer Security**, 21 (2). Recuperado en: <http://www.emeraldinsight.com/journals.htm?articleid=17090719> [Consultado 28 de enero 2016]

Carr, N. (2011) **¿Qué está haciendo internet con nuestras mentes?** México: Taurus.

Castaingts, J. (2002) **Simbolismos del dinero: antropología y economía una encrucijada**. México: UAM; Anthropos.

Castillo, P. (2015) **I2P: Una red anónima que deberías conocer**. En Security inside. Recuperado en: <http://securityinside.info/i2p-una-red-anonima-que-deberias-conocer/> [Consultado 19 de diciembre 2015]

Castromil, J. (2014) **Los ultraportátiles resisten en el reinado de las tabletas**. En 20 minutos. Recuperado en: <http://www.20minutos.es/noticia/2195188/0/mejores/ordenadores/ultraportatiles/> [Consultado 20 de febrero 2016]

Centre for International Governance Innovation (2016) **Seven in ten (71%) global citizens say the “dark net” should be shut down**. En Cigionline. Recuperado en: https://www.cigionline.org/sites/default/files/factum_2016_cigiipsos_survey_darknet_0.pdf [Consultado 8 de mayo 2016]

Chapple, M., Ballad, B., Ballad, T. y Banks, E. (2014) **Access control, authentication, and public key infrastructure**. 2a ed. Burlington, Massachusetts: Jones & Bartlett Learning.

Cisneros, M. (2012) **Cómo elaborar trabajos de grado**. Bogotá: Ecoe Ediciones.

Cisterna, F. (2005) **Categorización y triangulación como procesos de validación del conocimiento en investigación cualitativa**. En *Theoria*, 14 (1). Recuperado en: <http://www.redalyc.org/articulo.oa?id=29900107> [Consultado 17 de febrero 2016]

Clarke, I., Sandberg, O., Wiley, B. y Hong, T. (2001) **Freenet: a distributed anonymous information storage and retrieval system**. En Stanford. Recuperado en: <http://snap.stanford.edu/class/cs224w-readings/clarke00freenet.pdf> [Consultado 17 de diciembre 2016]

Codina, L. (2003) **Internet invisible y web semántica: ¿El futuro de los sistemas de información en línea?** En *Revista Tradumática*, (2). Recuperado en: <http://www.fti.uab.es/tradumatica/revista> [Consultado 20 de enero 2016]

Computer geek (2012) **What is the difference between a web browser and a search engine?** En Computer Geek. Recuperado en: <http://www.computer-geek.net/what-is-the-difference-be-va-47.html> [Consultado 28 de febrero 2016]

Congreso de los Estados Unidos Mexicanos (1995) **Ley Federal de Telecomunicaciones** (Última reforma publicada DOF 16-01-2013), Capítulo I, Disposiciones generales. En Cámara de diputados. Recuperado en: http://www.sct.gob.mx/fileadmin/migrated/content_uploads/Ley_Federal_de_Telecomunicaciones.pdf [Consultado 8 de marzo 2015]

----- (2014) **Ley Federal de Telecomunicaciones y Radiodifusión**. Título décimo sexto, capítulo único. Medios de impugnación. En Secretaría de Comunicaciones y Transportes. Recuperado en: <http://www.sct.gob.mx/fileadmin/Comunicaciones/LFTR.pdf> [Consultado 9 de marzo 2016]

Conner-Sax, K. y Krol, E. (1999) **The whole Internet: the next generation**. Sebastopol, California: O' Reilly.

Conrad, B. y Shirazi, F. (2014) **A survey on Tor and I2P**. En Geti2p. Recuperado en: https://geti2p.net/static/pdf/icimp_2014_1_40_30015.pdf [Consultado 13 de febrero 2016]

Constantin, L. (2016) **Privacy-conscious users rejoice: You can now use Facebook's Android app over Tor**. En CSO. Recuperado en: http://www.csoonline.com/article/3024779/security/privacy-conscious-users-rejoice-you-can-now-use-facebooks-android-app-over-tor.html#tk.rss_all [Consultado 23 de enero 2016]

Conti, M., Crane, S., Frassetto, T., Homescu, A., Koppen, G., Larsen, P., Liebchen, C., Perry, M. y Sadeghi, A. (2016) **Selfrando: Securing the Tor Browser against De-anonymization Exploits**. En Proceedings on Privacy Enhancing Technologies, (4). Recuperado en: https://www.ics.uci.edu/~perl/pets16_selfrando.pdf [Consultado 20 de junio de 2016]

Contreras, M. (2015) **Windows XP aún sigue siendo más usado que Windows 8.1**. En Fayer wayer. Recuperado en: <https://www.fayerwayer.com/2015/04/windows-xp-aun-sigue-siendo-mas-usado-que-windows-8-1/> [Consultado 7 de marzo 2016]

Contreras, S. (2014) **Los limites en la era digital**. Etcétera: para entender a los medios, 165, pp.37 – 41.

Corcuera, J. y Arnaus, R. (1998) **Internet para todos**. Madrid: Prensa Técnica.

Cordón, J. (2010) **Las nuevas fuentes de información: información y búsqueda documental en el contexto de la web 2.0**. Madrid: Ediciones Pirámide.

Cornelius, I. (2010) **Information policies and strategies**. London: Facet.

Corona, E. (2014) **Las mejores laptops económicas**. En Vive USA. Recuperado en: <http://www.viveusa.mx/articulo/2014/08/19/compras/las-mejores-laptops-economicas> [Consultado 17 de febrero 2016]

Cortez, M. (2015) **Mariana's Web**. En Revistas Bolivianas. Recuperado en: http://www.revistasbolivianas.org.bo/pdf/rits/n9/n9_a14.pdf [Consultado 30 de enero 2016]

Council of the American Library Association (2008) **Standards for accreditation of master's programs in library & information studies**. American Library Association. Recuperado en: http://www.ala.org/accreditedprograms/sites/ala.org/accreditedprograms/files/content/standards/standards_2008.pdf [Consultado 24 de agosto de 2016]

Council on Library and Information Resources (2002) **Building a national strategy for preservation: issues in digital media archiving**. En Council on Library and Information Resources. Recuperado en: <http://www.clir.org/pubs/reports/pub106/pub106.pdf> [Consultado 30 de enero 2016]

Craig, C. (2014) **Advantages and disadvantages of Linux**. En Renewablecs. Recuperado en: <https://renewablepcs.wordpress.com/about-linux/advantages-of-using-linux/> [Consultado 26 de febrero 2016]

Crespo, A. (2016) **Remcos, otro malware que está a la venta en la Dark Web**. En Redes zone. Recuperado en: <http://www.redeszone.net/2016/08/07/remcos-otro-malware-que-esta-a-la-venta-en-la-dark-web/> [Consultado 13 de agosto 2016]

----- (2016) **La red Tor gana seguridad gracias a los nuevos dominios .onion**. En Redes zone. Recuperado en: <http://www.redeszone.net/2016/08/14/troyano-bancario-scylex-aparece-la-dark-web/> [Consultado 21 de agosto 2016]

Criddle, L. (2016) **What is social engineering?** En Webroot. Recuperado en: <http://www.webroot.com/hk/en/home/resources/tips/online-shopping-banking/secure-what-is-social-engineering> [Consultado 4 de marzo 2016]

Crisol, L. (2015) **How to Use the Built-in Windows Defender Antivirus on Windows 10**. En How to geek. Recuperado en: <http://www.howtogeek.com/220232/how-to-use-the-built-in-windows-defender-antivirus-on-windows-10/> [Consultado 22 de febrero 2016]

Croll, A. (2010) **Técnicas de monitorización Web**. Madrid: Anaya Multimedia, depósito legal.

Dachis, A. (2013) **Las mejores y peores marcas: cómo escoger un portátil que no falle.** En Gizmodo en español. Recuperado en: <http://es.gizmodo.com/las-mejores-y-peores-marcas-como-escoger-un-portatil-q-1468106074> [Consultado 17 de febrero 2016]

De Charras, D. (2006) **Redes, burbujas y promesas: algunas reflexiones críticas acerca del proyecto sociedad de la información y la nueva economía.** Argentina: Prometeo libros.

Devine, J. y Egger-Sider, F. (2009) **Going beyond Google: The invisible web in learning and teaching.** New York: Neal Schuman Publishers.

Dhanjani, N., Ríos, B. y Hardin, B. (2009) **La nueva generación hacker.** Madrid: Anaya Multimedia, depósito legal.

Di Trocchio, F. (1998) **Las mentiras de la ciencia: por qué y cómo engañan los científicos.** Madrid: Alianza.

Diario 24 horas (2012) **Vigila policía federal red informática del país.** En Diario 24 horas. Recuperado en: <http://www.24-horas.mx/vigila-policia-federal-red-informatica-del-pais/> [Consultado 10 de enero 2014]

Díaz, Y. (2008) **Medios de Transmisión no confinados.** En Teleinformática-electiva iv. Recuperado en: <http://teleinformatica-electivaiv.blogspot.mx/2008/07/medios-de-transmisin-no-confinados-o.html> [Consultado 26 de febrero 2016]

Digital Citizens Alliance and RiskIQ shows (2015) **How content theft sites and malware are exploited by cybercriminals to hack into internet users' computers and personal data.** En Digital Citizens Alliance. Recuperado en: <https://media.gractions.com/314A5A5A9ABBBBC5E3BD824CF47C46EF4B9D3A76/0f03d298-aedf-49a5-84dc-9bf6a27d91ff.pdf> [Consultado 19 de diciembre 2015]

Dimensión macabra. (2014) **Desmintiendo fotos de la Deep Web** [Episodio 1]. Dimensión macabra. Recuperado en: <https://www.youtube.com/watch?v=sPqevB3jZxI&index=1&list=PLeqhKxfHwY4U5i6tNSNXfrQH5AQJZfAj9> [Consultado 13 de febrero 2016]

Dingledine, R. (2002) **Pre-alpha: run an onion proxy now!** En Archives Seul. Recuperado en: <http://archives.seul.org/or/dev/Sep-2002/msg00019.html> [Consultado 28 de enero 2016]

Dirección General de Bibliotecas UNAM (2011) **Servicio de acceso remoto a BIDI UNAM.** En BIDI UNAM. Recuperado en: http://bidi.unam.mx/web/sbdsite/mailling/foll_bidiago/foll_bidiagoAR.html [Consultado 3 de marzo 2016]

Dpa (2015) **Multa millonaria a ATT por robo de datos en México y otros países.** En La Jornada en internet. Recuperado en: <http://www.jornada.unam.mx/ultimas/2015/04/08/multa-millonaria-a-att-por-robo-de-datos-en-mexico-y-otros-paises-9222.html> [Consultado 8 de abril 2015]

DTIC Editores (2014) **Trustwave presenta precios de Malware en el mercado negro.** En Securitic. Recuperado en: <http://www.securitic.com.mx/noticias/1073-trustwave-presenta-precios-de-malware-en-el-mercado-negro> [Consultado 1 de agosto 2014]

El país (2016) **Dos años por espiar a su exnovia con un programa en el móvil.** En El país. Recuperado en: http://politica.elpais.com/politica/2016/01/17/actualidad/1453069620_328953.html [Consultado 28 de abril 2016]

El Universal (2015) **Presentan México Leaks, una plataforma para información anónima.** En El universal. Recuperado en: <http://www.eluniversal.com.mx/computacion-tecno/2015/mexico-leaks-plataforma-anonima-102719.html> [Consultado 21 de marzo 2015]

Emmanuel, H. (2014) **¿Qué es la Deep Web?** En Marcianos. Recuperado en: <http://marcianosmx.com/que-es-la-deep-web/> [Consultado 27 de enero 2015]

Enriquekpo (2013) **Mi experiencia en la DeepWeb y los niveles 5, 6, 7 y 8.** En Taringa. Recuperado en: <http://www.taringa.net/posts/info/16786901/Mi-experiencia-en-la-DeepWeb-y-los-niveles-5-6-7-y-8.html> [Consultado 30 de enero 2016]

Entrena, D. (2006) **El empleo de información privilegiada en el mercado de valores: un estudio de su régimen administrativo sancionador.** Cizur Menor, Navarra: Thomson Civitas.

Escalante, F. (2004) **El derecho a la privacidad**. México: Instituto Federal de Acceso a la Información y Protección de Datos.

Falla, F. (Conductor). Rodriguez, F. (Productor). (2013) **Los huesos de nadie** [Episodio 30]. Cuarto milenio. Recuperado en: <http://fansmilenio3.com/cuarto-milenio-8x30-los-huesos-de-nadie-07042013/> [Consultado 29 de febrero 2016]

Fenollosa, A. (2015) **¿Cuál es el mejor navegador web?** 2016. En Programador web Valencia. Recuperado en: <https://programadorwebvalencia.com/cual-es-el-mejor-navegador-web-2016/#.VtlgKuY0-t> [Consultado 27 de febrero 2016]

Ferrán, N. (2009) **Búsqueda y recuperación de la información**. Barcelona: UOC, 2009.

Finklea, K. (2015) **Dark Web**. En Congressional Research Service. Recuperado en: <https://www.fas.org/sqp/crs/misc/R44101.pdf> [Consultado 30 de enero 2016]

Foliveros (2014) **Cómo escoger la mejor computadora portátil**. En Hipertextual. Recuperado en: <http://hipertextual.com/archivo/2014/07/comprar-computador-portatil/> [Consultado 18 de febrero 2016]

Franganillo, M. (2015) **Cuando buscar en Google se convierte en un delito**. En El diario. Recuperado en: http://www.eldiario.es/hojaderouter/ilegales/Google-busquedas-delito-conspiracion-provocacion-tentativa_6_397620277.html [Consultado 1 de febrero 2016]

Franklin, C. y Coustan, D. (2016) **How operating systems work**. En Computer how stuff Works. Recuperado en: <http://computer.howstuffworks.com/operating-system.htm> [Consultado 22 de febrero 2016]

Fransson, J. (2011) **Efficient information searching on the Web: a handbook in the art of searching for information**. New Delhi, India: Ess Ess Publications.

Fulkenson, D. (2012) **Remote access technologies for library collections: tools for library users and managers**. Hershey, Pennsylvania: Information Science Reference.

Gabilondo, P. (2016) **Deep web: el mercado clandestino de las cuentas robadas.** En El confidencial. Recuperado en: http://www.elconfidencial.com/tecnologia/2016-08-05/precio-cuentas-robadas-deep-web_1242837/ [Consultado 13 de agosto de 2016]

Gabinete de Comunicación Estratégica (2015) **¿Qué tan conectado está México?** En Gabinete. Recuperado en: http://en2015.gabinete.mx/static/conectividad/Conectividad_mexico_2015.pdf [Consultado 14 de febrero 2015]

Gamella, J. y Álvarez, A. (1999) **Las rutas del éxtasis: drogas de síntesis y nuevas culturas juveniles.** Barcelona: Ariel.

García, A. (2016) **Un experimento detecta 110 servidores maliciosos en la red Tor.** En Grupo ADSL Zone. Recuperado en: <http://www.adslzone.net/2016/07/25/experimento-detecta-110-servidores-maliciosos-la-red-tor/> [Consultado 31 de julio de 2016]

García, L. (2000) **Diccionario del archivero-bibliotecario: terminología de la elaboración, tratamiento y utilización de los materiales propios de los centros documentales.** Gijón, Asturias: Trea.

García, L. (2003) **Extraer y visualizar información en internet: el web mining.** España: Trea.

Gilchrist, A. (2009) **Information science in transition.** London: Facet.

Givens, C. (2015) **Information privacy fundamentals for librarians and information professionals.** Lanham, Maryland: Rowman & Littlefield.

Gobierno de Monterrey (2015) **Reglamento de bibliotecas públicas municipales de Monterrey.** En Portal del Gobierno de Monterrey. Recuperado en: http://portal.monterrey.gob.mx/pdf/reglamentos/reg_bibliotecas.pdf [Consultado 21 de marzo 2016]

Gómez, P. (2012) **Derecho a la información: reflexiones contemporáneas.** México: UAM.

Gómez, M., Deslaires, J., y Álzate, M. (2010) **Como hacer tesis de maestría y doctorado.** Bogotá: Ecoe ediciones.

González, J. (1998) **Autopistas de la información e Internet: tecnología, servicios, peajes y normas de navegación**. Cáceres: Universidad de Extremadura.

González, I., Sánchez, G., Toscano, L., Prudente, M. y Aguilar, G. (2012) **Leyes de protección de datos personales en el mundo y la protección de datos biométricos – Parte I**, *Revista Seguridad Cultura de prevención para TI*, (13). Recuperado en: <http://revista.seguridad.unam.mx/numeros/numero-13> [Consultado 30 de enero 2016]

Gralla, P. (2007) **Cómo funciona Internet**. Madrid: Anaya Multimedia.

Graux, H. (2009) **Darknets and the future of freedom of expression in the information society**. En *Facing the Limits of the Law*. Berlín: Springer.

Greenberg, A. (2015) **New Dark-Web Market Is Selling Zero-Day Exploits to Hackers**. En *Wired*. Recuperado en: <http://www.wired.com/2015/04/therealdeal-zero-day-exploits/> [Consultado 12 de enero 2015]

Guardian Project (2014) **Orbot: Tor for Android**. En *Guardian Project*. Recuperado en: <https://guardianproject.info/apps/orbot/> [Consultado 23 de junio de 2016]

Guerrero, M. (2006) **Medios de comunicación y la función de transparencia**. México: Instituto Federal de Acceso a la Información y Protección de Datos.

Guim, J. (1997) **Internet: La guía más fácil para dominar la red**. España: Ediciones Gestión.

Guthrie, C. (2015) **9 things you can hire a hacker to do and how much it will (generally) cost**. En *Search data center*. Recuperado en: <http://www.businessinsider.com/9-things-you-can-hire-a-hacker-to-do-and-how-much-it-will-generally-cost-2015-5?op=1> [Consultado 17 de mayo 2015]

Hariri, N. (2013) **Do natural language search engines really understand what users want?** *Online Information Review*, 37 (2). Recuperado en: <http://dx.doi.org/10.1108/OIR-12-2011-0210> [Consultado 27 de febrero 2016]

Hedberg, S. (1996) **The telecommunications network of the new millennium.** *IEEE*, 4 (1). Recuperado en: <http://ieeexplore.ieee.org/xpl/articleDetails.jsp?arnumber=481661&newsearch=true&queryText=telecommunications%20network%20of%20the%20new%20millennium> [Consultado 13 de marzo 2016]

Hernon, P. (2003) **U.S. government on the Web: getting the information you need.** United States of America: Libraries Unlimited.

Himanen, P. (2002) **La ética del hacker y el espíritu de la era de la información.** En Destino. Recuperado en: <http://eprints.rclis.org/bitstream/10760/12851/1/pekka.pdf> [Consultado 1 de marzo 2013]

Howell, P. (2014) **I made my own Deep Web black market, and it took just 60 seconds.** En Deepstweb. Recuperado en: <http://www.dailydot.com/business/deepify-make-your-own-deep-web-black-market/> [Consultado 30 de enero 2016]

Huang, Q., Li, Q., Li, H y Yan, Z (2012) **An Approach to Incremental Deep Web Crawling Based on Incremental Harvest Model.** *Procedia Engineering*, 29. Recuperado en: <http://www.sciencedirect.com/science/article/pii/S1877705812001038> [Consultado 30 de enero 2016]

Huang, T., Zeng, Z., Li, C. y Leung, C. (2012) **Neural information processing.** Berlín: Springer.

Huerta, I. (2016) **Tlatlaya: cierran en definitiva acceso a expediente.** Aristegui noticias. Recuperado en: <http://aristeguinoticias.com/2706/mexico/tlatlaya-cierran-en-definitiva-acceso-a-expediente/> [15 de febrero de 2015]

Hughes, M. (2014) **How you can officially browse Facebook over Tor.** En Make use of. Recuperado en: <http://www.makeuseof.com/tag/can-officially-browse-facebook-tor/> [Consultado 12 de marzo 2016]

Huidobro, J. (1998) **Todo sobre comunicaciones.** Madrid: Paraninfo.

Hundie, K. (2003) **Library operations and Internet resources.** *The Electronic Library*, 21 (6). Recuperado en: <http://dx.doi.org/10.1108/02640470310509117> [Consultado 20 de marzo 2016]

Instituto Nacional de Estadística y Geografía (2014) **Hogares con Internet por medio de conexión, 2001 a 2014**. En INEGI. Recuperado en: <http://www3.inegi.org.mx/sistemas/sisept/default.aspx?t=tin202&s=est&c=19352> [Consultado 14 de febrero 2015]

----- (2014) **Hogares con conexión a Internet por entidad federativa, 2014**. En INEGI. Recuperado en: <http://www3.inegi.org.mx/sistemas/sisept/default.aspx?t=tin241&s=est&c=26489> [Consultado 14 de enero 2015]

----- (2014) **Usuarios de Internet por grupos de edad, 2001 a 2014**. En INEGI. Recuperado en: <http://www3.inegi.org.mx/sistemas/sisept/default.aspx?t=tin214&s=est&c=19446> [Consultado 14 de enero 2015]

Instituto Latinoamericano de la Comunicación Educativa (2012) **Redes de telecomunicaciones**. En: ILCE. Recuperado en: http://bibliotecadigital.ilce.edu.mx/sites/ciencia/volumen3/ciencia3/149/htm/sec_8.htm [Consultado 13 de marzo 2016]

Ingwersen, Peter (1999) **The role of libraries and libraries in organising digital information**. Libri, 49. Recuperado en: <http://www.librijournal.org/pdf/1999-1pp11-15.pdf> [Consultado 20 de enero 2016]

----- (2002) **Information retrieval interaction**. Londres: Taylor Graham Publishing.

Ibáñez Baleares, J. (2003) **Acceso a la información y aprendizaje informal en Internet**. *Revista Científica de Comunicación y Educación*. Recuperado en: http://www.google.com.mx/url?sa=t&rct=j&q=&esrc=s&source=web&cd=1&ved=0CBwQFjAA&url=http%3A%2F%2Fwww.revistacomunicar.com%2Fverpdf.php%3Fnumero%3D21%26articulo%3D21-2003-05&ei=WNodVdLDCImZgwTj14HACw&usq=AFQjCNEmc_kJ4qAexqPCFX0JzRln7daXuw [Consultado 21 de enero 2016]

Cossío, J. y Hernández, M. (2015) **La Transparencia y el acceso a la Información en los expedientes judiciales**. Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales. Recuperado en: <http://inicio.ifai.org.mx/Publicaciones/Transparencia%20y%20Acceso%20a%20a%20Informaci%C3%B3n%20en%20los%20Expedientes%20Judiciales.pdf> [10 de julio de 2016]

Internautas21 (2014) **Deep web: mi experiencia entrando a la Internet profunda**. En Internautas21. Recuperado en: <http://internautas21.com/mi-experiencia-entrando-a-la-deep-web/> [Consultado 27 de enero 2015]

Ist sara (2014) **Deep Web - Casos reales**. En DeepIstweb. Recuperado en: <http://deeplstweb.blogspot.mx/2014/11/mariana-web.html> [Consultado 30 de enero 2016]

Isunza, E. y Olvera, A. (2006) **Democratización, rendición de cuentas y sociedad civil participación ciudadana y control social**. México, D.F.: H. Cámara de Diputados, LIX Legislatura.

Infante, A. (2013) **Unofficial guide to Tor: really private browsing**. En Sluug. Recuperado en: http://www.sluug.org/resources/presentations/2013/2013-12-11_TOR.pdf [Consultado 13 de febrero 2016]

Informática hoy (2010) **¿Qué comprar? Las diferencias entre Notebook y Netbook**. En Informática hoy. Recuperado en: <http://www.informatica-hoy.com.ar/hardware-notebook-laptop/Que-comprar-Las-diferencias-entre-Notebook-y-Netbook.php> [Consultado 20 de febrero 2016]

----- (2010) **Tablets: ¿qué es eso?** En Informática hoy, Recuperado en: <http://www.informatica-hoy.com.ar/tablets/Tablets-que-es.php> [Consultado 20 de febrero 2016]

Information Week. (2013) **Va GDF contra delitos en internet: crea policía cibernética**. Information week, (228), 8.

Imgur (2013) **How to grow crystals**. En Imgur. Recuperado en: <http://imgur.com/gallery/BuF31> [Consultado 26 de junio de 2016]

IP location (2016) **What is the difference between public and private IP address?** En IP Location. Recuperado en: <https://www.iplocation.net/public-vs-private-ip-address> [Consultado 1 de marzo 2016]

Janes, J. (1998) **The Internet public library: an intellectual history.** *Library Hi Tech*, 16 (2). Recuperado en: <http://dx.doi.org/10.1108/07378839810303983> [Consultado 30 de enero 2016]

Jmaturana TI (2008) **¿Por qué Linux no sustituirá a Windows?** En Silicon. Recuperado en: http://www.silicon.es/por_que_linux_no_sustituira_a_windows-8111 [Consultado 21 de febrero 2016]

Kara, S. (2010) **Tráfico sexual: el negocio de la esclavitud moderna.** Madrid: Alianza.

Katz, J. y Rice, R. (2005) **Consecuencias sociales del uso de Internet.** Barcelona: UOC.

Kavindra, B. (2016) **The best Linux distros – 2016.** En Buddhilive. Recuperado en: <http://www.buddhilive.com/2016/01/the-best-linux-distros-2016.html> [Consultado 22 de febrero 2016]

Keerthi, R. (2015) **What is the Marianas web?** En Quora. Recuperado en: <https://www.quora.com/What-is-the-Marianas-web> [Consultado 30 de enero 2016]

Kemp, S. (2014) **Mitos en linux.** En Ingenierasa's blog. Recuperado en: http://www.ingenierasa.org/blog/Mitos_en_linux.html [Consultado 22 de febrero 2016]

Kent, A. (1988) **Encyclopedia of library and information science.** New York: Marcel Dekker.

Khandelwal, Swati (2016) **Former tor developer created malware for FBI to unmask tor users.** En The hacker news. Recuperado en: <http://thehackernews.com/2016/04/tor-unmask-malware.html> [Consultado 8 de mayo 2016]

----- (2016) **Silk Road 2.0 dark-web admin pleads guilty**. En The hackers news. Recuperado en: <http://thehackernews.com/2016/04/silk-road-dark-web.html> [Consultado 6 de abril 2016]

Khrennikov, I. (2014) **Putin Sets \$110,000 Bounty for Cracking Tor as Anonymous Internet Usage in Russia Surges**. En Bloomberg. Recuperado en: <http://www.bloomberg.com/news/2014-07-29/putin-sets-110-000-bounty-for-cracking-tor-as-anonymous-internet-usage-in-russia-surges.html> [Consultado 3 de agosto 2014]

Kovacs, D., y Elkordy, A. (2000) **Collection development in cyberspace: building an electronic library collection**. *Library Hi Tech*, 18 (4). Recuperado en: <http://www.emeraldinsight.com/journals.htm?articleid=861248&show=html> [Consultado 21 de enero 2016]

Kumar, M. (2015) **France will not ban public Wi-Fi or Tor Network, Prime Minister Valls confirms**. En The hacker news. Recuperado en: http://thehackernews.com/2015/12/France-tor-ban_10.html [Consultado 19 de diciembre 2015]

Labrousse, A. (1993) **La droga, el dinero y las armas**. México: Siglo XXI.

Lechuga, J. (2005) **Reflexiones acerca de la era de la información** (new economics). México: UAM.

Lenovo (2016) **What is a Tablet PC?** En Lenovo. Recuperado en: <http://shop.lenovo.com/us/en/faqs/laptop-faqs/what-is-a-tablet-pc/> [Consultado 20 de febrero 2016]

Lessig, L. (2001) **El código y otras leyes del ciberespacio**. Madrid: Grupo Santillana.

Levine, J., Baroudi, C. y Levine, M. (2006) **Internet para dummies**. México: ST editorial.

Locker, T. (2015) **Germany's most notorious Darknet drug dealer sentenced to only 7 years**. En Motherboard. Recuperado en: <http://motherboard.vice.com/read/germanys-most-notorious-darknet-drug-dealer-sentenced-to-only-7-years> [Consultado 19 de diciembre 2015]

López, J. (2016) **Iniciativa por la que se adiciona un capítulo al código penal federal denominado Violación a la intimidad (Revenge Porn)**. En Derecho, TIC y conocimiento abierto. Recuperado en: <http://jonathanlpeztor.blogspot.mx/2016/02/iniciativa-por-la-que-se-adiciona-un.html> [Consultado 8 de marzo 2016]

López y Quezada, R. (2013) **Cómo obtienen los reporteros la información**. México, D. F.: Universidad Nacional Autónoma de México.

Lozano Aguilar, C. (2013) **Los trolls cibernéticos**, *Revista Seguridad Cultura de prevención para TI*, (17). Recuperado en: <http://revista.seguridad.unam.mx/numeros/numero-17> [Consultado 14 de enero 2015]

Lyon, D. (2003) **Surveillance as social sorting: privacy, risk and digital discrimination**. London: Routledge.

Mac, R. (2013) **Who is Ross Ulbricht? Piecing together the life of the alleged libertarian mastermind behind Silk Road**. En Forbes. Recuperado en: <http://www.forbes.com/sites/ryanmac/2013/10/02/who-is-ross-ulbricht-piecing-together-the-life-of-the-alleged-libertarian-mastermind-behind-silk-road/#588cfb1122e9> [Consultado 30 de enero 2016]

Macbroadcast (2013) **Cjdns - The modular isp, the internet of the future?** [Episodio 23]. Blake Curran. Recuperado en: <https://www.youtube.com/watch?v=NRhMY-gdXDw> [Consultado 17 de febrero 2016]

Maldonado, Á. y Rodríguez, L. (2006) **La información especializada en internet**. 2a ed. España: CSIC.

Marin, E. (2015) **Anonymous comienza a eliminar la propaganda a favor de ISIS en la dark web**. En Gizmodo en español. Recuperado en: <http://es.gizmodo.com/anonymous-comienza-a-eliminar-la-propaganda-a-favor-de-1744630985> [Consultado 19 de octubre 2015]

----- (2016) **5 motivos para dejar de usar Google como buscador por defecto**. En Gizmodo en español. Recuperado en: <http://es.gizmodo.com/5-motivos-para-dejar-de-usar-google-como-buscador-por-d-1785519010> [Consultado 21 de agosto 2016]

Martín, M. (1993) **La producción social de comunicación**. 2da ed. Madrid: Alianza.

Martínez de Sousa, J. (2004) **Diccionario de bibliología y ciencias afines**. 3ra ed. Gijón, Asturias: Trea.

Martínez, J. y Lara, P. (2006) **La accesibilidad de los contenidos web**. España: editorial UOC.

Martínez, F. y Gutiérrez, B. (2010) **Cómputo en Nube: Ventajas y Desventajas**, *Revista Seguridad Cultura de prevención para TI*, (8). Recuperado en: <http://revista.seguridad.unam.mx/numero-08/c%C3%B3mputo-en-nube-ventajas-y-desventajas> [Consultado 14 de enero 2015]

Martos, A. (2012) **Cómo buscar en internet**. Madrid: Anaya Multimedia.

McClure, S., Scambray, J. y Kurtz, G. (2000) **Hackers: secretos y soluciones para la seguridad de redes**. Madrid; México: Osborne/McGraw-Hill.

McCreadie, M. y Rice, R. (1999) **Trends in analyzing access to information. Part I: cross-disciplinary conceptualizations of access**. *Information processing and management: an international journal archive*, 35 (1).

McFarland, C., Paget, F. y Samani, R. (2015) **Data economy, the Marketplace for stolen digital information**. En Intel Security Group. Recuperado en: <http://www.mcafee.com/us/resources/reports/rp-hidden-data-economy.pdf> [Consultado 18 de enero 2016]

McKiernan, G. (2001) **The Hidden Web**. *Science & Technology Libraries*, 20 (4). Recuperado en: http://www.tandfonline.com/doi/abs/10.1300/J122v20n04_08#preview [Consultado 28 de febrero 2016]

Méndez, M. (2014) **Tails, el OS anónimo, en USB y gratuito que utiliza Edward Snowden**. En Gizmodo en español. Recuperado en: <http://es.gizmodo.com/tails-el-os-anonimo-y-en-usb-que-edward-snowden-aconse-1563333168> [Consultado 23 de enero 2015]

Mendoza, M. (2014) **Cómo configurar Tor utilizando Vidalia**. En We live security. Recuperado en: <http://www.welivesecurity.com/la-es/2014/07/14/como-configurar-tor-utilizando-vidalia/> [Consultado 13 de febrero 2016]

Merino, M. (2014) **¿Cómo serán las bibliotecas en un futuro cercano?** En Tic beat. Recuperado en: <http://www.ticbeat.com/tecnologias/como-vern-las-bibliotecas-en-futuro-cercano/> [Consultado 6 de marzo 2015]

Metz, P. (2000) **Principles of selection for electronics resources**. Library Trends, 48 (4).

Mongardini, C. (2007) **Miedo y sociedad**. Madrid: Alianza.

Moore, N. (2000) **The Internet and the library**. Library Review, 49 (9). Recuperado en: <http://dx.doi.org/10.1108/00242530010354029> [Consultado 20 de abril 2016]

Morales, E. (1991) **Sociedad e información**. Revista AIDBA. 12 (2).

Morales, E. (2006) **Infodiversidad y cibercultura: globalización e información en América latina**. Argentina: Alfagrama.

Morán, A., Servín, A. y Alquicira, O. (2015) **TIC (Internet) y ciberterrorismo**. Revista Seguridad Cultura de prevención para TI, (23). Recuperado en: <http://revista.seguridad.unam.mx/numeros/numero-23> [Consultado 12 de abril 2015]

Motos, V. (2015) **Script para detectar nodos maliciosos en Tor**. En Hack players. Recuperado en: <http://www.hackplayers.com/2015/12/script-para-detectar-nodos-maliciosos-en-tor.html> [Consultado 21 de diciembre 2015]

Nácar, J. (2015) **Policía Federal se fortalece en la lucha contra delitos cibernéticos**. En MSN noticias. Recuperado en: <http://prodigy.msn.com/es-mx/noticias/mexico/polic%C3%ADa-federal-se-fortalece-en-la-lucha-contra-delitos-cibern%C3%A9ticos/ar-AAfHUHW?li=AA5a7e&ocid=mailsignout> [Consultado 19 de diciembre 2015]

Newitz, A. **8 de noviembre de 2015. 9 datos básicos sobre seguridad que los expertos desearían que supieras.** En Gizmodo en español. Recuperado en: <http://es.gizmodo.com/9-datos-basicos-sobre-seguridad-que-los-expertos-desear-1723071993> [Consultado 10 de noviembre de 2015]

Ortega, R. (2011) **Tablets: la revolución táctil.** En Recursos Tic. Recuperado en: <http://recursostic.educacion.es/observatorio/web/fr/equipamiento-tecnologico/hardware/1012-tablets-la-revolucion-tactil-> [Consultado 20 de febrero 2016]

Pacheco, W. (2015) **¿Cómo entrar a la deep web y qué cosas necesitas saber al respecto?** En Batanga. Recuperado en: <http://www.batanga.com/tech/55817/como-entrar-a-la-deep-web-y-que-cosas-necesitas-saber-al-respecto> [Consultado 27 de enero 2015]

Palmer, C. (2004) **EFF Joins Forces with Tor Software Project.** En Electronic Frontier Foundation. Recuperado en: <https://www.eff.org/press/archives/2004/12/21-0> [Consultado 28 de enero 2016]

Páramo, T. (2006) **Sociedad y comunicación: una mirada al siglo XXI.** México: UAM, Unidad Iztapalapa: Plaza y Valdés.

Pardo, M. (1997) **Cómo elegir un proveedor de Internet.** Madrid: Anaya Multimedia.

Pash, A. (2012) **How to crack a Wi-Fi network's WPA password with Reaver.** En Life hacker. Recuperado en: <http://lifelifehacker.com/5873407/how-to-crack-a-wi-fi-networks-wpa-password-with-reaver> [Consultado 27 de febrero 2016]

Pastor, J. (2015) **Cómo ha cambiado internet después de las filtraciones de Snowden.** En Xataka, Recuperado en: <http://www.xataka.com/privacidad/como-ha-cambiado-internet-despues-de-las-filtraciones-de-snowden> [Consultado 9 de enero 2016]

PC Actual (2012) **Consejos PC Actual para elegir el portátil perfecto.** En PC Actual. Recuperado en: http://www.pcactual.com/articulo/zona_practica/paso_a_paso/paso_a_paso_har_dware/10961/consejos_actual_para_elegir_portatil_perfecto.html [Consultado 20 de febrero 2016]

----- (2014) **Analizamos 8 portátiles y 8 Ultrabooks con Windows 8.** En PC Actual, Recuperado en: http://www.pcactual.com/articulo/laboratorio/comparativas/12779/analizamos_portatiles_ultrabooks_con_windows.html [Consultado 21 de febrero 2016]

Peachey, P. (2013) **Eric Eoin Marques: 28-year-old architect's son from Dublin accused of being world's biggest dealer in child abuse images.** En Independent. Recuperado en: <http://www.independent.co.uk/news/world/europe/eric-eoin-marques-28-year-old-architect-s-son-from-dublin-accused-of-being-world-s-biggest-dealer-in-8782756.html> [Consultado 31 de enero 2016]

Pedley, P. (2001) **The invisible web: searching the hidden parts of the internet.** London: Aslib-IMI.

Pingdom (2012) **The incredible story of the first PC, from 1965.** En Tech blog. Recuperado en: <http://royal.pingdom.com/2012/08/28/the-first-pc-from-1965/> [Consultado 19 de febrero 2016]

Pool, W. (2014) **Guiados: par trenzado, coaxial y fibra óptica.** En Telecomunicaciones portafolio. Recuperado en: <http://telecomunicacionesportafolio.blogspot.mx/2014/12/21-guiados-par-trenzado-coaxial-y-fibra.html> [Consultado 26 de febrero 2016]

----- (2014) **No guiados: radiofrecuencia, microondas, satélite e infrarrojo.** En Telecomunicaciones portafolio. Recuperado en: <http://telecomunicacionesportafolio.blogspot.mx/2014/12/22no-guiados-radiofrecuencia-microondas.html> [Consultado 26 de febrero 2016]

Pot, J. (2012) **4 Reasons i'm glad i own a netbook and not a tablet.** En Make use of. Recuperado en: <http://www.makeuseof.com/tag/4-reasons-glad-netbook-tablet-opinion/> [Consultado 18 de febrero 2016]

Proceso (2014) **Colaboradora de Valor por Tamaulipas, sufrió amenazas antes de ser asesinada.** En Proceso. Recuperado en: <http://www.proceso.com.mx/?p=385068> [Consultado 17 de mayo 2015]

Quincoces, A. (2015) **Internet profundo: El mundo ilegal en la Web.** En Sin embargo. Recuperado en: <http://www.sinembargo.mx/02-08-2015/1435895> [Consultado 3 de agosto 2015]

Quintin, C. (2013) **Tor Is For Everyone: Why You Should Use Tor?** En Electronic Frontier Foundation. Recuperado en: <https://www.eff.org/deeplinks/2014/06/why-you-should-use-tor> [Consultado 2 de agosto 2014]

Ramos, L. (2016) **Políticas de información en bibliotecas, archivos y museos.** En Seminario de investigación sobre políticas de información. Conferencia pronunciada en la Universidad Nacional Autónoma de México.

Randall, N. (1995) **Aprendiendo Internet en 21 días.** México: Prentice Hall.

Reference and User Services Association (2010) **Guidelines for Implementing and Maintaining Virtual Reference Services.** En American Library Association. Recuperado en: <http://www.ala.org/rusa/sites/ala.org.rusa/files/content/resources/guidelines/virtual-reference-se.pdf> [Consultado 31 de enero 2016]

Reitman, R. (2016) **With rule 41, little-known committee proposes to grant new hacking powers to the government.** En Electronic Frontier Foundation. Recuperado en: <https://www.eff.org/deeplinks/2016/04/rule-41-little-known-committee-proposes-grant-new-hacking-powers-government> [Consultado 8 de mayo 2016]

Rendón, M. (2005) **Bases teóricas y filosóficas de la bibliotecología.** 2a ed. México: UNAM, Centro Universitario de Investigaciones Bibliotecológicas.

Reuters (2015) **Lanza EU plan de sanciones financieras contra ciberataques.** En La Jornada en internet. Recuperado en: <http://www.jornada.unam.mx/ultimas/2015/04/01/lanza-estados-unidos-programa-de-sanciones-a-ciberataques-3017.html> [Consultado 1 de abril 2015]

Revilla, Á. (2014) **Los cristales de 4chan.** [Episodio 22]. En DrossRotzank. Recuperado en: <https://www.youtube.com/watch?v=P7pdXv1BS7U> [Consultado 26 de junio de 2016]

Revista del consumidor (2012) **Estudio de calidad: Computadoras portátiles y tabletas, tu mundo**. Revista del consumidor. Recuperado en: http://www.consumidor.gob.mx/wordpress/wp-content/uploads/2012/08/RC426_Computadoras_OK.pdf [Consultado 23 de enero 2016]

----- (2014) **Estudio de calidad: dile hola a tu nueva computadora Laptops, ultraportátiles y todo en uno**. Revista del consumidor. Recuperado en: <http://www.consumidor.gob.mx/wordpress/?p=17652> [Consultado 23 de enero 2016]

----- (2015) **Estudio de calidad: las computadoras más impersonales a revisión**. Revista del consumidor. Recuperado en: http://www.consumidor.gob.mx/wordpress/wp-content/uploads/2015/09/computadoras_impersonales.pdf [Consultado 23 de enero 2016]

Righter, R. (1982) **El control de la información: política, prensa y tercer mundo**. Madrid: Pirámide.

Rodríguez, B. (2002) **El documento: entre la tradición y la renovación**. España: Trea.

Rolfbroer (2011) **Search engine algorithm basics**. En Moz. Recuperado en: <https://moz.com/blog/search-engine-algorithm-basics> [Consultado 27 de febrero 2016]

Rouse, M. (2011) **Cloud storage service**. En Tech target. Recuperado en: <http://searchcloudstorage.techtarget.com/definition/cloud-storage-service> [Consultado 27 de abril 2016]

----- (2011) **Darknet**. En Tech target. Recuperado en: <http://searchnetworking.techtarget.com/definition/darknet> [Consultado 27 de abril 2016]

Rowlands, I. (1997) **Understanding information policy: proceedings of a workshop held at Cumberland Lodge, Windsor Great Park**. New Providence, New Jersey: Bowker-Saur.

RT (2015) **Tor Project accuses FBI of paying university to ‘deanonymize’ users without warrant.** En RT. Recuperado en: <https://www.rt.com/usa/321756-tor-project-fbi-cmu-attack/> [Consultado 23 de enero 2016]

----- (2016) **Tor Project moves to lessen dependency on US gov’t.** En RT. Recuperado en: <https://www.rt.com/usa/329870-tor-govt-funding-crowdsourcing/> [Consultado 23 de enero 2016]

Rubin, R. (2004) **Foundations of library and information Science.** United States of America: Neal Schuman Publishers.

Ruthven, I. y Kelly, D. (2011) **Interactive information seeking, behaviour and retrieval.** London: Facet Publishing.

Singh, S. (2004) Collection management in the electronic environment. The Bottom Line: Managing Library Finances, 17 (2). Recuperado en: <http://www.emeraldinsight.com/journals.htm?articleid=860825&show=html> [Consultado 10 de enero 2014]

Salazar, I. (2005) **Las profundidades de Internet: accede a la información que los buscadores no encuentran y descubre el futuro inteligente de la red.** Asturias: TREA.

Salvador, J. (2006) **Recuperación de la información.** Argentina: Alfagrama.

Salvador, J. y Angos, J. (2000) **Técnicas de recuperación de información: aplicación con Dialog.** Gijón, Asturias: Trea.

Sánchez, Á. (2015) **Resuelve de forma sencilla tus dudas entre un PC de escritorio y uno portátil.** En About. Recuperado en: <http://computadoras.about.com/od/comprar-computadora/bb/Antes-De-Comprar-Una-Computadora.htm> [Consultado 17 de febrero 2016]

Sánchez, A. (2014) **17 detenidos en la operación ONYMOUS contra el crimen organizado en la Deep Web.** En Hipertextual. Recuperado en: <http://hipertextual.com/2014/11/onymous-deep-web> [Consultado 21 de diciembre 2014]

Sánchez, A. (1997) **Territorios virtuales: de internet hacia un nuevo concepto de la simulación.** México: Taurus.

Segu Info (2014) **TOR confirma que el anonimato en la Deep Web fue roto.** En Segu Info: noticias sobre seguridad de la información. Recuperado en: http://blog.segu-info.com.ar/2014/08/tor-confirma-que-el-anonimato-en-la.html?utm_source=feedburner&utm_medium=feed&utm_campaign=Feed%3A+NoticiasSeguridadInformatica+%28Noticias+de+Seguridad+de+la+Informaci%C3%B3n%29 [Consultado 3 de agosto 2014]

Self.deepweb (2015) **Does the internet really have 8 layers/levels?** En Reddit. Recuperado en: https://www.reddit.com/r/deepweb/comments/35ei8s/does_the_internet_really_have_8_layerslevels/ [Consultado 30 de enero 2016]

Sheldon, T. (1994) **LAN times: enciclopedia de redes networking.** México: McGraw-Hill Interamericana.

Shera, J. (1990) **Los fundamentos de la educación bibliotecológica.** México: UNAM, Centro Universitario de Investigaciones Bibliotecológicas.

Sherali, S. (2015) **An analysis of tools for online anonymity.** *International Journal of Pervasive Computing and Communications*, 11 (4). Recuperado en: <http://dx.doi.org/10.1108/IJPCC-08-2015-0030> [Consultado 28 de febrero 2016]

Simonite, T. (2015) **Los datos más sensibles se guardan en los ordenadores más vulnerables.** En Technology review. Recuperado en: <http://www.technologyreview.es/informatica/47938/los-datos-mas-sensibles-se-guardan-en-los/> [Consultado 10 de agosto 2015]

SlashDot (2015) **TheRealDeal Market: venta de exploit en la Deep Web.** En Segu Info. Recuperado en: <http://blog.segu-info.com.ar/2015/05/therealdeal-market-venta-de-exploit-en.html> [Consultado 12 de julio 2015]

Spector, L. (2013) **Why you may want a desktop instead of a laptop.** En PC world. Recuperado en: <http://www.pcworld.com/article/2048257/why-you-may-want-a-desktop-instead-of-a-laptop.html> [Consultado 17 de febrero 2016]

Spotz, K. (2014) **Lo que he aprendido como traficante de drogas de Internet.** En Motherboard. Recuperado en: <http://motherboard.vice.com/es/read/lo-que-he-aprendido-siendo-traficante-de-drogas-en-internet> [Consultado 19 de diciembre 2015]

Stacey, A. y Stacey, A. (2004) **Effective information retrieval from the Internet: an advanced user's guide**. Oxford: Chandos.

Stallman, R. (2016) **Linux y el sistema GNU**. En GNU. Recuperado en: <http://www.gnu.org/gnu/linux-and-gnu.es.html> [Consultado 7 de marzo 2016]

Stevenson, D. (2015) **AMD vs Intel: Why AMD will always be the underdog but ARM still beats Intel for mobile**. En PC Advisor. Recuperado en: <http://www.pcadvisor.co.uk/feature/pc-components/amd-vs-intel-3528212/> [Consultado 21 de febrero 2016]

Suber, P. (2004) **Open Access Overview**, En Legacy earth. Recuperado en: <http://legacy.earlham.edu/~peters/fos/overview.htm> [Consultado 27 de marzo 2015]

Sullivan, J. (2011) **2010 Free Software Awards announced**. En Free Software Foundation. Recuperado en: <https://www.fsf.org/news/2010-free-software-awards-announced> [Consultado 28 de enero 2016]

Syverson, P. (2013) **Onion Routing**. En Onion Router. Recuperado en: <http://www.onion-router.net/> [Consultado 28 de enero 2016]

Takahashi, H. (2015) **La mafia digital secuestra México**. Revista emeequis.

Talens, S. y Hernández, J. (1997) **Internet: redes de computadores y sistemas de información**. Madrid: Paraninfo.

Taylor, A. (2004) **The organization of information**. 2a ed. Colorado: libraries Unlimited.

Télam (2014) **Rusia ofrece 110 mil dólares al que logre hackear la red anónima Tor**. En Télam: Agencia nacional de noticias. Recuperado en: <http://www.telam.com.ar/notas/201407/72368-rusia-ofrece-110-mil-dolares-al-que-logre-hackear-la-red-anonima-tor.html> [Consultado 5 de agosto 2014]

Than, K. (2012) **James Cameron Completes Record-Breaking Mariana Trench Dive**. En National Geographic. Recuperado en: <http://news.nationalgeographic.com/news/2012/03/120325-james-cameron-mariana-trench-challenger-deepest-returns-science-sub/> [Consultado 30 de enero 2016]

The Freenet Project Inc (2015) **What is Freenet?** En Freenet Project. Recuperado en: <https://freenetproject.org/about.html> [Consultado 17 de febrero 2016]

The Internet Assigned Numbers Authority (2016) **IANA**. En The Internet Assigned Numbers Authority. Recuperado en: <http://www.iana.org/> [Consultado 3 de marzo 2016]

The Invisible Internet Project (2015) **I2P**. En The Invisible Internet Project. Recuperado en: <https://geti2p.net/es/comparison/freenet> [Consultado 17 de febrero 2016]

The onion router (2016) **Why is it called Tor?** En Tor. Recuperado en: <https://www.torproject.org/docs/faq.html.en#WhyCalledTor> [Consultado 28 de enero 2016]

Tic beat (2015) **La red anónima TOR, en peligro de ciberataques en 2015**. En Tic beat. Recuperado en: http://www.ticbeat.com/seguridad/la-red-anonima-tor-en-peligro-de-ciberataques-en-2015/?utm_content=buffercb547&utm_medium=social&utm_source=twitter.com&utm_campaign=buffer [Consultado 11 de julio 2015]

Todd, S. (1999) **A guide to the Internet and World Wide Web**. *Structural Survey*, 17 (1). Recuperado en: <http://www.emeraldinsight.com.pbidi.unam.mx:8080/doi/full/10.1108/02630809910263614> [Consultado 14 de enero 2016]

Torres, M. (2005) **La función social de las bibliotecas universitarias**. *Boletín de la Asociación Andaluza de bibliotecarios*, 20 (80). Recuperado en: <http://dialnet.unirioja.es/servlet/dcart?info=link&codigo=2173486&orden=95050> [Consultado 28 de enero 2016]

Torres, G. (2003) **Hacia un modelo de servicios en la biblioteca digital**. *Investigación Bibliotecológica*, 17 (35). Recuperado en: <http://www.revistas.unam.mx/index.php/ibi/article/view/4021/3571> [Consultado 31 de enero 2016]

Torres, G. y Juárez, B. (2008) **Los sistemas de organización del conocimiento y el manejo de contenidos digitales**. Biblioteca Universitaria, 11 (1). Recuperado en: <http://www.redalyc.org/pdf/285/28512651002.pdf> [Consultado 22 de junio del 2016]

Torres, G., Sánchez, E., Rodríguez, A. y Guerra, J. (2015) ***The Blended Librarian and the Disruptive Technological Innovation in the Digital World***. Open Access Library Journal, 2. Recuperado en: https://www.researchgate.net/publication/280947367_The_Blended_Librarian_and_the_Disruptive_Technological_Innovation_in_the_Digital_World [Consultado 25 de junio de 2016]

Torres, G. (2013) **How the VDSL connection works**. En Hardware. Recuperado en: <http://www.hardwaresecrets.com/how-the-vdsl-connection-works/> [Consultado 24 de febrero 2016]

Tramullas, J. y Olvera, M. (2001) **Recuperación de la información en Internet**. Madrid: Ra-Ma.

Travieso, M. (2003) **Las publicaciones electrónicas: una revolución en el siglo XXI**. *ACIMED*, 11 (2). Recuperado en: <http://eprints.rclis.org/5101/1/publicaciones.pdf> [Consultado 4 de febrero 2016]

Treloar, A. (1994) **Classifying Internet Access Tools**. *Resource Sharing & Information Networks*, 9 (2). Recuperado en: http://www.tandfonline.com/doi/abs/10.1300/J121v09n02_04 [Consultado 19 de enero 2016]

Treviño, D. (2015) **¿Quién te conoce?** Revista Seguridad Cultura de prevención para TI, (24). Recuperado en: http://revista.seguridad.unam.mx/sites/revista.seguridad.unam.mx/files/revistas/pdf/24_RevistaSeguridad-Aproximacion_al_malware.pdf [Consultado 28 de enero 2016]

UNESCO. (2002) **Memoria del mundo: directrices para la salvaguarda del patrimonio documental**. París: UNESCO, División de la sociedad de la información.

UNESCO (2005) **De la sociedad de la información a las sociedades del conocimiento**. En Hacia las sociedades del conocimiento. Recuperado en: <http://unesdoc.unesco.org/images/0014/001419/141908s.pdf> [Consultado 13 de febrero 2016]

Vaca, J. (1997) **Los secretos de la seguridad en internet**. España: Anaya Multimedia.

Valero, D. (2015) **¿Qué sistema operativo es más seguro? Un estudio sorprende con sus resultados.** En Grupo ADSL Zone. Recuperado en: <http://www.adslzone.net/2015/02/23/sistema-operativo-seguro/> [Consultado 21 de febrero 2016]

Vallès, J. (2002) **Ciencia política: una introducción.** 2a ed. España: Ariel.

Veblen, T. (1992) **Teoría de la clase ociosa.** México: Fondo de Cultura Económica.

Velasco, R. (2015) **La red Tor gana seguridad gracias a los nuevos dominios .onion.** En Redes zone. Recuperado en: http://www.redeszone.net/2015/09/14/la-red-tor-gana-seguridad-gracias-a-los-nuevos-dominios-onion/?utm_content=buffer420a8&utm_medium=social&utm_source=twitter.com&utm_campaign=buffer [Consultado 19 de diciembre 2015]

----- (2016) **La red Tor no está preparada para trabajar con conexiones IPv6.** En Redes zone. Recuperado en: <http://www.redeszone.net/2016/08/19/la-red-tor-no-esta-preparada-trabajar-conexiones-ipv6/> [Consultado 21 de agosto 2016]

Villaseñor, A. (2014) **Computadora genérica vs computadora de marca ¿Cuál comprar?** En Armando ayúdame. Recuperado en: <http://armandoayudame.com/tecnologia/computadora-generica-vs-computadora-de-marca-cual-comprar/> [Consultado 18 de febrero 2016]

Vota, W. (2012) **4 Reasons why desktop computers are better than mobile devices in ICT4D.** En ITC Works. Recuperado en: <http://www.ictworks.org/2012/04/16/4-reasons-why-desktop-computers-are-better-mobile-devices-ict4d/> [Consultado 17 de febrero 2016]

Voutssás, J. (2010) **Preservación documental digital y seguridad informática.** Investigación bibliotecológica, 24 (50). Recuperado en: <http://www.journals.unam.mx/index.php/ibi/article/view/21416> [Consultado 18 de junio de 2016]

Vratonjic, N., Huguenin, K., Bindschaedler, V. y Hubaux, J. (2014) **A location-privacy threat stemming from the use of shared public IP addresses**. *IEEE transactions on mobile computing*, 13 (11). Recuperado en: <http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=6757043&isnumber=6913596> [Consultado 3 de marzo 2016]

Walp, R., Ulema, M. y Michel, M. (2009) **Economic engineering for improving access to the worldwide telecommunications network**. *IEEE*, 47 (11). Recuperado en: <http://ieeexplore.ieee.org/xpl/login.jsp?tp=&arnumber=5307483&url=http%3A%2F%2Fieeexplore.ieee.org%2Fiel5%2F35%2F5307452%2F05307483.pdf%3Farnumber%3D5307483> [Consultado 13 de marzo 2016]

Ward, M. (2015) **Drogas y pornografía, los sitios más populares en la red oscura**. En BBC. Recuperado en: http://www.bbc.com/mundo/noticias/2015/01/141231_tecnologia_tor_red_oscura_paginas_populares_trafico_ig [Consultado 12 de julio 2015]

Warner, J. (2010) **Human information retrieval**. Cambridge, Massachusetts: Massachusetts Institute of Technology.

Warren, C. (2012) **How does high speed internet actually work?** En Webopedia. Recuperado en: <http://mashable.com/2012/11/07/high-speed-internet-technologies/#8CaMZQ6D4PqB> [Consultado 24 de febrero 2016]

Wasik, J. (1999) **Building and maintaining digital reference services**. En ERIC Digest. Recuperado en: <http://files.eric.ed.gov/fulltext/ED427794.pdf> [Consultado 31 de enero 2016]

Web Wise Team (2012) **What is wireless internet (Wi-Fi)?** En BBC. Recuperado en: <http://www.bbc.co.uk/webwise/guides/about-wifi> [Consultado 26 de febrero 2016]

Wei, W. (2016) **26-Year-Old Hacker Sentenced to Record 334 Years in Prison**. En The hacker news. Recuperado en: <http://thehackernews.com/2016/01/hacker-sentenced-prison.html> [Consultado 11 de enero 2016]

Whitley, S. (2007) **Prison time for viewing porn?** En ABC News. Recuperado en: <http://abcnews.go.com/2020/LegalCenter/prison-time-viewing-porn/story?id=2785054> [Consultado 1 de febrero 2016]

Wilhoit, K. y Hilt, S. (2015) **North American underground: the glass Tank**. En TrendLabs. Recuperado en: <http://www.trendmicro.com/cloud-content/us/pdfs/security-intelligence/white-papers/wp-north-american-underground.pdf> [Consultado 21 de diciembre 2015]

Wlodarz, D. (2014) **The Apple myth: why security through obscurity isn't security**. En Beta news. Recuperado en: <http://betanews.com/2014/04/07/the-apple-myth-why-security-through-obscurity-isnt-security/> [Consultado 22 de febrero 2016]

Wolton, D. (2000) **Sobrevivir a internet: conversaciones con Oliver Jay**. España: Gedisa.

World Wide Web Consortium (2016) **Tim Berners-Lee**. En W3C. Recuperado en: <https://www.w3.org/People/Berners-Lee/> [21 de agosto 2016]

Zahumenszky, C (2013) **La red cifrada TOR recomienda abandonar Windows**. En Gizmodo en español. Recuperado en: <http://es.gizmodo.com/la-red-cifrada-tor-recomienda-abandonar-windows-1043218659> [Consultado 10 de agosto 2013]

----- (2015) **Cómo empezar a utilizar el navegador anónimo Tor, paso a paso**. En Gizmodo en español. Recuperado en: <http://es.gizmodo.com/los-mejores-consejos-para-mantener-de-verdad-tu-privaci-1681089272> [Consultado 23 de enero 2015]

Zavia, M. (2015) **Una semana en la deep web: esto es lo que me he encontrado**. En Xataka. Recuperado en: <http://www.xataka.com/analisis/una-semana-en-la-deep-web-esto-es-lo-que-me-he-encontrado> [Consultado 15 de febrero 2016]

Yazdan, N. (2006) **The invisible web: an empirical study of cognitive invisibility**. Journal of Documentation, (62). Recuperado en: <http://www.emeraldinsight.com/doi/abs/10.1108/00220410610688732> [Consultado 12 de abril de 2015]

Zipper, G. (productor) Schiller, M. (productor) y Winter, A. (director) (2015) **Deep Web**. [Video documental]. Estados Unidos: Epix network.

Ziming, L. (2004) **The evolution of documents and its impacts.** *Journal of Documentation*, 60 (3). Recuperado en: <http://www.emeraldinsight.com/journals.htm?articleid=864247&show=html> [Consultado 30 de enero 2016]

Zittrain, J. y Palfrey, J. (2007) **Internet filtering: the politics and mechanisms of control.** En OII. Recuperado en: www.oii.ox.ac.uk/research/publications/RR14.pdf [Consultado 28 de enero 2016]

Žygimantas (2015) **8 Best hackintosh laptops with guides and comparison.** En Pick notebook. Recuperado en: <http://picknotebook.com/blog/best-hackintosh-laptop/> [Consultado 21 de marzo 2016]

Anexos

Anexo A
Cedulas de la red oscura Tor

Red oscura Tor
Número de sitio investigado: 1-A
Nombre del sitio: Tor box Autor: No hay datos URL: http://torbox3uio6wchz.onion/
Materia general: Mensajes por correo electrónico -- Personas anónimas
<p>Idioma: Inglés</p> <p>Fecha de adquisición de la URL: 24 de agosto 2015</p> <p>Fecha de acceso: 23 de febrero 2016. Tiempo de navegación: 2:00 minutos 12 de marzo 2016. Tiempo de navegación: 46 segundos 17 de marzo 2016. Tiempo de navegación: 2:17 minutos</p> <p>Tipo de acceso conceptual: no requerido Clasificación de la información: reservada Contenido: servicio de mail escondido, sin revelar la ubicación e identidad por medio de un registro previo, dentro de Tor.</p> <p>Última fecha de actualización del sitio: No hay datos</p>

Red oscura Tor
Número de sitio investigado: 2-A
Nombre del sitio: SIGAINT Autor: No hay datos URL: sigaintevyh2rzvw.onion
Materia general: Mensajes por correo electrónico -- Personas anónimas
<p>Idioma: Inglés</p> <p>Fecha de adquisición de la URL: 24 de agosto 2015</p> <p>Fecha de acceso: 23 de febrero 2016. Tiempo de navegación: 1:59 minutos 12 de marzo 2016. Tiempo de navegación: 1:27 minutos 18 de marzo 2016. Tiempo de navegación: 1:45 minutos</p> <p>Tipo de acceso conceptual: no requerido Clasificación de la información: reservada Contenido: servicio de mail escondido, sin revelar la ubicación e identidad por medio de un registro previo dentro de Tor.</p> <p>Última fecha de actualización del sitio: 2015, 24 de octubre</p>

Red oscura Tor
Número de sitio investigado: 3-A
Nombre del sitio: Mail Tor Autor: No hay datos URL: mail2tor2zyjdctd.onion
Materia general: Mensajes por correo electrónico -- Personas anónimas
Idioma: Inglés
Fecha de adquisición de la URL: 24 de agosto 2015
Fecha de acceso: 23 de febrero 2016. Tiempo de navegación: 1:30 minutos 12 de marzo 2016. Tiempo de navegación: 1:12 minutos 15 de marzo 2016. Tiempo de navegación: 2:24 minutos
Tipo de acceso conceptual: no requerido Clasificación de la información: reservada Contenido: servicio de e-mail para mantener la privacidad dentro de Tor.
Última fecha de actualización del sitio: No hay datos

Red oscura Tor
Número de sitio investigado: 6-A
Nombre del sitio: Deep web radio Autor: Zoidberg URL: http://76qugh5bey5gum7l.onion/
Materia general: Transmisión (Radio) -- Libertad de información
Idioma: Inglés
Fecha de adquisición de la URL: 21 de junio 2015
Fecha de acceso: 23 de febrero 2016. Tiempo de navegación: 1:20 minutos 12 de marzo 2016. Tiempo de navegación: 1:16 minutos 18 de marzo 2016. Tiempo de navegación: 2:34 minutos
Tipo de acceso conceptual: no requerido Clasificación de la información: pública accesible Contenido: servicio de radio, 5 estaciones de radio.
Última fecha de actualización del sitio: 2016, 17 de marzo

Red oscura Tor
Número de sitio investigado: 7-A
Nombre del sitio: Cebolla chan 3.0 Autor: MyBB URL: http://s6cco2jylmxqcdeh.onion/
Materia general: Libertad de expresión Materia general: Libertad de información
Idioma: Inglés
Fecha de adquisición de la URL: 21 de junio 2015
Fecha de acceso: 23 de febrero 2016. Tiempo de navegación: 2:10 minutos 12 de marzo 2016. Tiempo de navegación: 2:11 minutos 17 de marzo 2016. Tiempo de navegación: 1:50 minutos
Tipo de acceso conceptual: no requerido Clasificación de la información: interna Contenido: foro con registro previo sobre opiniones e información proporcionada por los miembros, el foro permite todo tipo de contenidos a excepción de pornografía infantil.
Última fecha de actualización del sitio: 2016, 17 de marzo

Red oscura Tor
Número de sitio investigado: 8-A
Nombre del sitio: The Hidden Wiki Autor: Zayaya & K0mradz URL: http://zqktlwi4fecvo6ri.onion/
Materia general: Sitios web -- Directorios
Idioma: Inglés
Fecha de adquisición de la URL: 21 de junio 2015
Fecha de acceso: 23 de febrero 2016. Tiempo de navegación: 1:08 minutos 12 de marzo 2016. Tiempo de navegación: 1:40 minutos 17 de marzo 2016. Tiempo de navegación: 2:16 minutos
Tipo de acceso conceptual: no requerido Clasificación de la información: pública accesible Contenido: enlace a la Hidden Wiki, servicio de enlaces agrupados en temas a manera de directorio.
Última fecha de actualización del sitio: 2016, 17 de marzo

Red oscura Tor
Número de sitio investigado: 9-A
Nombre del sitio: Torch Autor: No hay datos URL: http://xmh57jrznw6insl.onion/
Materia general: Motores de búsqueda en Web
Idioma: Inglés
Fecha de adquisición de la URL: 21 de junio 2015
Fecha de acceso: 23 de febrero 2016. Tiempo de navegación: 1:50 minutos 12 de marzo 2016. Tiempo de navegación: 3:24 minutos 16 de marzo 2016. El sitio no fue alcanzable, sin conexión al sitio
Tipo de acceso conceptual: requerido Clasificación de la información: pública accesible Contenido: servicio de motor de búsqueda.
Última fecha de actualización del sitio: No hay datos

Red oscura Tor
Número de sitio investigado: 12-A
Nombre del sitio: Beneath VT Autor: No hay datos URL: http://74ypjgjf6oejmax.onion/
Materia general: Virginia Polytechnic Institute and State University Materia general: Túneles -- Diseño y construcción
Idioma: Inglés
Fecha de adquisición de la URL: 21 de junio 2015
Fecha de acceso: 23 de febrero 2016. Tiempo de navegación: 2:20 minutos 12 de marzo 2016. Tiempo de navegación: 2:29 minutos 15 de marzo 2016. Tiempo de navegación: 1:05 minutos
Tipo de acceso conceptual: requerido Clasificación de la información: pública accesible Contenido: información sobre la construcción y riesgos de los túneles y tuberías de vapor de Virginia.
Última fecha de actualización del sitio: 2015

Red oscura Tor
Número de sitio investigado: 13-A
Nombre del sitio: How to be a lying ninja Autor: Suid Lizard URL: http://kpynyvym6xqi7wz2.onion/lyingninja.txt
Materia general: Autoengaño
Idioma: Inglés
Fecha de adquisición de la URL: 21 de junio 2015
Fecha de acceso: 23 de febrero 2016. Tiempo de navegación: 2:01 minutos 12 de marzo 2016. Tiempo de navegación: 1:04 minutos 14 de marzo 2016. Tiempo de navegación: 1:42 minutos
Tipo de acceso conceptual: requerido Clasificación de la información: pública accesible Contenido: información para entrenar a una persona en el arte de mentir como un experto.
Última fecha de actualización del sitio: No hay datos

Red oscura Tor
Número de sitio investigado: 14-A
Nombre del sitio: How to get detailed information on anybody Autor: Waldo URL: http://kpynyvym6xqi7wz2.onion/fuksomeone.txt
Materia general: Espionaje
Idioma: Inglés
Fecha de adquisición de la URL: 21 de junio 2015
Fecha de acceso: 23 de febrero 2016. Tiempo de navegación: 1:30 minutos 12 de marzo 2016. Tiempo de navegación: 2:25 minutos 18 de marzo 2016. Tiempo de navegación: 5:25 minutos
Tipo de acceso conceptual: requerido Clasificación de la información: pública accesible Contenido: información de cómo obtener la localización domiciliaria y otros datos críticos de una persona a partir de un dato concreto.
Última fecha de actualización del sitio: 2006, 18 de octubre

Red oscura Tor
Número de sitio investigado: 15-A
Nombre del sitio: Infection Autor: No hay datos URL: http://kpynyvym6xqi7wz2.onion/iNFECTioN_CooKBooK.txt
Materia general: Terrorismo -- Bioterrorismo Materia general: Delitos por computadora Materia general: Espionaje Materia general: Tarjetas de identificación -- Falsificaciones
Idioma: Inglés Fecha de adquisición de la URL: 21 de junio 2015 Fecha de acceso: 23 de febrero 2016. Tiempo de navegación: 2:42 minutos 12 de marzo 2016. Tiempo de navegación: 1:20 minutos 18 de marzo 2016. Tiempo de navegación: 3:30 minutos Tipo de acceso conceptual: requerido Clasificación de la información: pública accesible Contenido: manual sobre sustancias nocivas, intervención telefónica, crack informático, tarjetas de crédito y terrorismo. Última fecha de actualización del sitio: 2006, 18 de octubre

Red oscura Tor
Número de sitio investigado: 16-A
Nombre del sitio: Link parasite underground links Autor: No hay datos URL: http://kpynyvym6xqi7wz2.onion/links.html
Materia general: Sitios web -- Directorios
Idioma: Inglés Fecha de adquisición de la URL: 21 de junio 2015 Fecha de acceso: 23 de febrero 2016. Tiempo de navegación: 2:00 minutos 12 de marzo 2016. Tiempo de navegación: 1:20 minutos 15 de marzo 2016. Tiempo de navegación: 2:30 minutos Tipo de acceso conceptual: no requerido Clasificación de la información: pública accesible Contenido: servicio de enlaces a sitios de la web superficial. Última fecha de actualización del sitio: No hay datos

Red oscura Tor
Número de sitio investigado: 17-A
Nombre del sitio: Tor links .onion link list Autor: No hay datos URL: http://torlinkbgs6aabns.onion/
Materia general: Sitios web -- Directorios
Idioma: Inglés y Polaco
Fecha de adquisición de la URL: 21 de junio 2015
Fecha de acceso: 23 de febrero 2016. Tiempo de navegación: 1:20 minutos 12 de marzo 2016. Tiempo de navegación: 3:00 minutos 14 de marzo 2016.
Tipo de acceso conceptual: no requerido Clasificación de la información: pública accesible Contenido: reemplazo moderado de la Hidden wiki, servicio de enlaces convencionales y no convencionales a sitios y servicios relacionados con servicios financieros, bienes digitales, política, erotismo, asesoría legal, pornografía, servicios de hackeo.
Última fecha de actualización del sitio: No hay datos

Red oscura Tor
Número de sitio investigado: 19-A
Nombre del sitio: Alpha-7-bravo blog (A7B) Autor: A7B URL: http://opnju4nyz7wbypme.onion/weblog/index.html
Materia general: Vigilancia electrónica -- Control social Materia general: Política mundial Materia general: Blogs
Idioma: Inglés
Fecha de adquisición de la URL: 21 de junio 2015
Fecha de acceso: 23 de febrero 2016. Tiempo de navegación: 3:00 minutos 12 de marzo 2016. Tiempo de navegación: 3:08 minutos 16 de marzo 2016. Tiempo de navegación: 1:18 minutos
Tipo de acceso conceptual: requerido Clasificación de la información: pública accesible Contenido: blog acerca de cuestiones geopolíticas, vigilancia y secreto de Estado.
Última fecha de actualización del sitio: 2015, 28 de diciembre

Red oscura Tor
Número de sitio investigado: 20-A
Nombre del sitio: Imperial library Autor: Las Zenow URL: http://xfmro77i3lixucja.onion/
Materia general: Bibliotecas e Internet Materia general: Piratería (Derechos de autor) Materia general: Recursos electrónicos de información
Idioma: Inglés
Fecha de adquisición de la URL: 21 de junio 2015
Fecha de acceso: 23 de febrero 2016. Tiempo de navegación: 2:05 minutos 12 de marzo 2016. Tiempo de navegación: 2:02 minutos 14 de marzo 2016. Tiempo de navegación: 1:48 minutos
Tipo de acceso conceptual: no requerido Clasificación de la información: reservada Contenido: servicio de catálogo de libros para su lectura y descarga sobre temas de ciencia ficción, fantasía, paranormal, historia, misterio, erotismo, psicología entre otros. El usuario puede aportar libros al repositorio.
Última fecha de actualización del sitio: 2015, 15 de junio

Red oscura Tor
Número de sitio investigado: 21-A
Nombre del sitio: Radical militant library Autor: No hay datos URL: http://c3jemx2ube5v5zpg.onion/
Materia general: Bibliotecas e Internet Materia general: Piratería (Derechos de autor) Materia general: Recursos electrónicos de información
Idioma: Inglés
Fecha de adquisición de la URL: 21 de junio 2015
Fecha de acceso: 23 de febrero 2016. Tiempo de navegación: 1:42 minutos 12 de marzo 2016. Tiempo de navegación: 4:02 minutos 14 de marzo 2016. Tiempo de navegación: 1:50 minutos
Tipo de acceso conceptual: no requerido Clasificación de la información: reservada Contenido: servicio de catálogo de libros para su descarga sobre temas de historia alternativa, anarquía, seguridad informática, fantasía, Horror, guerra, sátira, misterio entre otros.

Última fecha de actualización del sitio: 2016, 13 de marzo

Red oscura Tor

Número de sitio investigado: 22-A

Nombre del sitio: **Military manuals**

Autor: No hay datos

URL: http://nope7beergoa64ih.onion/Military_manuals/

Materia general: Guerra -- Manuales

Materia general: Ciencia militar

Idioma: Inglés

Fecha de adquisición de la URL:

24 de agosto 2015

Fecha de acceso:

23 de febrero 2016. Tiempo de navegación: 1:59 minutos

12 de marzo 2016. Tiempo de navegación: 1:31 minutos

15 de marzo 2016. Tiempo de navegación: 1:50 minutos

Tipo de acceso conceptual: requerido

Clasificación de la información: pública accesible

Contenido: servicio de descarga sobre manuales de armamentos militares, vehículos y utilidades tácticas.

Última fecha de actualización del sitio: 2013, 10 de junio

Red oscura Tor

Número de sitio investigado: 23-A

Nombre del sitio: **Index of /**

Autor: No hay datos

URL: <Http://hioxliwisp6mi.onion>

Materia general: Repositorios -- Recursos de información electrónicos

Idioma: Inglés

Fecha de adquisición de la URL:

24 de agosto 2015

Fecha de acceso:

23 de febrero 2016. Tiempo de navegación: 1:50 minutos

12 de marzo 2016. Tiempo de navegación: 1:41 minutos

17 de marzo 2016. Tiempo de navegación: 1:45 minutos

Tipo de acceso conceptual: no requerido

Clasificación de la información: pública accesible

Contenido: repositorio de documentación y contenidos de texto y audiovisuales para su visualización o descarga.

Última fecha de actualización del sitio: 2015, 30 de septiembre

Red oscura Tor
Número de sitio investigado: 24-A
Nombre del sitio: Save the sea kittens! Autor: No hay datos URL: http://wtwfzc6ty2s6x4po.onion/
Materia general: Repositorios -- Recursos de información electrónicos
Idioma: Inglés
Fecha de adquisición de la URL: 24 de agosto 2015
Fecha de acceso: 23 de febrero 2016. Tiempo de navegación: 2:02 minutos 12 de marzo 2016. Tiempo de navegación: 1:45 minutos 15 de marzo 2016. Tiempo de navegación: 1:37 minutos
Tipo de acceso conceptual: no requerido Clasificación de la información: reservada Contenido: repositorio sobre distintos contenidos mediante acceso regulado con registro previo, solo para usuarios registrados.
Última fecha de actualización del sitio: 2016, 10 de octubre

Red oscura Tor
Número de sitio investigado: 25-A
Nombre del sitio: Sipulikanava Autor: No hay datos URL: http://2i7aalqdpiuw36nu.onion/
Materia general: Contenidos generados por los usuarios
Idioma: Finlandés
Fecha de adquisición de la URL: 24 de agosto 2015
Fecha de acceso: 23 de febrero 2016. Tiempo de navegación: 3:12 minutos 12 de marzo 2016. Tiempo de navegación: 1:22 minutos 15 de marzo 2016. Tiempo de navegación: 2:02 minutos
Tipo de acceso conceptual: requerido Clasificación de la información: interna Contenido: foro sobre distintos temas.
Última fecha de actualización del sitio: 2014, 13 de marzo

Red oscura Tor
Número de sitio investigado: 26-A
Nombre del sitio: 100x Your bitcoins in only 24 Hours Autor: No hay datos URL: http://rjuvjyygjqm6mlqm.onion/
Materia general: Moneda – Bitcoin Materia general: Industria de servicios financieros
Idioma: Inglés Fecha de adquisición de la URL: 13 de noviembre 2015 Fecha de acceso: 23 de febrero 2016. Tiempo de navegación: 2:50 minutos 12 de marzo 2016. Tiempo de navegación: 1:37 minutos 14 de marzo 2016. Tiempo de navegación: 1:45 minutos Tipo de acceso conceptual: requerido Clasificación de la información: pública accesible Contenido: servicios sobre la moneda digital Bitcoin para optimizar los procesos de transferencia y obtener mejores ganancias. Última fecha de actualización del sitio: 2016

Red oscura Tor
Número de sitio investigado: 29-A
Nombre del sitio: Pirate crackers Autor: No hay datos URL: http://pirateceo5dz3q4b.onion/
Materia general: Delitos por computadora Materia general: Espionaje
Idioma: Inglés Fecha de adquisición de la URL: 7 de febrero 2016 Fecha de acceso: 23 de febrero 2016. Tiempo de navegación: 1:20 minutos 12 de marzo 2016. Tiempo de navegación: 1:11 minutos 16 de marzo 2016. Tiempo de navegación: 1:30 minutos Tipo de acceso conceptual: requerido Clasificación de la información: pública accesible Contenido: servicios de monitoreo sobre personas y patrones de comportamiento así como acceso a la privacidad ajena. Última fecha de actualización del sitio: No hay datos

Red oscura Tor
Número de sitio investigado: 30-A
Nombre del sitio: Thunder's place Autor: Raizen07 URL: http://thundersplv36ecb.onion/
Materia general: Pene -- Aspectos sociales
Idioma: Inglés
Fecha de adquisición de la URL: 7 de febrero 2016
Fecha de acceso: 23 de febrero 2016. Tiempo de navegación: 2:20 minutos 12 de marzo 2016. Tiempo de navegación: 1:20 minutos 18 de marzo 2016. Tiempo de navegación: 2:01 minutos
Tipo de acceso conceptual: requerido Clasificación de la información: pública accesible Contenido: servicio gratuito sobre estrategias para agrandar el pene del hombre sin pastillas o medicamentos.
Última fecha de actualización del sitio: 2016, 26 de febrero

Red oscura Tor
Número de sitio investigado: 32-A
Nombre del sitio: Grams Autor: No hay datos URL: http://grams7enufi7jmdl.onion/
Materia general: Drogas -- Tráfico Materia general: Motores de búsqueda en Web
Idioma: Inglés
Fecha de adquisición de la URL: 7 de febrero 2016
Fecha de acceso: 23 de febrero 2016. Tiempo de navegación: 1:10 minutos 12 de marzo 2016. Tiempo de navegación: 2:00 minutos 16 de marzo 2016. Tiempo de navegación: 1:50 minutos
Tipo de acceso conceptual: requerido Clasificación de la información: pública accesible Contenido: servicio de motor de búsqueda dedicado para la búsqueda de productos referentes a las drogas ilícitas.
Última fecha de actualización del sitio: No hay datos

Red oscura Tor
Número de sitio investigado: 34-A
Nombre del sitio: BB Compendium Autor: No hay datos URL: http://nope7beergoa64ih.onion/
Materia general: Sitios web -- Directorios Materia general: Drogas -- Tráfico Materia general: Explosivos militares Materia general: Pirotecnia
Idioma: Inglés Fecha de adquisición de la URL: 7 de febrero 2016 Fecha de acceso: 23 de febrero 2016. Tiempo de navegación: 1:45 minutos 12 de marzo 2016. Tiempo de navegación: 1:18 minutos 16 de marzo 2016. Tiempo de navegación: 1:50 minutos Tipo de acceso conceptual: requerido Clasificación de la información: pública accesible Contenido: directorio sobre documentos sobre química, drogas, explosivos, fuegos artificiales y pirotecnia. Última fecha de actualización del sitio: No hay datos

Red oscura Tor
Número de sitio investigado: 36-A
Nombre del sitio: Zilion 2.0 Autor: Lucas Azu URL: http://zilionku2adniig6.onion/
Materia general: Libertad de expresión Materia general: Personas anónimas
Idioma: Portugués Fecha de adquisición de la URL: 7 de febrero 2016 Fecha de acceso: 23 de febrero 2016. Tiempo de navegación: 1:45 minutos 12 de marzo 2016. Tiempo de navegación: 1:18 minutos 16 de marzo 2016. Tiempo de navegación: 2:14 minutos Tipo de acceso conceptual: no requerido Clasificación de la información: pública accesible Contenido: espacio para comentar sobre la libertad de expresión y el anonimato en las redes oscuras. Última fecha de actualización del sitio: 2015, 2 de junio

Red oscura Tor
Número de sitio investigado: 37-A
Nombre del sitio: Flashlight an info beam in the darkweb Autor: Comunidad de la deep Web URL: http://kxojoy6ygyju4h6lwn.onion/
Materia general: Periodismo en línea -- Estados Unidos
Idioma: Inglés
Fecha de adquisición de la URL: 7 de febrero 2016
Fecha de acceso: 23 de febrero 2016. Tiempo de navegación: 2:20 minutos 12 de marzo 2016. Tiempo de navegación: 1:22 minutos 12 de marzo 2016. Tiempo de navegación: 1:05 minutos
Tipo de acceso conceptual: no requerido Clasificación de la información: pública accesible Contenido: portal de noticias sobre el ámbito político, del entretenimiento, económico y social de Estados Unidos.
Última fecha de actualización del sitio: 2016, 16 de marzo

Red oscura Tor
Número de sitio investigado: 35-A
Nombre del sitio: Adult webcomics list Autor: No hay datos URL: http://xcomics5vvoiyary2.onion/
Materia general: Caricaturas y dibujos animados -- Arte erótico Materia general: Caricaturas y dibujos animados -- Pornografía
Idioma: Inglés
Fecha de adquisición de la URL: 7 de febrero 2016
Fecha de acceso: 23 de febrero 2016. Tiempo de navegación: 1:40 minutos 12 de marzo 2016. Tiempo de navegación: 1:30 minutos 15 de marzo 2016. Tiempo de navegación: 2:23 minutos
Tipo de acceso conceptual: no requerido Clasificación de la información: pública accesible Contenido: dibujos en torno al erotismo y la pornografía.
Última fecha de actualización del sitio: 2016, 14 de marzo

Red oscura Tor
Número de sitio investigado: 33-A
Nombre del sitio: Euro guns Autor: No hay datos URL: http://2kka4f23pcxgqkp.onion/
Materia general: Tráfico de armas
Idioma: Inglés
Fecha de adquisición de la URL: 7 de febrero 2016
Fecha de acceso: 23 de febrero 2016. Tiempo de navegación: 1:20 minutos 12 de marzo 2016. Tiempo de navegación: 1:10 minutos 15 de marzo 2016. Tiempo de navegación: 2:22 minutos
Tipo de acceso conceptual: requerido Clasificación de la información: pública accesible Contenido: venta de armas de fuego.
Última fecha de actualización del sitio: No hay datos

Red oscura Tor
Número de sitio investigado: 28-A
Nombre del sitio: Selling a few new iPhone 5S phone Autor: Tendon Mike URL: http://sla2tcypjz774dno.onion/iphone.html
Materia general: iPhone (Teléfono inteligente)
Idioma: Inglés
Fecha de adquisición de la URL: 7 de febrero 2016
Fecha de acceso: 23 de febrero 2016. Tiempo de navegación: 2:30 minutos 12 de marzo 2016. Tiempo de navegación: 1:20 minutos 17 de marzo 2016. Tiempo de navegación: 1:05 minutos
Tipo de acceso conceptual: requerido Clasificación de la información: pública accesible Contenido: presunto producto iphone5S, 32 GB seminuevo al precio de \$400 dólares.
Última fecha de actualización del sitio: 2015, 17 de septiembre

Anexo B

Cedulas de la red oscura Freenet

Red oscura Freenet
Número de sitio investigado: 39-B
Nombre del sitio: Classics in the history of psychology Autor: Christopher D. Green URL: http://127.0.0.1:8888/USK@wNW1qGBP10gzbGn4hYHEMWx6jJ0rpOZ0GFQeVCEdFQ,ZhYtQYew3l5BxS47fTTjZF6NAk0chlT8qm6F6pIBolo,AQACAAE/psychclassics/0/
Materia general: Psicología -- Filosofía
Idioma: Inglés
Fecha de adquisición de la URL: 26 de febrero 2016
Fecha de acceso: 26 de febrero 2016. Tiempo de navegación: 5:00 minutos 12 de marzo 2016. Tiempo de navegación: 1:03 minutos 15 de marzo 2016. Tiempo de navegación: 4:03 minutos
Tipo de acceso conceptual: requerido Clasificación de la información: reservada Contenido: recursos electrónicos en torno a la psicología, contenidos textuales.
Última fecha de actualización del sitio: 2004

Red oscura Freenet
Número de sitio investigado: 40-B
Nombre del sitio: Fefes blog Autor: No hay datos URL: http://127.0.0.1:8888/freenet:USK@qSMEn6R2N1wUOoV83FBidWbFnZBvOrQohXhf3jBsCtk_0FFLouA~e57kN8v2gUlkwzAkraCL56QasY466WNe5w,AQACAAE/feffe/7/
Materia general: Vigilancia electrónica -- Control social
Idioma: Alemán
Fecha de adquisición de la URL: 26 de febrero 2016
Fecha de acceso: 26 de febrero 2016. Tiempo de navegación: 4:00 minutos 12 de marzo 2016. Tiempo de navegación: 2:34 minutos 18 de marzo 2016. Tiempo de navegación: 3:34 minutos
Tipo de acceso conceptual: no requerido Clasificación de la información: pública accesible Contenido: asuntos referentes a la vigilancia por parte del FBI, la CIA y la NSA.

Última fecha de actualización del sitio: 2016, 25 de febrero

Red oscura Freenet
Número de sitio investigado: 41-B
Nombre del sitio: Freereader Autor: US-CERT URL: http://127.0.0.1:8888/USK@v6ob9GPozFxxWWsqC2blieEHhqNTZNRy~LUSopuH1Zp0,KBQnlq8J8JjDrgJBDX1oR3mQgKTWa4GNXuZ1a9KHbao,AQACAAE/freenet-security/21/
Materia general: Seguridad informática Materia general: Internet -- Medidas de seguridad Materia general: World Wide Web -- Medidas de seguridad
Idioma: Inglés
Fecha de adquisición de la URL: 26 de febrero 2016
Fecha de acceso: 26 de febrero 2016. Tiempo de navegación: 2:20 minutos 12 de marzo 2016. Tiempo de navegación: 1:20 minutos 14 de marzo 2016. Tiempo de navegación: 2:34 minutos
Tipo de acceso conceptual: requerido Clasificación de la información: pública accesible Contenido: vulnerabilidades sobre la conexión a internet y navegación en la Web.
Última fecha de actualización del sitio: 2016,16 de febrero

Red oscura Freenet
Número de sitio investigado: 42-B
Nombre del sitio: Software user's rights Autor: D.J. Bernstein URL: http://127.0.0.1:8888/USK@Y3LfwNt2bqpTbZ6R8XwnV5c~Ebd2kEoFkjimYs5tVp8,5CoRfZ~1ZyJVDYnlePdX4KTh32zo0zTVsURM9laFO5Y,AQACAAE/licensefreesoftware/11/
Materia general: Sistemas operativos (Computadoras) Materia general: Programas de código abierto para computadoras
Idioma: Inglés
Fecha de adquisición de la URL: 26 de febrero 2016
Fecha de acceso: 26 de febrero 2016. Tiempo de navegación: 2:00 minutos 12 de marzo 2016. Tiempo de navegación: 1:05 minutos 15 de marzo 2016. Tiempo de navegación: 2:15 minutos

Tipo de acceso conceptual: requerido
Clasificación de la información: pública accesible
Contenido: sitio sobre el problema de la licencia en los sistemas operativos propietarios.

Última fecha de actualización del sitio: No hay datos

Red oscura Freenet

Número de sitio investigado: 43-B

Nombre del sitio: **FMS Site of herb**

Autor: No hay datos

URL: <http://127.0.0.1:8888/USK@5FeJUDg2ZdEqo-u4yoYWc1zF4tgPwOWIqcAJVGCORv8,ptJ1y0YBkdU9S5DeYC8AsLH0SrmTE9S3w2HKZvI5QKo,AQACAAE/fms/2947/>

Materia general: Vigilancia electrónica -- Control social

Idioma: Francés

Fecha de adquisición de la URL:
26 de febrero 2016

Fecha de acceso:
26 de febrero 2016. Tiempo de navegación: 4:30 minutos
12 de marzo 2016. Tiempo de navegación: 1:21 minutos
17 de marzo 2016. Tiempo de navegación: 3:07 minutos

Tipo de acceso conceptual: requerido
Clasificación de la información: interna
Contenido: foro de discusión sobre asuntos referentes al avance tecnológico y la gestión del Estado sobre la sociedad.

Última fecha de actualización del sitio: 2016, 27 de febrero

Red oscura Freenet

Número de sitio investigado: 44-B

Nombre del sitio: **Blindday: the prequel to House of Symmetry**

Autor: IOKU

URL:

<http://127.0.0.1:8888/USK@pDheBdjAnRNsMPofjq646R9CSYnOcTbJBgN466Q3YkQ,h23ch5nBqgfmOknqWXXbh-G4miWFoK9jHvnhlzzb3W8>

Materia general: Literatura

Idioma: Inglés

Fecha de adquisición de la URL:
26 de febrero 2016

Fecha de acceso:
26 de febrero 2016. Tiempo de navegación: 3:35 minutos
12 de marzo 2016. Tiempo de navegación: 1:10 minutos

14 de marzo 2016. Tiempo de navegación: 3:44 minutos

Tipo de acceso conceptual: no requerido

Clasificación de la información: pública accesible

Contenido: primer capítulo sobre literatura amateur, precuela de La casa de la simetría.

Última fecha de actualización del sitio: No hay datos

Red oscura **Freenet**

Número de sitio investigado: 45-B

Nombre del sitio: **Stories by Kursk**

Autor: Kursk

URL:

<http://127.0.0.1:8888/USK@HFkUMpijKyGYryVL7eC4wWt8NSHUsLoYWu9Ow2nmuyw,pzhx3cX~UrVXJvr1VNLaq6x6rQq9NF1RIIMW65od9Rw,AQACAAE/Stories/113/>

Materia general: Literatura inmoral

Materia general: Sexo en la literatura

Idioma: Inglés

Fecha de adquisición de la URL:

26 de febrero 2016

Fecha de acceso:

26 de febrero 2016. Tiempo de navegación: 3:34 minutos

12 de marzo 2016. Tiempo de navegación: 1:20 minutos

14 de marzo 2016. Tiempo de navegación: 1:25 minutos

Tipo de acceso conceptual: no requerido

Clasificación de la información: pública accesible

Contenido: historias pornográficas y eróticas en texto.

Última fecha de actualización del sitio: No hay datos

Red oscura **Freenet**

Número de sitio investigado: 46-B

Nombre del sitio: **BDSM and fetish pics**

Autor: Mr Fixit

URL:

<http://127.0.0.1:8888/USK@FI7KNxSeiQr38OzWbpWI4~74cPWrGxQpWjY5tQqN8WQ,wUAEgc~97EiUGRQOt~7UOXJCQJ0KftWNOiRZj6PFOOg,AQACAAE/BDSMandFetishPics/4/>

Materia general: Sadomasoquismo

Materia general: Heridas y lesiones -- Aspectos eróticos

Idioma: Inglés

Fecha de adquisición de la URL:

26 de febrero 2016

Fecha de acceso:

26 de febrero 2016. Tiempo de navegación: 3:00 minutos
12 de marzo 2016. Tiempo de navegación: 1:30 minutos
17 de marzo 2016. Tiempo de navegación: 2:19 minutos

Tipo de acceso conceptual: no requerido
Clasificación de la información: pública accesible
Contenido: fotografías sobre disciplina, dominación y sumisión, sadismo y masoquismo.

Última fecha de actualización del sitio: No hay datos

Red oscura **Freenet**

Número de sitio investigado: 47-B

Nombre del sitio: **Bureau d' investigation**

Autor: No hay datos

URL:

<http://127.0.0.1:8888/USK@rvuAHShUG2SRov95Mc8M86Cnk7eMT1XlxfHtio~95T8,loX~vLWUXMHBa3etcr9nrvfeb59ngAYzQL2rM-bluWQ,AQACAAE/bdi/13/>

Materia general: Vigilancia electrónica -- Control social

Materia general: Personas anónimas

Materia general: Espionaje

Materia general: Blogs

Idioma: Francés

Fecha de adquisición de la URL:

26 de febrero 2016

Fecha de acceso:

26 de febrero 2016. Tiempo de navegación: 3:34 minutos

12 de marzo 2016. Tiempo de navegación: 1:20 minutos

17 de marzo 2016. Tiempo de navegación: 1:53 minutos

Tipo de acceso conceptual: requerido

Clasificación de la información: pública accesible

Contenido: blog acerca de temas como la manipulación del Estado y el uso inadecuado de las tecnologías, con datos censurados u omitidos.

Última fecha de actualización del sitio: 2015, 12 de octubre

Red oscura **Freenet**

Número de sitio investigado: 48-B

Nombre del sitio: **The end: goodbye world**

Autor: No hay datos

URL:

<http://127.0.0.1:8888/USK@1doG4wfofCUOCmQ~tCgVuA8RewjV57olsGCQ9PWrsUo,G4bXzX7keOFMXE97aG1FSRTkpARxc0f1WQ3GkKStyVk,AQACAAE/flog/42/>

Materia general: Personas desaparecidas

Materia general: Vigilancia electrónica -- Control social

Materia general: Personas anónimas

Materia general: Seguridad informática
Materia general: Internet -- Medidas de seguridad
Materia general: World Wide Web -- Medidas de seguridad

Idioma: Inglés

Fecha de adquisición de la URL:
26 de febrero 2016

Fecha de acceso:
26 de febrero 2016. Tiempo de navegación: 2:00 minutos
12 de marzo 2016. Tiempo de navegación: 1:10 minutos
14 de marzo 2016. Tiempo de navegación: 4:39 minutos

Tipo de acceso conceptual: no requerido

Clasificación de la información: pública accesible

Contenido: boletín informativo acerca de la desaparición y muerte del hacktivista Gantros.

Última fecha de actualización del sitio: No hay datos

Red oscura **Freenet**

Número de sitio investigado: 49-B

Nombre del sitio: **From the mountain side**

Autor: No hay datos

URL: <http://127.0.0.1:8888/freenet:USK@sYx7aHo61nAkmSk~wF3bd5FcHBkslYqW-SBFXQ7Q26o,C67S4oWfnO0usIF3VNkQv0E3jtmPvdd-RYv-3Qzzpd4,AQACAAE/From-The-Mountain-Side/155/>

Materia general: Conspiraciones

Materia general: Delitos políticos

Idioma: Inglés

Fecha de adquisición de la URL:
26 de febrero 2016

Fecha de acceso:
26 de febrero 2016. Tiempo de navegación: 4:00 minutos
12 de marzo 2016. Tiempo de navegación: 1:30 minutos
17 de marzo 2016. Tiempo de navegación: 1:27 minutos

Tipo de acceso conceptual: requerido

Clasificación de la información: pública accesible

Contenido: documentos relacionados a las conspiraciones, falsas banderas y nuevo orden mundial.

Última fecha de actualización del sitio: 2015, 7 de octubre

Red oscura Freenet
Número de sitio investigado: 50-B
Nombre del sitio: El blog del burgués Autor: No hay datos URL: http://127.0.0.1:8888/USK@28fa8bSAkypjJHLPWo7u-b83~e8aC3pzmKdB1JjqzrE,rG2YHGn5y-auP033Lr59zo9kflwUg0cBLX~W8xPN2wA,AQACAAE/burgues/10/
Materia general: Capitalismo -- Latinoamérica Materia general: Comunismo -- Latinoamérica Materia general: Socialismo -- Latinoamérica Materia general: Globalización Materia general: Blogs
Idioma: Español Fecha de adquisición de la URL: 26 de febrero 2016 Fecha de acceso: 26 de febrero 2016. Tiempo de navegación: 3:50 minutos 12 de marzo 2016. Tiempo de navegación: 2:20 minutos 18 de marzo 2016. Tiempo de navegación: 1:50 minutos Tipo de acceso conceptual: requerido Clasificación de la información: pública accesible Contenido: reflexiones parciales en torno al capitalismo, socialismo y comunismo así como la incidencia de la globalización en las culturas de latinoamericanas, el autor el blog se basa en las teorías sobre el marxismo, autonomismo y comunismo libertario. Última fecha de actualización del sitio: 2015, 7 de septiembre

Red oscura Freenet
Número de sitio investigado: 51-B
Nombre del sitio: House of symmetry Autor: IOKU URL: http://127.0.0.1:8888/USK@CjdrIlg9kZn0mzmKTPuofupZmsdvB5Ruas7wyZrekRmM,uhrRURkJ18IOGtTraf4wVQ1LSIweOXcipZ9BNwv4Kgw,AQACAAE/symmetry/19/
Materia general: Literatura
Idioma: Inglés Fecha de adquisición de la URL: 26 de febrero 2016 Fecha de acceso: 26 de febrero 2016. Tiempo de navegación: 2:50 minutos 12 de marzo 2016. Tiempo de navegación: 1:50 minutos 17 de marzo 2016. Tiempo de navegación: 1:36 minutos Tipo de acceso conceptual: no requerido

Clasificación de la información: pública accesible

Contenido: análisis de los personajes de la novela así como la evolución de los personajes.

Última fecha de actualización del sitio: No hay datos

Red oscura **Freenet**

Número de sitio investigado: 52-B

Nombre del sitio: **Magic: the gathering is turing complete**

Autor: No hay datos

URL:

<http://127.0.0.1:8888/USK@Orc~rSZFDggHpZe4csLKGGsUtcOK7MUcfAGSHCD9aoA,RBmaEx3Y0DN-xZkheNimwKyl7cvEnaXKC-lbt-LSinY,AQACAAE/magic-turing/0/>

Materia general: Juegos de rol -- Teoría, métodos, etc.

Idioma: Inglés

Fecha de adquisición de la URL:

26 de febrero 2016

Fecha de acceso:

26 de febrero 2016. Tiempo de navegación: 3:00 minutos

12 de marzo 2016. Tiempo de navegación: 2:10 minutos

17 de marzo 2016. Tiempo de navegación: 1:10 minutos

Tipo de acceso conceptual: requerido

Clasificación de la información: pública accesible

Contenido: temas sobre una situación compleja en el juego de cartas Magic en software para computadoras personales.

Última fecha de actualización del sitio: 2015

Red oscura **Freenet**

Número de sitio investigado: 53-B

Nombre del sitio: **The library – mangas**

Autor: The collector

URL:

<http://127.0.0.1:8888/USK@LUpeSVCEWfysR~7Ha5gTa7tZXZMSbBXUQ356h3xcz~U,PLJlGGioNPiEptlgVkhC8ek8qHou4PoL2Ga1Cj2S~E,AQACAAE/TheLibrary/28/>

Materia general: Caricaturas y dibujos animados

Materia general: Novelas gráficas

Idioma: Inglés

Fecha de adquisición de la URL:

26 de febrero 2016

Fecha de acceso:

26 de febrero 2016. Tiempo de navegación: 3:00 minutos

12 de marzo 2016. Tiempo de navegación: 50 segundos

17 de marzo 2016. Tiempo de navegación: 1:47 minutos

Tipo de acceso conceptual: no requerido
Clasificación de la información: pública accesible
Contenido: opiniones, documentos y contenidos referentes al anime y el manga.

Última fecha de actualización del sitio: 2015, 5 de julio

Red oscura **Freenet**

Número de sitio investigado: 54-B

Nombre del sitio: **Polska-wolnosc**

Autor: No hay datos

URL:

<http://127.0.0.1:8888/USK@w41ssgyI3Z4hHP69f1TzLre6xUh68s22VkDdTS5i2o0,zjJeoAOhYaRzO5s8DA68URLYHPqgUb1Xn2bj1Rnyzk8,AQACAAE/polska-wolnosc/2/>

Materia general: Vigilancia electrónica -- Control social

Materia general: Personas anónimas

Materia general: Seguridad informática

Materia general: Internet -- Medidas de seguridad

Materia general: World Wide Web -- Medidas de seguridad

Idioma: Polaco

Fecha de adquisición de la URL:
26 de febrero 2016

Fecha de acceso:
26 de febrero 2016. Tiempo de navegación: 1:20 minutos
12 de marzo 2016. Tiempo de navegación: 1:20 minutos
15 de marzo 2016. Tiempo de navegación: 3:03 minutos

Tipo de acceso conceptual: requerido
Clasificación de la información: pública accesible
Contenido: En la libertad de Polonia, se muestra una postura en contra la vigilancia de Estado y advertencia sobre el posible monitoreo así como consejos de navegación en la freenet.

Última fecha de actualización del sitio: 2015, 23 de abril

Red oscura Freenet
Número de sitio investigado: 55-B
Nombre del sitio: Charles Darwin freesite Autor: No hay datos URL: http://127.0.0.1:8888/USK@gKt0nm9bc7xJe-jE9ojJlvrBrB6a8zylc5PsZb~Yb3k,2wAD7PAe9X2VX3KIVH6Vy19dkLz7mDLQNYzy5vo085s,AQACAAE/charles_darwin_online/147/
Materia general: Salud e higiene -- Estados Unidos Materia general: Salud pública -- Estados Unidos Materia general: Problemas sociales -- Estados Unidos Materia general: Selección de grupos (Evolución)
Idioma: Inglés Fecha de adquisición de la URL: 27 de febrero 2016 Fecha de acceso: 27 de febrero 2016. Tiempo de navegación: 3:20 minutos 12 de marzo 2016. Tiempo de navegación: 2:11 minutos 18 de marzo 2016. Tiempo de navegación: 3:00 minutos Tipo de acceso conceptual: requerido Clasificación de la información: pública accesible Contenido: información y contenidos que abordan problemas de salud y sociales de los ciudadanos de los Estados Unidos de América. Última fecha de actualización del sitio: 2015, 3 de abril

Red oscura Freenet (127.0.0.1:8888)
Número de sitio investigado: 56-B
Nombre del sitio: The white revolutionary Autor: No hay datos URL: http://127.0.0.1:8888/USK@Cnw3sXc8qcDJX7lhyqhNonnGxAcf39FYHfucyoBeG-k,0kXv~DDhXp4TFseGBhctEegyf-QNEmAMc0gDkNeYcmU,AQACAAE/SeditionPress/5/wr1.html
Materia general: Xenofobia Materia general: Nacionalsocialismo Materia general: Islam -- Opinión pública extranjera
Idioma: Inglés Fecha de adquisición de la URL: 27 de febrero 2016 Fecha de acceso: 27 de febrero 2016. Tiempo de navegación: 2:40 minutos 12 de marzo 2016. Tiempo de navegación: 3:00 minutos 18 de marzo 2016. Tiempo de navegación: 1:04 minutos Tipo de acceso conceptual: requerido

Clasificación de la información: pública accesible

Contenido: crítica al islam y al capitalismo como posibles orígenes de la autodestrucción humana desde una postura xenofóbica.

Última fecha de actualización del sitio: 2015, 1 de abril

Red oscura Freenet

Número de sitio investigado: 57-B

Nombre del sitio: **Agorism: revolutionary market anarchism**

Autor: No hay datos

URL: <http://127.0.0.1:8888/USK@flkEtTMu6F3f7Y48dB4mmZiyFbB-iddMGBvtruSE3Vc,sFg1GrDfJ-k6BE8VmqqQjw~iOgOKu-aws8law90GeY8,AQACAAE/agorism/13/>

Materia general: Vigilancia electrónica -- Control social

Idioma: Inglés

Fecha de adquisición de la URL:
27 de febrero 2016

Fecha de acceso:
27 de febrero 2016. Tiempo de navegación: 4:00 minutos
12 de marzo 2016. Tiempo de navegación: 1:50 minutos
17 de marzo 2016. Tiempo de navegación: 2:12 minutos

Tipo de acceso conceptual: requerido

Clasificación de la información: pública accesible

Contenido: situación actual del Estado como elemento de represión y regulación económica sobre los individuos. Se aborda el tema sobre la anarquía de mercado sin instituciones intermediarias.

Última fecha de actualización del sitio: No hay datos

Red oscura Freenet

Número de sitio investigado: 58-B

Nombre del sitio: **The infidel's tavern archive of content censored by muslim terrorism, rogue states, and politically correct sympathizers**

Autor: No hay datos

URL: <http://127.0.0.1:8888/USK@o9r~5sKSkZZAx~tkhJCw0~R3qIMEZwUyJ6o8LWHNZE,R-m32j5VImY2uh8ECKsKba1MhPB6mq7lgFTRaaqa4k,AQACAAE/infidel/53/>

Materia general: Islam -- Siglo XXI

Materia general: Islam -- Opinión pública extranjera

Materia general: Terrorismo -- Aspectos religiosos -- Islam

Materia general: IS (Organization)

Idioma: Inglés

Fecha de adquisición de la URL:
27 de febrero 2016

Fecha de acceso:

27 de febrero 2016. Tiempo de navegación: 3:40 minutos

12 de marzo 2016. Tiempo de navegación: 3:50 minutos

18 de marzo 2016. Tiempo de navegación: 2:23 minutos

Tipo de acceso conceptual: requerido

Clasificación de la información: pública accesible

Contenido: crítica de Charlie Ebdó hacia el Islam y el grupo terrorista ISIS.

Última fecha de actualización del sitio: 2016, 21 de febrero

Anexo C

Cedulas de la red oscura I2P

Red oscura I2P
Número de sitio investigado: 59-C
Nombre del sitio: Hidden gate Autor: No hay datos URL: http://hiddengate.i2p/wiki/%D0%97%D0%B0%D0%B3%D0%BB%D0%B0%D0%B2%D0%BD%D0%B0%D1%8F_%D1%81%D1%82%D1%80%D0%B0%D0%BD%D0%B8%D1%86%D0%B0
Materia general: Personas anónimas Materia general: Seguridad informática Materia general: Internet -- Medidas de seguridad Materia general: World Wide Web -- Medidas de seguridad
Idioma: Ruso Fecha de adquisición de la URL: 28 de febrero 2016 Fecha de acceso: 28 de febrero 2016. Tiempo de navegación: 4:00 minutos 12 de marzo 2016. Tiempo de navegación: 2:30 minutos 15 de marzo 2016. Tiempo de navegación: 5:00 minutos Tipo de acceso conceptual: requerido Clasificación de la información: pública accesible Contenido: manuales sobre los usos y las utilidades de la red oscura I2P. Última fecha de actualización del sitio: 2016, 20 de febrero

Red oscura I2P
Número de sitio investigado: 60-C
Nombre del sitio: Tracker2 postman Autor: No hay datos URL: http://tracker2.postman.i2p/
Materia general: Repositorios -- Recursos de información electrónicos Materia general: Contenidos generados por los usuarios Materia general: Recursos electrónicos de información Materia general: Piratería (Derechos de autor)
Idioma: Inglés Fecha de adquisición de la URL: 28 de febrero 2016 Fecha de acceso: 28 de febrero 2016. Tiempo de navegación: 3:50 minutos 12 de marzo 2016. Tiempo de navegación: 2:17 minutos 16 de marzo 2016. Tiempo de navegación: 1:42 minutos

Tipo de acceso conceptual: requerido

Clasificación de la información: reservada

Contenido: lista de enlaces acerca de películas, series de tv, hacking de software propietario y temas sobre el anonimato en Internet por torrent.

Última fecha de actualización del sitio: 2016, 16 de marzo

Red oscura I2P

Número de sitio investigado: 61-C

Nombre del sitio: **General informations: first informations and steps**

Autor: No hay datos

URL: <http://echelon.i2p/I2Pguide/general.html>

Materia general: Personas anónimas

Materia general: Seguridad informática

Materia general: Internet -- Medidas de seguridad

Materia general: World Wide Web -- Medidas de seguridad

Idioma: Inglés

Fecha de adquisición de la URL:

28 de febrero 2016

Fecha de acceso:

28 de febrero 2016. Tiempo de navegación: 3:30 minutos

12 de marzo 2016. Tiempo de navegación: 4:00 minutos

18 de marzo 2016. Tiempo de navegación: 1:20 minutos

Tipo de acceso conceptual: requerido

Clasificación de la información: pública accesible

Contenido: información general sobre el funcionamiento de i2p, se explican sus principales objetivos, como lo son el anonimato y cifrado de los datos. Se menciona la versión 1.0 y la intención de actualizar el software cada uno o dos meses, se recomienda utilizar la última versión.

Última fecha de actualización del sitio: 2009, 9 de agosto

Red oscura I2P

Número de sitio investigado: 62-C

Nombre del sitio: **ANONCOIN: privacy-centric currency**

Autor: No hay datos

URL: <http://anoncoin.i2p/>

Materia general: Moneda -- Anoncoin

Materia general: Industria de servicios financieros

Idioma: Inglés

Fecha de adquisición de la URL:

28 de febrero 2016

Fecha de acceso:

28 de febrero 2016. Tiempo de navegación: 3:00 minutos

12 de marzo 2016. Tiempo de navegación: 1:50 minutos

18 de marzo 2016. Tiempo de navegación: 3:30 minutos

Tipo de acceso conceptual: requerido

Clasificación de la información: pública accesible

Contenido: software para la gestión de las transacciones de moneda digital descentralizada con el objetivo de proporcionar privacidad a los usuarios para la compra y venta en las redes oscuras.

Última fecha de actualización del sitio: 2016, 14 de marzo

Red oscura **I2P**

Número de sitio investigado: 63-C

Nombre del sitio: **Planet**

Autor: No hay datos

URL: <http://planet.i2p/>

Materia general: Repositorios -- Recursos de información electrónicos

Materia general: Contenidos generados por los usuarios

Materia general: Piratería (Derechos de autor)

Materia general: Recursos electrónicos de información

Idioma: Inglés, Francés y Ruso

Fecha de adquisición de la URL:

28 de febrero 2016

Fecha de acceso:

28 de febrero 2016. Tiempo de navegación: 4:00 minutos

12 de marzo 2016. Tiempo de navegación: 2:30 minutos

14 de marzo 2016. Tiempo de navegación: 2:44 minutos

Tipo de acceso conceptual: requerido

Clasificación de la información: reservada

Contenido: lista de enlaces acerca de películas, series de tv, hacking de software propietario y temas sobre el anonimato en Internet por torrent.

Última fecha de actualización del sitio: 2016, 14 de marzo

Red oscura **I2P**

Número de sitio investigado: 64-C

Nombre del sitio: **Diftracker**

Autor: No hay datos

URL: <http://diftracker.i2p/>

Materia general: Repositorios -- Recursos de información electrónicos

Materia general: Contenidos generados por los usuarios

Materia general: Piratería (Derechos de autor)

Idioma: Multilinguaje
Fecha de adquisición de la URL: 28 de febrero 2016
Fecha de acceso: 28 de febrero 2016. Tiempo de navegación: 2:50 minutos 12 de marzo 2016. Tiempo de navegación: 1:30 minutos 14 de marzo 2016. Tiempo de navegación: 5:15 minutos
Tipo de acceso conceptual: requerido Clasificación de la información: reservada Contenido: listados sobre enlaces a distintos contenidos como software, cine y series de tv por torrent.
Última fecha de actualización del sitio: 2016

Red oscura I2P
Número de sitio investigado: 65-C
Nombre del sitio: Forum Autor: No hay datos URL: http://forum.i2p/index.php
Materia general: Personas anónimas Materia general: Seguridad informática Materia general: Internet -- Medidas de seguridad Materia general: World Wide Web -- Medidas de seguridad Materia general: Blogs
Idioma: Alemán, Ruso, Chino e Inglés
Fecha de adquisición de la URL: 28 de febrero 2016
Fecha de acceso: 28 de febrero 2016. Tiempo de navegación: 3:35 minutos 12 de marzo 2016. Tiempo de navegación: 4:30 minutos 18 de marzo 2016. Tiempo de navegación: 3:32 minutos
Tipo de acceso conceptual: requerido Clasificación de la información: interna Contenido: blog de comentarios relacionados a temas como la seguridad, desarrollo, compatibilidad de software y problemas referentes a I2P.
Última fecha de actualización del sitio: 2016, 13 de marzo

Red oscura I2P
Número de sitio investigado: 66-C
Nombre del sitio: Open4you Autor: No hay datos URL: http://open4you.i2p/
Materia general: Alojamiento web

Materia general: Desarrollo de sitios web
Idioma: Inglés y Ruso
Fecha de adquisición de la URL: 28 de febrero 2016
Fecha de acceso: 28 de febrero 2016. Tiempo de navegación: 1:20 minutos 12 de marzo 2016. Tiempo de navegación: 1:10 minutos 17 de marzo 2016. Tiempo de navegación: 2:36 minutos
Tipo de acceso conceptual: requerido Clasificación de la información: pública accesible Contenido: alojamiento de contenidos dentro de la red I2P con servicio de respaldo y restricciones para contenidos acerca de la pornografía infantil, compra y venta de drogas, además de que se prohíbe propaganda sobre el Islam y el jihad.
Última fecha de actualización del sitio: 2013

Red oscura I2P
Número de sitio investigado: 67-C
Nombre del sitio: Pastethis Autor: No hay datos URL: http://pastethis.i2p/
Materia general: Libertad de expresión Materia general: Libertad de información Materia general: Contenidos generados por los usuarios
Idioma: Inglés y Ruso
Fecha de adquisición de la URL: 28 de febrero 2016
Fecha de acceso: 28 de febrero 2016. Tiempo de navegación: 3:00 minutos 12 de marzo 2016. Tiempo de navegación: 2:25 minutos 16 de marzo 2016. El sitio no fue alcanzable, sin conexión al sitio
Tipo de acceso conceptual: no requerido Clasificación de la información: pública accesible Contenido: mensajes colocados por distintos usuarios.
Última fecha de actualización del sitio: 2016, 12 de marzo

Red oscura I2P
Número de sitio investigado: 68-C
Nombre del sitio: I2P wiki Autor: Unconscious

URL:
http://nrbnshsndzb6homcipymkkngngw4s6twediqottzqdfyvrvjw3pq.b32.i2p/index.php?title=Main_Page

Materia general: Personas anónimas
Materia general: Seguridad informática
Materia general: Internet -- Medidas de seguridad
Materia general: World Wide Web -- Medidas de seguridad

Idioma: Multilinguaje

Fecha de adquisición de la URL:
28 de febrero 2016

Fecha de acceso:
28 de febrero 2016. Tiempo de navegación: 3:45 minutos
12 de marzo 2016. Tiempo de navegación: 2:00 minutos
15 de marzo 2016. Tiempo de navegación: 4:30 minutos

Tipo de acceso conceptual: requerido

Clasificación de la información: pública accesible

Contenido: información sobre las configuraciones e instalaciones para la mejora del uso sobre I2P.

Última fecha de actualización del sitio: 13 de marzo de 2016