

Deep Web

Amenazas y protección
en la red oculta

2ª
Edición
Actualizada



Facundo David Gallo Serpillo



Ra-Ma®

edü
Ediciones de la U

Deep Web

Amenazas y protección en la red oculta

2ª edición

Facundo David Gallo Serpillo



Gallo Serpillo, Facundo David

Deep Web. Amenazas y protección en la red oculta. 2ª edición / Facundo David Gallo Serpillo. Bogotá: Ediciones de la U, 2026

162 p. ; 24 cm.

ISBN 978-628-7912-50-2 ePUB 978-628-7912-52-6 PDF 978-628-7912-51-9

1. Informática 2. Seguridad informática 3. Ciberseguridad I. Tít.

5 cd. - Thema: UR

Edición original publicada por © Editorial Ra-Ma (España)

Edición autorizada a Ediciones de la U para Colombia

Área: Informática

Primera edición: Bogotá, Colombia, julio de 2026

ISBN 978-628-7912-50-2

© Facundo David Gallo Serpillo

© Ra-ma Editorial

Calle Jarama, 3-A (Polígono Industrial Igarsa) 28860 Paracuellos de Jarama

www.ra-ma.es y www.ra-ma.com / E-mail: editorial @ra-ma.com

Madrid, España

© Ediciones de la U - Carrera 27 #27-43 - Tel. (+57) 601 6455049

www.edicionesdelau.com - E-mail: editor@edicionesdelau.com

Bogotá, Colombia

Ediciones de la U es una empresa editorial que, con una visión moderna y estratégica de las tecnologías, desarrolla, promueve, distribuye y comercializa contenidos, herramientas de formación, libros técnicos y profesionales, e-books, e-learning o aprendizaje en línea, realizados por autores con amplia experiencia en las diferentes áreas profesionales e investigativas, para brindar a nuestros usuarios soluciones útiles y prácticas que contribuyan al dominio de sus campos de trabajo y a su mejor desempeño en un mundo global, cambiante y cada vez más competitivo.

Coordinación editorial: Daniela Parra G.

Carátula: Ediciones de la U

Impresión: DGP Editores SAS

Calle 63 No. 70 D - 34, Pbx. (571) 7217756

Impreso y hecho en Colombia

Printed and made in Colombia

No está permitida la reproducción total o parcial de este libro, ni su tratamiento informático, ni la transmisión de ninguna forma o por cualquier medio, ya sea electrónico, mecánico, por fotocopia, por registro y otros medios, sin el permiso previo y por escrito de los titulares del Copyright.

*A mi familia por permitirme la ventaja de escribir
a largas horas de la noche,
incluso cuando se torna difícil compaginarlo
con las obligaciones personales.*

*A las Fuerzas y Cuerpos de Seguridad del Estado español, por su
encomiable labor en la lucha contra el crimen organizado en la Dark Net.*

*A los investigadores que descendieron en busca de su propio Kraken
y no hallaron más que el desasosiego o la rendición.
Que la presente obra sirva como motor de impulso
para nunca rendirse ante lo improbable.*

ÍNDICE

SOBRE EL AUTOR.....	11
PRÓLOGO	13
INTRODUCCIÓN	17
EL KRAKEN	18
CURSO DE BUCEO PARA TODOS LOS PÚBLICOS.....	19
CAPÍTULO 1. CURSO RÁPIDO DE BUCEO POR LA DEEP WEB	21
1.1 APRECIACIÓN DESDE LAS ORILLAS	22
1.2 FILOSOFÍA DE LA RED TOR	23
1.3 MEDIDAS QUE FACILITA EL ANONIMATO A LOS USUARIOS	25
1.4 MEDIOS ALTERNATIVOS DE EXPLORACIÓN	26
1.4.1 Freenet, la red de túneles olvidados	27
1.4.2 I2P, el camino hacia lo invisible.....	27
1.5 ÚLTIMA ADVERTENCIA.....	28
CAPÍTULO 2. COMENZANDO LA EXPLORACIÓN DE LA DEEP WEB	
ZONA FÓTICA (0 - 1000 MS. DE PROFUNDIDAD).....	29
2.1 P2P Y TORRENTS. ESAS EXTRAÑAS FUERZAS SIMBIÓTICAS.....	30
2.2 CUANDO LOS RESTOS DE LAS PROFUNDIDADES SALEN A FLOTE ...	32
2.2.1 La mazmorra de lo grotesco, un mítico buceador	32
2.2.2 Sad Satan	35
2.2.3 El misterio “432”	37
2.2.4 Cryptome	44

CAPÍTULO 3. LLEGAMOS A LA ZONA INTERMEDIA DE LA DEEP WEB**ZONA BATIAL (1000 MS. - 4000 MS. DE PROFUNDIDAD).....49**

- 3.1 COMO GUIARSE EN LA OSCURIDAD 50
 - 3.1.1 Torch, AHMIA y DarkSearch..... 50
 - 3.1.2 HiddenWiki 52
 - 3.1.3 Hosting y creación de webs..... 54
 - 3.1.4 Cuentas de correos 59
- 3.2 COMUNICACIONES A NINGUNA PARTE 60
 - 3.2.1 Confesionarios..... 61
 - 3.2.2 Chateando con desconocidos 62
 - 3.2.3 Avistamiento del submarino “OnionChan” 64

CAPÍTULO 4. NOS ADENTRAMOS EN LA OSCURIDAD DE LA DEEP WEB**ZONA ABISAL (4000 MS. - 6000 MS. DE PROFUNDIDAD)67**

- 4.1 “SIN SENTIDOS” 68
- 4.2 OBJETOS HUNDIDOS..... 68
 - 4.2.1 Los vapores químicos..... 68
 - 4.2.2 Bienvenidos al Silk Road 73
 - 4.2.3 Herederos del Silk Road..... 76
 - 4.2.4 Venta de anabólicos..... 78
 - 4.2.5 El mercado de las armas..... 79
 - 4.2.6 Tarjetas de crédito clonadas y bancos offshore 84
 - 4.2.7 Venta de pasaportes y nacionalidades falsas 88
 - 4.2.8 Herramientas de hacking y 0-Days 90
- 4.3 LA FAUNA MÁS SALVAJE 93
 - 4.3.1 Asesinos a sueldo 93
 - 4.3.2 Piratas informáticos..... 94
 - 4.3.3 Filias 95

CAPÍTULO 5. MÁS ALLÁ DE LA DEEP WEB**ZONA HADAL (6000 MS. - 11000 MS. DE PROFUNDIDAD).....99**

- 5.1 MÁS ALLÁ DE LA OSCURIDAD..... 100
- 5.2 EL MITO DEL EJÉRCITO FANTASMA 100
- 5.3 LA FOSA DE LAS MARIANAS 103
 - 5.3.1 Dominios adicionales 105
 - 5.3.2 La libertad 107
- 5.4 LA LEYENDA DEL KRAKEN Y LA REDROOM 112
 - 5.4.1 Introducción a RedRoom o DarkRoom..... 112
 - 5.4.2 El objetivo 114
 - 5.4.3 La imagen enigmática 117
 - 5.4.4 El video en diferido 122
 - 5.4.5 La cuenta atrás..... 130
 - 5.4.6 Conclusión..... 131

BLOQUE 2. METODOLOGÍAS DE INVESTIGACIÓN EN LA RED TOR	133
CAPÍTULO 6. FUNDAMENTOS DE CIBERINVESTIGACIÓN	
MEDIDAS DE SEGURIDAD Y APROXIMACIÓN METODOLÓGICA.....	135
6.1 MEDIDAS DE SEGURIDAD.....	136
6.1.1 Principios rectores en la ciberinvestigación	136
6.1.2 Axiomas para la navegación segura en la red Tor.....	137
6.2 APROXIMACIÓN METODOLÓGICA	139
CAPÍTULO 7. MÉTODOS PASIVOS DE CIBERINVESTIGACIÓN	
HONEYPOTS E INSPECCIÓN DE TRÁFICO.....	143
7.1 USO DE HONEYPOTS PARA ESTUDIOS DEMOGRÁFICOS	144
7.2 MONITORIZACIÓN DE TRÁFICO EN LA RED TOR.....	149
GLOSARIO DE TÉRMINOS.....	155
REFERENCIAS.....	157
ÍNDICE ALFABÉTICO	159

SOBRE EL AUTOR

Como doctor en criminología e ingeniero informático, me he tomado la licencia de arropar la obra bajo alguna que otra pincelada técnica gracias a mis conocimientos en el campo de la ciberseguridad, mientras que mi perfil académico me ha permitido aplicar didáctica en aquellas ocasiones donde la terminología se antoja compleja e inabarcable.

He trabajado desde los 18 años en el sector de la informática, y actualmente me dedico en cuerpo y alma a mis funciones como profesor doctor e investigador; aún no he bajado la guardia, sigo cometiendo errores de los cuales aprendo mucho, y me queda combustible por quemar.

Facundo Gallo Serpillo





PRÓLOGO

Entre las paradojas de estos tiempos de incertidumbre se encuentran el progresivo sacrificio de la privacidad en aras de una, hipotética, mayor seguridad y, sobre todo, una inconsciente y generalizada devaluación del anonimato. Mientras Estados y organizaciones, con sus correspondientes instituciones y agencias, comités y defensores del ciudadano, se empeñan en defender la privacidad y proteger los datos personales, son muchas las personas que asisten apáticas e indiferentes, incluso contrariadas, a este complejo montaje de normas, órganos, requisitos y consentimientos que no quieren o no pueden entender. No es difícil tener la impresión de que los gobernantes están caminando en dirección contraria al sentir de los ciudadanos para quienes la idea de privacidad y el valor del anonimato no necesariamente tienen el mismo significado. Por otra parte, sin embargo, esos mismos Estados y organizaciones, con sus correspondientes instituciones y agencias, están embarcados en el debate sobre la encriptación alegando motivos de seguridad ciudadana o nacional para justificar el acceso a los datos personales y al ámbito de la privacidad que, con tanta insistencia y medios, por otra parte, aseguraban querer defender.

En la sociedad de la vigilancia, el anonimato, ese bien tan preciado y cada vez más escaso, es el fundamento y la razón de ser de la Deep Web donde no hay seguridad, ni parece posible aplicar la legalidad: un alto precio a pagar. Entre la utopía de un mundo sin vigilancia y la distopía de un mundo sin reglas, la Deep Web sigue siendo un mundo desconocido para la gran mayoría. Con esa obra Facundo David Gallo ofrece al lector la posibilidad de entender ese mundo bipolar.

Esta monografía se estructura en cinco capítulos que responden a una atractiva, a la par que didáctica y dinámica, organización secuencial. Tras un primer capítulo introductorio, la división zonal de las superficies del mar obra el milagro

—por mérito del autor— de adentrarnos de un modo prácticamente visual, pero realmente conceptual, en el proceloso mundo de la Deep Web.

El primer capítulo, bajo el ilustrativo título “Curso rápido de buceo”, ofrece una panorámica precisa del objeto de esta monografía prodigando información y conocimientos sobre la filosofía de las profundidades —en las que se cruza el umbral hacia lo desconocido y se entra en el imperio del anonimato—, las medidas de compresión para el buceo —que permiten ese anonimato— y los medios alternativos de exploración como la Freenet o el Invisible Internet Project (I2P).

Tras esta explicación introductoria, el lector agradecerá la advertencia con la termina el capítulo I y comprenderá su significado al completo, incluido el agradecimiento a las fuerzas y cuerpos de seguridad del Estado, al final del inquietante trayecto que proponen sus páginas. No hay que olvidar, como advierte el autor, que la filosofía de la red Tor “se basa en asegurar el anonimato de los usuarios, haciéndolo incompatible con los controles y estándares de seguridad que garantizan las trazabilidades o registros de usuarios, de tal manera que resulta complejo aplicar medidas de restricción legal sobre los contenidos publicados”.

A partir de ahí, los capítulos II a V se explican como un tránsito desde las zonas Fótica a Batial, Abisal y, finalmente, Hadal en una exploración que permite, en una progresión creciente en este avance metafórico, pero no por ello menos inquietante, hacia esas profundidades, conocer y comprender el significado, el entramado y el funcionamiento de esta suerte de submundos que constituye la Deep Web.

En el capítulo II, dedicado a la llamada Zona Fótica (0 a 1.000 ms. de profundidad), próxima a la Surface Web que conocemos, el autor explica la tecnología P2P, el archivo Torrent y el Protocolo BitTorrent que opera mediante un modelo de funcionamiento distribuido basado en fragmentar el fichero destino entre varios hosts y con un nodo generador principal denominado semilla. La filosofía que subyace detrás de esta metodología consiste en situar a cada nuevo usuario como punto de distribución. Sobre esa base conceptual, se analizan, ilustrando con imágenes y tablas, los casos de la Mazmorra de lo Grotesco, Sad Satan, el complejo entramado de símbolos del misterio “432” y sus significados y la Fundación Cryptome, un extenso archivo de supuestas filtraciones que parecen involucrar a los gobiernos estadounidense y británico.

El capítulo III se ocupa de la Zona Batial (1.000 a 4.000 ms. de profundidad), definido como el hábitat de una escasa fauna que nada libremente pero que nunca se aproxima a la superficie y en la que sus habitantes deben recurrir al único alimento existente: la depredación de otros organismos. Este capítulo se subdivide en un

primer apartado sobre “Como guiarse en la oscuridad” y uno segundo denominado “comunicaciones a ninguna parte”.

El primero se construye buscando referentes conforme al modelo de la Surface Web para guiarnos sobre algunos de sus contenidos. El autor identifica y explica el tipo de buscadores como Torch, AHMIA y DarkSearch, que presentan ventajas e inconvenientes. Hidden Wiki cumple funciones similares, salvando las distancias, a las de una Wikipedia. Los sistemas de hosting y para la creación de webs siguen una lógica también similar en la medida en que pueden contratarse a terceros o crearse por el usuario mismo, si se tienen los conocimientos necesarios a esos efectos. Imágenes y tablas informan sobre condiciones y precios con la particularidad de que no hay límites en cuanto al uso, pero tampoco garantías de que, efectivamente, se vaya a cumplir con el servicio contratado y pagado por adelantado. El dilema libertad *versus* seguridad se manifiesta de un modo tan extremo que incluso le hace perder su significado. Siguiendo con las referencias conocidas, las cuentas de correo funcionan con una lógica parecida a las conocidas en la Surface Web.

En cambio, las denominadas “Comunicaciones a ninguna parte” se sitúan en un territorio algo diferente. Aunque responden a las mismas necesidades de la Surface Web, las dinámicas son distintas: confesionarios donde se confiesa lo que sería inconfesable; chats donde se habla de lo que no debería verbalizarse; y foros, como OnionChan, que funciona como un Guadiana con intervalos activos e inactivos y contenidos consistentes, básicamente, en la circulación de material ilícito, que el autor ilustra con imagen y datos.

El capítulo IV lleva al lector a la Zona Abisal (4.000 a 6.000 ms. de profundidad) donde el autor le recibe explicando el significado del término abismo: un lugar profundo y frío por la ausencia total de luz habitado por animales con apariencia monstruosa y movido por dinámicas vitales alejadas de todo sentido común. Es la Dark Net.

En una breve introducción, bajo el título “Sin sentidos”, se advierte sobre la irracionalidad de los contenidos y sobre la forma en la que el autor aborda su análisis que se articula en una parte dedicada a los denominados objetos hundidos y otra sobre la llamada fauna más salvaje. Drogas, armas, tarjetas de crédito, pasaportes o herramientas cibernéticas maliciosas entran en la primera categoría y se explican con una profusión de imágenes y datos que permiten calibrar el alcance y la naturaleza de este mercado. Asesinos a sueldo, que se publican abiertamente en esta red, y piratas informáticos, que trabajan al otro lado de la legalidad, protagonizan ese escenario dentro de la fauna más salvaje.

El capítulo V corresponde a la Zona Hadal (6.000 a 11.000 ms. de profundidad) que significa lugar de muerte. Leyendas y mitos, como el del ejército fantasma,

coexisten en este espacio con una realidad en la hay dominios independientes –“.loki” o “.clos”– o portales como “liberté”. Una atención especial dedica el autor a la denominada leyenda del Kraken de la Deep Web: la RedRoom o DarkRoom donde supuestamente se practica el asesinato en directo. Imágenes de capturas de pantalla, datos y tablas cuidadosamente explicadas por el autor consiguen transportar al lector al núcleo duro de la zona Hadal.

Este recorrido experto por la Deep Web es posible gracias a la maestría profesional, técnica y expositiva de Facundo Gallo Serpillo. Además de su actual función como profesor doctor en la Universidad Internacional de La Rioja, Facundo Gallo Serpillo ha trabajado como consultor de ciberseguridad, seguridad informática y gobierno de la seguridad en distintas empresas y en instituciones públicas, en una larga trayectoria de compromiso personal y profesional con la ciberseguridad. Solo la combinación de una grandísima experiencia y unos sólidos conocimientos con una definida vocación y un compromiso personal con la ciberseguridad puede explicar la entidad y el valor del trabajo realizado con esta inmersión en los mundos subterráneos de la Deep Web. A su Doctorado en Criminología, el autor suma un Grado en Ingeniería Informática, creando el entramado perfecto para escribir una obra científicamente sólida, técnicamente impecable y comprensible para cualquiera que quiera acercarse al conocimiento de la Deep Web. Con mi enhorabuena por el trabajo va también mi agradecimiento por haberme permitido el honor de prologar esta extraordinaria monografía.

Margarita Robles.

Catedrática de Universidad. Departamento de Derecho, Universidad de Granada



INTRODUCCIÓN

La presente obra, en su segunda –y actualizada– versión, mantiene una exposición con enfoque divulgativo como eje vertebrador; de este modo, el contenido presentado en el primer bloque está acompañado de un conjunto de evidencias recogidas entre los años 2015 y 2020 sobre el amplio mundo de mitos y hechos de dudosa credibilidad que subyacen en la Deep Web, más en concreto en la denominada red Tor. Por otro lado, la presente versión expande su *corpus* documental con un segundo bloque destinado a metodologías de ciberinvestigación en la red Tor, sumando contenido técnico de interés para el colectivo de ingenieros, criminólogos, agentes del orden, y detectives privados.

Aunque muchos hayan oído hablar de los términos Deep Web y Dark Net, y otros aún desconozcan por completo su significado, la realidad es que nunca deja indiferente a nadie. La cara oculta de la gran red de redes sigue atrapando a todo aquel que se adentra en su toda su amplitud, donde los límites divisorios entre legalidad e ilegalidad son imperceptibles. En la redacción de este libro se emplean términos como navegar y bucear, conocidos y utilizados por todos, para describir como nos movemos por la red; de igual forma se ha pretendido dotar de “materia” a ese lado oscuro de Internet, y para ello he utilizado una figura retórica de un ser mitológico: